

# Ruijie Reyee RG-RAP Series Access Points ReyeeOS 1.219

Web-based Configuration Guide



Document Version: V1.3 Date: 2023-09-06 Copyright © 2023 Ruijie Networks

## Copyright

Copyright © 2023 Ruijie Networks

All rights are reserved in this document and this statement.

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



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. Some or all of the products, services or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Ruijie Networks does not make any express or implied statement or guarantee for the content of this document.

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

This manual is for reference only. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

# Preface

## **Intended Audience**

This document is intended for:

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

## **Technical Support**

- Official website of Ruijie Reyee: <u>https://www.ruijienetworks.com/products/reyee</u>
- Technical support website: <u>https://ruijienetworks.com/support</u>
- Case portal: <u>https://caseportal.ruijienetworks.com</u>
- Community: <u>https://community.ruijienetworks.com</u>
- Technical support Email: <u>service\_rj@ruijienetworks.com</u>

### Conventions

### 1. GUI Symbols

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

### 2. Signs

The signs used in this document are described as follows:

## 🕕 Warning

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

#### A Caution

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

#### 🚺 Note

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. Note

This manual introduces the features of the RG-RAP series access points and instructs users to configure the device.

# Contents

Preface	I
1 Fast Internet Access	1
1.1 Configuration Environment Requirements	1
1.1.1 PC	1
1.2 Default Configuration	1
1.3 Login to Eweb	1
1.3.1 Connecting to the Access Point	1
1.3.2 Configuring the IP Address of the Management Client	2
1.3.3 Logging in to the Web Page	2
1.4 Work Mode	3
1.4.1 AP Mode	3
1.4.2 Router Mode	3
1.4.3 Wireless Repeater Mode	3
1.5 Configuration Wizard (Router Mode)	4
1.5.1 Getting Started	4
1.5.2 Configuration Steps	5
1.6 Configuration Wizard (AP Mode)	7
1.6.1 Getting Started	7
1.6.2 Configuration Steps	7
1.7 Configuration Wizard (Wireless Repeater Mode)	8
1.7.1 Getting Started	8
1.7.2 Configuration Steps	8
1.8 Introduction to the Eweb GUI	10

1.8.1 Single Management Webpage	10
1.8.2 Dual Management Webpages	12
2 Network Monitoring	
2.1 Viewing the Network Information	15
2.2 Adding Network Devices	17
2.2.1 Wired Connection	17
2.2.2 AP Mesh	
2.3 Managing Network Devices	
2.4 Configuring Network Planning	
2.4.1 Configuring Wired VLAN	
2.4.2 Configuring Wi-Fi VLAN	
2.5 Troubleshooting Fault Alerts	
3 Wi-Fi Network Settings	
3.1 Configuring AP Groups	
3.1.1 Overview	
3.1.2 Procedures	
3.2 Configuring SSID and Wi-Fi Password	
3.3 Hiding the SSID	
3.3.1 Overview	
3.3.2 Configuration Steps	
3.4 Checking Wireless Clients	
3.5 Configuring Wi-Fi Band	
3.6 Configuring Band Steering	42
3.7 Configuring Wi-Fi 6	43

3.8 Configuring Layer-3 Roaming	44
3.9 Configuring AP Isolation	45
3.10 Adding a Wi-Fi Network	46
3.11 Configuring a Guest Wi-Fi	47
3.11.1 Overview	47
3.11.2 Configuration Steps	47
3.12 Configuring Wireless Rate Limiting	48
3.12.1 Overview	48
3.12.2 Configuration Steps	49
3.13 Configuring Wi-Fi Blacklist or Whitelist	51
3.13.1 Overview	51
3.13.2 Configuration Steps	52
3.14 Optimizing Wi-Fi Network	53
3.14.1 Overview	53
3.14.2 Getting Started	
	53
3.14.3 Optimizing the Radio Channel	
3.14.3 Optimizing the Radio Channel	54
	54
3.14.4 Optimizing the Channel Width	54 55 56
3.14.4 Optimizing the Channel Width	54 55 56 57
<ul><li>3.14.4 Optimizing the Channel Width</li><li>3.14.5 Optimizing the Transmit Power</li><li>3.14.6 Configuring the Multicast Rate</li></ul>	54 55 56 57 58
<ul> <li>3.14.4 Optimizing the Channel Width</li> <li>3.14.5 Optimizing the Transmit Power</li> <li>3.14.6 Configuring the Multicast Rate</li></ul>	54 55 56 57 58 59
<ul> <li>3.14.4 Optimizing the Channel Width</li> <li>3.14.5 Optimizing the Transmit Power</li> <li>3.14.6 Configuring the Multicast Rate</li> <li>3.14.7 Configuring the Client Limit</li></ul>	54 55 56 57 58 59 59

3.14.12 Configuring WIO62	2
3.14.13 Configuring Wi-Fi Roaming Optimization (802.11k/v)63	3
3.15 Configuring Healthy Mode64	1
3.16 Configuring XPress	5
3.17 Configuring Wireless Schedule66	5
3.18 Enabling Reyee Mesh	5
3.19 Configuring AP Load Balancing67	7
3.19.1 Overview	7
3.19.2 Configuring Client Load Balancing67	7
3.19.3 Configuring Traffic Load Balancing69	)
3.20 Wireless Authentication77	1
3.20.1 Overview	1
3.20.2 Configuring One-click Login on Ruijie Cloud7	1
3.20.3 Configuring Voucher Authentication on Ruijie Cloud	5
3.20.4 Configuring Account Authentication on Ruijie Cloud82	2
3.20.5 Configuring SMS Authentication on Ruijie Cloud89	)
3.20.6 Configuring an Authentication-Free User List on Eweb Management System98	5
3.20.7 Displaying Authenticated Users on Eweb Management System	3
3.20.8 Displaying Authenticated Users on Ruijie Cloud98	3
4 Network Settings	,
4.1 Switching Work Mode	)
4.1.1 Work Mode	)
4.1.2 Self-Organizing Network Discovery	)
4.1.3 Configuration Steps	9

4.1.4 Viewing Device Role10	)1
4.2 Configuring Internet Connection Type (IPv4)10	)1
4.3 Configuring Internet Connection Type (IPv6)102	)2
4.4 Configuring LAN Port	)3
4.5 Configuring Repeater Mode104	)4
4.5.1 Wired Repeater104	)4
4.5.2 Wireless Repeater10	)5
4.6 Creating a VLAN	)7
4.7 Configuring Port VLAN	9
4.8 Changing MAC Address	1
4.9 Changing MTU11	1
4.10 Configuring DHCP Server	2
4.10.1 DHCP Server	2
4.10.2 Configuring the DHCP Server Function11	2
4.10.3 Displaying Online DHCP Clients11	3
4.10.4 Displaying the DHCP Static IP Address List11	4
4.11 Link Aggregation	4
4.12 Configuring DNS	5
4.13 Hardware Acceleration	5
4.14 Configuring Port Flow Control11	6
4.15 Configuring ARP Binding	6
4.16 Configuring LAN Ports	7
4.17 IPv6 Settings	8
4.17.1 Overview	8

4.17.2 IPv6 Basic	
4.17.3 IPv6 Address Assignment Methods	
4.17.4 Enabling IPv6	
4.17.5 Configuring the IPv6 Address for the WAN Port	
4.17.6 Configuring the IPv6 Address for the LAN Port	
4.17.7 Viewing DHCPv6 Clients	
4.17.8 Configuring the Static DHCPv6 Address	
4.17.9 Configuring the IPv6 Neighbor List	
5 System Settings	
5.1 PoE	
5.2 PoE Settings	
5.3 Setting the Login Password	
5.4 Setting the Session Timeout Duration	
5.5 Setting and Displaying System Time	
5.6 Configuring Reboot	
5.6.1 Rebooting the Current Device	
5.6.2 Rebooting All Devices in the Network	
5.6.3 Rebooting the Specified Device	
5.7 Configuring Scheduled Reboot	
5.7.1 Configuring Scheduled Reboot for the Current Device	
5.8 Configuring Backup and Import	
5.9 Restoring Factory Settings	
5.9.1 Restoring the Current Device to Factory Settings	
5.9.2 Restoring All Devices to Factory Settings	136

5.10 Performing Upgrade and Checking System Version136
5.10.1 Online Upgrade136
5.10.2 Local Upgrade137
5.11 Switching System Language137
5.12 Configuring LED Status Control138
6 Network Diagnosis Tools 139
6.1 Network Check139
6.2 Network Tools140
6.3 Alarms
6.4 Fault Collection142
7 FAQs 143
7.1 Login Failure143
7.2 Factory Setting Restoration143
7.3 Password Loss143

# **1** Fast Internet Access

# **1.1 Configuration Environment Requirements**

## 1.1.1 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.

# **1.2 Default Configuration**

## Table 1-1 Default Web Configuration

Item	Default			
IP address	10.44.77.254			
Username/Password	Username and password are not required at your first login and you can configure the access point directly.			

# 1.3 Login to Eweb

## 1.3.1 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>Configuring the IP Address of the Management Client</u>.

Wireless Connection

On a mobile phone or laptop, search for wireless network **@Ruijie-S**XXXX (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>Configuring the IP Address of the Management Client</u>.

## **1.3.2 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 Eweb system 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.

## 1.3.3 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.

1 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.

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

<b>Ruijie</b>   Hi, RAP6		
🗄 Password		
Log Forgot Password?	In English 🗸	

Username and password are not required at your first login and you can configure the access point directly. For device security, you are advised to set the management password after your first login to the web management system. After the password is set, you need to enter the password when you log in to the web management system again. 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.

## 🛕 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.

## 1.4 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. If you want to switch the work mode, see <u>Switching Work Mode</u>.

## 1.4.1 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.

## 1.4.2 Router Mode

The device supports NAT 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. NAT 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 Eweb again.

## 1.4.3 Wireless Repeater Mode

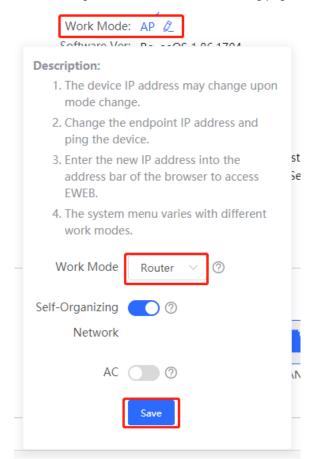
The device does not support the routing and DHCP server functions in the wireless repeater mode. IP addresses of the clients are assigned and managed by the primary router. On an available network, the device can be connected to the primary router through wireless connection to expand the Wi-Fi coverage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

# 1.5 Configuration Wizard (Router Mode)

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

## 1.5.1 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.
- 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.
- (2) 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>Switching Work Mode</u> for more details.



## 1.5.2 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.

#### 1 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.

Ruíjie		r Device					English ~ [	
	Total Devices: 1. Please make sure that the	device count and to	opology are corre	ect. The unmanage	ed switch will not appe	ar in the list.	Ø	
	Net Status ( <b>Online Dev</b>	vices / Total )	Router 0 Route		Switch 0 / 0 Switches		Refresh O	
	My Network							
	test (1 devices)						~	
	Model		SN	IP	MAC	Software Ver		
	SER A P RAP6262(G) [	[Master] G1Q	WA2V000477	192.168.120.2	AA:11:AA:00:04:77	ReyeeOS 1.75.1410		
			Redi	scover	Start Setup			

## 2. Creating a Network Project

Click Start Setup to configure the Internet connection type, Wi-Fi network and management password.

- (1) Network Name: Identify the network where the device is located.
- (1) **Internet**: Configure the Internet connection type according to requirements of the local Internet Service Provider (ISP).
  - **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.
- (2) **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.
- (3) Management Password: The password is used for logging in to the management page.
- (4) **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.
- (5) **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.

Ruffe Rcycc Create Network				English 🗸 🕒 Exit
* Net	twork Name	Example: XX hotel.		
Networ	rk Settings			
		PPPoE  DHCP  Static IP Checking IP assignment		
	* SSID			
Wi-	-Fi Password 🔘	Security Open		
Manage	ement Passw	vord (Please remember the passw	ord.)	
* M		Please remember the management pass	> <sub>77</sub> 4	
	Password			
Country	y/Region/Tin	ne Zone	$\sim$	
* Cou	untry/Region	China (CN)	~	
1	* Time Zone (	(GMT+8:00)Asia/Shanghai	~	
	Previou	Js Create Network & Connect		

Click Create Network & Connect. The device will deliver the initialization and check the network connectivity.

* Nc	Operation succeeded.	
	Network Name: demo SSID: @Ruijie-s0477	
	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.

#### 1 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.

# 1.6 Configuration Wizard (AP Mode)

## 1.6.1 Getting Started

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

## 1.6.2 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.

Ruíjie Rcycc	Create Network			English 🗸 🕒 Exit
	* Network Name	Example: XX hotel.		
	Network Settings			
	Internet	DHCP      Static IP		
	* SSID	@Ruijie-s0477		
	Wi-Fi Password	• Security Open		
			<u>≻</u> ,,≮	
	Management Pas	sword (Please remember the pass	sword.)	
	* Management Password	Please remember the management pass	٦ <sub>٣</sub>	
	Country/Region/	Time Zone	~	
	* Country/Region	China (CN)	~	
	* Time Zone	(GMT+8:00)Asia/Shanghai	~	
		Create Network & Connect		

# 1.7 Configuration Wizard (Wireless Repeater Mode)

## 1.7.1 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.

#### 🛕 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.

## 1.7.2 Configuration Steps

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

Ruijie						English 🗸 🕞 Exit
	Total Devices: 4. Other Devic Please make sure that the device count a	Ø				
	Net Status ( <b>Online Devices / Total</b> )	Router 0 Router	Switch 0 / 0 Switches	ি 1/1 APs	7 3 Other Devices	Refresh Q
	My Network					
	Unnamed Network (1 devices)					~
	Model	SN	IP	MAC	Software Ver	
	AP RAP2260(E) [Master]	G1QH6WX000610	172.26.1.32	EC:B9:70:23:A4:BF	ReyeeOS 1.86.	
	Other Devices ()					
	New Device (1 devices)	Add to My Networ	k			>
	EWEB ECB970F24902 (1 devices)	Add to My Networ				>
		Redis	cover	Start Setup		

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

WAN port is not connected with network cable				
Ethernet status				
Connected Please connect the WAN port to the Internet.				
WAN LAN				
172.26.1.32				
Cancel Wireless Repeater Check Again				

(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**.

R	Wireless Repeate			English 🗸 🕞 Exit
			G	
		5G @Ruijie-s1577_5G	1 🛜	
		5G xiaoxi_5G	£ 🛜	
		5G ruijie-guest	<b></b>	
		5G ruijie-802.1x	A 🛜	
R	Wireless Repeate	, ,		English 🗸 🕞 Exit
		Confirm SSID and Wi-Fi Key:		
		Primary Router SSID @Ruijie-s1577_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.

Local Router Wi-Fi New Wi-Fi Same as Primary Router Wi-Fi * SSID (2.4G) @Ruijie-s1577_5G_plus * SSID (5G) @Ruijie-s1577_5G_plus_5G * Wi-Fi Password	🕞 Exit
* SSID (2.4G) @Ruijie-s1577_5G_plus * SSID (5G) @Ruijie-s1577_5G_plus_5G * Wi-Fi Password	
<pre>@Ruijie-s1577_5G_plus * SSID (5G) @Ruijie-s1577_5G_plus_5G * Wi-Fi Password</pre>	
* SSID (5G) @Ruijie-s1577_5G_plus_5G * Wi-Fi Password	
<pre>@Ruijie-s1577_5G_plus_5G * Wi-Fi Password</pre>	
* Wi-Fi Password	
12345678 💿	
Previous Save	

## **1.8 Introduction to the Eweb GUI**

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>Switching Work Mode</u>.

As to the RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-RAP6262 models, please refer to Dual Management Webpages.

As to other RAP models, please refer to Single Management Webpage.

## 1 Note

When the self-organizing network is enabled, the Eweb GUI is subject to the master device in the network. If the master device supports the dual management webpages, the slave device also displays the dual management webpages.

## 1.8.1 Single Management Webpage

#### 1. Network-wide Management

The device works in self-organizing network mode by default. The Web page displays the network-wide management menu on the left side, in which you can check the current status of all devices in the network, and modify network-wide configuration, including global Wi-Fi network management configuration (APs and Wi-Fi), routing management configuration (if routers exist in the network), switch management configuration, and network-wide management configuration (time, password, network-wide reboot, and other system settings).

Ruíjie I &Rcycc	test > Ruijie (Slave) 0		English 🗸 🧹	) 288 会 @ 这 [-
Source S	Device Info         Setup>           Image: Hostname: Ruijie         SN: G1QH6WX000610           Image: RAP2260(E)         Image: Image: Right and the set of the	Wi-Fi Rrimary Wi-Fi: @Ruijie-m0848 Security: No	Guest WI-Fi: Security: No	Setup>
≧ Switches ﷺ Network ✓	Net Status ( <b>Online Devices / Total )</b>	↓ 1.88Kbps Switch 0 / 1 Switches	হ 1/2 APs	Refresh O 0 Online Clients
	Real-Time Flow (Kbps)	Uplink Flow Downlink Flow	5:51 23:26:02 23:26:13 23:26	Kbps > WAN >
«Collapse				

## 2. Standalone Management

• If a device is in self-organizing network mode, click the name of the currently logged in device or click **Manage** of a specified device in the device list to configure and manage the device.

Rujje	test > Ruijie (Slave) 🕖					English 🗸 🙆	88 <b>@</b>	<u>بة</u> 🗗
옹Overview	i AP List							?
⊗ Online Clients	AP List Group: All Groups	Expand		IP/MAC/hostname/S	N/SoftWare Ver	Q List Filter	Batch Ad	_
ବ୍ Wireless	Action	Hostname ≑	IP ≑	MAC \$	Status ≑	Model ≑	Clients \$	
APs Wi-Fi	🖄 🔞 Manage 🖱 Reboot	Ruijie	192.168.110.240	EC:B9:70:23:A4:BF	Online	RAP2260(E)	0	R
Clients Blacklist/Whitelist	□ Ø Manage U Reboot	Ruijie	192.168.110.29	AA:11:AA:00:04:77	Offline	RAP6262(G)	1	R

Rujje Rcycc	test > Ruijie (Sla	Image: Second secon	e: Ruijie P: 192.168.110.240	SN: G1QH6WX000 MAC: EC:B9:70:23:A4	(') Reboot
Online Clients	🧃 AP List	Overview Basics V Wireles	ss $\vee$ Advanced $\vee$	Diagnostics ~ System	× ]
Router	AP List G	Overview			
		Memory Usage 56%	Online Clients		2 days 3 hours 25 minutes 33 seconds
Wi-Fi	Sea 🖉 Ma	30 %	0	Systime: 20	022-03-31 23:30:09
Clients	🗌 💮 Mai	Device Details			
Blacklist/Whitelist		Model: RAP2260(E)			me: Ruijie 🖉
Radio Frequency	< 1	SN: G1QH6WX0006 Work Mode: AP 2	10		AC: EC:B9:70:23:A4:BF ole: Slave AP () (Master AC: 192.168.110.1)
LAN Ports		Hardware Ver: 1.00			/er: ReyeeOS 1.61.1817

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

Rujje	test 👌 Ruijie 🕖		English - 🛆 🎇 🖨 🔍 📺 🕞
Basics	Overview		
⊕ Basics ~ ∵Wireless ~	Memory Usage <b>57%</b>	Online Clients	Status: Online Duration: 2 days 3 hours 29 minutes 50 seconds Systime: 2022-03-31 23:34:26
금 Advanced ∨ ♀ Diagnostics ∨	Device Details		
-∰e-System ∨	Model: RAP2260(E) SN: G1QH6WX000610 Work Mode: AP 2 Software Ver: ReyeeOS 1.61.1817		stname: Ruijie & MAC: EC:B9:70:23:A4:BF are Ver: 1.00
	Primary Wi-Fi: @Ruijie-s1234 Security: No		st Wi-Fi:
	Connected Disconnected	WAN LA 192.168.110.240	N
« Collapse			

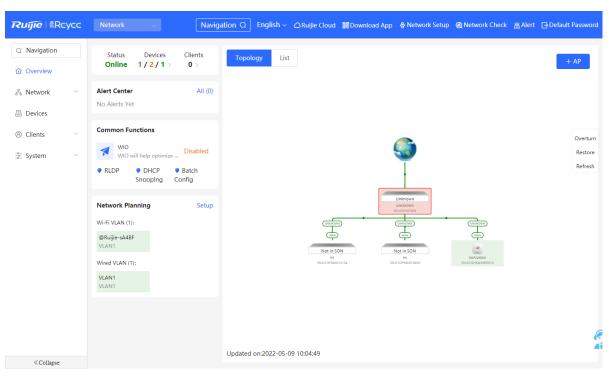
## 1.8.2 Dual Management Webpages

## 1. Introducing the Management Mode

If the self-organizing network is disabled (The function is enabled by default. See <u>Switching Work Mode</u> for details.), the device works in the local device mode displayed on the Web page.

If the self-organizing network is enabled, the device can work in the network mode and the local device mode. The two modes can be switched on the Web page.

- Network mode: View the management information of all devices in the network, and configure all devices based on network management.
- Local Device mode: Only configure the currently logged in devices.



#### Network mode webpage

Local Device mode webpage

<b>Ruíjíe</b>   @Rcycc	Local Device(RAP $\lor$	English ~	pp 🔮 Network Setup 🔘 Network Check - 満 Alert 🕞 Default Password
윦 Overview ④ Basics · · ·	Overview		
<ul> <li>☆ Advanced ~</li> <li>④ Diagnostics ~</li> </ul>	Memory Usage <b>59</b> %	Online Clients O	Status: Online Uptime: 2 days 20 hours 22 minutes 36 seconds Systime: 2022-05-09 10:05:46
	Device Details Model: RAP2260(E) MAC: EC:89:70:23:A4:BF Hardware Ver: 1.00 Wi-Fi Wi-Fi Primary Wi-FI: @Ruljie-sA4BF Security: No Ethernet status	Hostname: Ruijie & Work Mode: AP & Software Ver: ReyeeOS 1.86.	
«Collapse	Connected	WAN LAN 172.26.1.32	

## 2. Switching the Management Mode

Click the current management mode in the navigation bar, and select the mode in the drop-down box to switch the work mode of the device.

Rujje	Network V		Navigation Q	English 🗸 🛆	<b>@</b> (	Q	ю	₿
Network	^ ( C	urrently in Netv	work mode.	,				
Network Local Devi	ce(RAP	Clients 0 >	Торо	Ιος				

# 2 Network Monitoring

## 🛕 Caution

The functions mentioned in this chapter are supported by only RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2260, RG-RAP1261, RG-RAP1260, and RG-RAP6262.

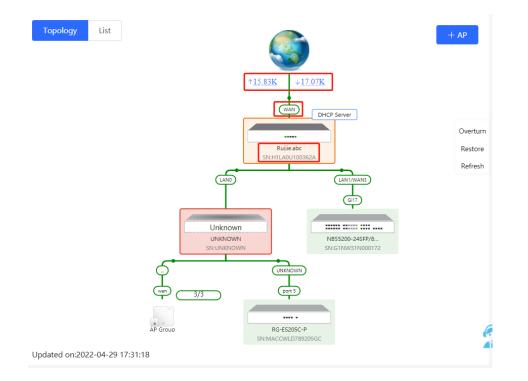
## In Network mode, select Overview.

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.

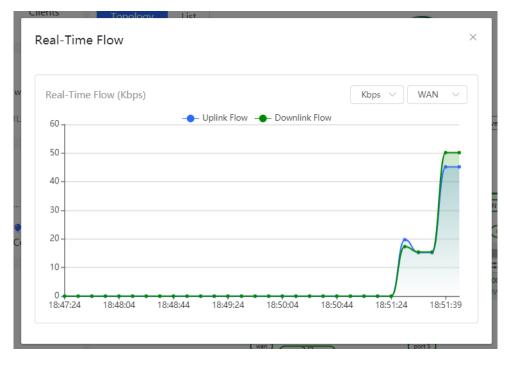


# 2.1 Viewing the Network Information

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 flow data and view the real-time flow.



 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.

Topology List	EGW	Hostname <mark>: Ruijie.abc</mark> Model:EG205G SN:H1LA0U100362A	Q	Software Ver:ReyeeOS 1.86. MGMT IP:192.168.110.1 MAC: 00:74:9c:87:6d:85	.1619	
• IELSER • IELSE	<ul> <li>Port Status</li> <li>VLAN Info</li> <li>Port</li> <li>More</li> </ul>	Port Status		AN2 WAN1 WAN		
		VLAN			Edit 🛇	
Re Ease Re Ease P		Default VLAN				
		Interface	IP	IP Range	Remark	
		LAN0,1	192.168.110.1	192.168.110.1- 192.168.110.254		6
Updated on:2022-04-29 17:31:18						

• 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.

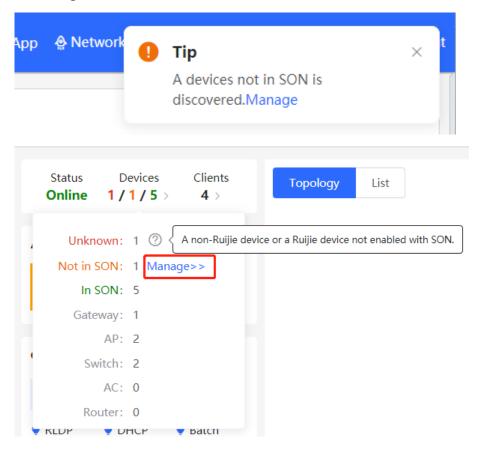
Topology	List	+ AP
	↑ <u>14.05K</u> ↓ <u>22.45K</u>	
	WAN DHCP Server	
	Ruijie.abc	Overturn Restore
		Refresh

# 2.2 Adding Network Devices

## 2.2.1 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 **Manage** 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.

<i>Network List</i> Every network varies in devices and	configuration. You can add c	devices of Other Netwo	rk to My Network.		?
My Network					
工位网关 (5 devices)					~
Model	SN	IP	MAC	Software Ver	
Router EG205G [Master]	H1LA0U100362A	192.168.110.1	00:74:9C:87:6D:85	ReyeeOS	
A P RAP2200(E)	1234942570021	192.168.110.152	00:D0:F8:15:08:48	AP_/	
A P RAP2260(G)	G1QH2LV00090C	192.168.110.102	C4:70:AB:A8:69:17	ReyeeOS	
Switch NBS5200-24SFP/8GT4XS	G1NW31N000172	192.168.110.89	00:D3:F8:15:08:5B	ReyeeOS	
Switch RG-ES205C-P	MACCWLD789205GC	192.168.110.226	78:11:22:33:44:55	ESW_	
Other Network 工位网关 (1 devices)	Add to My Network				>

<ul> <li>Network List</li> <li>Every network varies in devices an</li> </ul>	d configuration. You can ado	d devices of Other Netw	ork to My Network.		?
My Network					
[位网关 (5 devices)					~
Nodel	SN	IP	MAC	Software Ver	
Router EG205G [Master]	H1LA0U100362A	192.168.110.1	00:74:9C:87:6D:85	ReyeeOS	
A P RAP2200(E)	1234942570021	192.168.110.152	00:D0:F8:15:08:48	AP.	
A P RAP2260(G)	G1QH2LV00090C	192.168.110.102	C4:70:AB:A8:69:17	ReyeeOS	
Switch NBS5200-24SFP/8GT4XS	G1NW31N000172	192.168.110.89	00:D3:F8:15:08:5B	ReyeeOS	
Switch RG-ES205C-P	MACCWLD789205GC	192.168.110.226	78:11:22:33:44:55	ESW_	
Other Network					
[位网关 (1 devices)	Add to My Network				~
Model	SN	IP	MAC	Software Ver	
A P EAP602	MACC522376524	192.168.110.200	00:10:F8:75:33:72	AP	

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.

f Add Device	to My Network	×
* Password	Please enter the management password	
	Forgot Password Add	

## 2.2.2 AP Mesh

## 1 Note

This function is not supported by RG-RAP1200(F) and RG-RAP2200(F).

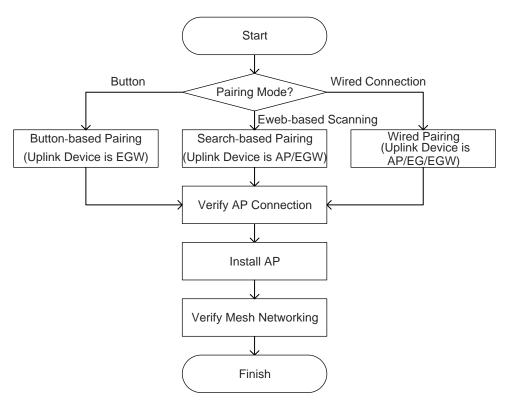
## 1. Overview

After being powered on and enabled with Mesh (see 3.18\_\_\_\_\_ 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 Eweb 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 Procedure



## 3. Configuration Steps for Button-based Pairing (Uplink Device is an EGW Router)

## 🛕 Caution

- Only EG105GW-X and EG105GW(T) support button-based pairing and each router can be paired with up to 15 new APs.
- The new AP must be in factory status.
- It can be scanned only when the live network is enabled with Mesh (see <u>3.18 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 **Overview** page to make sure that the new AP has connected to the uplink device in wireless mode.

Ruíjie I & Rcycc	Network 🗸	Navigation Q English - 🛆 🛔	@ ă 🖯
Q Navigation	StatusDevicesClientsOnline3 / 3 / 1 >5 >	Topology List	+ AP
<ul> <li>Network</li> <li>Devices</li> </ul>	Alert Center         All (1)           The network contains different types o         A device (MACCWIFI7XN86,MACC6262	+33.42K J15.23K	
Gateway Clients Management	Common Functions WIO WIO will help optimize Disabled	EGIDSON(T) Streeting Wirelens Wirelens	Overturn Restore Refresh
tanin System ∽	WAN      LAN     Network     Check  Network Planning     manage	Winners)         Winners)           28         48           54225000         5542510/02040011584           5542510/02040011584         5542510/020000014	
	WI-FI VLAN (1): Add WEITENG98768962 VLAN1 Wired VLAN (1): Add	47 	e

- (4) Power off the new AP and install it as planned.
- (5) Log in to the Eweb of a device on the target network. In Network 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.

Overview		Device List								
Network 🗸	•	A devices not in SON	is discovered.	Manage						
Devices	Devi	ce List 😋 Group	All Groups	Expand Cha	inge Group	Basic Info	RF Information	Model		
Gateway							IP/MAC/host	name/SN/S Q	Delete Offline	Devices Batch Upgrade
) Clients Management		SN \$	Status ≑	Hostname 🌩	MAC A	ddress ≑	IP Address ≑	Clients ≑	Device Group	Relay Information ¢
System 🗸		G1NQCAM001084	Online	Ruijie 🖉	80:05:	38:F0:19:90	192.168.110.31 🖉	0	egw做主/Default	The second secon
		G1QH2LV000084	Online	Ruijie 🖉	C4:70:/	\B:A8:67:CF	192.168.110.152 🖉	0	egw做主/Default	중 5G View Details
	¢	1 10/m	<b>.</b>							Total 2

Click **View Details** following the **SSI**.

ssic Info     RF Information     Model       IP/MAC/hostname/SN/S Q     Image: Delete Offline Devices     Batch Upgrade       Image: State of the state of
Noise Floor: -86 dBm
Utilization: 13 %
RSSI: -37 dBm Good Negotiation Rate: 866 Mbps Uptime: 4 minutes 4 seconds Details
7.CF Uplink Local Details
EWR     Ruijie       Ruijie     Ruijie       Model:     EG105GW(T)       Model:     RAP2260(G)
6

#### 4. Configuration Steps for Search-based Pairing (Uplink Device is an AP or EGW Router)

## A Caution

- The new AP must be in factory status.
- It can be scanned only when the live network is enabled with Mesh (see 3.18\_\_\_\_ 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 AP or EGW router on the target network.
- (2) Log in to the Eweb of a device on the target network. In Network mode, click +AP in the upper right corner of the Overview page to scan the APs in other networks not plugged in with Ethernet cables.

Ruíjie	Network   Currently in Netw	ork mode. Rayligation Q English ~ 🛆 👌 🍭	<u>بة</u>
Q Navigation	Status Devices Clients Online 3/2/1 > 7 >	Topology List +	АР
Overview			
🖧 Network	Alert Center All (1)		
Devices	The network contains different types o A device (MACC6262GGN74,MACC162 )	+15.29K +11.49K	
🖽 Gateway	Common Functions	ECISORAV(T)	Overturn
⑧ Clients Management	WIO WIO will help optimize Disabled	(Weien)	Restore Refresh
:e= :a= System ∨	WAN LAN Network Check		
	Network Planning manage		
	Wi-Fi VLAN (1): Add	(WAN)	
	WEITENG98768962 VLAN1	Not in SON	
		UNIX OF THE OWNER WAS	0

(3) 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.

Rujje	Network 🗸			Navigation Q	English -> 🛆 🔮 🍭	ы с	}
Q. Navigation       ① Overview       ⊕ Network       ▷ Devices	Network List     Every network varies in devices an     My Network     egw脫主 (2 devices)	d configuration. You can add devices of Othe	r Network to My Network.			?	
🖽 Gateway	Other Device						
Clients Management	New Device (1 devices)	Add to My Network				~	
	Model	SN	BSSID	RSSI	Device Location ⑦		
	A P RAP2260(G)	G1QH2LV000084	c4:70:ab:a8:67:cf	۱ ج	Hostname Ruijie MAC 00:D0:F8:14:5C:C3 Address		
		Re	-scan				(
Ruíjie . Rcycc	Network 🗸	Navigation	Q English ~ @Remo	e O&M  👌 Network Set	tup @Network Check <u>満</u> Alert	🕞 Log O	Dut
Q Navigation	Network List     Every network varies in devices and configu	ration. You can add devices of Other Network to M	ly Network.			?	
음 Network	Adding 1 devices to my network 0 devices have						
Devices	My Network						
<ul> <li>Gateway</li> <li>Olients Managemént</li> </ul>	egw做主 (2 devices) Other Device	渋					
System		The networks are merging					
	Model	SN	BSSID	RSSI	Device Location ⑦		
	A P RAP2260(G)	G1QH2LV000084	c4:70:ab:a8:67:cf	<u></u>	Hostname Ruijie MAC 00:D0:F8:14:5C:C3 Address		
		Re-	scan				(
<b>Ruijie</b> l &Rcycc	Network V	Navigation	Q English ∽ _∩ Remot	≥ O&M	up @Network Check	🕞 Log Oi	ut
Q Navigation	Network List     Every network varies in devices and configu	ration. You can add devices of Other Network to M	y Network.			0	
🖧 Network	My Network						
Devices B Gateway	egw微主 (3 devices)						
Clients Management	Other Device		×				
System V	New Device (1 devices) Add	t 🕑 Network merging succeeded.	ок	RSSI	Device Location ⑦		
	AP RAP2260(G)	G1QH2LV000084	c4:70:ab:a8:67:cf	ę	Hostname Ruijie MAC 00:D0:F8:14:5C:C3 Address		
		Re-s	can				

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

Ruíjie I & Rcycc	Network 🗸	Navigation Q English ~ 🛆 🔮	@ ă G
Q Navigation	StatusDevicesClientsOnline3 / 3 / 1 >5 >	Topology List	+ AP
Network     Devices	Alert Center         All (1)           The network contains different types o         A device (MACCWIFI7XN86,MACC6262	+33.42K +15.23K (WM) DIP2 Server	
<ul> <li>Gateway</li> <li>Clients Management</li> </ul>	Common Functions	Conversion and Conver	Overturr Restore Refresh
∵en System ∨	WIO will help optimize Disabled WAN PLAN Network Check	Image: Constraint of the second se	kerresn
	Network Planning manage		
	Wi-Fi VLAN (1):         Add           WEITENG98768962         VLAN1	3/3 A Grange	
	Wired VLAN (1): Add		

- (5) Power off the new AP and install it as planned.
- (6) Log in to the Eweb of a device on the target network. In Network mode, choose Devices > AP. Make sure

⑦ 5G in the Relay that the new AP is online and the corresponding entry contains icon Information column. The icon indicates that wireless backhaul is performed through the 5 GHz radio.

Overview		Device List								
Network 🗸	•	A devices not in SON	is discovered.	Manage						
Devices	Devi	ce List 😋 Group:	All Groups	Expand Cha	inge Group	Basic Info	RF Information	Model		
Gateway							IP/MAC/hos	tname/SN/S <sup>,</sup> Q	🗇 Delete Offline	Devices Batch Upgrade
Clients Management		SN \$	Status 🌲	Hostname 🗘	MAC	Address ≑	IP Address 🗘	Clients ≑	Device Group	Relay Information
System ~		G1NQCAM001084	Online	Ruijie 🖉	80:05	:88:F0:19:90	192.168.110.31 🖉	0	egw做主/Default	SG View Details
		G1QH2LV000084	Online	Ruijie 🖉	C4:70:	:AB:A8:67:CF	192.168.110.152 🖉	0	egw做主/Default	중 5G View Details
	4	1	<b>.</b>							Total

Click View Details following the

icon to obtain information about the uplink device and

RSSI.

Device A device		is discovered.	Manage									
vice Lis	t 😋 Group:	All Groups	Expand	Change Group	Basic Inf	RF Information Mod		🗇 Delete Offline	Devices	Batch Upg	,rade	
S	SN ≑	Status 🌲	Hostname 💠 MAC Address 💠			Noise Floor: - <b>86 dBm</b> Channel Utilization: 13 %			Relay Information			
G1NQ	CAM001084	Online	Ruijie 🖉	80:05:88:F0:19:90		Negotiation Rate: 86	RSSI: -37 dBm Good Negotiation Rate: 866 Mbps Uptime: 4 minutes 4 seconds			중 5G View Details		
G1QH	12LV000084	Online	Ruijie 🖉 C4:70:AB:A8:67:CF			Uplink Local			● <b>5G</b> View Details			
1	10/pag	je 🗸				Ruijie Model: EG105GW(T)		Ruijie : RAP2260(G)		То	ital 2	
						Model: EG105GW(T) SN: WEITENG987689 IP: 192.168.110.1	SN: C	: RAP2260(G) 51QH2LV000084 92.168.110.152	J			

#### 5. Configuration Steps for Wired Pairing (Uplink Device is an AP, EG Router, or EGW Router)

## 🛕 Caution

- The new AP must be in factory status.
- It can be scanned only when the live network is enabled with Mesh (see <u>3.18 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 Eweb of a device on the target network. In **Network** mode, choose **Devices** and make sure that the new AP is online.

Q Navigation	All (2)	Gateway <b>(0)</b>	AP (1)	Switch (0) AC	(0) Router (1)					
Overview		<b>ce List</b> vices not in SON i	is discovered.	120200						
පී Network 🗸	- A de	vices not in 30141	is discovered. In	лападе						
Devices	Device List C     IP/MAC/hostname/SN/S C     Image: Delete Offline Devices     Batch Upgrad									
🖽 Gateway		SN \$	Status ≑	Hostname ≑	MAC Address $\Leftrightarrow$	IP Address ≑	Software Ver	Model ≑		
8 Clients Management	used w	EITENG987689	Online	Ruijie [Master] 🖉	00:D0:F8:14:5C:C3	10.18.108.1 🖉	ReyeeOS 1.218.1308	EG105GW(1		
ter System ∨	🗌 G1	NQCAM001084	Online	Ruijie 🖉	80:05:88:F0:19:90	192.168.110.31 🖉	ReyeeOS 1.218.2427	RAP2200(E		
	< 1	> 10/pag	e v					Total 2		

- (3) Unplug the Ethernet cable, power off the new AP, and install it as planned.
- (4) Log in to the Eweb of a device on the target network. In Network 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.

Q Navigation	All (3) Gateway	y (0) AP (2)	Switch (0) AC						
Overview									
Network	Device List     A devices not	t in SON is discovered.	Manage						
	Device List D		Encoder Char	nge Group Basic Info	Dr. Information	Model			
Devices	Device List 😋	Group: All Groups	Expand Chang	nge Group Basic Info		stname/SN/S-Q	🗊 Delete Offline	Devices Ba	tch Upgrade
🗄 Gateway									
8 Clients Management	SN \$	Status 💠	Hostname 💠	MAC Address $\mbox{$\updownarrow$}$	IP Address 💠	Clients ≑	Device Group	Relay Informa	tion
-a -a -a System	G1NQCAM0	001084 Online	Ruijie 🖉	80:05:88:F0:19:90	192.168.110.31 🖉	0	egw做主/Default	The second secon	w
	G1QH2LV0	000084 Online	Ruijie 🖉	C4:70:AB:A8:67:CF	192.168.110.152 🖉	0	egw做主/Default	<b>≈ 5G</b> Vie Details	w
		10/0200							Total 2
lick View Det	ails following	na the	<u>्रि</u> 5G	icon to d	btain infor	rmation	about the	uplink c	levice
	t <b>ails</b> followin	ng the	÷ 10	icon to c	btain infor	rmation	about the	uplink c	levice
SSI. II (3) Gateway (0) Device List		ng the	C (0) Route		obtain infor	rmation :	about the	uplink c	levice
SSI. II (3) Gateway (0) Pevice List A devices not in S	) AP (2) SON is discovered. M	ng the switch (0) AC	C <b>(0)</b> Route	er (1)		rmation	about the	uplink c	levice
SSI. III (3) Gateway (0) Device List	) AP (2) SON is discovered. M	ng the switch (0) AC	C <b>(0)</b> Route	er (1) Nasic Info			about the		device ch Upgrade
SSI. II (3) Gateway (0) Pevice List A devices not in S	) AP (2) SON is discovered. M	ng the switch (0) AC	C <b>(0)</b> Route	er (1) Hasic Info IP/ s ≑ N	nation Model WAC/hostname/SN oise Floor: -86 dE Channel 13 %	] √/S Q ■ Bm	Delete Offline Dev		ch Upgrade
SSI. Il (3) Gateway (0) Pevice List A devices not in S Device List © Gra	) AP (2) S SON is discovered. M oup: All Groups Status \$	ng the Switch (0) AC Ianage Expand Chang	C (0) Route	er (1) Hasic Info RF Inforr IP/ s ¢ 9:90 Negoti	nation Model VAC/hostname/SM Channel 13 % Utilization: 13 % RSSI: -37 dĒ ation Rate: 866 M	J √S Q Bm Bm Good 1bps	Delete Offline Dev	/ices Bat	ch Upgrade
SSI. II (3) Gateway (0) Pevice List Device List © Gro SN \$	) AP (2) SON is discovered. M SON is discovered. M oup: All Groups Status \$	ng the Switch (0) AC lanage Expand Chang Hostname \$	C (0) Route ge Group Ba	er (1) Hasic Info RF Inforr IP/I s ¢ Negoti Uptime 57:CF	nation Model WAC/hostname/SN Channel 13 % RSSI: -37 dE ation Rate: 866 M : 4 minutes 4 secc Uplink	J V/S Q Bm Bm Good Ibps onds	Delete Offline Dev	rices Bat Relay Informati ≑ 중 5G View	ch Upgrade ion
SSI. II (3) Gateway (0) Pevice List Device List C Gro SN ¢ G1NQCAM0010 G1QH2LV00002	) AP (2) SON is discovered. M SON is discovered. M oup: All Groups Status \$	ng the Switch (0) AC Ianage Expand Chang Hostname \$ Ruijie 2	C (0) Route ge Group B MAC Address 80:05:88:F0:19	er (1) Hasic Info RF Inforr IP/ S S S S S S S S S S S S S	nation Model WAC/hostname/SM Channel 13 % RSSI: -37 df ation Rate: 866 M : 4 minutes 4 secc Uplink 50 wa 50 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	J V/S Q Bm Bm Good Ibps onds G G	Delete Offline Dev	rices Bat Relay Informat ≎ © 5G View Details © 5G View	ch Upgrade ion
SSI. III (3) Gateway (0) Pevice List Device List © Gro SN ¢ G1NQCAM0010 G1QH2LV00000	) AP (2) S SON is discovered. M oup: All Groups Status \$ 084 Online 84 Online	ng the Switch (0) AC Ianage Expand Chang Hostname \$ Ruijie 2	C (0) Route ge Group B MAC Address 80:05:88:F0:19	ar (1)	nation Model WAC/hostname/SN Channel 13 % RSSI: -37 dE ation Rate: 866 M : 4 minutes 4 secc Uplink SS	J J Sm Sm Good Ibps onds	Delete Offline Dev	rices Bat Relay Informat ≎ © 5G View Details © 5G View	ch Upgrade ion v

### 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 Eweb of a device on the target network. In Network mode, choose Devices > AP and click the serial number of the Mesh AP with the WAN port to be enabled.

Q Navigation	All (3) Gateway (0)	AP (2)	Switch (0) AC	C (0) Router (1)				
Overview	Device List							
🖧 Network	A devices not in SON i	is discovered.	Manage					
Devices	Device List 😋 Group:	All Groups	Expand Chang	ge Group Basic Info		Model		
🖽 Gateway						tname/SN/S Q	Delete Offline	Devices Batch Upgrade
Ø Clients Management	SN \$	Status ≑	Hostname 🌲	MAC Address 🌩	IP Address ≑	Clients 🌩	Device Group	Relay Information
-®- -o- System	G1NQCAM001084	Offline	Ruijie	80:05:88:F0:19:90	192.168.110.31	0	egw做主/Default	No data 😋
	G1QH2LV000084	Online	Ruijie 🖉	C4:70:AB:A8:67:CF	192.168.110.152 🖉	0	egw做主/Default	The second secon
	< 1 > 10/pag	e ~						Total 2

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

Radio Frequency	Overview Online Clients Network - WLAN - Advanced - Diagnostics - System -
▶ More	<ul> <li>Enable WAN</li> <li>The WAN port is used as a wired uplink port of the AP by default. When the device works in the wireless repeater mode, the WAN port is disabled by default. If you want to establish a wireless connection to extend network coverage, please enable this port.</li> </ul>
	Enable
	Save

#### 7. Querying Mesh APs and Mesh Details

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

) Navigation	Status Devices Clients Online 3/3/1 > 5 >	Topology List + AP
Overview		
Po Network	Alert Center All (1)	
🗟 Devices	The network contains different types o > A device (MACCWIFI7XN86,MACC6262 >	+ 18.24K + +23.13K
🖽 Gateway	Common Functions	Overturn
Ø Clients Management	WIO WIO will help optimize Disabled	Consolution         Restore           (minus)         (minus)         Refresh
-o -o o System	WAN     AN     AN     An     An     An     An     An	Wirefers) Wirefers) at at Unknown R422000 R4223000 Unknown
	Network Planning manage	SR-GTH2CAM001064 SPK-GTCH2CA000064 SPK-GTCH2CA000064
	Wi-Fi VLAN (1): Add	
	WEITENG98768962 VLAN1	Al Grave
	Wired VLAN (1): Add	

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

Device List A devices not in SON is vice List C Group: J		_	e Group Basic Info		Model tname/SN/S-Q	🗇 Delete Offline	Devices Batch Upgrade
		_	Basic Info			Delete Offline	Devices Batch Upgrade
VICE LIST G GIOSPI						Delete Offline	Devices Batch Upgrade
SN \$	Status 🗘	Hostname \$	MAC Address $\ \diamondsuit$	IP Address $\Leftrightarrow$	Clients 🗘	Device Group	Relay Information
G1NQCAM001084	Online	Ruijie 🖉	80:05:88:F0:19:90	192.168.110.31 🖉	0	egw做主/Default	SG View Details
G1QH2LV000084	Online	Ruijie 🖉	C4:70:AB:A8:67:CF	192.168.110.152 🖉	0	egw做主/Default	SG View Details
	G1NQCAM001084	G1NQCAM001084 Online	GINQCAM001084 Online Ruijie 2	G1NQCAM001084 Online Ruijie & 80:05:88:f0:19:90	G1NQCAM001084 Online Ruijie & 80:05:88:50:19:90 192.168.110.31 &	G1NQCAM001084 Online Ruijie & 80:05:88:F0:19:90 192.168.110.31 & 0	GINQCAM001084 Online Ruijie & 80:05:88:F0:19:90 192.168.110.31 & 0 egw微主/Default

(3) Query Mesh networking details.

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

All (3)	Gateway (0)	AP (2)	Switch (0)	AC <b>(0)</b>	Router (1)			
	<b>Device List</b> A devices not in SON is	discovered.	Manage					
Devi	ice List 😋 Group: .	All Groups	Expand	hange Group	Basic Info	RF Information Model	/S Q 🗇 Delete Offline I	Devices Batch Upgrade
	SN \$	Status ≑	Hostname	\$ MAC	Address 🌲	Noise Floor: -86 dB Channel Utilization: 13 %	m	Relay Information
	G1NQCAM001084	Online	Ruijie 🖉	80:0	5:88:F0:19:90	RSSI: -37 dB Negotiation Rate: 866 MI Uptime: 4 minutes 4 seco	bps	<b>╤ 5G</b> View Details
	G1QH2LV000084	Online	Ruijie 🖉	C4:7	):AB:A8:67:CF	Uplink	AP	<b>╤ 5G</b> View Details
<	1 > 10/page	2 ~				<b>Ruijie</b> Model: EG105GW(T) SN: WEITENG987689 IP: 192.168.110.1	Ruijie Model: RAP2260(G) SN: G1QH2LV000084 IP: 192.168.110.152	Total 2

# 2.3 Managing Network Devices

Click **List** at the top left corner of the topology or click **Devices** in the menu bar to switch to the device list view, and view the information of all devices in the self-organizing network (SON). You can perform configurations and management on all devices by logging in to only one device in the network.

Ruíjie	Network 🗸	Navigation Q English ~ 🛆 🗱 🔮 @ 🖄 🗗
Q Navigation	Status     Devices     Clients       Online     1 / 6 >     3 >	+ AP
Overview		
움 Network 🌱	Alert Center All (0)	<u></u>
🖻 Devices	No Alerts Yet	↑ <u>84.26K</u> ↓ <u>40.67K</u>
🖽 Gateway	Common Functions	Overturn
8 Clients	WIO WII will help optimize Disabled	Rulinade Restore

Тор	ology List				IP/MAC,	/hostname/SN/S Q	Batch Upgrade
	SN \$	Status ≑	Hostname 🌲	MAC ≑	IP ≑	Software Ver	Model \$
	MACCWLD789205GC	Online	ruijie 🖉	78:11:22:33:44:55	192.168.110.226	ESW_	RG-ES205C-P
Local	H1LA0U100362A	Online	Ruijie.abc [Master] 🖉	00:74:9C:87:6D:85	192.168.110.1 🖉	ReyeeOS	EG205G
	G1NW31N000172	Online	Ruijie 🖉	00:D3:F8:15:08:5B	192.168.110.89 🖉	ReyeeOS	NBS5200- 24SFP/8GT4XS
	1234942570021	Online	RAP2200e 🖉	00:D0:F8:15:08:48	192.168.110.152 🖉	AP.	RAP2200(E)
	G1QH2LV00090C	Online	Ruijie 🖉	C4:70:AB:A8:69:17	192.168.110.102 🖉	ReyeeOS	RAP2260(G)
	1 > 10/page						Total 5

• Click **SN** to configure the specified device.

		×	MSW	Hostname: Ruijie 🖉 Model:NBS5200-24SFP/8GT4XS	Software Ver:ReyeeOS 1.86.1704 MGMT IP:11.1.1.89	
Ŧ				SN:G1NW31N000172	MAC: 00:D3:F8:15:08:5B	
Торс	ology List		<ul> <li>Port Status</li> </ul>	Port Status		
	SN \$	Status ≑	VLAN Info	Port Status		
	MACCWLD789205GC	Online	Port			Panel View
	H1LA0U100362A	Online	Route Info		17 19 21 23 17 19 21 23	
	G1NW31N000172	Online	RLDP More	2 4 6 8 10 12 14 16	18         20         22         24         18         20         22         24	25 26 27
		Offline	-			
	1234942570021	Online		VLAN		Edit @
	MACC522376524	Online				
2	1 → 10/page			VLAN1 VLAN33 VLAN88		
	10/page			Interface IP	IP Range	Remark
				Gi2,Gi4,Gi6,Gi17- 24,Te25-28,Ag1-4,Ag8 11.1.1.89		
				1 3 5 7 9 11 13 15	17 19 21 23 17 19 21 23	

• Select the offline device and click **Delete Offline Devices** to remove the device from the list and the topology.

Тор	ology List				IP/MAC	C/hostname/SN/S Q	Batch Upgrade
	SN \$	Status ≑	Hostname 🌲	MAC \$	IP ≑	Software Ver	Model 🌲
	MACCWLD789205GC	Online	ruijie 🖉	78:11:22:33:44:55	192.168.110.226		RG-ES205C-P
Local	H1LA0U100362A	Online	Ruijie.abc [Master] 🖉	00:74:9C:87:6D:85	192.168.110.1 🌊		EG205G
	G1NW31N000172	Online	Ruijie 🖉	00:D3:F8:15:08:5B	11.1.1.89 🖉		NBS5200- 24SFP/8GT4XS
	G1QH2LV00090C	Offline	Ruijie	C4:70:AB:A8:69:17	192.168.110.102	Sector State	RAP2260(G)
	1234942570021	Online	RAP2200e 🖉	00:D0:F8:15:08:48	192.168.110.152 🖉		RAP2200(E)
	MACC522376524	Online	Ruijie 🖉	00:10:F8:75:33:72	192.168.110.200 🖉		EAP602

# 2.4 Configuring Network Planning

The **Overview** page displays the configuration of **Network Planning** at the bottom left corner, including **Wi-Fi VLAN** and **Wired VLAN**.

Ruíjie Rcycc	Network   Currently in Network	twork mode.	Navigation Q English ~ C	CRemote O&M ♠ Network	
Q Navigation	Status         Devices         Clients           Online         10 / 2 >         0 >	Topology List			A devices not in SON is discovered.Manage
Overview					
중 Network 🗸	Alert Center All (2)				
Devices	The network contains different types o A device (H1QH9QY007751,12345678 >				
⑧ Clients Management	The uplink link cannot be configured > The uplink port of device G1PD3AB70 >				Overturn
📲 System 🗸			<b>2</b>		Restore
ar system	Common Functions				Refresh
	WIO WIO will help optimize Disabled		WAN		
	RLDP     OHCP     Batch Config     Snooping		Not in SON		
		្		UNKNOWN	UNIDIOWN
	Network Planning manage		(gent 0) (G23)	WAN	
	WI-FI VLAN (1): Add	AP Group	Not in SON         IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	FP	Not in SON
	@Ruijie-s0830 VLAN1		5NE1254567890123 5NE01PD3A870777	16 SN:MACC202605233	SNEMACC/RESECCOTF
	Wired VLAN (3): Add				
	VLAN0001         VLAN0002           VLAN1         VLAN2				
	VLAN0003 VLAN3	Updated on:2022-12-12 10:19:51			4
«Collapse					

- Click manage to go to the Network Planning page for configuration (Network > Network Planning). You can add or edit the Network Planning configuration for the live network.
- Click Add to configure Wi-Fi VLAN or Wired VLAN for the live network.
- Click the SSID to edit the Wi-Fi configuration. For details, see Chapter 3 Wi-Fi Network Settings.

Online 10 / 2 > 0 >		
		×
Alert Center All (2)	* SSID @Ruiiie-s0830	
The network contains different types o A device (H1QH9QY007751,12345678 >	* SSID @Ruijie-s0830	
The uplink link cannot be configured > The uplink port of device G1PD3AB70 >	Band • 2.4G + 5G 2.4G 5G	
• • •	Security Open ~	
Common Functions	Expand	
WIO WIO will help optimize Disabled	· · · · · · · · · · · · · · · · · · ·	
RLDP     DHCP     Batch Config     Snooping	Cancel	ОК
		UNKNOWN
Network Planning manage	(wan) 7/7 (port)	Gi23
Wi-Fi VLAN (1): Add	Not in SON A5 Group RG-5218GC-F	NB55100-24GT45FP
@Ruijie-s0830 VLAN1	#P Group SN/1234567890123	SN:G1PD3AB707716

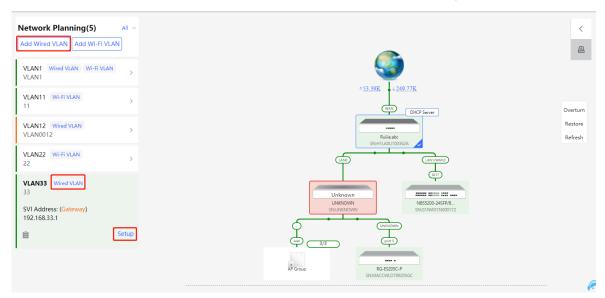
### 2.4.1 Configuring Wired VLAN

- (1) Go to the **Wired VLAN** page for configuration.
- Method 1: Click Add beside Wired VLAN in the Network Planning area on the Overview page to add the

wired VLANs.

Configure Network Planning (Add Wired VI AN

Method 2: Click manage in the Network Planning area on the Overview page to go to the Network Planning page for configuration (Network > Network Planning). Click Add Wired VLAN to add the wired VLANs to the live network or select the available wired VLANs. Click Setup to configure the wired VLANs.



(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.

configure rectron in hanning, rad trined to int		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
1 Configure VLAN Parameters	2 Configure Wired Access	3 Confirm Config Delivery
Description:		
* VLAN ID:	33	
Address Pool Server	• Gateway	
Gateway/Mask:	192.168.33.1 / 255.255.255.0	
DHCP Pool:		
IP 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.

<	gure VLAN Parameters Configure Wired VLAN >
UNKNOWN VUKNO VUKNO VUKNO VUKNO VUKNO VUKNO VUKNO VUKNO VUKNO VUKNO VUKNO VUKNO VUKNO VUKNO VU	8

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

Configure Network Planning/Add W	ired VLAN			×
1 Configure VLAN	Parameters	2 Configure Wired Access	3 Confirm Config Delivery	
WAR EG210 SN:123456	DHCP Server	device(s). The following configuration w Add VLAI DHCP Po	IP range 192.168.33.1~192.168.33.254, configuration will be del vill be delivered: NN 33.IP: 192.168.33.1 Subnet Mask: 255.255.255.0 pol. Start: 192.168.33.1 End IP Address:192.168.33.254 2.168.33.1 Lease Time(Min)480	livered to
		Previous Save		

# 2.4.2 Configuring Wi-Fi VLAN

- (1) Go to the **Wired VLAN** page for configuration.
- Method 1: Click Add beside Wi-Fi VLAN in the Network Planning area on the Overview page to add the Wi-Fi VLANs.
- Method 2: Click manage in the Network Planning area on the Overview page to go to the Network Planning page for configuration (Network > Network Planning). Click Add Wi-Fi VLAN to add the Wi-Fi VLANs to the live network or select the available Wi-Fi VLANs. Click Setup to configure the Wi-Fi VLANs.

Network Planning(3) All ~	<
Add Wired VLAN Add Wi-Fi VLAN	
VLAN1 Wi-Fi VLAN >	Overturn Restore Refresh
VLAN10 >	+0.00 +0.00 (WN) DHCP Server
VLAN12 Wi-Fi VLAN VLAN12	EGIO5GW-E SK-NACK16277F22
SVI Address: (Gateway) 192.168.12.1	
DHCP Pool (Enable) 192.168.12.1/255.255.255.0 IP Count: 254 Lease Time(Min): 480	
È Setup	
	Not in SON         Not in SON           RAP2260E         R6           SN/GTQH6W0X000610         SN/GTQP94K016658
	<del>≈ 12345678</del>

(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
The configuration will take effect after being delivered to AP.	
* SSID	
Band <b>O</b> 2.4G + 5G O 2.4G O 5G	
Security Open ~	
Collapse	
Wireless Schedule         All Time	
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 Next faster speed. )	

(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

1 Configure Wireless Access	2 Configure VLAN F	Parameters	3 Confirm Config Delivery
Description:			
* VLAN ID:	13		
topo.addressPool	• Gateway		
Gateway/Mask:	192.168.13.1	/ 255.255.255.0	
DHCP Pool:			
IP Range:	192.168.13.1	- 192.168.13.254	
	Previous	Next	

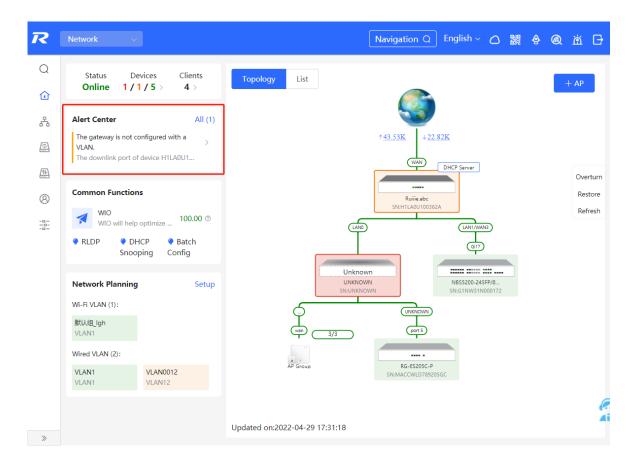
×

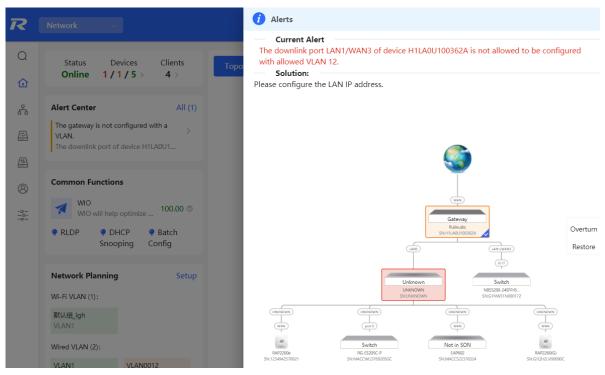
(3) Please confirm the delivered configurations and click **Save**. The configurations will take effect after a few minutes.

Configure Network Planning/Add Wi-Fi VLAN		×
1 Configure Wireless Access	2 Configure VLAN Parameters	3 Confirm Config Delivery
Overturn Restore	To configure (VLAN13) with IP range 192.168.13. device(s). The following configuration will be delivered:	1~192.168.13.254, configuration will be delivered to
	Add VLAN 13.IP 192.168.13.1 Subnet Max EG105GW-E MACCR16277F22	
Not in SON R422000 Skt6 (c)HeWX000610		
	Previous Save	· · · · · · · · · · · · · · · · · · ·

# 2.5 Troubleshooting Fault Alerts

The **Overview** page displays the fault alerts and handling suggestions if faults occur in the network. Click the fault alert in **Alert Center** to view the faulty device, fault details and handling suggestions, and troubleshoot device faults by referring to the handling suggestions.





# **3** 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>Configuring AP Groups</u>.

# 3.1 Configuring AP Groups

### 3.1.1 Overview

After the self-organizing network is enabled, the device can act as the master 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.

### 3.1.2 Procedures

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: In Network mode, choose Devices > AP

For other RAP models, choose **WLAN > APs** 

(1) View the information of all APs in the current network, including the basic information, RF information and models. You can click **SN** to configure the device.

All <b>(1)</b>	Gateway (0)	AP (1)	Switch <b>(0)</b>	AC (0)	Router <b>(0)</b>						
	<b>Device List</b> A devices not in SON i	is discovered.	Manage								
Devi	ice List 🕃 Group:	All Groups	Expand	Change Group	Basic Info	RF Information	Model				
						IP/N	IAC/hostname/S	sn/s Q	🗇 Delete Off	line Devices	Batch Upgrade
	SN 🌩	Status 💠	Hostname	÷	MAC \$	IP 🔶	Clients ≑	Device (		Relay Informatio ≑	n
Local	G1QH6WX000610	Online	Ruijie [Maste	r] 🖉 EC:E	39:70:23:A4:BF	172.26.1.32 🖉	0	defaultNet	work/默认	Wired View Details	
<	1 > 10/pag	ie 🗸									Total 1

(1) Click **Expand** to view all groups on the left part of the **Device List** page. Click + to create a new group.

Up to 8 groups can be added. You can click *to* edit the group name and click *to* delete the group. The default group cannot be deleted and its name cannot be edited.

Devi	<b>ce List </b> ີ Group:	All Groups	Expand	Change	Group
	SN 🔶	Status ≑	Hostnar	me 🌲	MAC
Lacal	G1QH6WX000610	Online	Ruijie [M	aster] 🖉	EC:B9:70:
Devi	<b>ce List </b> ۞ Group:	All Groups	Collapse		
Search	by Group		sn \$		
✓ All G Defat	Groups + ult 2 🖻	uta G1	QH6WX0006	1	

(2) 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.

Search by Group       Image: Clients + Client	Device List	Group: All Group	ps Collapse C	Change Group	Basic Info RF I	nformation Model	IP/MAC/hostna	me/SN/S Q	🖻 Delete Offline Dev	ices Batch Upgrade
Default 🛛 🔟 G10H6WX000610 Online Ruijie (Master) 化 EC:89:70:23:A4:8F 172:26:1.32 化 0 test/取込组		P V	SN 🜩	Status 💠	Hostname 🌲	MAC ≑	IP 🔶	Clients ≑	Device Group	·
		2 🖬 🖉	G1QH6WX000610	Online	Ruijie [Master] 🖉	EC:B9:70:23:A4:BF	172.26.1.32 🖉	0	test/默认组	Wired View Details

Change Group	)	×
Select Group	Select	^
	Default test	el
		91

# 3.2 Configuring SSID and Wi-Fi Password

- (1) Go to the page for configuration.
- Method 1: Choose A Network ( TWLAN) > Wi-Fi > Wi-Fi Settings. Select the target Wi-Fi.
- Method 2: Choose Retwork ( WLAN) > Wi-Fi > Wi-Fi List. Select the target Wi-Fi in the list and click Edit in the action column.
- (1) Click the target Wi-Fi network, change the SSID and Wi-Fi password of the Wi-Fi network, and click Save.

#### A 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.

Wi-Fi Settings Device G	roup: Default $\lor$	
Up to 8 SSIDs can be added.		
Default @Ruijie-s0830 Default VLAN Band:2.4G + 5G	+ Add Guest Wi-Fi	+ Add Wi-Fi
* SSID @Ruiji	ie-s0830	
Band 🧿 2.4G	+ 5G 2.4G 5G	
Security Open	~	
	Expand	
	Save	

# 3.3 Hiding the SSID

### 3.3.1 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.

# 3.3.2 Configuration Steps

- (1) Go to the page for configuration.
- Method 1: Choose <sup>1</sup> Network ( WLAN) > Wi-Fi > Wi-Fi Settings. Select the target Wi-Fi.
- Method 2: Choose Retwork ( WLAN) > Wi-Fi > Wi-Fi List. Select the target Wi-Fi in the list and click Edit in the action column.
- (1) Click Expand, turn on Hide SSID in the expanded settings and click Save.

#### 🛕 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.

Wi-Fi Settings Device Group: Default V					
Up to 8 SSIDs can be	added.				
Default @Ruijie-s0830 Default VLAN Band:2.4G + 50		+ Add Guest Wi-Fi	+ Add Wi-Fi		
* SSID	@Ruijie-s08	330			
Band (	<b>2</b> .4G + 5G	○ 2.4G ○ 5G			
Security	Open	~			
	C	ollapse			
Wireless Schedule	All Time	~			
VLAN	The same V	LAN as AP $\sim$			
Hide SSID	(The S	SID is hidden and must be	manually entered.)		

# 3.4 Checking Wireless Clients

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-RAP6262 models:

If the self-organizing network is disabled, choose	<u> </u>	WLAN > Clients
--	----------	----------------

If the self-organizing network is enabled, in **Network** mode, choose Olients > **Online Clients** > **Wireless** For other RAP models:

### Choose **WLAN** > Clients

Check information about all wireless clients connected to the Wi-Fi network. Click **Add to Blacklist** to disconnect a client and ban the client from accessing the Wi-Fi network.

Wireles	s Client L	ist							C Refresh	Advanced Search
Userna me	MAC	IP	SN	Duratio n	RSSI	Rate	Ban	d SSID	Channel	Action
NULL	72 b8: 52 40	192.168. 110.194	G1QH6 W	2022- 04-01 09:40:36	-66	24M	5G	@Ruijie s1234	- 64	Add to Blacklist
Onlin	Online Clients									
Online (	Clients							Search by IP	/MAC/Usernam	Refresh
Us	ername/Typ	e	Access Lo	cation		IP/MAC		Currer	it Rate	Wi-Fi
	হু 2.4G		G1QH6WX	000610	62	172.26.1.73 2:cf:2f:84:bd:dt	0	Up:0.0 Down:	0bps 0.00bps	Channel:13 RSCP:-87 Duration:7 minutes 55 seconds Negotiation Rate:1M

### Table 3-1 Description of Wireless Client Information

Item	Description	
Username	Name of a client	
MAC	MAC address of the client	
IP	IPv4 address of the client	
SN	SN of the device associated with the client	
Duration	Time when the client connects to the Wi-Fi network	
RSSI	RSSI of the Wi-Fi network associated with the client	
Rate/Negotiation Rate	Association rate of the client and AP	
Band	Band type of the Wi-Fi network, to which the client connects	
SSID	Name of the Wi-Fi network associated with the client	
Channel	Channel of the Wi-Fi network associated with the client	
Current Rate	Uplink and downlink data rate.	

# 3.5 Configuring Wi-Fi Band

- (1) Go to the page for configuration.
- Method 1: Choose The Network ( WLAN) > Wi-Fi > Wi-Fi Settings. Select the target Wi-Fi.
- Method 2: Choose K Network ( WLAN) > Wi-Fi > Wi-Fi List. Select the target Wi-Fi in the list and click Edit in the action column.
- (1) 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.

Wi-Fi Settings Device Group: Default ~	
Up to 8 SSIDs can be added.	
Default @Ruijie-s0830 Default VLAN + Add Guest Wi Band:2.4G + 5G	-Fi + Add Wi-Fi
* SSID @Ruijie-s0830	
Band • 2.4G + 5G • 2.4G •	5G
Security Open	~
Save	

# 3.6 Configuring Band Steering

#### 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 A Network ( WLAN) > Wi-Fi > Wi-Fi Settings. Select the target Wi-Fi.
- Method 2: Choose Network ( WLAN) > Wi-Fi > Wi-Fi List. Select the target Wi-Fi in the list and click Edit in the action column.
- Click Expand, turn on Band Steering in the expanded settings, and click Save. After the function is enabled, the client supporting 5 GHz selects the 5G Wi-Fi network preferentially.

Default @Ruijie-s08 Default VLA Band:2.4G +	N	+ Add Guest Wi-Fi	+ Add Wi-Fi
* SSID	@Ruijie-s	50830	
Band	• 2.4G + 5	5G 2.4G 5G	
Security	Open	~	~
		Collapse	
Wireless Schedule	All Time	~	
VLAN	The same	• VLAN as AP	/
Hide SSID	(The	e SSID is hidden and must be	e manually entered.)
Client Isolation	Prev	vent wireless clients of this V	<i>N</i> i-Fi from communicating with one another
Band Steering	(The	e 5G-supported client will ac	ccess 5G radio preferentially.)

# 3.7 Configuring Wi-Fi 6

#### 🛕 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 
   Arrow Network (
   WLAN) > Wi-Fi > Wi-Fi Settings. Select the target Wi-Fi.
- Method 2: Choose Retwork ( WLAN) > Wi-Fi > Wi-Fi List. Select the target Wi-Fi in the list and click Edit in the action column.

(1) Click **Expand**, turn on **Wi-Fi6** in the expanded settings, and click **Save**. After this function is enabled, wireless clients can enjoy faster Internet access service.

		Collapse
Wireless Schedule	All T	ime v
VLAN	The	same VLAN as AP
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.)
Wi-Fi6		(802.11ax high-speed wireless connectivity.) ⑦
	Do you	want to edit RF parameters? Navigate to Radio Frequency for configuration.
		Save

# 3.8 Configuring Layer-3 Roaming

- (1) Go to the page for configuration.
- Method 1: Choose A Network ( WLAN) > Wi-Fi > Wi-Fi Settings. Select the target Wi-Fi.
- Method 2: Choose Retwork ( WLAN) > Wi-Fi > Wi-Fi List. Select the target Wi-Fi in the list and click Edit in the action column.
- (1) Click **Expand**, turn on **Layer 3 Roaming** in the expanded settings and click **Save**. The client will keep the IP address unchanged in this Wi-Fi network, improving roaming experience across VLANs.

	Collapse
Wireless 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.)
XPress	(The client will experience faster speed.)
Layer 3 Roaming	(The client will keep the IP address unchanged on the Wi-Fi network.)
Wi-Fi6	(802.11ax high-speed wireless connectivity.) ⑦
	Do you want to edit RF parameters? Navigate to Radio Frequency for configuration.
	Save

# 3.9 Configuring AP Isolation

- (1) Go to the page for configuration.
- Method 1: Choose A Network ( TWLAN) > Wi-Fi > Wi-Fi Settings. Select the target Wi-Fi.
- Method 2: Choose Network ( WLAN) > Wi-Fi > Wi-Fi List. Select the target Wi-Fi in the list and click Edit in the action column.
- (1) Click **Expand**, 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.

Default @Ruijie-s08 Default VLAI Band:2.4G + 5	+ Add Guest Wi-F	i	+ Add Wi-Fi
* SSID	@Ruijie-s0830		
Band	• 2.4G + 5G	G	
Security	Open	~	
	Collapse		
Wireless Schedule	All Time	~	
VLAN	The same VLAN as AP	~	
Hide SSID	(The SSID is hidden and mu	st be i	manually entered.)
Client Isolation	Prevent wireless clients of t	nis Wi	-Fi from communicating with one ar

# 3.10 Adding a Wi-Fi Network

- (1) Go to the page for configuration.
- Method 1: Choose Network ( WLAN) > Wi-Fi > Wi-Fi Settings.
- Method 2: Choose Retwork ( WLAN) > Wi-Fi > Wi-Fi List.
- (1) Click Add, enter the SSID and Wi-Fi password and click OK to add a Wi-Fi network. Click Expand to configure more Wi-Fi features in the expanded settings. After the Wi-Fi network is added successfully, it will be displayed in the list. The client will be able to scan the new Wi-Fi network.

				×
* SSID	homewifi			
Band	• 2.4G + 5G	) 2.4G	) 5G	
Security	WPA_WPA2-F	PSK	~	
* Wi-Fi Password	•••••		> <sub>775</sub> 4	
	Exp	and		
			Cancel	ОК

# 3.11 Configuring a Guest Wi-Fi

# 3.11.1 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.

### 3.11.2 Configuration Steps

Choose Retwork ( The Wi-Fi > Wi-Fi Settings.

Click **Add Guest Wi-Fi** to configure the SSID and password of the Guest Wi-Fi. Click **Expand** to configure the effective time period and other Wi-Fi features in the expanded settings. Click **Save**, and the guest Wi-Fi network will be created. Guests can access the guest Wi-Fi network by entering the SSID and Wi-Fi password.

Wi-Fi Settings Device Gr	oup: Default 🗸	
Up to <b>8</b> SSIDs can be added.		
Default @Ruijie-s0830 Default VLAN Band:2.4G + 5G	+ Add Guest Wi-Fi	+ Add Wi-Fi

		×
* SSID	@Ruijie-guest-0830	
Band	• 2.4G + 5G 2.4G 50	Ĵ
Security	WPA_WPA2-PSK	$\sim$
* Wi-Fi Password	•••••••	*
	Expand	
	Ca	ancel OK

# 3.12 Configuring Wireless Rate Limiting

#### A Caution

This function is supported by only RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2260, and RG-RAP6262.

### 3.12.1 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.

- 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.

# 3.12.2 Configuration Steps

1. Configuring Client-based Rate Limiting

Choose Retwork ( WLAN) > LimitSpeed > Client-based Rate Limiting.

- (1) Enable Wireless Rate Limiting.
- (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-based Rate Limiting	Wi-Fi-based Rate Limiting	AP-based Rate Limiting	Packet-based Rate Limiting		
<i>Client-based Rate</i> The rate limiting mo	Limiting de based on wireless clients can limit	or provide the bandwidth for s	pecific clients.		
Client-based Rate	Limiting				+ Add 🗇 Delete Selected
Up to 512 entries can b	e added.				
Client MAC	U	plink Rate Limit	Downlink Rate Limit	Remarks	Action
			No Data		
< 1 > 10/pa	age v				Total 0
Add			×		
* Client MAC	Example: 00:11:22:33:4	14:55			
Uplink Rate	No Limit by Default.	Kbps 🗸			
Limit	Current: Kbps. Range: 1	-1700000 Kbps			
Downlink Rate	No Limit by Default.	Kbps 🗸			
Limit	Current: Kbps. Range: 1	1-1700000 Kbps			
Remarks					
		Cancel	ж		

#### 2. Configuring SSID-based Rate Limiting

Choose Ketwork ( TWLAN) > LimitSpeed > SSID-based Rate Limiting.

- (3) Enable Wireless Rate Limiting.
- (4) 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 🚺				
Client-based Rate Limiting	SID-based Rate Limiting AP-based	ed Rate Limiting	Packet-based Rate Limiting	
Users indicates that all clien		limit in average.	ate Limit per User indicates that all clients connected to th	e SSID use the same rate limit. Rate Limit All
SSID-based Rate Limitin	ng Device Group: Default V		1	re you sure you want to add a Wi-Fi? Click to g
SSID	Uplink	Rate Limit	Downlink Rate Limit	Action
333	Rate Limit Al	Users <b>1111K</b> bps	No Limit	Edit Disable
111	Ν	o Limit	No Limit	Edit Disable
wbctest	Ν	o Limit	No Limit	Edit Disable
@Ruijie-guest-6D8	5 Rate Limit A	ll Users <b>111K</b> bps	Rate Limit Per User <b>2M</b> bps	Edit Disable
Edit			×	
Uplink Rate Limit	• Rate Limit Per User	Rate Limit Al	ll Users ⊘	
Rate Limit	No Limit by Default.	Kbps 🗸		
	Current: Kbps. Range: 1-1	700000 Kbps		
Downlink Rate Limit	• Rate Limit Per User	🔘 Rate Limit Al	ll Users	
Rate Limit	No Limit by Default.	Kbps 🗸		
	Current: Kbps. Range: 1-1	700000 Kbps		
		Cancel	ОК	

### 3. Configuring AP-based Rate Limiting

Choose Retwork ( WLAN) > LimitSpeed > 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**.

#### Web-based Configuration Guide

Wireless Rate Limiting			
Client-based Rate Limiting	Wi-Fi-based Rate Limiting	AP-based Rate Limiting	Packet-based Rate Limiting
	-		ed to the network use the preset rate limiting value. ate limit per user.
AP-based Rate Lin	niting		
Uplink Rate Limit	O No Limit O Rate Limit Per Us	<ul> <li>Wechat texts, voice me</li> </ul>	essages and webpage services: 1 Mbps to 2 Mbps,
		Real-time video calls     Ultra HD/4K/Blue-ray	and HD videos: 2 Mbps to 4 Mbps, videos and live videos: 5 Mbps to 10 Mbps,
	Kbps $\sim$	· Other: You are not ad	vised to set the value to 20 Mbps. It may affect the Internet experience of other users in the internal network.
	Current: Kbps. Range: 1-1700000 Kl	bps	
Downlink Rate Limit	O No Limit • Rate Limit Per Us	ser	
	Kbps $\sim$		
	Current: Kbps. Range: 1-1700000 Kl	bps	
	ОК		

#### 4. Configuring Packet-based Rate Limiting

Choose Retwork ( WLAN) > LimitSpeed > 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	D		
Client-based Rate Limiting	Wi-Fi-based Rate Limiting	AP-based Rate Limiting	Packet-based Rate Limiting
			If the internet access is still slow and unstable when no client needs large amounts of traffic, you are advised to set the
Packet-based Rate	Limiting		
Broadcast Rate Limiting	🔿 Disable 🔷 Limit All 📀	Limit Part	
	ARP Packet DHCP Packe	t	
Multicast Rate Limiting	🗆 Disable 🛛 Limit All 💽	Limit Part	
	MDNS Packet SSDP Pac	ket	
* Rate Limit	Кbр	s ∨	
(	Current: 0 Kbps. Range: 1-170000	10 Kbps	
	Save		

# 3.13 Configuring Wi-Fi Blacklist or Whitelist

#### 3.13.1 Overview

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

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

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

#### A Caution

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

# 3.13.2 Configuration Steps

#### 1. Configuring a Global Blacklist/Whitelist

# Choose Olients ( WLAN) > Blacklist/Whitelist > Global Blacklist/Whitelist.

Select the blacklist or whitelist mode and click **Add** to configure a blacklist or whitelist client. In the **Add** window, enter the MAC address and remark of the target client 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 blacklist will be forced offline and not allowed to access the Wi-Fi network. The global blacklist and whitelist settings take effect on all Wi-Fi networks of the access point.

	As except blacklisted ST	TAs are allowed to access Wi-Fi.	<ul> <li>Only the whitelisted STAs</li> </ul>	are allowed to access W	'i-Fi.
Blocked	d WLAN Clients			+ Add	Delete Selecte
Up to 25	56 members can be add	led.			
	MAG	c	Remark	A	ction
	00:E0:4C:3	6:0B:EA	forbidden	Edit	Delete
	00:11:22	OUI		Edit	Delete
	Match Type	• Full O Prefix (O	UI)		
			4455		
	* MAC	Example: 00:11:22:33:	:44:55		
	* MAC Remark	Example: 00:11:22:33:			

#### 2. Configuring an SSID-based Blacklist/Whitelist

Choose Olients ( WLAN) > Blacklist/Whitelist > SSID-Based Blacklist/Whitelist.

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

Global Blacklist/Whitelist	SSID-Based Blacklist/Whitelist		
<i>i</i> Note: OUI matching Rule: 1. In the Black	used to allow or reject a client's request to o rule and SSID-based blacklist/whitelist are su dist mode, the clients in the blacklist are not elist mode, only the clients in the whitelist ar	<pre>upported by only RAP Net and P32 (and later v allowed to connect to the Wi-Fi network.</pre>	rersions).
Device Group: test	Vhitelist	disted STAs are allowed to access Wi-Fi.	
test	Blocked WLAN Cli	ents	+ Add Delete Selected
	Up to <b>256</b> members ca	n be added.	
	MA	C Remark	Action
		No Data	

# 3.14 Optimizing Wi-Fi Network

#### 3.14.1 Overview

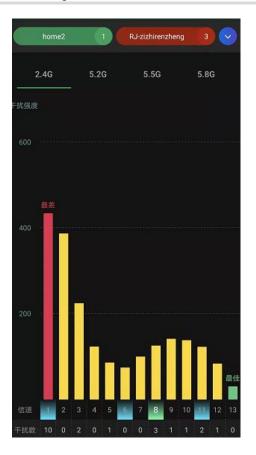
The device detects the surrounding wireless environment and selects the appropriate configuration upon poweron. However, network stalling caused by wireless environment changes cannot be avoided. You can optimize the network with one single click, analyze the wireless environment around the access point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

#### 🛕 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.

### 3.14.2 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.



# 3.14.3 Optimizing the Radio Channel

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-RAP6262 models:

- Configure the master device. Choose A Network ( Twice WLAN) > Radio Frequency
- Configure the slave device. Choose Obvices > Select the target device in the device list and click SN > Radio Frequency

For other RAP models:

- Configure the master device. Choose **WLAN** > Radio Frequency
- Configure the slave device. Choose WLAN > APs > Select the target device in the device list and click
   Manage > WLAN > Radio Frequency

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.

i Tip: Changing co	nfiguration requires a reboot and clients v	vill be reconnected.		
Radio Frequenc	y Device Group: Default ~			
Country/Region	China (CN)	]		
2.4G Channel Width	Auto ~	5G Channel Width	Auto	
Multicast Rate (Mbps)	Auto $\lor$	Multicast Rate (Mbps)	Auto	
0		0	Auto	
Client Count Limit	64	Client Count Limit	36 (5.18GHz)	
Disconnection	0	Disconnection	40 (5.2GHz) 44 (5.22GHz)	
D Threshold	isable -85dBm -65d	3m Threshold	0i 48 (5.24GHz)	۶m
0		0	52 (5.26GHz)	
— The settings are v	valid for only current device		56 (5.28GHz) 60 (5.3GHz)	_
2.4G Channel	Auto ~	5G Channel	Auto	
	O Auto Lower Low Medium Hig	Transmit Power	O Auto Lower Low Medium Hi	igh
Roaming ⊘	O Low 40% 80% Hig	h Roaming 🗇	O 40% 80% Hi	igh

# 3.14.4 Optimizing the Channel Width

Choose A Network ( TWLAN) > Radio Frequency.

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 and 40 MHz and 80 MHz and 160 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.

<i>i</i> Tip: Changing co	nfiguration requires a reboot and clients will l	be reconnected.	
Radio Frequenc	y Device Group: Default >		
2.4G Channel Width	Auto ~	5G Channel Width	Auto ^
Multicast Rate (Mbps)	Auto ~	Multicast Rate (Mbps)	Auto 20MHz 40MHz
Client Count Limit	64	Client Count Limit	80MHz 160MHz
Disconnection D Threshold	O isable -85dBm -65dBm	Disconnection Threshold	Disable -85dBm -65dBm
The settings are settings.	valid for only current device	0	
2.4G Channel	Auto	5G Channel	Auto
	O Auto Lower Low Medium High	Transmit Power	O Auto Lower Low Medium High

### 3.14.5 Optimizing the Transmit Power

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-RAP6262 models:

- Configure the master device. Choose A Network ( The WLAN) > Radio Frequency
- Configure the slave device. Choose Operator Devices > Select the target device in the device list and click SN > Radio Frequency

For other RAP models:

- Configure the master device. Choose 🛜 WLAN > Radio Frequency
- Configure the slave device. Choose WLAN > APs > Select the target device in the device list and click
   Manage > WLAN > Radio Frequency

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**.

<i>i</i> Tip: Changing cont	figuration requires a reboot and cli	ents will be reconn	rected.		
Radio Frequency	Device Group: Default				
Country/Region	China (CN)	~			
2.4G Channel Width	Auto	~	5G Channel Width	Auto	^
Multicast Rate (Mbps)	Auto	~	Multicast Rate (Mbps)	Auto	
0			Ø	20MHz 40MHz	
Client Count Limit	64		Client Count Limit	80MHz	
Disconnection (	C		Disconnection	160MHz	
Dis Threshold	able -85dBm	-65dBm	Threshold	isable -85dBm	-65dBm
0			0		
	lid for only current device				
2.4G Channel	Auto	~	5G Channel	Auto	~
Transmit Power ( Au	O s s s uto Lower Low Medium		Transmit Power	-	edium High
Roaming ગ 🌔	-	High		O Low 40%	80% High
-	C	-65dBm	_	O Disable -85dBm	-65dBm

# 3.14.6 Configuring the Multicast Rate

### 🛕 Caution

This function is supported by only RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP6260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2260, and RG-RAP6262.

# Choose Retwork ( Tweat WLAN) > Radio Frequency.

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**.

i Tip: Changing co	nfiguration requires a reboot and clients w	ill be reconnected.		
Radio Frequenc	y Device Group: Default V			
Country/Region	China (CN) ~			
2.4G Channel Width	Auto ~	56 Channel Width	Auto	~
Multicast Rate (Mbps)	Auto ~	Multicast Rate (Mbps)	Auto	^
0		0	Auto	
Client Count Limit	64	Client Count Limit	OFDM 6	
			OFDM 9	
Disconnection	0	Disconnection	OFDM 12	
D Threshold	isable -85dBm -65dE	3m Threshold	OFDM 18	3m
0		0	OFDM 24	
			OFDM 36	
The settings are	alid for only current device		OFDM 48	
2.4G Channel	Auto ~	5G Channel	Auto	~
Transmit Power	0	Transmit Power	0	
	Auto Lower Low Medium Hig	h	Auto Lower	Low Medium High

### 3.14.7 Configuring the Client Limit

Choose Retwork ( The WLAN) > Radio Frequency.

If the access point is associated with too many clients, it will have a lower performance, affecting user experience. After you configure the threshold, new clients over the threshold will not be allowed to access the Wi-Fi network. You can lower the threshold if there is requirement for bandwidth per client. You are advised to keep the default settings unless there are special cases. After adjusting the configuration, click **Save**.

i Tip: Changing con	figuration requires a reboot and clie	nts will be reconnected.			
Radio Frequency	Device Group: Default				
Country/Region	China (CN)	~			
2.4G Channel Width	Auto	~	5G Channel Width	Auto	~
Multicast Rate (Mbps)	Auto	~	Multicast Rate (Mbps)	Auto	~
0			0		
Client Count Limit	64		Client Count Limit	512	
Disconnection Disconnection Threshold	O sable -85dBm s	65dBm	Threshold	· ·	-65dBm
0			0		
— The settings are va	alid for only current device				
2.4G Channel	Auto	v	5G Channel	Auto	~
Transmit Power A	O uto Lower Low Medium	High		O Auto Lower Low Medium	High

#### 🚺 Note

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

# 3.14.8 Configuring the Kick-off Threshold

# Choose Retwork ( Twice WLAN) > Radio Frequency.

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**.

i Tip: Changing cor	nfiguration requires a reboot and clients	will be reconnected.	
Radio Frequency	/ Device Group: Default V		
Country/Region	China (CN)		
2.4G Channel Width	Auto	5G Channel Width	Auto
Multicast Rate (Mbps)	Auto ~	Multicast Rate (Mbps)	Auto
0		0	
Client Count Limit	64	Client Count Limit	512
Disconnection Di Threshold	O sable -85dBm -65c	Bm Disconnection Threshold	O isable -85dBm -65dBm
Disconnection Di Threshold	O sable -85dBm -65c		O
Di Threshold ⑦	O -85dBm -65c	Bm D D Threshold	O
Di Threshold ⑦	sable -85dBm -65c	Bm D D Threshold	O isable -85dBm -65dBm

#### 🛕 Caution

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

### 3.14.9 Configuring the Roaming Sensitivity

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-RAP6262 models:

- Configure the master device. Choose Part ( The WLAN) > Radio Frequency
- Configure the slave device. Choose O Devices > Select the target device in the device list and click SN > Radio Frequency

For other RAP models:

- Configure the master device. Choose **WLAN** > Radio Frequency
- Configure the slave device. Choose WLAN > APs > Select the target device in the device list and click
   Manage > WLAN > Radio Frequency

()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 Frequency	Device Group: Default						
Country/Region	China (CN)	~					
2.4G Channel Width	Auto	~	5G Channel Width	Auto			~
Multicast Rate (Mbps)	Auto	~	Multicast Rate (Mbps)	Auto			~
0			0				
Client Count Limit	64		Client Count Limit	512			
Disconnection Disconnection Threshold	•	-65dBm	Disconnection Threshold	O isable	-85dBm		-65dBm
0			0				
— The settings are va	alid for only current device						
2.4G Channel	Auto	~	5G Channel	Auto			~
Transmit Power A	O	High	Transmit Power	-	• • Lower Low	Medium	High
	O .ow 40% 80%	High	-	O Low	40%	80%	High
-	O sable -85dBm	-65dBm		O isable	-85dBm		-65dBm
Response RSSI Dis Threshold	-	-65dBm	Response RSSI D Threshold	O isable	-85dBm		-65dBm

### 3.14.10 Configuring Access Threshold

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260 and RG-RAP6262 models:

- Configure the master device. Choose 6 Network ( WLAN) > Radio Frequency
- Configure the slave device. Choose Over Select the target device in the device list and click SN > Radio Frequency

For other RAP models:

• Configure the master device. Choose **WLAN** > Radio Frequency

Configure the slave device. Choose  $\bigcirc$  WLAN > APs > Select the target device in the device list and click Manage > WLAN > Radio Frequency

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 Frequency	/ Device Group: Default V				
Country/Region	China (CN) ~				
2.4G Channel Width	Auto V 5G Channel Width	Au	to		~
Multicast Rate (Mbps)	Auto V Multicast Rate (Mbps)	Au	to		~
0	0				
Client Count Limit	64 Client Count Limit	512	2		
Disconnection	O Disconnection Isable -85dBm Threshold		-85dBm		-65dBm
Threshold 🖉	o mesnoid 🏈				
— The settings are v	alid for only current device				
2.4G Channel	Auto V 56 Channel	Au	to		~
Transmit Power	O Transmit Power	O Auto	Lower Low	Medium	High
0 -	C Roaming (2) Low 40% 80% High	O Low	40%	80%	High
	O Access Threshold (2) sable -85dBm -65dBm	O Disable	-85dBm		-65dBm
Response RSSI	C Response RSS	$\sim$			

### 3.14.11 Configuring Response RSSI Threshold

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260 and RG-RAP6262 models:

- Configure the master device. Choose A Network ( TWLAN) > Radio Frequency
- Configure the slave device. Choose Over Select the target device in the device list and click SN > Radio Frequency

For the other RAP models:

• Configure the master device. Choose 🛜 WLAN > Radio Frequency

Configure the slave device. Choose	-	WLAN > APs >	Select the	target	device	in the	device	list	and cli	ck
Manage > WLAN > Radio Frequency										

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 Frequency	Device Group: Default		
Country/Region	China (CN)	~	
2.4G Channel Width	Auto	SG Channel Width	Auto
Multicast Rate (Mbps)	Auto	✓ Multicast Rate (Mbps)	Auto
0		0	
Client Count Limit	64	Client Count Limit	512
Disconnection	0	Disconnection	
Threshold	sable -85dBm	-65dBm Threshold	Disable -85dBm -65dBn
0		0	
	alid for only current device	0	
	alid for only current device	⊙ 5G Channel	Auto
— The settings are va	Auto		
The settings are vo 2.4G Channel Transmit Power	Auto	<ul> <li>✓ 5G Channel</li> <li>Transmit Power</li> </ul>	
The settings are va 2.4G Channel Transmit Power A Roaming ③	Auto	<ul> <li>✓ 5G Channel</li> <li>Transmit Power</li> <li>High</li> <li>Roaming ⑦</li> </ul>	O Auto Lower Low Medium High
The settings are va 2.4G Channel Transmit Power A Roaming ©	Auto Outo Lower Low Medium Outo 40% 80%	→ 5G Channel Transmit Power High Roaming ③	Auto Lower Low Medium High O Low 40% 80% High
The settings are vo 2.4G Channel Transmit Power A Roaming © L Access Threshold ©	Auto Outo Lower Low Medium Outo 40% 80%	SG Channel Transmit Power High Roaming ③ High Access Threshold ③	Auto Lower Low Medium High O Low 40% 80% High
The settings are vo 2.4G Channel Transmit Power A Roaming © L Access Threshold ©	Auto Ouuto Lower Low Medium Outo 40% 80% Osable -85dBm	SG Channel Transmit Power High Roaming ③ High Access Threshold ③	Auto Lower Low Medium High O Low 40% 80% High O Disable -85dBm -65dBm

#### 3.14.12 Configuring WIO

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: In Network mode, choose RAP6262 models: In Network >WIO

For the other RAP models: Choose **WLAN** > WIO

Check I have read the notes. And click Network Optimization to optimize the wireless network. 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.

#### 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.

Network Optimization	Optimization Record	Wi-Fi Roaming Optimization (802.11	k/v)		
Ø		Q,	<i>1</i> 9		
Start		Scanning	Optimizi	ng	Finisł
	Description:				
		e the self-organizing network to maximi			n online.
	Notes:	e device supporting Wi-Fi roaming optin	lization (802.11K/V), this featur	e is enabled at the same time.	
	1. During network optin	nization, the APs will switch channels, for recommended you enable network opti	· · ·	he process will last for a while, subje	ect to the
		location is running in the backend, netwo		e try again later.	
		n is not supported by the device without			
	<b>—</b>	not be rolled back once optimization sta	arts.		
	I have read the note	S.			
	Network Optimizatio	n			
1					
Scheduled C	Optimization				
Scheduled	d Optimization				
Optimize t	he network performa	nce at a scheduled time for a be	etter user experience.		
	Enable				
	Day Sun	$\sim$			
	Time 03	> : 00 ~			
		· 00 ·			
		Save			

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

#### A Caution

This function is not supported by RG-RAP1200(F) and RG-RAP2200(F).

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: In Network mode, choose RAP6262 models: In Network models: In Network mode, choose RAP6262 models: In Network models: In Networ

For the other RAP models: Choose **WLAN > WIO > Wi-Fi Roaming Optimization (802.11k/v)**.

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.



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	Optimization Record Wi-Fi Roaming Optimiz	zation (802.11k/v)	
⊘	Q,	59	0
Start	Scanning	Optimizing	Finis
	Description:		
	signal and faster speed during the roaming process		
	To ensure smart roaming effect, the WLAN environ Notes:	ment will be auto scanned when Wi-Fi roaming optimization is first	enabled.
		vill switch channels, forcing the clients to go offline. The process wil	l last for 2 minutes.
	Enable		
Network Optimization	Optimization Record Wi-Fi Roaming Optimiza	ation (802.11k/v)	
⊘ ———		<i>\$</i> ?	
Start	Scanning	Optimizing	Finish
12%	Wi-Fi Roaming Optimization (8 Start: 2022-09-28 19:56:03 Expected Time: 2 minute	802.11k/v)Scanning	
Network Optimization	Optimization Record Wi-Fi Roaming Optimiza	ation (802.11k/v)	
⊘	⊙	⊘	⊘
Start	Scanning	Optimizing	Finish
$\bigcirc$	Optimizing Optimiation finished on 2022-09-28 19:56:40 Time: 37 seconds To ensure smart roaming effect, please Click Here to Disable	o scan the WLAN environment again if the topology changes.	

# 3.15 Configuring Healthy Mode

Choose Retwork ( The 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.

	hy mode. The device will decrease its transmit power to reduce radiation. onfiguration requires a reboot and clients will be reconnected.
Healthy Mode	Device Group: Default V
Enable	
Effective Time	All Time 🗸
	Save

# 3.16 Configuring XPress

- (1) Go to the page for configuration.
- Method 1: Choose A Network ( WLAN) > Wi-Fi > Wi-Fi Settings. Select the target Wi-Fi.
- Method 2: Choose Retwork ( WLAN) > Wi-Fi > Wi-Fi List. Select the target Wi-Fi in the list and click Edit in the action column.
- Click Expand, turn on XPress in the expanded settings and click Save. After XPress is enabled, the gaming traffic will be prioritized, ensuring a more stable gaming experience.

* SSID	@Ruijie-s0830
Band	2.4G + 5G ○ 2.4G ○ 5G
Security	Open ~
	Collapse
Wireless 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. )

# 3.17 Configuring Wireless Schedule

- (1) Go to the page for configuration.
- Method 1: Choose The Network ( WLAN) > Wi-Fi > Wi-Fi Settings. Select the target Wi-Fi.
- Method 2: Choose Network ( WLAN) > Wi-Fi > Wi-Fi List. Select the target Wi-Fi in the list and click Edit in the action column.
- (1) Click **Expand**, select a scheduled time span to turn on Wi-Fi and click **Save**. Clients will be allowed to access the Internet only in the specified time span.

* SSID	@Ruijie-s0830			
Band	<b>9</b> 2.4G + 5G	) 2.4G	○ 5G	
Security	Open		$\sim$	
	Colla	apse		
Wireless Schedule	All Time		^	]
VLAN	All Time			
	Weekdays			
Hide SSID	Weekends			manuall <u>y</u>
Client Isolation	Custom			·Fi from

## 3.18 Enabling Reyee Mesh

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: In Network mode, choose A Network > Reyee Mesh

For the other RAP models: Choose **WLAN > APs > Manage > Advanced > Reyee 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.

After enabling Reyee Mesh, you can set up a Mesh network through Mesh pairing between the devices that support Reyee Mesh.

Enable
Save

# 3.19 Configuring AP Load Balancing

#### 🛕 Caution

This function is supported by only RG-RAP series access points.

#### 3.19.1 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.

#### 3.19.2 Configuring Client Load Balancing

Choose http://www.choose Choose Choos

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

Load Balancing	1				+ Add	Delete Selected
lighter load. Example: Add AP1 a	into a group and enabl and AP2 into a group a P2 is associated with 2	nd select client load ba	n load is unbalanced in t alancing. Set both the clie I balancing. New clients'	ent count thresh	old and difference to 3	. AP1 is associated
Group Na	ame Type		Rule		Members	Action
			No Data			
Add				:	×	
* Group Name						
* Туре	Client Load Bal	ancing		~		
* Rule	client count on t 3, clie group. After a cli 10 tin the AP upon the	en the currently a he AP with the lig ents can associate ent association is nes, the client will next attempt.	3 Clients ssociated client cou htest load reaches only to another AP denied by an AP fo be allowed to assoc	int and in the		
* Members	Enter an AP na	me or SN.		~		

#### Table 3-2 Client load balancing configuration

Parameter	Description
Group Name	Enter the name of the AP load balancing group.
Туре	Select Client Load Balancing.

Cancel

Parameter	Description
	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.
Rule	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 reaches 3, 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.

# 3.19.3 Configuring Traffic Load Balancing

Choose Retwork ( WLAN) > Wi-Fi > 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
Add A lighte Examp with 5	r load. ble: Add AP1 and AP2 int	p and enable load bal o a group and select o iated with 2 clients, tri	ancing. When load is unbalanced in the group, o lient load balancing. Set both the client count tl ggering load balancing. New clients'attempt t	nreshold and difference to 3. AP	1 is associated
	Group Name	Туре	Rule	Members	Action
			No Data		

Add		>
* Group Name		
* Type	Traffic Load Balancing	
* Rule	When the traffic load on an AP reaches 5	
	*100Kbps and the difference between the current traffic and	
	the traffic on the AP with the lightest load reaches	
	5 *100Kbps, clients can associate only to another	
	AP in the group. After a client association is denied by an AP	
	for 10 times, the client will be allowed to associate	
	to the AP upon the next attempt.	
* Members	Enter an AP name or SN.	

Table 3-3	Traffic load	balancing	configuration
-----------	--------------	-----------	---------------

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.

ОК

Cancel

# 3.20 Wireless Authentication

#### 🛕 Caution

This function is supported by only RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2260, and RG-RAP6262.

#### 3.20.1 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 Eweb management system (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 Eweb management system 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.

#### 3.20.2 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 > Authentication > Captive Portal, and select a network that needs to configure wireless authentication.
- (2) Click **Add** to open the portal template configuration page.

# Add Synchronize

(3) Configure basic information of the portal template.

Name	Portal_one-click login					*	
Description							
Login Options	One-click Login	Voucher	Account	SMS	Registration	🕒 🔲 Facebook Account	
	Access Duration (Min)	Custon	n	<b>~</b>			
	Access Times Per Day	Unlimit	ed				~
Show Balance Page							
Post-login URI	https://www.ruijienetworks.com	n					

#### Table 3-4 Basic Information of the Portal Template

Parameter	Description
Name	Indicates the name of a captive portal template.
Description	Indicates the description of a captive portal template.
Login Options	Select <b>One-click Login</b> , which indicates login without the username and password. You can set the access duration and access time per day.
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.

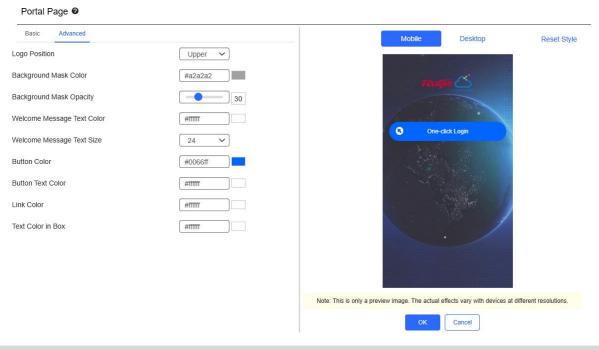
(4) In the **Portal Page** area, click **Basic** to configure basic information for the portal page.

Portal Page 0		
Basic Advance	ed	Mobile Desktop Reset Style
_ogo	Image     No Image	
_ogo Image 🛛	Default Logo Upload	reugio 🖒
Background	Solid Color	
Background Image	Default Image Upload	One-click Login
Languages	English × +	All and a second second
Welcome Mess	age 💿 Text 🔿 Image 🛛	
Text	60 characters remaining	
		. /
Marketing Mess	sage 60 characters remaining	
Terms & Condit	tions	
		Note: This is only a preview image. The actual effects vary with devices at different resolutions.
	1	OK Cancel
	1	
Copyright	60 characters remaining	

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.				
Background	Select the background with the image or the solid color.				
Background Image	When <b>Background</b> is set to <b>Image</b> , upload the background image or select the default image.				
Background Color	When <b>Background</b> is set to <b>Solid Color</b> , configure the background color. The default value is <b>#ffffff</b> .				
Language	<ul> <li>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.</li> <li>Welcome Message: Select the welcome message with the image or text.</li> <li>Marketing message: Enter the marketing message.</li> <li>Terms &amp; Conditions: Enter terms and conditions.</li> <li>Copyright: Enter the copyright.</li> <li>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.</li> <li>One-click Login After One-click Login Is enabled.</li> </ul>				

#### Table 3-5 Basic Information of the Portal Page

(5) In the **Portal Page** area, click **Advanced** to configure advanced information for the portal page.



Parameter	Description	
Logo Position	Select the logo position (Upper, Middle, or Lower).	
Background Mask Color	Select the background mask color. The default value is #a2a2a2.	
Background Mask Opacity	Select the background mask opacity (0-100).	
Welcome Message Text Color	Select the welcome message text color. The default value is #ffffff.	
Welcome Message Text Size	Select the welcome message 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.	

Table 3-6 Advanced Information of the Portal Page

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

#### 2. Enabling One-click Login for an SSID

- Log in to Ruijie Cloud, choose Project > Configuration > Devices > Wireless > SSID, and select a network that needs to configure wireless authentication.
- (2) If the SSID that needs to enable wireless authentication is not created, click 🚩 to open the SSID

configuration page. If the SSID that needs to enable wireless authentication is created, click in the **Action** column. The following content only describes configurations related to wireless authentication. For details about other SSID configuration parameters, see the Ruijie Cloud Cookbook.

SSID							
WLAN ID	SSID	Encryption Mode	Hidden	Forward Mode	Radio	Auth Mode	Action
1	WiFi 60	Open	No	Bridge	1	Auth Disabled	۲ آ

(3) Enable **Auth** (disabled by default) and configure authentication-related parameters. After the configuration, click **OK** to save the configurations.

#### 🚺 Note

When **Encryption Mode** is set to a value other than **WPA2-Enterprise(802.1x)**, **Auth** is available and you can select whether to perform wireless authentication.

Auth 🧲	0			
Mode Capti	ve Portal	~		
Seamless Online @	1 Day	~		
Select or add a new portal.				
Portal_SMS	Portal_account	Portal_voucher	Portal_one-click login	
Ruge	reugre 🛆	reuge 🖄	Ruge 🖄 🏹	
	and the second second			
SMS Login	Account Login	Voucher Login	One-click Login	
+86 Phone Number	Account	Access Code		
Get Code	Password	C Login		
Verification Code	Login			
Login		Z		
•	One-click Login			
		OK Cancel		

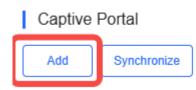
- Mode: Set it to Captive Portal.
- Seamless Online: Determine whether to enable Seamless Online as required, which is enabled by default.
   After Seamless Online is enabled, users do not need to be authenticated when they go online again in the specified period of time.
- Select or add a new portal: Select a portal template with the authentication mode set to One-click Login. If the configured template does not meet the requirements, click or add a new portal to create a portal template.
- (4) Click **Save** for the configuration to take effect.

							Save More -
Wireless Configurat	tion						^
SSID 🖨							
WLAN ID	SSID	Encryption Mode	Hidden	Forward Mode	Radio	Auth Mode	Action
WLAN ID	\$\$ID LJW_22	Encryption Mode Open	Hidden	Forward Mode Bridge	Radio 1,2	Auth Mode Captive Portal	Action

#### 3.20.3 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 > Authentication > Captive Portal, and select a network that needs to configure wireless authentication.
- (2) Click Add to open the portal template configuration page.



(3) Configure basic information of the portal template.

Name	Portal_voucher					*
Description						
Login Options	One-click Login	Voucher	Account	SMS	Registration	beta 🔲 Facebook Account
Show Balance Page 🛛						
Post-login URL 🛛	https://www.ruijienetwo	rks.com				

#### Table 3-7 Basic Information of the Portal Template

Parameter	Description
Name	Indicates the name of a captive portal template.
Description	Indicates the description of a captive portal template.
Login Options	Select <b>Voucher</b> , 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.

#### (4) In the **Portal Page** area, click **Basic** to configure basic information for the portal page.

#### Portal Page @

Basic Advanced		Mobile Desktop Reset S
go	Image O No Image	
go Image 🛛	Default Logo Upload	reugin 🖆
ckground	Image Solid Color	
ckground Image 🛛	Default Image Upload	O Voucher Login
anguages	English × +	Access Code
Welcome Message	e O Text O Image Ø	Login
Text	60 characters remaining	and the second sec
Marketing Messag	e 60 characters remaining	•
Terms & Condition	s	
		Note: This is only a preview image. The actual effects vary with devices at different resolution
		OK Cancel
8	1	
Copyright	60 characters remaining	

#### Table 3-8 Basic Information of the Portal Page

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.			
Background	Select the background with the image or the solid color.			
Background Image	When <b>Background</b> is set to <b>Image</b> , upload the background image or select the default image.			
Background Color	When <b>Background</b> is set to <b>Solid Color</b> , configure the background color. The default value is <b>#ffffff</b> .			
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. Voucher Login: After <b>Voucher Login</b> is enabled, you can customize the names of controls related to voucher authentication. Voucher Login <b>Reset</b> Title © Show 60 characters remaining Voucher Login Voucher Code Placeholder 60 characters remaining Login Switching Button 60 characters remaining Voucher Login			

(5) In the **Portal Page** area, click **Advanced** to configure advanced information for the portal page.

#### Portal Page 0

Basic Advanced		Mobile Desktop Reset Style
Logo Position	Upper 🗸	
Background Mask Color	#a2a2a2	RUME CS
Background Mask Opacity	30	
Welcome Message Text Color	#11111	
Welcome Message Text Size	24 🗸	Voucher Login
Button Color	#0066ff	Access Code
Button Text Color	#fffff	Login
Link Color	#fffff	
Text Color in Box	#11111	. /
		Note: This is only a preview image. The actual effects vary with devices at different resolutions.
		OK Cancel

Parameter	Description
Logo Position	Select the logo position (Upper, Middle, or Lower).
Background Mask Color	Select the background mask color. The default value is #a2a2a2.
Background Mask Opacity	Select the background mask opacity (0-100).
Welcome Message Text Color	Select the welcome message text color. The default value is #ffffff.
Welcome Message Text Size	Select the welcome message 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.

#### Table 3-9 Advanced Information of the Portal Page

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

#### 2. Enabling Voucher Authentication for an SSID

- Log in to Ruijie Cloud, choose Project > Configuration > Devices > Wireless > SSID, and select a network that needs to configure wireless authentication.
- (2) If the SSID that needs to enable wireless authentication is not created, click to open the SSID

configuration page. If the SSID that needs to enable wireless authentication is created, click in the

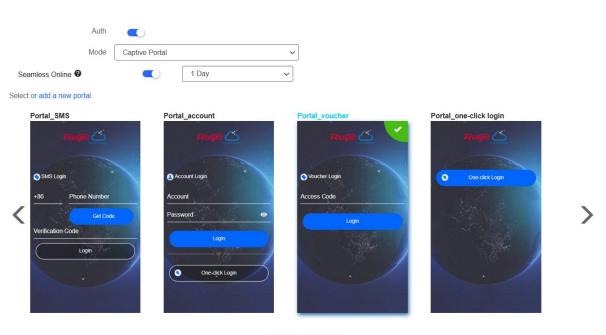
Action column. The following content only describes configurations related to wireless authentication. For details about other SSID configuration parameters, see the Ruijie Cloud Cookbook.

SSID							
WLAN ID	SSID	Encryption Mode	Hidden	Forward Mode	Radio	Auth Mode	Action
1	WiFi_60	Open	No	Bridge	1	Auth Disabled	i.

(3) Enable **Auth** (disabled by default) and configure authentication-related parameters. After the configuration, click **OK** to save the configurations.

- Ci	Note

When **Encryption Mode** is set to a value other than **WPA2-Enterprise(802.1x)**, **Auth** is available and you can select whether to perform wireless authentication.





- Mode: Set it to Captive Portal.
- Seamless Online: Determine whether to enable Seamless Online as required, which is enabled by default. After Seamless Online is enabled, users do not need to be authenticated when they go online again in the specified period of time.
- Select or add a new portal: Select a portal template with the authentication mode set to Voucher. If the configured template does not meet the requirements, click or add a new portal to create a portal template.
- (4) Click **Save** for the configuration to take effect.

							Save More -
Wireless Configuration	on						^
SSID 🔁							
WLAN ID	\$ SID	Encryption Mode	Hidden	Forward Mode	Radio	Auth Mode	Action
WLAN ID	SSID LJW_22	Encryption Mode Open	Hidden	Forward Mode Bridge	Radio 1,2	Auth Mode Captive Portal	Action

#### 3. Adding a Voucher

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

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

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

Add user group		Х
* User group name	test	
	User Group Policy	
Price		
	-	
Concurrent devices	3	~
Period	30Minutes	~
Quota (j)	100 MB	$\vee$
Maximum upload rate	Unlimited	~
Maximum download rate	Unlimited	~
Bind MAC on first use		
		Cancel OK

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 ∨ Advance setting ∨	Custom	
	Cancel	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
	Alphanumeric 0-9, a-z
Voucher length	Alphabetic a-z
	Numeric 0-9
	Cancel OK

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

Voucher length	6 ^	]
	6	
	7	
	8	
	9	

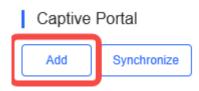
#### (4) Obtain the voucher code from the voucher list.

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

### 3.20.4 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 > Authentication > Captive Portal, and select a network that needs to configure wireless authentication.
- (2) Click  $\boldsymbol{Add}$  to open the portal template configuration page.



(3) Configure basic information of the portal template.

Name	Portal_account					*	
Description							
Login Options	One-click Login	Voucher	Account	SMS	Registration	bota 📃 Facebook Account	ıt
Show Balance Page 🛛							
Post-login URL 🛛	https://www.ruijienetwork	s.com					

#### Table 3-10 Basic Information of the Portal Template

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

(4) In the **Portal Page** area, click **Basic** to configure basic information for the portal page.

#### Portal Page @

Basic Advance	ed	Mobile Desktop Reset Style
go	Image     No Image	
go Image 🛿	Default Logo Upload	Têujje 📥
ckground	Image     Solid Color	
ckground Image 🕻	Default Image Upload	Account Login
anguages	English × +	Account
Welcome Messa	age 🔹 Text 🔷 Image 🛛	Password 📀
Text	60 characters remaining	Login
Marketing Mess	age 60 characters remaining	. /
Terms & Conditi	ions	
		Note: This is only a preview image. The actual effects vary with devices at different resolutions.
		OK Cancel
	1	
	60 characters remaining	

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.						
Background	Select the background with the image or the solid color.						
Background Image	When <b>Background</b> is set to <b>Image</b> , upload the background image or select the default image.						
Background Color	When <b>Background</b> is set to <b>Solid Color</b> , configure the background color. The default value is <b>#ffffff</b> .						
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 Login • Account Placeholder • Account Placeholder • Copyright • Copin • Copyright • Copin • Copyright • Copyright						

#### Table 3-11 Basic Information of the Portal Page

(5) In the **Portal Page** area, click **Advanced** to configure advanced information for the portal page.

#### Portal Page @

Basic Advanced		Mobile Desktop Reset Style
Logo Position	Upper V	
Background Mask Color	#a2a2a2	rtujne
Background Mask Opacity	30	
Welcome Message Text Color	#11111	Account Login
Welcome Message Text Size	24 🗸	Account
Button Color	#0066ff	Password
Button Text Color	#111111	and the second second
Link Color	#ffffff	Login
Text Color in Box	#ffffff	
		·
		Note: This is only a preview image. The actual effects vary with devices at different resolutions.
		OK Cancel

Parameter	Description
Logo Position	Select the logo position (Upper, Middle, or Lower).
Background Mask Color	Select the background mask color. The default value is #a2a2a2.
Background Mask Opacity	Select the background mask opacity (0-100).
Welcome Message Text Color	Select the welcome message text color. The default value is #ffffff.
Welcome Message Text Size	Select the welcome message 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.

#### Table 3-12 Advanced Information of the Portal Page

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

#### 2. Enabling Account Authentication for an SSID

- Log in to Ruijie Cloud, choose Project > Configuration > Devices > Wireless > SSID, and select a network that needs to configure wireless authentication.
- (2) If the SSID that needs to enable wireless authentication is not created, click to open the SSID

configuration page. If the SSID that needs to enable wireless authentication is created, click  $\square$  in the

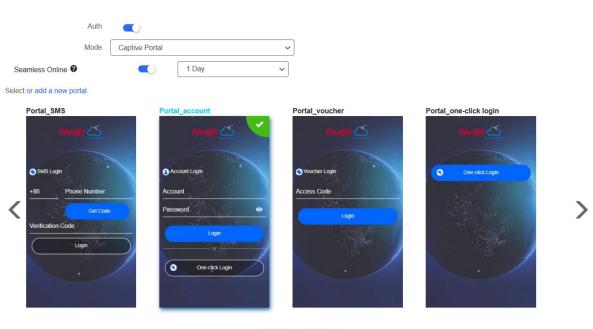
Action column. The following content only describes configurations related to wireless authentication. For details about other SSID configuration parameters, see the Ruijie Cloud Cookbook.

SSID							
WLAN ID	SSID	Encryption Mode	Hidden	Forward Mode	Radio	Auth Mode	Action
1	WiFi_60	Open	No	Bridge	1	Auth Disabled	. ii.

(3) Enable **Auth** (disabled by default) and configure authentication-related parameters. After the configuration, click **OK** to save the configurations.

Û	Note

When **Encryption Mode** is set to a value other than **WPA2-Enterprise(802.1x)**, **Auth** is available and you can select whether to perform wireless authentication.





- Mode: Set it to Captive Portal.
- Seamless Online: Determine whether to enable Seamless Online as required, which is enabled by default. After Seamless Online is enabled, users do not need to be authenticated when they go online again in the specified period of time.
- Select or add a new portal: Select a portal template with the authentication mode set to Account. If the configured template does not meet the requirements, click or add a new portal to create a portal template.
- (4) Click **Save** for the configuration to take effect.

							Save More -
Wireless Configurat	tion						^
SSID 🔁							
	6600	Examples Made	Uldan	Conversed Manufac	Destin	A value and a star	A
WLAN ID	SSID LJW_22	Encryption Mode Open	Hidden	Forward Mode Bridge	Radio 1,2	Auth Mode Captive Portal	Action

#### 3. Adding an Account

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

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

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

Add user group		Х
* User group name	test	
	User Group Policy	
Price		
	-	
Concurrent devices	3	~
Period	30Minutes	~
Quota (j)	100 MB	$\vee$
Maximum upload rate	Unlimited	~
Maximum download rate	Unlimited	~
Bind MAC on first use		
		Cancel OK

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) 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, the user can use this account to log in remotely using a VPN.



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.

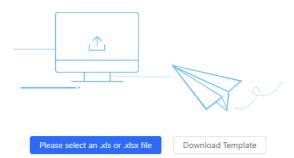
- Adding accounts through batch import
  - a Click Bulk import.

#### 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.

#### 🛕 Note

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

Alias User group Email
test
test
test
}

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

Account	Voucher	User Group	≪ E-sharing	١							O ₽ 8
Add accou	Bulk import	One-click send	More v • Te	otal Accounts: 3 🏾 A	ctivated Accounts: 0	• Expired Accounts: 0				Accour	nt C
	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	-		∠Cī
	test4	test4	test	Not used	30Minutes	Empty	Empty.	2023-02-13 16:42:21	-		∠CŌ
	test2	test2	test	Not used	30Minutes	Empty	Empty	2023-02-13 16:42:21	-		∠Cī

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

#### 3.20.5 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  $\bigcirc$  > Account.

Ruíjie 📥	Home	Project			🔤 res-testas-001_ V 📀 📫	<u> </u>
Project 255	ь	Device 53	Alarm 24	<b>8</b>		Account Sub Accou Release No
		• 1 devices have new version.				Switch to C

(2) Add Twilio account information and click Save.

User Info		
Modify Password		
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
Delete Account		

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

Captive Portal			
Ad	d	Synchronize	

(3) Configure basic information of the portal template.

Name	Portal_SMS *
Description	
Login Options	One-click Login Voucher Account SMS Registration Facebook Account
	Twilio Account SID
	Auth Token
	Auth Phone
Show Balance Page 🛛	
Post-login URL 🛛	https://www.ruijienetworks.com

Table 3-13	Basic Information of the Portal Template	
------------	--	--

Parameter	Description
Name	Indicates the name of a captive portal template.
Description	Indicates the description of a captive portal template.
Login Options	Select <b>SMS</b> , 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.

(4) In the **Portal Page** area, click **Basic** to configure basic information for the portal page.

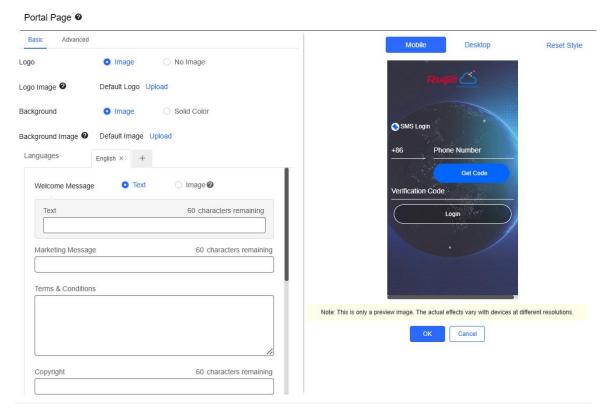


Table 3-14	Basic Information of the Portal Page
	Bable internation of the Fortar Fuge

Parameter	Description
Logo	Select whether to display the logo image.
Logo Image	When <b>Logo</b> is set to <b>Image</b> , upload the logo picture or select the default logo.
Background	Select the background with the image or the solid color.
Background Image	When <b>Background</b> is set to <b>Image</b> , upload the background image or select the default image.

Parameter	Description			
Background Color	When <b>Background</b> is set to <b>Solid Color</b> , or default value is <b>#ffffff</b> .	configure the background color. The		
	<ul> <li>Select the language of the portal page and the portal page as required. You can click languages.</li> <li>Welcome Message: Select the welcor</li> <li>Marketing message: Enter the market</li> <li>Terms &amp; Conditions: Enter terms and</li> <li>Copyright: Enter the copyright.</li> <li>SMS Login: After SMS Login is enable of the controls related to SMS authentice</li> </ul>	to add portal pages in other me message with the image or text. ting message. conditions.		
	SMS Login	Reset		
Language	Title ◎ Show	60 characters remaining		
	Phone Number Placeholder	60 characters remaining		
	Phone Number Verification Code Placeholder	60 characters remaining		
	Verification Code			
	Verification Code Button	60 characters remaining		
	Get Code			
	Login Button	60 characters remaining		
	Login	C0 obsractors remaining		
Switching Button 60 characters rer				

(5) In the **Portal Page** area, click **Advanced** to configure advanced information for the portal page.

#### Portal Page @

Basic Advanced		Mobile Desktop Reset Style
Logo Position	Upper 🗸	
Background Mask Color	#a2a2a2	Rugio 📥
Background Mask Opacity	30	
Welcome Message Text Color	#ffffff	SMS Login
Welcome Message Text Size	24 🗸	+86 Phone Number
Button Color	#0066ff	Get Code
Button Text Color	######	Verification Code
Link Color	#fffff	Login
Text Color in Box	#fffff	
		·

a na sa sana na manana 🖌 ita 🖡 ka na na mana ka 🖉 ka na manana na na manana 🗧 sa sa sana na manana sa na manana na ma
---

ок	Cancel

Parameter	Description
Logo Position	Select the logo position (Upper, Middle, or Lower).
Background Mask Color	Select the background mask color. The default value is #a2a2a2.
Background Mask Opacity	Select the background mask opacity (0-100).
Welcome Message Text Color	Select the welcome message text color. The default value is #ffffff.
Welcome Message Text Size	Select the welcome message 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.

#### Table 3-15 Advanced Information of the Portal Page

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

#### 3. Enabling SMS Authentication for an SSID

 Log in to Ruijie Cloud, choose Project > Configuration > Devices > Wireless > SSID, and select a network that needs to configure wireless authentication. (2) If the SSID that needs to enable wireless authentication is not created, click 📍 to open the SSID

configuration page. If the SSID that needs to enable wireless authentication is created, click in the **Action** column. The following content only describes configurations related to wireless authentication. For details about other SSID configuration parameters, see the Ruijie Cloud Cookbook.

s	SID							
	WLAN ID	SSID	Encryption Mode	Hidden	Forward Mode	Radio	Auth Mode	Action
	1	WiFi_60	Open	No	Bridge	1	Auth Disabled	.Ŵ.

(3) Enable **Auth** (disabled by default) and configure authentication-related parameters. After the configuration, click **OK** to save the configurations.

#### 🚺 Note

When **Encryption Mode** is set to a value other than **WPA2-Enterprise(802.1x)**, **Auth** is available and you can select whether to perform wireless authentication.

Auth				
Mode Captive Portal	~			
Seamless Online 🛛 🔍	1 Day 🗸			
Select or add a new portal.				
rtuga 🖄 💙	count Logn unt Logn	ortal_voucher	Portal_one-click login	>

- Mode: Set it to Captive Portal.
- Seamless Online: Determine whether to enable Seamless Online as required, which is enabled by default. After Seamless Online is enabled, users do not need to be authenticated when they go online again in the specified period of time.
- Select or add a new portal: Select a portal template with the authentication mode set to SMS. If the configured template does not meet the requirements, click or add a new portal to create a portal template.
- (4) Click **Save** for the configuration to take effect.

Wireless Configurat	tion					l	Save More -
SSID 🖨							
WLAN ID	SSID	Encryption Mode Open	No	Forward Mode Bridge	Radio	Auth Mode Captive Portal	Action
			vious Page 1 of		*,£	oupor o Fortar	10 • 1 in total

#### 3.20.6 Configuring an Authentication-Free User List on Eweb Management System

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** ( **WLAN**) > Wireless Auth > Allowlist > User 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		
User Allowlist	t		+ 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: 1.1.1.1.1.100 Cancel OK 2. Configuring an Authentication-Free Public IP Address OK (1) Choose Network ( ♥ WLAN) > Wireless Auth > Allowlist > IP Allowlist. (2) Click Add to open the configuration page.

Cloud Integration	Allowlist	Client List					
<i>i</i> A user config	ured with whitelis	sted IP or MAC address ca	n access the Internet without a	uthentication.			
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 🗸						Total 0

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

Ac	ld				×
	* IP / IP Range	Example: 1.1.1.1-1.1.1.100			
				Cancel	ОК
3.	Configuring a Do	main Name Allowlist			
(1)	Choose Retw	vork ( 🛜 WLAN) > Wireless Auth	> Allowlist > Domain Allow	vlist.	

(2) Click **Add** to open the configuration page.

Cloud Integration Allowlist Client Li	ist	
<ul> <li>A user configured with whitelisted IP or N</li> </ul>	MAC address can access the Internet without authentication.	
User Allowlist IP Allowlist Domai	ain Allowlist MAC Blocklist/Allowlist	
Domain Allowlist		+ Add 🗇 Delete Selected
Up to <b>100</b> entries can be added.		
	URL	Action
	No Data	
< 1 > 10/page >		Total 0

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

Cancel

Add				×
ł	* URL			
			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 ( 🛜 WLAN) > Wireless Auth > Allowlist > MAC Block
--

(2) Click Add to open the MAC address allowlist or blocklist configuration page.

Cloud Integration Allow	st Client List	
<i>i</i> A user configured with v	vhitelisted IP or MAC address can access the Internet without authentication.	
User Allowlist IP Allow	vlist Domain Allowlist MAC Blocklist/Allowlist	
MAC Allowlist		+ Add 🗇 Delete Selected
Up to <b>250</b> entries can be a	ided.	
	MAC Address	Action
	No Data	
< 1 > 10/page		Total 0
MAC Blocklist		+ Add 🗊 Delete Selected
Up to <b>250</b> entries can be a	lded.	
	MAC Address	Action
	No Data	
< 1 > 10/page		Total 0
3) Configure th	e MAC address of a wireless STA. After the configuration, click <b>OK</b> .	
Add		×
* MAC Ac	Idress Example: 00:11:22:33:44:55	

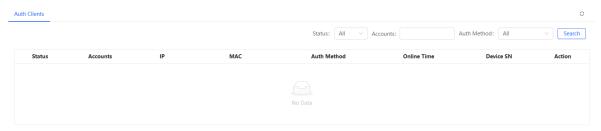
97

### 3.20.7 Displaying Authenticated Users on Eweb Management System

Choose 🕯	P Netwo	rk ( 🛜	WLAN) > Wire	less Auth >	Client List	to display au	thenticated u	sers.
Note	)							
The client	going offlin	e will no	t disappear im	mediately. Ins	stead, the cl	ient will stay	on the list for	three more
minutes.								
Cloud Integratio	n Allowlist	Client List					IP/MAC	Q ↓ Batch Logout
i The client	t going offline will no	t disappear imr	nediately. Instead, the client	will stay in the list for th	hree more minutes.			
Us	ername	IP	MAC Address	Online Time	Auth Type	Connect the SSID	Access Name	Action
< <b>1</b> >	10/page ~			NO D	ala			Total 0

#### 3.20.8 Displaying Authenticated Users on Ruijie Cloud

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



## **4** 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-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2260, RG-RAP1261, RG-RAP1260, and RG-RAP6262: Click Manage Network Device.
- For the other RAP models: Choose **WLAN > APs >** Select the target device in the device list and click **Manage**.

## 4.1 Switching Work Mode

#### 4.1.1 Work Mode

See Work Mode for details.

#### 4.1.2 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 standalone 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.

#### 4.1.3 Configuration Steps

#### 1 Note

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

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: In Local Device mode, choose overview > Device Details

For other RAP models: Choose ( The weak of the second seco

Click the current work mode to change the work mode.

Hostname: Ruijie       • RAP	9 SN: G1QW.	7	IP: 172.26.1.209	() Reboot
Overview Basics ~ Security ~	Advanced $\vee$ Diagnostics $\vee$	System ~		
Overview				
Memory Usage <b>31</b> %	Online Clients		Status: Online Duration: 16 hours 45 minutes 21 se Systime: 2022-04-01 09:43:49	econds
Device Details				
Model: RAP SN: G1Q Work Mode: Router 2 Hardware Ver: 1.00		N F	IME: Ruijie 2 MAC: AA:11:A Role: Master AP <b>0</b> Ver: ReyeeOS 1.75.1410	
AAR PI				

**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.

	Description:
	<ol> <li>The device IP address may change upon mode change.</li> </ol>
	<ol><li>Change the endpoint IP address and ping the device.</li></ol>
1	<ol> <li>Enter the new IP address into the address bar of the browser to access EWEB.</li> </ol>
	4. The system menu varies with different work modes.
	Work Mode Router 🗸 🕐
	Self-Organizing 🔵 🕐
	Network
	AC 🕥 💿
	Save

#### A Caution

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

#### 4.1.4 Viewing Device Role

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: In **Local Device** mode, choose **Control Overview** > **Device Details** 

For other RAP models: Choose ( The WLAN > APs > Manage) The Overview > Device Details

()If the self-organizing network is enabled, you can view the device role on the **Device Details** page.

Master AP/AC: The device can manage downlink devices.

Slave AP/Device: The device has been managed by an AC. The slave Aps are managed by the master AP/AC in a unified manner. Some wireless network settings cannot be edited alone, and thus the master AP/AC delivers configurations to edit the network settings in a unified manner.

**Device Details** 

 Model:
 RAP2261(E)

 MAC Address:
 58:69:6C:22:08:30

 Hardware Ver:
 1.00

Hostname: Ruijie & Work Mode: Router & Software Ver: ReyeeOS 1.218.2415 SN: MACCR10825107 Role: Master AP

## 4.2 Configuring Internet Connection Type (IPv4)

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: In Local Device mode, choose ONE Network > WAN > WAN

For other RAP models: Choose ( The WLAN > APs > Manage >) Wetwork > WAN > WAN

Select the Internet connection type after confirming with the ISP. For detailed configuration, see <u>Work Mode</u>. After completing the configuration, click **Save**.

i wan	
* Internet	DHCP ~
	No username or password is required for DHCP clients.
IP Address	192.168.111.210
Subnet Mask	255.255.255.0
Gateway	192.168.111.1
DNS Server	192.168.111.1
	Advanced Settings
	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.

## 4.3 Configuring Internet Connection Type (IPv6)

#### A Caution

This function is supported by only RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2260, RG-RAP1261, RG-RAP1260, and RG-RAP6262 in the AP mode.

In Local Device mode, choose Wave > WAVe > WAVe Settings.

Select the Internet connection type after confirming with the ISP. For detailed configuration, see <u>Work Mode</u>. After completing the configuration, click **Save**.

WAN WAN_V6 Set	tings	
* Internet	Null	^
IPv6 Address IPv6 Prefix	DHCP Static IP Null	
Gateway		
DNS Server		
	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.

## 4.4 Configuring LAN Port

#### 🛕 Caution

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

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: In Local Device mode, choose Wetwork > LAN > LAN Settings

For other RAP models: Choose ( TWLAN > APs > Manage >) Retwork > 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 Sett	ings DHCP	Clients Stat	tic IP Addresses						
<b>i</b> L	AN Settings								?
LAN	Settings							+ Add	Delete Selected
Up to	8 entries can b	e added.							
	IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
	192.168.120.2	255.255.255.0	Default VLAN	-	Enabled	192.168.120.2	253	30	Edit Delete

Edit			×
* IÞ	192.168.120.2		
* Subnet Mask	255.255.255.0		
Remark	Remark		
* MAC	aa:11:aa:00:04:78		
DHCP Server			
		Cancel	ОК

## 4.5 Configuring Repeater Mode

#### 🛕 Caution

RG-RAP1200(F) access point do not support this function.

#### 4.5.1 Wired Repeater

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: In Local Device mode, choose Wetwork > Repeater Mode

	 6		
For other RAP models: Choose (	WLAN > APs > Manage >)	Network >	Repeater 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.

#### 🛕 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 in	Router mode.	
• Access Point	O Wireless Repeater	
		tion between a primary router and a secondary router, extending network coverage. of the local router to the LAN port of the primary router.
Wired Repeater		
	Check	

#### 4.5.2 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.

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: In Local Device mode, choose ONetwork > Repeater Mode

For other RAP models: Choose ( The WLAN > APs > Manage >) Retwork > Repeater Mode

(1) 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.

The device is wor	king in <b>Access Point</b> mode	
O Router	O Access Point	• Wireless Repeater
<i>i</i> • The loc • It is rec	ode allows you to establish a al device will work as a secon ommended to select a 5G Wi oops, wireless repeater is not	-Fi of the primary device.
Wireless Re	peater	
Primary D	Device	
*	SSID Select	

Г

SSID	5G	✓ Re-sca	n	
SSID	BSSSID	Security	Channel	RSSI
damo	ec:b9:70:68:3b:86	OPEN	161	-18 dBm High
HUAWEI- 11111111	4c:50:77:42:61:58	WPA2PSK	36	-34 dBm High
@ew1800	c6:70:ab:8c:bf:b5	OPEN	36	-34 dBm High
HUAWEI- 11111111	4c:50:77:42:61:5e	WPA2PSK	149	-36 dBm High
@Ruijie- ew1800_5G	82:05:88:90:20:12	OPEN	64	-37 dBm High

- (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.
  - If New Wi-Fi is selected, you can set a local Wi-Fi name and password. Clients will search out different Wi-Fi signals.

The device is working in	Access Point mode.
O Router	Access Point Vireless Repeater
<ul> <li>The local devi</li> <li>It is recommendation</li> </ul>	ows you to establish a wireless connection between a primary device and a secondary device, extending network coverage. ce will work as a secondary device. nded to select a 5G Wi-Fi of the primary device. ireless repeater is not allowed to be configured.
Wireless Repeat	er
Primary Device	
* SSID	@ew1800 Select
- Local Device	
Local Router Wi-Fi	New Wi-Fi     Same as Primary Router Wi-Fi
* SSID(2.4G)	@ew1800_plus
* SSID(5G)	@ew1800_plus_5G
Wi-Fi Password	A blank value indicates no encryption.
	Save

#### 🛕 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.

## 4.6 Creating a VLAN

#### A Caution

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

For	RG-RAP2260(G),	RG-RAP2260(E),	RG-RAP6260(G),	RG-RAP6262(G),	RG-RAP2260(H),	RG-		
RAP	6260(H), RG-RAP6	5260(H)-D, RG-RAF	P2266, RG-RAP226	60, RG-RAP1261,	RG-RAP1260 and	RG-		
RAP	RAP6262 models: In Local Device mode, choose ON Network > LAN > LAN Settings							
For o	For other RAP models: Choose ( The weak of the second seco							

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

LAN Settings DHCP	Clients Sta	tic IP Addresses						
i LAN Settings								0
LAN Settings							+ Add	Delete Selected
Up to <b>8</b> entries can be	added.							
IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
192.168.120.2	255.255.255.0	Default VLAN	-	Enabled	192.168.120.2	253	30	Edit Delete
Add	FIP 172.2	6.2.11		×				
* Subnet Ma	ask 255.2	55.255.0						
* VLAN Rema		ırk						

AA:11:AA:B4:16:E4

Cancel

#### Table 4-1 VLAN Configuration

\* MAC

DHCP Server

Parameter	Description
IP	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	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>Configuring DHCP</u> <u>Server</u> .

#### A 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.

## 4.7 Configuring Port VLAN

#### 🛕 Caution

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

For RG-RAP2260(C	G), RG-RAP2260(E),	RG-RAP6260(G),	RG-RAP6262(G),	RG-RAP2260(H),	RG
RAP6260(H), RG-R	AP6260(H)-D, RG-RA	P2266, RG-RAP226	60, RG-RAP1261,	RG-RAP1260 and	RG
RAP6262 models: In	Local Device mode, cl	noose 🕀 Network	> LAN		
For other RAP model	s: Choose ( 🛜 WLAN	<pre>&gt; APs &gt; Manage &gt;)</pre>	Hetwork > LA	N	
(1) On the LAN Sett	<b>ings</b> tab page, turn on	Port VLAN, and clic	<b>OK</b> in the confirmation	ation dialog box.	
LAN Settings Por	t VLAN				
i LAN Settings					
Port VLAN					
LAN Settings			+ Add	Delete Selected	
Up to <b>4</b> entries car	n be added.				
	VLAN ID		Remark	Action	
	99		test	Edit Delete	

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

. . . . .

			×
* VLAN ID	3		
Remark	Remark		
		Cancel	ОК

- (2) Switch to the **Port VLAN** tab page and configure VLANs for the port. Click the option box below the port, select the mapping between a VLAN and the port from the drop-down list box, and click **Save**.
  - UNTAG: Configure the VLAN as the native VLAN of the port. That is, when receiving a packet from this VLAN, the port removes the VLAN tag from the packet and forwards the packet. When receiving an untagged packet, the port adds the VLAN tag to the packet and forwards the packet through the VLAN. Only one VLAN can be configured as an untagged VLAN on each port.
  - **TAG**: Configure the VLAN as an allowed VLAN of the port, but the VLAN cannot be the native VLAN. That is, VLAN packets carry the original VLAN tag when they are forwarded by the port.
  - Not Join: Configure the port not to allow packets from this VLAN to pass through. For example, if VLAN 10 and VLAN 20 are not added to port 2, port 2 will neither receive nor send packets from or to VLAN 10 and VLAN 20.

LAN Settings	Port VLAN
<i>i</i> Port VLAM Please choo	N ose LAN Settings to create a VLAN first and configure port settings based on the VLAN.
Port VLAN	
Connected	Disconnected
VLAN 1(WAN	
VLAN 99	Not Joir 🗸

## 4.8 Changing MAC Address

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: In Local Device mode, choose WAN > WAN > WAN

For other RAP models: Choose ( TWLAN > APs > Manage >) WW Network > 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 Network > LAN.

#### A 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	Range: 2-232 and 234-4090.
* MTU	1500
* MAC	ec:b9:70:23:a4:bf
	Save

## 4.9 Changing MTU

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: In Local Device mode, choose ONE Network > WAN > WAN

For other RAP models: Choose ( The weak of the second seco

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	Range: 2-232 and 234-4090.
* MTU	1500
* MAC	ec:b9:70:23:a4:bf
	Save

## 4.10 Configuring DHCP Server

#### 🛕 Caution

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

#### 4.10.1 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.

#### 4.10.2 Configuring the DHCP Server Function

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: In Local Device mode, choose ONE Network > LAN > LAN Settings

For other RAP models: Choose ( TWLAN > APs > Manage >) Retwork > 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.

#### A 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.

Edit		×
* IP	192.168.120.2	
* Subnet Mask	255.255.255.0	
Remark	Remark	
* MAC	aa:11:aa:00:04:78	
DHCP Server		]
* Start	192.168.120.2	
* IP Count	253	
* Lease Time(Min)	30	
	Cancel	ОК

#### 4.10.3 Displaying Online DHCP Clients

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: In Local Device mode, choose ONE Network > LAN >DHCP Clients

For other RAP models: Choose ( 🛜 WLAN > APs > Manage >) 🕮 Network > 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.

LAN Set	ttings	DHCP Clients	Static IP Addresses			
0	View DH0	CP clients.				0
DHC	CP Clier	nts	Searc	ch by Hostname/IP/MA(	Q C Refresh	+ Batch Convert
Up t	to <b>300</b> IF	P-MAC bindings can be	added.			
	No.	Hostname	IP	MAC	Remaining Lease Time(min)	Status
	1	nova <u></u> G- f5a 97	192.168.120.172	42:11:26:	23	Convert to Static IP
	2	no 5- 7d2c 32	192.168.120.35	72:26:e8	13	Convert to Static IP
	3	R17	192.168.120.236	00:e0:4	19	Convert to Static IP

#### 4.10.4 Displaying the DHCP Static IP Address List

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: In Local Device mode, choose ONE Network > LAN > Static IP Addresses

For other RAP models: Choose ( The WLAN > APs > Manage >) Retwork > 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.

LAN Settings	DHCP Clients	Static IP Addresses			
<i>i</i> Static IP	Address List				?
Static IP Ac	ddress List		Search by IP/MAC	Q + Add	Delete Selected
Up to <b>300</b> er	ntries can be added.				
No.	IP		MAC		Action
□ 1	192.168.1	120.64	12:33:e3:b9:d9:36		Edit Delete

## 4.11 Link Aggregation

#### 🛕 Caution

The function is supported by only RG-RAP2260(H).

In Local Device mode, choose Advanced > Link Aggregation.

Link Aggregation can improve the throughput in the network and deal with link congestion.

<i>i</i> Link Aggregation	<b>on</b> 2.3ad link aggregation on the client and connect it to port LAN2,LAN1.
Link Aggregation	
	LAN2 LAN1
	Save

## 4.12 Configuring DNS

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-RAP6262 models: In Local Device mode, choose Advanced > Local DNS For other RAP models: Choose ( WLAN > APs > Manage >) 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.



## 4.13 Hardware Acceleration

#### A Caution

This function is supported by only RAP2260(H), RAP6260(H), RG-RAP6260(H)-D, RAP2260, RG-RAP1261, RG-RAP1260, and RAP6262.

In Local Device mode, choose 💼 Advanced > Hardware Acceleration.

After Hardware acceleration is enabled, the Internet access speed will be improved.

<i>i</i> Hardware Acce	eleration Acceleration is enabled, the Internet access speed will be improved and clients will not be rate-limited.
Enable	
	Save

## 4.14 Configuring Port Flow Control

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: In Local Device mode, choose 🗄 Advanced > Port Settings

For other RAP models: Choose ( The WLAN > APs > Manage >) 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 Port Set	ettings ntrol can relieve the data congestion caused by ports at different speeds and improve the network speed.
Flow C	Control
	Save

## 4.15 Configuring ARP Binding

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

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: In Local Device mode, choose Security > ARP List

For other RAP models: Choose ( **WLAN** > APs > Manage >) 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.

i The dev	ice learns IP-MAC mapping of all d	evices connected to its interfaces	s. You can bind or filter the MAC address	s. (?)
ARP List	Search by	IP/MAC Q	+ Add Ø Bind Selected	Delete Selected
Up to 256	IP-MAC bindings can be added.			
No.	MAC	IP	Туре	Action
1	12:33:e3:b9:d9:36	192.168.120.64	Dynamic	
2	00:e0:4c:36:0b:ea	192.168.120.236	Static	Edit Delete
3	30:0d:9e:7e:13:a1	172.26.1.1	Dynamic	

(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.

* IP	Enter or select an IP address.
* MAC	Enter or select a MAC address.
	12:33:e3:b9:d9:36 (192.168.120.64)
	00:e0:4c:36:0b:ea (192.168.120.236)

## 4.16 Configuring LAN Ports

#### 🛕 Caution

Add

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

Choose Retwork ( The WLAN) > 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.

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.

<ul> <li>LAN Port Settings</li> <li>The configuration takes effect only for the AP with a LAN port, e.g., EAP101.</li> <li>Note: The configured LAN port settings prevail. The AP device with no LAN port settings will be enabled with default settings.</li> </ul>					
Default Settings	;				
VLAN ID		Add VLAN			
	(Range: 2-232 and 234-4090. A blank value indic WAN port.) AP device with no LAN port settings <b>O</b> Save	ates the same VLAN as			
LAN Port Setting	gs	+ Add	Delete Selected		
Up to 8 VLAN IDs or	32 APs can be added (1 APs have been added).				
VLAN ID	¢ Applied t	0	Action		
5	Ruijie		Edit Delete		

## 4.17 IPv6 Settings

#### 🛕 Caution

This function is supported only by RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2260, and RG-RAP6262 in the router mode.

#### 4.17.1 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.

#### 4.17.2 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, 800:0:0:0:0:0:0:0:1, 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, **800:0:0:0:0:0:0:0:1** 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. NAT66

IPv6-to-IPv6 Network Address Translation (NAT66) is the process of converting the IPv6 address in an IPv6 packet header to another IPv6 address. NAT66 prefix translation is an implementation of NAT66. It replaces the IPv6 address prefix in the packet header with another IPv6 address prefix to achieve IPv6 address translation. NAT66 can realize mutual access between an intranet and Internet.

#### 4.17.3 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.

#### 4.17.4 Enabling IPv6

In Local Device mode, choose ONetwork > IPv6 Address.

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

0	<ul> <li>IPv6 Address</li> <li>1. When IPv6 is enabled, The MTU of IPV4 WAN port need higher than 1280.</li> <li>2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to Untagged and set the other VLANs to Non-added.</li> </ul>
	Enable
Tips	
•	Are you sure you want to enable IPv6 address? Cancel OK

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.

	IPv6 is enab				need higher than 1 hoose Port VLAN	LAN to Untagge	d and set the o	ther VLANs to Non-add
E	Enable 🧲							
WAN Settings	LAN Se	ettings	DHCPv6 (	lients	Static DHCPv6			
* In	ternet	DHCP			~			
IPv6 Ac	ddress							
IPv6	Prefix							
Ga	iteway							
DNS	Server							
1	NAT66							
		Sav	e					

#### 4.17.5 Configuring the IPv6 Address for the WAN Port

In Local Device mode, choose WAN Settings.

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

	enabled, The MTU of IPV4 WAN port need hig set more than one IPv6 LAN, please choose F	gher than 1280. Port VLAN to set only one VLAN to Untagged and set the other VLANs to Non-add
Enable		
WAN Settings LAI	N Settings DHCPv6 Clients Stati	c DHCPv6
* Internet	DHCP	^
IPv6 Address	DHCP	
IPv6 Prefix	Static IP Null	
Gateway		
DNS Server		
NAT66		
	Save	

#### Table 4-2 IPv6 Address Configuration Parameters of the WAN Port

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

Parameter	Description
	address is displayed. If <b>Internet</b> is set to <b>Static IP</b> , you need to manually configure this parameter.
NAT66	If the current device cannot access the Internet in DHCP mode or cannot obtain the IPv6 address prefix, you must enable NAT66 to assign the IPv6 address to an intranet client.

#### 4.17.6 Configuring the IPv6 Address for the LAN Port

In Local Device mode, choose ONE 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 NAT66 function (see <u>4.17.5</u> Configuring the IPv6 Address for the WAN Port).

<ul> <li>IPv6 Address</li> <li>1. When IPv6 is enabled, The MTU of IPv4 WAN port need higher than 1280.</li> <li>2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to Untagged and set the other VLANs to Non-added.</li> </ul>							
	Enable 🔵						
WAN Setting	gs LAN Settings	DHCPv6 Clients Stat	tic DHCPv6				
LAN Set	ttings					+ Add	elete Selected
Up to 8	entries can be added.						
	VLAN ID	IPv6 Assignment	Subnet Prefix Name	Subnet ID	Subnet Prefix Length	IPv6 Address/Prefix Length	Action
	Default	Auto		0	64		Edit Delete

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	Auto	?
IPv6 Address/Prefix Length	Auto DHCPv6 SLAAC Null	0
	Cancel	ОК

#### You can click Advanced Settings to configure more address attributes.

Edit		×
IPv6 Assignment	Auto	0
IPv6 Address/Prefix	Example: 2000::1	0
Length	Advanced Settings	
Subnet Prefix Name	Default	0
Subnet Prefix Length	64	0
Subnet ID	0	0
* Lease Time (Min)	30	0
DNS Server	Example: 2000::1, each separated by a comma	
	Cancel	ОК

#### Table 4-3 IPv6 Address Configuration Parameters of the LAN Port

Parameter	Description
Subnet Prefix Name	Configure the interface from which the prefix is obtained, for example,

Parameter	Description
	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. <b>0</b> 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.

#### 4.17.7 Viewing DHCPv6 Clients

In Local Device mode, choose Over 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.

	Pv6 is enabled, The N	/ITU of IPV4 WAN port i i one IPv6 LAN, please o		nly one VLAN to Untagged and set the other VI	LANs to Non-added.	
E	nable 🔵					
WAN Settings	LAN Settings	DHCPv6 Clients	Static DHCPv6			
<i>i</i> DHCPv6 You can v		nts information on this p	page.			
DHCPv6 Cl	ients				Search by IPv6 Address/DUIE Q	+ Batch Convert
No.	Hostnan	ne	IPv6 Address	Remaining Lease Time(min)	DUID	Status
				No Data		
< 1 >	10/page 🗸					Total 0

#### 4.17.8 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.

In Local Device mode, choose	Wetwork > IPv6 Address > Static DHCPv6.
------------------------------	---

IPv6 Address  1. When IPv6 is enabled, Th 2. If you want to set more th			one VLAN to Untagged a	nd set the other VLANs to Non-adde	d.	
Enable 🚺						
WAN Settings LAN Settings	DHCPv6 Clients	Static DHCPv6				
i Static IP Address List						
Static IP Address List				Search by IPv6 Address/DUI[	Q + Add	Delete Selected
Up to <b>200</b> entries can be added	d.					
No.	IPv6 Address		DUID		Actio	1
			No Data			
< 1 > 10/page >						Total 0
(1) Click Add.						
Add			×			
* IPv6 Address	Example: 2000::1					
* DUID	Example: 000300	0100d0f819685f				
		Cancel	ОК			

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

#### 4.17.9 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.

Ir	In Local Device mode, choose Security > IPv6 Neighbor List.								
	IPve	Neighbo	or List		Search by IP Address/MAC A	Q + Add	Ø Bind Selected	Delete Selecte	ed
	Upf	o <b>256</b> IP-M	IAC bindings can be added.						
		No.	MAC Address	IP Address	Туре	Ethernet	status	Action	
		1	58:69:6c:22:08:30	fe80::5a69:6cff:fe22:830	Dynamic	WA	N		
		2	42:93:d6:46:2e:ab	fe80::5e1a:a95:3ed7:9be4	Dynamic	LAI	N		
		3	f8:e4:3b:13:21:6f	fe80::9120:5120:d4df:562b	Dynamic	LAN	N		
		1	10/page V					Tot	otal 3

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

Add		$\times$
* Interface	Select ~	
* IPv6 Address	Please enter an IPv6 address.	
* MAC Address	Please enter a MAC address.	
	Cancel	ок

(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 Neig	ghbor List		Search by IP Address/MAC A	Q + Add	
Up to 256	IP-MAC bindings can be added.				
No.	MAC Address	IP Address	Туре	Ethernet stat	us Action
□ 1	58:69:6c:22:08:30	fe80::5a69:6cff:fe22:830	Dynamic	WAN	@ Bind
2	42:93:d6:46:2e:ab	fe80::5e1a:a95:3ed7:9be4	Dynamic	LAN	∂ Bind
3	f8:e4:3b:13:21:6f	fe80::9120:5120:d4df:562b	Dynamic	LAN	∂ Bind
< 1	> 10/page >				Total :

# **5** System Settings

## 5.1 PoE

#### Caution

Only RG-RAP1200(P) supports this function.

#### Choose Wireless > APs > Manage > Basics > PoE.

The device supplies power to PoE powered devices through ports. You can check the total power, current consumption, remaining consumption, and whether PoE power supply status is normal. Move the cursor over a port. The power switch icon 💶 appears. You can click it to control whether to enable PoE on the port.

<ul><li></li></ul>	Hostname: Ruijie	SN: G1	PW61G000208	IP:	MAC: 00:D0:F8:15:78:44		() Reboot
Overview Basics ~	Advanced $\checkmark$ Diagnostics $\checkmark$	System	~				
i РоЕ							
PoE Consumption	n Details						
Max Consumption	15.4W		Current Consumption	0.0W		Remaining Consumption 15.4W	
PoE Device Panel							
Powered On	Powered Off PoE Erro	or					
			Current	Consumption:	0.0W		

## 5.2 PoE Settings

#### Caution

This function is supported by only RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2260, RG-RAP1261, RG-RAP1260, and RG-RAP6262.

In Local Device mode, choose 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.

<i>i</i> PoE Settings		
Power Mode	Auto	~
Current Mode	IEEE 802.3bt	
Energy Saving	Full-power Mode	~ ⑦
Band	○ 2.4G ○ 5G	2.4G+5G
Current Power	51W	
	Save	

## 5.3 Setting the Login Password

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-RAP6262 models:

If the device works in self-organizing network mode, and **Network** mode webpage is displayed, choose **System** > Login Password

In standalone mode: Choose System > Login > Login Password
For other RAP models:
In self-organizing network mode: Choose Network > Password
In standalone mode: Choose System > Login > 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.

-0-

<i>i</i> Change the login	password. Please log in a	gain with the new password later.
* Old Password		
* New Password		
* Confirm Password		
	Save	

### 5.4 Setting the Session Timeout Duration

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-RAP6262 models:

If the device works in self-organizing network mode, and Local Device mode webpage is displayed, choose

System > Login		
In standalone mode: Cho For other RAP models:	oose System > Login > Sessio	n Timeout
In self-organizing network	mode: Choose 🛜 WLAN > APs >	Manage > System > Login > Session Timeout
	ed on the Web page within a period of m operations again, enter the passwo	<b>n Timeout</b> time, the session is automatically disconnected. rd to log in again. The default timeout duration is
i Session Timeou	t	
* Session Timeout	3600	seconds
	Sava	

## 5.5 Setting and Displaying System Time

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-RAP6262 models:

If the device works in self-organizing network mode, and **Network** mode webpage is displayed, choose **System Time** 

In standalone mode: Choose System > System Time

For other RAP models:

In self-organizing network mode: Choose **Network > 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.

#### 🛕 Caution

In self-organizing network mode, the system time of all devices in the network will be changed synchronously.

<i>i</i> Configure and vie	ew system time (The device h	nas no RTC mo	dule. The time settings will not	be saved upon reboot).
Current Time	2022-04-01 10:14:00	dit		
* Time Zone	(GMT+8:00)Asia/Shangl	hai v		
* 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			

## 5.6 Configuring Reboot

#### 🛕 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.

#### 5.6.1 Rebooting the Current Device

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H),	RG-
RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and	RG-
-0-	
RAP6262 models: In Local Device mode, choose System > Reboot > Reboot	
For other RAP models:	
In self-organizing network mode: Choose 🐨 WLAN > APs > Reboot	
In standalone mode: Choose System > Reboot > Reboot	
Click <b>Reboot</b> . The device will restart.	
<i>i</i> Please keep the device powered on during reboot.	
Reboot	

#### 5.6.2 Rebooting All Devices in the Network

In self-organizing network mode, you can reboot all devices in the network in batches.

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: In **Network** mode, choose **System** > **Reboot** > **Reboot** 

For other RAP models: Choose **Network > Reboot & Reset > Reboot** 

Click Reboot, select All Devices, and click Reboot All Device to reboot all devices in the current network.

Reboot	Scheduled Reboot		
<b>i</b> F	Please keep the device pow	vered on during reboot.	
	Select 🔘 Local	• All Devices	<ul> <li>Specified Devices</li> </ul>
	Reboot All	Device	

#### 🛕 Caution

It takes time to reboot all devices in the current network. The action may affect the whole network. Please be cautious.

#### 5.6.3 Rebooting the Specified Device

In self-organizing network mode, you can reboot specified devices in the network in batches.

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: In **Network** mode, choose **System** > **Reboot** > **Reboot** 

For other RAP models: Network > Reboot & Reset > Reboot

Click **Reboot**, click **Specified Devices**, select required devices from the **Available Devices** list, and click **Add** to add devices to the **Selected Devices** on the right. Click **Reboot**. Specified devices in the **Selected Devices** list will be rebooted.

eboot Sch	eduled Reboot				
<i>i</i> Please kee	p the device powered on during reboot.				
Select	O Local O All Devices		• Specified Devic	tes	
	Available Devices	1/1		Selected Devices	0/0
	Q Search by SN/Model			Q Search by SN/Model	
	G1QH6WX000610 - RAP2260(E)	1	< Delete	No data	
_	duled Reboot				
Select	O Local O All Devices		• Specified Devices	;	
	Available Devices	0/0		Selected Devices	1/1
	Q Search by SN/Model			Q Search by SN/Model	
	No data		< Delete	G1QH6WX000610 - RAP2260(E)	
Г	Reboot				

## 5.7 Configuring Scheduled Reboot

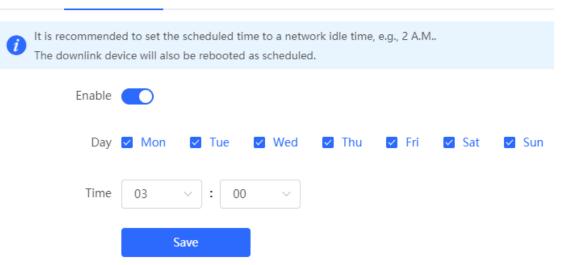
#### 5.7.1 Configuring Scheduled Reboot for the Current Device

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>Setting the Session Timeout Duration</u>.

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-RAP6262 models: Choose System > Reboot > Scheduled Reboot For other RAP models: To configure scheduled reboot for the current device, choose ( WLAN > APs > Manage >) System > Reboot > Scheduled Reboot To configure scheduled reboot for all devices in the network, choose Network>> Scheduled Reboot To configure scheduled reboot for all devices in the network, choose Configure scheduled Reboot To configure scheduled reboot for all devices in the network, choose Configure scheduled Reboot 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 Enable, 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



## 5.8 Configuring Backup and Import

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: Choose System > Management > Backup & Import

For other RAP models: Choose ( **WLAN > APs > Manage >**) **System > Management > 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.

Backup & Import	Reset				
	sion is much later than the cu led to choose <mark>Restore</mark> before			tion may be missing. rice will be rebooted automatically	?
Backup Profile					
Backup Profile	Backup				
Import Profile					
File Path	Please select a file.	Browse	Import		

## 5.9 Restoring Factory Settings

#### 5.9.1 Restoring the Current Device to Factory Settings

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-
RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-
RAP6262 models: In Local Device mode, choose System > Management > Reset
For other RAP models: Choose ( The weak of the second seco
Click <b>Reset</b> to restore the current device to the factory settings.
Backup & Import Reset
<i>i</i> Resetting the device will clear the current settings. If you want to keep the setup, please Backup Profile first.
Reset
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>Configuring Backup and Import</u>). Therefore, exercise caution when performing this operation.

#### 5.9.2 Restoring All Devices to Factory Settings

In the self-organizing network mode, all devices in the network will be restored to factory settings.

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-RAP6262 models: In **Network** mode, choose **System** > **Management** > **Reset** 

Click **All Devices**, select whether to enable **Unbind Account** and Click **Reset All Devices**. All devices in the network will be restored to factory settings.

Backup & Import	Reset
<i>i</i> Resetting the d	evice will clear the current settings. If you want to keep the configuration, please Backup Config first.
Select	Local O All Devices
Option	Unbind Account (The devices of this account will be removed from Ruijie Cloud and will not be managed by this account).
	Reset All Devices

#### Caution

The operation will clear all configuration of all devices in the network. Therefore, exercise caution when performing this operation.

## 5.10 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.

#### 5.10.1 Online Upgrade

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

For other RAP models: Choose ( **WLAN** > **APs** > **Manage** >) **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.

Online Upgrade	Local Upgrade
<i>i</i> Online up	grade will keep the current configuration. Please do not refresh the page or close th
Current Version	ReyeeOS 1.86.
New Version	ReyeeOS 1.
Description	1. 2.
Tip	<ol> <li>If your device cannot access the Internet, please click Download File.</li> <li>Choose Local Upgrade to upload the file for local upgrade.</li> </ol>
	Upgrade Now

#### 5.10.2 Local Upgrade

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: In Local Device mode, choose System > Upgrade > Local Upgrade

For other RAP models: Choose ( **WLAN > APs > Manage >**) **System > Upgrade > Local Upgrade** 

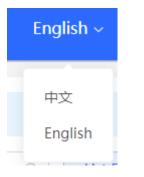
You can view the current software version, hardware version and device model. If you want to upgrade the device with the configuration retained, check **Keep** Setup. Click **Browse**, select an upgrade package on the local PC, and click **Upload** to upload the file. The device will be upgraded.

Online Upgrade	Local Upgrade
<i>i</i> Please do	not refresh the page or close the browser.
Model	RAP
Current Version	ReyeeOS 1.86.
Keep Config	<ul><li>(If the target version is much later than the current version, it is recommended not to keep the configuration.)</li></ul>
File Path	Please select a file. Browse Upload

## 5.11 Switching System Language

Choose English > in the upper right corner of the Web page.

Click a required language to switch the system language.



## 5.12 Configuring LED Status Control

#### 🛕 Caution

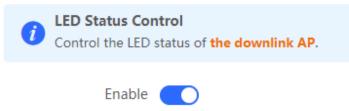
The LED Status Control function is not supported in the standalone mode (self-organizing network is not enabled).

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: Choose RAP6262 models: Choose

For other RAP models: Choose The WLAN > LED

Turn on the LED of all downlink access points in the network.





## 6 Network Diagnosis Tools

## 6.1 Network Check

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

(1) Click in the navigation bar, or choose **Diagnostics** > **Network Check** and go to the **Network Check** page.

					I	
Ruíjie   ®Rcycc	English 🗸 🛆 Ruijie Clo	id  🎇 Download App	A Network Setup	Network Check	尚 Alert	Default Password

(1) Click Start to perform the network check and show the result.

<i>i</i> Network Check Start	
i Network Check	
Recheck	
WAN/LAN Cable	
Auto-Negotiated Speed	
WAN Port	
LAN & WAN Address Conflict	
оор	
DHCP Server Conflict	
P Address Conflict	
Route	
Next Hop Connectivity	
DNS Server	
P Session Count	

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.	

### 6.2 Network Tools

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

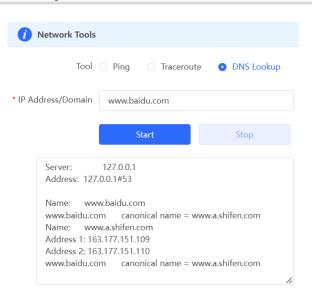
RAP6262 models: In Local Device mode, choose *Option Diagnostics > Network Tools* 

For other RAP models: Choose ( Twee Network Tools 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.

<i>i</i> Network Tools			i Network Tools	i	
Тоо	• Ping O Traceroute	O DNS Lookup	Tool	Ping • Traceroute	e 🔿 DNS Lookup
Туре	• IPv4 O 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
	Start	Stop	max, 46 byte	www.baidu.com (163.177.1 packets 11.1 (192.168.111.1) 0.621 (	
PING www.baidu.com (163.177.151.109): 64 data bytes 72 bytes from 163.177.151.109: seq=0 ttl=51 time=18.896 ms 72 bytes from 163.177.151.109: seq=1 ttl=51 time=18.686 ms 72 bytes from 163.177.151.109: seq=2 ttl=51 time=18.284 ms 72 bytes from 163.177.151.109: seq=3 ttl=51 time=20.310 ms		ms 2 172.20.74.1 (172.20.74.1) 2.271 ms 9.091 ms 8.565 ms 3 172.20.255.109 (172.20.255.109) 2.974 ms 6.424 ms 10.932 ms 4 * * * 5 172.22.0.249 (172.22.0.249) 1.902 ms 1.453 ms 1.081 ms 6 112.111.60.97 (112.111.60.97) 3.215 ms 3.290 ms 2.794 ms 7 218.104.229.69 (218.104.229.69) 2.890 ms 2.639 ms			



## 6.3 Alarms

For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

RAP6262 models: In Network mode, choose RAP6262 models: In Network > Alarms

For other RAP models: Choose ( **WLAN > APs > Manage >**) Oliagnostics > Alarms

The Alarms 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 type of alarm, you will not discover and process all alarms of this type promptly. Therefore, exercise caution when performing this operation.

Alert List						View Unfollowed Ale
xpand	Alerts		Sug	ggestion		Action
~	There is more the LAN network.	an one DHCP server ir	n the Ple	ase disable the extra DHC	P server in the LAN network.	Delete Unfollow
	Hostname	SN	Туре	Time	Details	Action
	Ruijie	1234567891234	EG210G-P	2022-04-24 09:39:08	A DHCP server conflict occurs in LAN network: MAC:58:69:6c:00:00:01,1 P:192.168.11.1,VLAN ID:233; MAC:UNKNOWN,IP:192 .168.112.1,VLAN ID:233	Delete

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

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

_		
	ОК	Cancel

Click **View Unfollowed Alarm** to view the unfollowed alarm. You can follow the alarm again in the pop-up window.

View Unfollowed Alert	×
There is more than one DHCP server in the LAN network.	
Re-follow	

## 6.4 Fault Collection

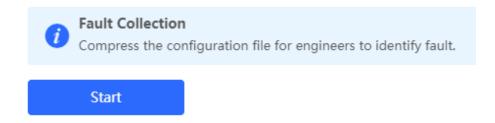
For RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G), RG-RAP6262(G), RG-RAP2260(H), RG-RAP6260(H), RG-RAP6260(H)-D, RG-RAP2266, RG-RAP2260, RG-RAP1261, RG-RAP1260 and RG-

Cancel

RAP6262 models: In Local Device mode, choose Oligonostics > Fault Collection

For RAP models: Choose ( WLAN > APs > Manage >) Clagnostics > 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.



# **7** FAQs

## 7.1 Login Failure

#### > What can I do when I failed to log in to the Eweb management system?

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.

## 7.2 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 Eweb management system using the default IP address (10.44.77.254).()

## 7.3 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 master router. Please check the configuration of the master 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.