



Ruijie Reyee Series Access Points

Web-Based Configuration Guide_R55

Copyright Statement

Ruijie Networks©2021

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

Exemption Statement

This document is provided “as is”. The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

Thank you for using our products.

Audience

This manual is intended for:

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

Obtaining Technical Assistance

- Ruijie Networks Website: <https://www.ruijienetworks.com/>
- Technical Support Website: <https://ruijienetworks.com/support>
- Case Portal: <https://caseportal.ruijienetworks.com>
- Community: <https://community.ruijienetworks.com>
- Technical Support Email: service_rj@ruijienetworks.com
- Skype: [service_rj@ruijienetworks.com](https://www.skype.com/people/service_rj@ruijienetworks.com)

Related Documents

Documents	Description
Command Reference	Describes the related configuration commands, including command modes, parameter descriptions, usage guides, and related examples.
Hardware Installation and Reference Guide	Describes the functional and physical features and provides the device installation steps, hardware troubleshooting, module technical specifications, and specifications and usage guidelines for cables and connectors.

Conventions

This manual uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in boldface .
<i>italic</i> font	Arguments for which you supply values are in <i>italics</i> .
[]	Elements in square brackets are optional.
{ x y z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

1 Overview

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

Web-based management involves a Web server and a Web client. The Web server is integrated in a device, and is used to receive and process requests from the client, and return processing results to the client. The Web client usually refers to a browser, such as Google Chrome IE, or Firefox.

1.1 Conventions

In this document, texts in bold are names of buttons (for example, **OK**) or other graphical user interface (GUI) elements (for example, **ARP List**).

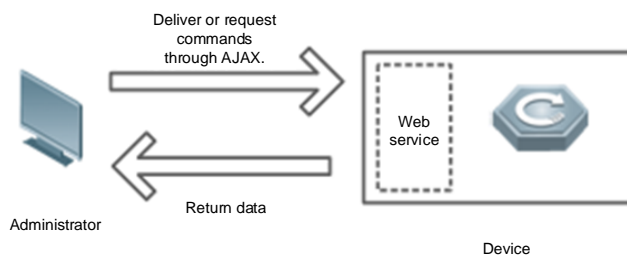
2 Configuration Guide

2.1 Preparation

Scenario

As shown in the figure below, an administrator can access the device from a browser and configure the device through the eWeb management system.

Figure 2-1-1 Data Exchange Principle



Remarks	The eWeb management system combines various device commands and then delivers them to the device through AJAX requests. The device then returns data based on the commands. A Web service is available on the device to process basic HTTP protocol requests.
----------------	---

Deployment

Configuration Environment Requirements

Client requirements:

- An administrator can log into the eWeb management system from a Web browser to manage devices. The client refers to a PC or some other mobile endpoints such as laptops or tablets.
- Google Chrome, Firefox, IE10.0 and later versions, and some Chromium-based browsers (such as 360 Extreme Explorer) are supported. Exceptions such as garble or format error may occur if an unsupported browser is used.
- 1024 x 768 or a higher resolution is recommended. If other resolutions are used, the page fonts and formats may not be aligned and the GUI is less artistic, or other exceptions may occur.
- The client IP address is set in the same LAN network as the device IP address, such as 192.168.110.X. The subnet mask is 255.255.255.0. Alternatively, you can set the IP assignment mode to **Obtain an IP address automatically** or enter **ruiyi.cn** into the address bar of the browser to access eWeb. The default gateway is device management address 192.168.110.1.

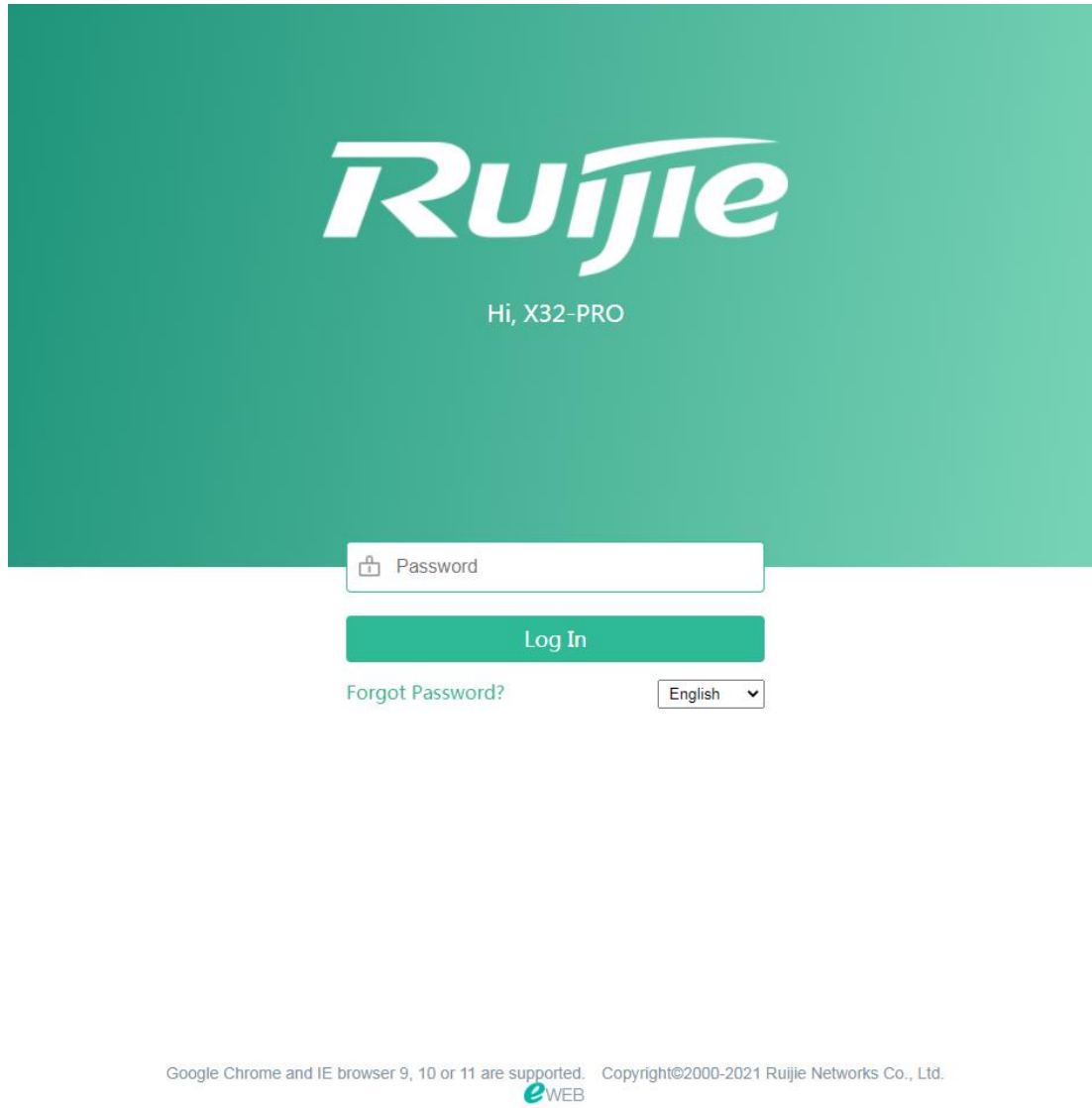
Server requirements:

- The device is enabled with Web service (enabled by default).

- The device is configured with a management IP address (Default: 192.168.110.1). You can enter <http://192.168.110.1> to access the eWeb management system.

To log into the eWeb management system, open the Google Chrome browser, and enter <http://192.168.110.1> into the address bar, and press **Enter**.

Figure 2-1-2 Login Page



Enter the password and click **Login**.

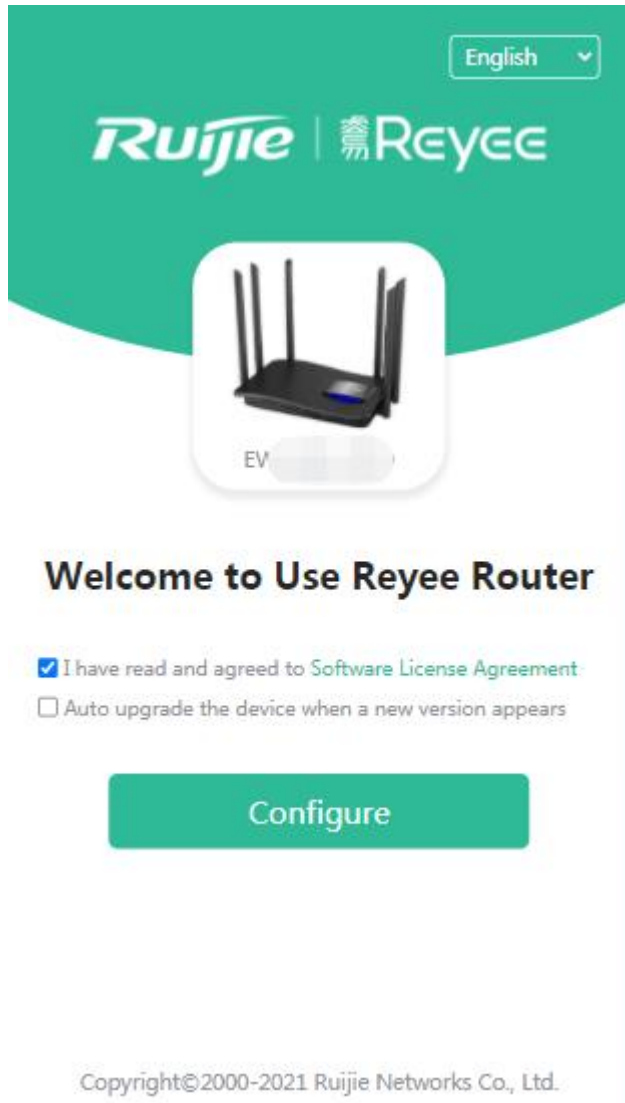
2.2 Wizard

You will enter the **Wizard** page without login at initial setup.

2.2.1 Welcome Page

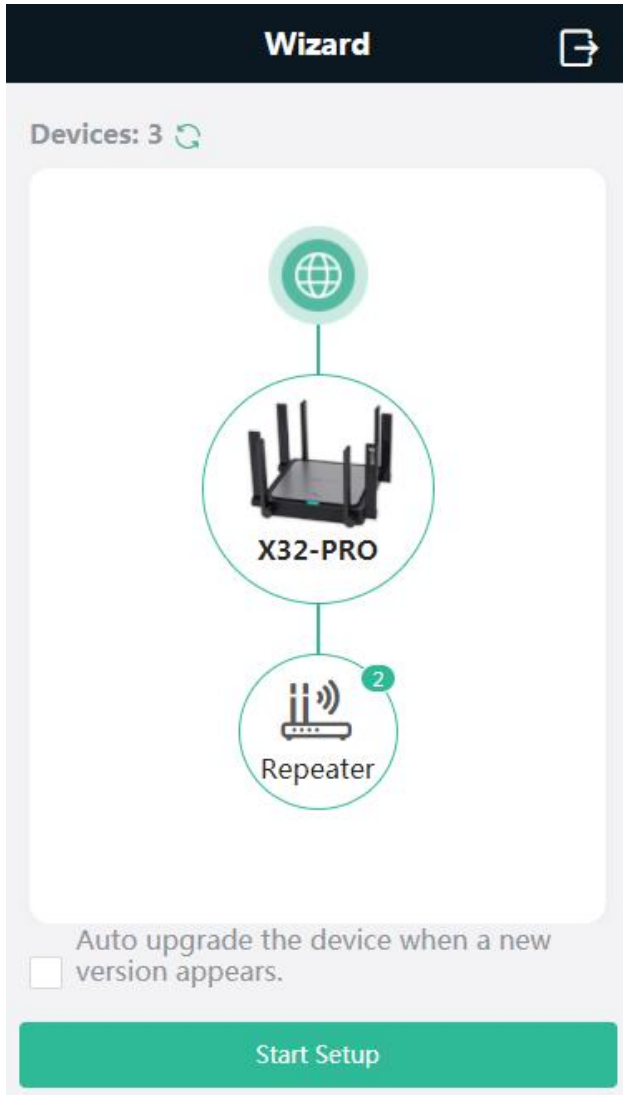
The welcome page will appear when you configure the device for the first time.

Figure 2-2-1 Welcome Page



The network status will be displayed when you configure the device for the second time.

Figure 2-2-2 Wizard Page




If the network are configured with repeaters, their number is displayed. (In the above figure, X32G-PRO is the primary router.)

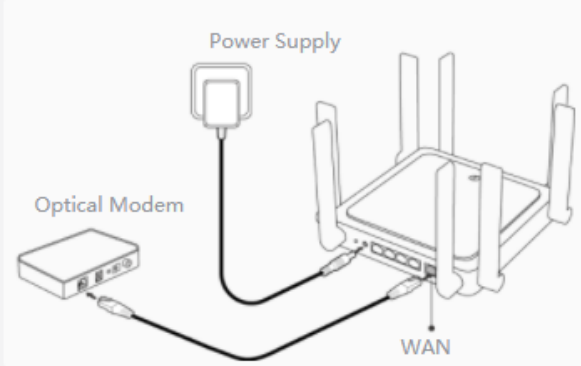
2.2.2 Network Settings

When the device is not connected via network cables, the following page is displayed.

Figure 2-2-3 Network Settings

Wizard 

ⓘ No cable is detected. Please plug in cables according to the diagram.



The diagram illustrates the correct cable connections for the router. An Optical Modem is connected to the WAN port of the router. A Power Supply is connected to the router's power input. A WAN cable is also connected to the WAN port. The router has several antennas on top.

Re-Check

If you want to extend your Wi-Fi range

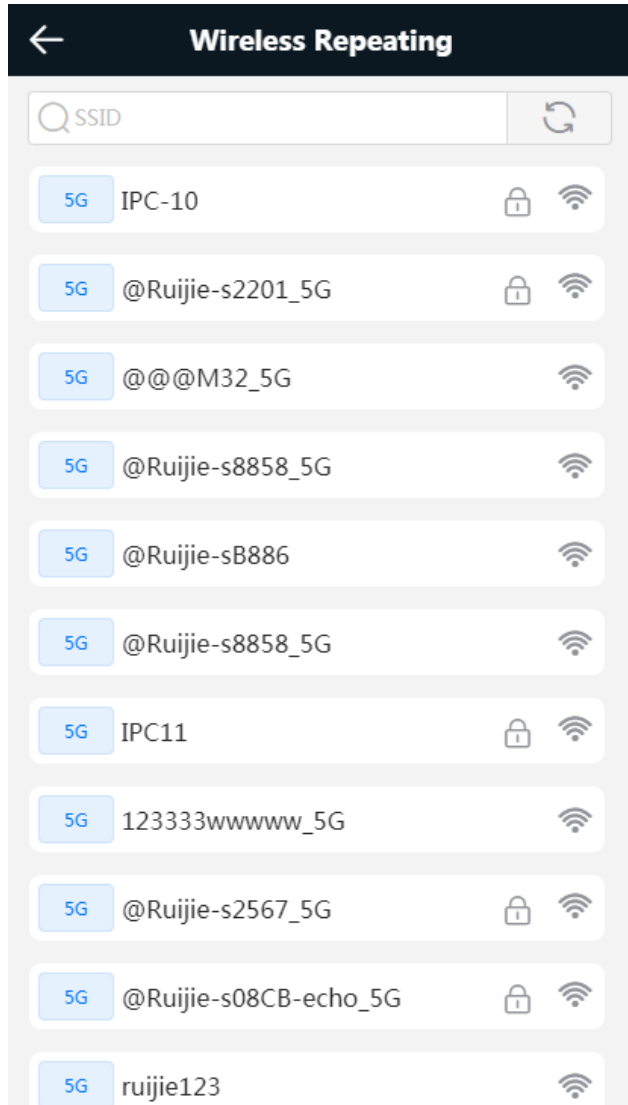
[Mesh Networking](#) [Wireless Repeater](#)

You can also "perform configuration without a cable"

2.2.2.1 Wireless Repeating

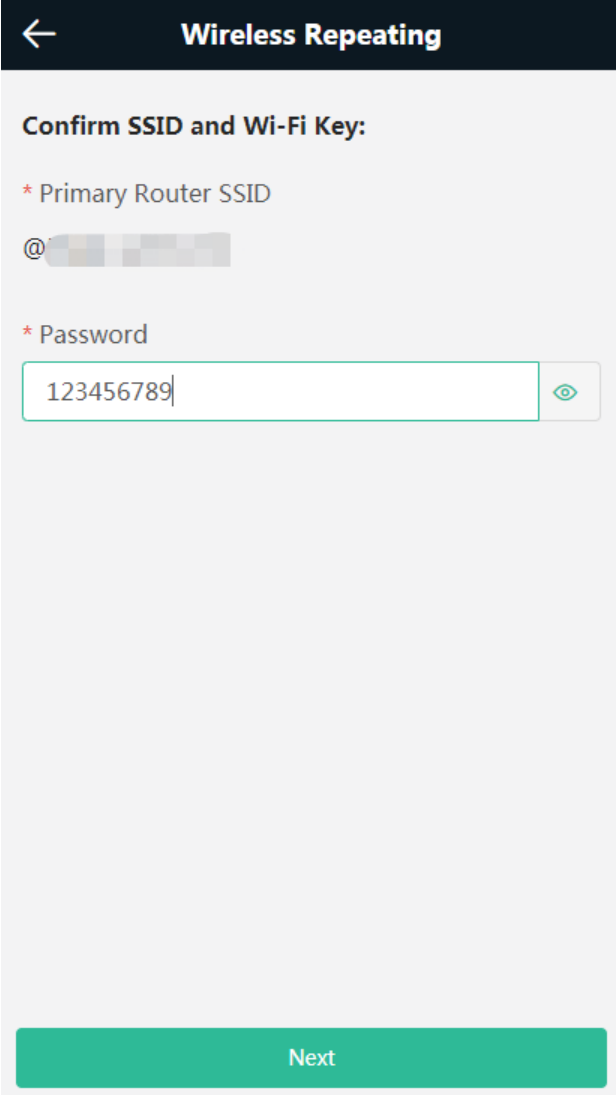
To scan nearby Wi-Fi, click **Wireless Repeating**.

Figure 2-2-7 Wi-Fi List



Select a Wi-Fi to be repeated.

Figure 2-2-8 Wireless Repeating 1



← **Wireless Repeating**

Confirm SSID and Wi-Fi Key:

* Primary Router SSID

@ [blurred SSID]

* Password

123456789

Next

Enter the Wi-Fi password of the primary router (This item will not be displayed if the primary router Wi-Fi is open).

Click **Next** to set the wireless information and management password of the device (This configuration applies to only new devices).

Figure 2-2-9 Wireless Repeating 2

Wireless Repeating

New SSID and Wi-Fi Key:

SSID (2.4G)
@Ruijie..._plus

* SSID (5G)
@Ruijie...lus_5G

* Wi-Fi Password Security
123456789

Management Password (Please remember the password.)

Same as Wi-Fi Password

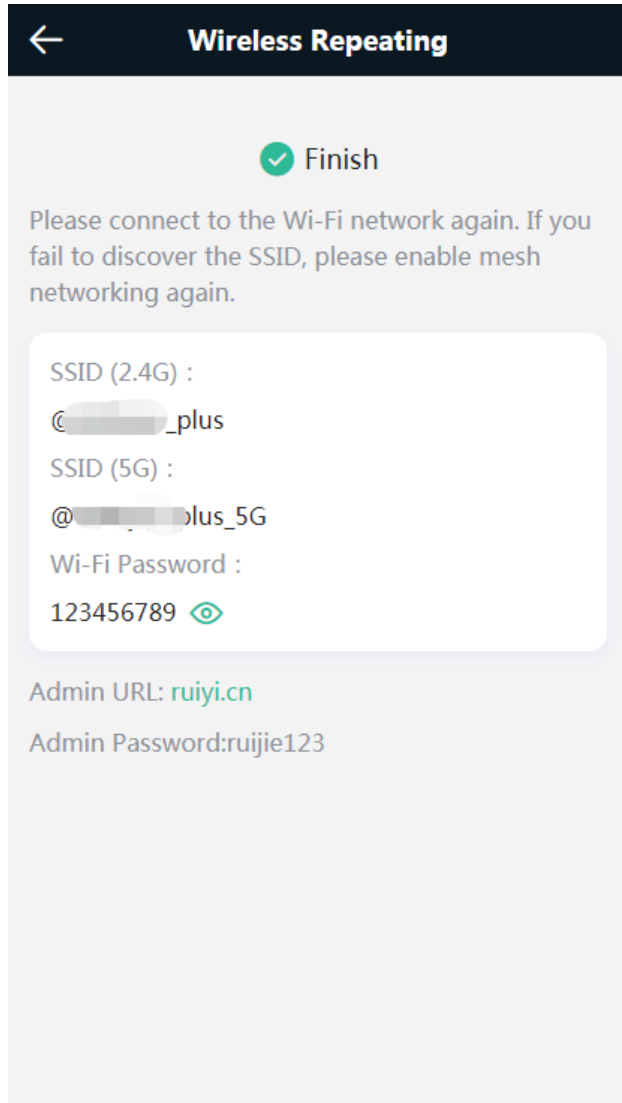
* Management Password
.....

Medium

Next

Click **Next** to complete the configuration.

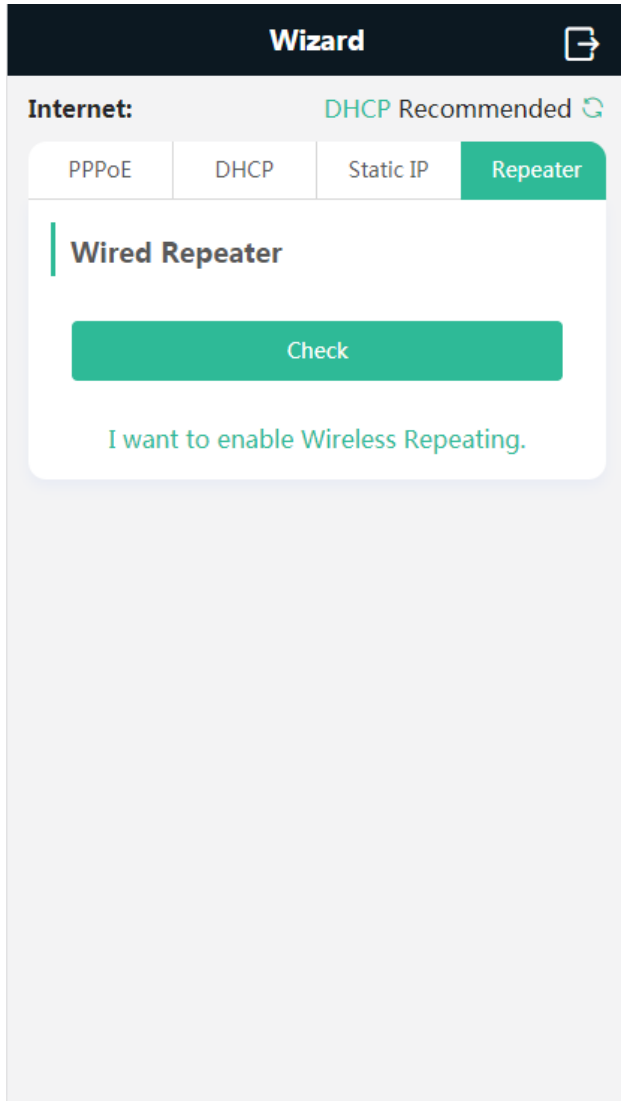
Figure 2-2-10 Completing Wireless Repeating Configuration



2.2.2.2 Wired Repeating

When the device is connected via network cables, the wired repeater can be configured. (This option is ready for new devices only).

Figure 2-2-11 Wired Repeating



Click **Check**, and enter the local router SSID, password and management password.

Click **Save** to complete the configuration.

Figure 2-2-12 Wired Repeater Page

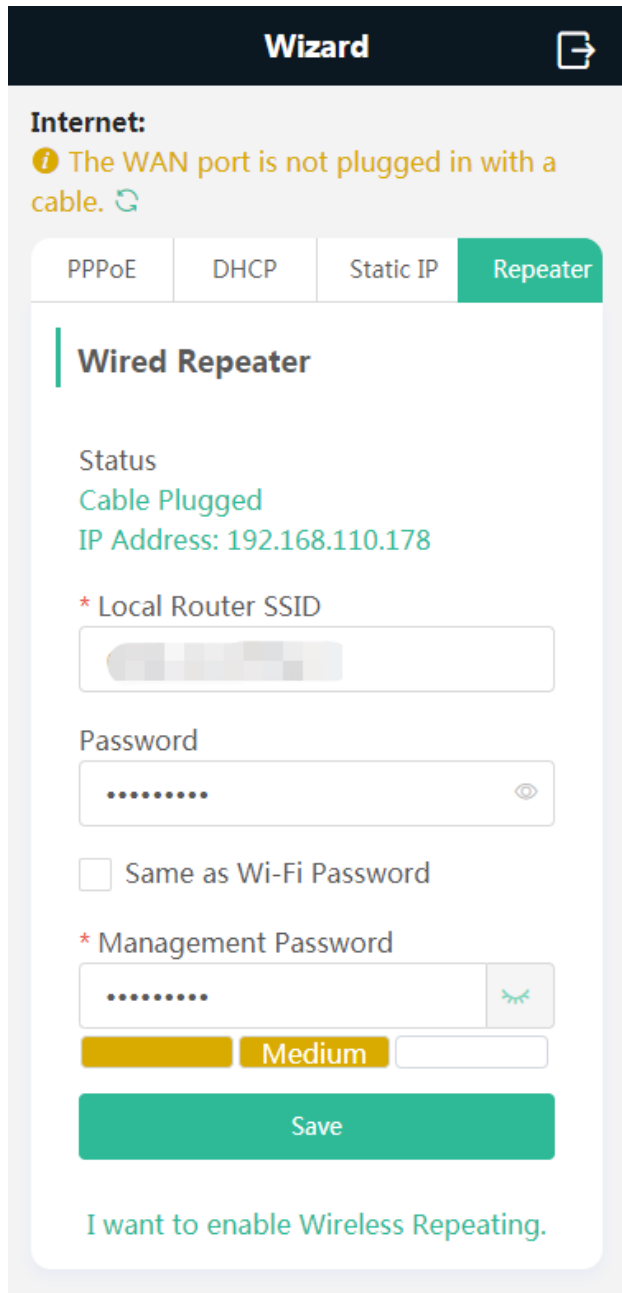
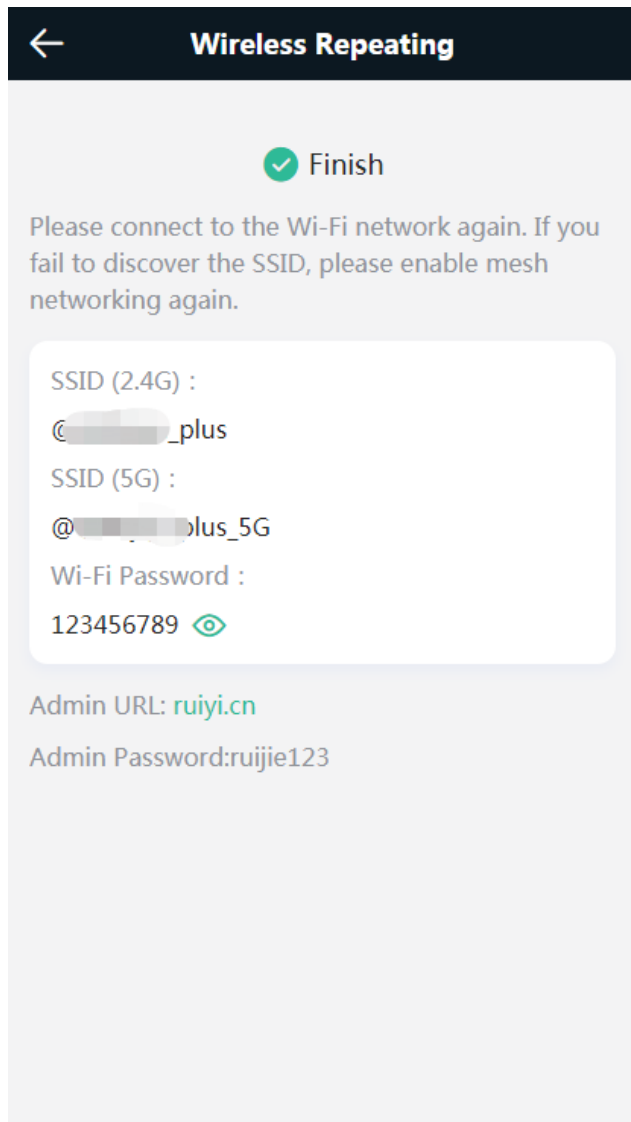


Figure 2-2-13 Completing Configuration

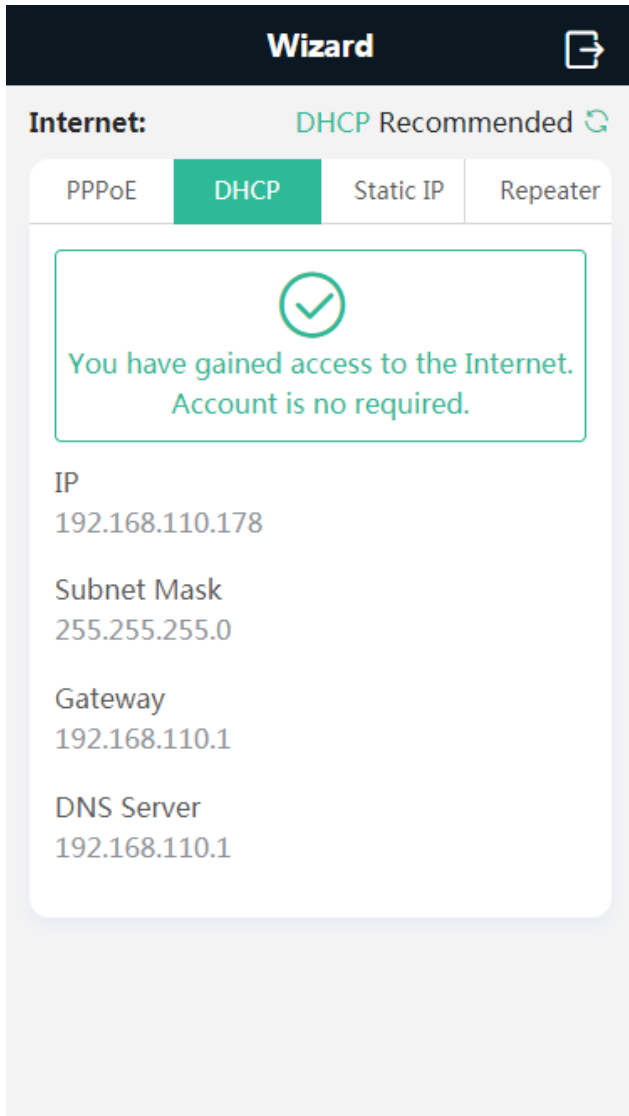


2.2.2.3 Internet

When the device is not configured with the repeating configuration, you can access the Internet through the following means:

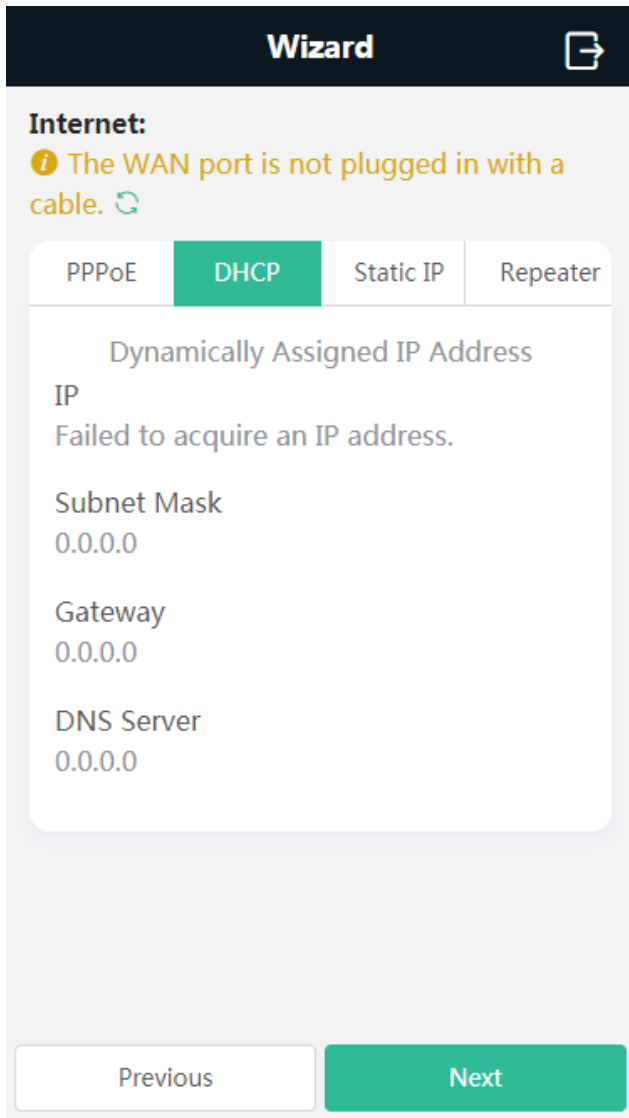
If the device fails to access the Internet, the system will check IP assignment automatically. It is recommended to select DHCP.

Figure 2-2-14 Normal Connection



If the device is not plugged in with a network cable, click **Next**.

Figure 2-2-15 DHCP



If you select PPPoE, please enter the PPPoE account provided by the ISP.

Figure 2-2-16 PPPoE

Wizard

Internet: DHCP Recommended

PPPoE | DHCP | Static IP | Repeater

* Username Provided by ISP

Please enter a PPPoE username.

* Password Obtain Account from Old Device

Password

Previous Next

If you select the static IP address, enter the IP address, Subnet Mask, Gateway IP and DNS Server as below.

Figure 2-2-17 Static IP

Wizard

Internet: DHCP Recommended

PPPoE | DHCP | **Static IP** | Repeater

* IP
192.168.110.178

* Subnet Mask
255.255.255.0

* Gateway
192.168.110.1

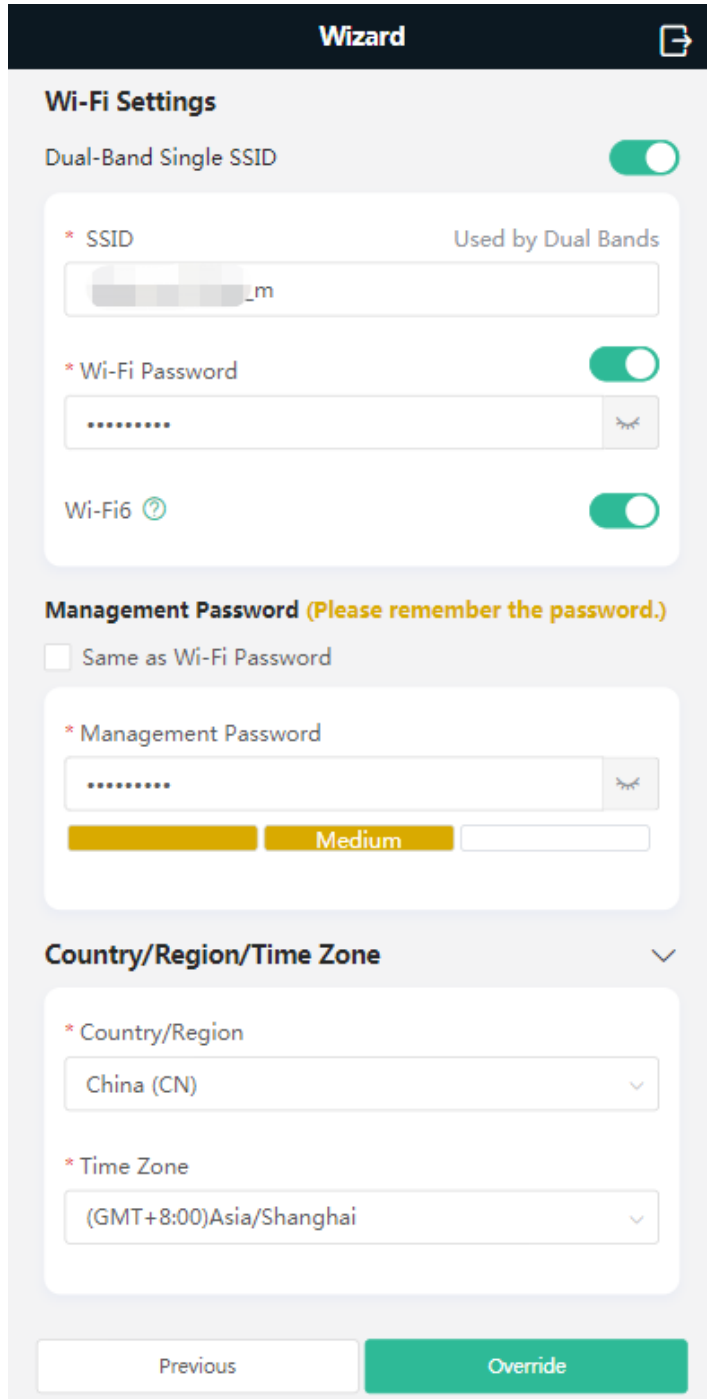
* DNS Server
192.168.110.1

Previous | **Next**

2.2.3 WiFi Settings

This module allows you to configure the SSID, WiFi password and management password.

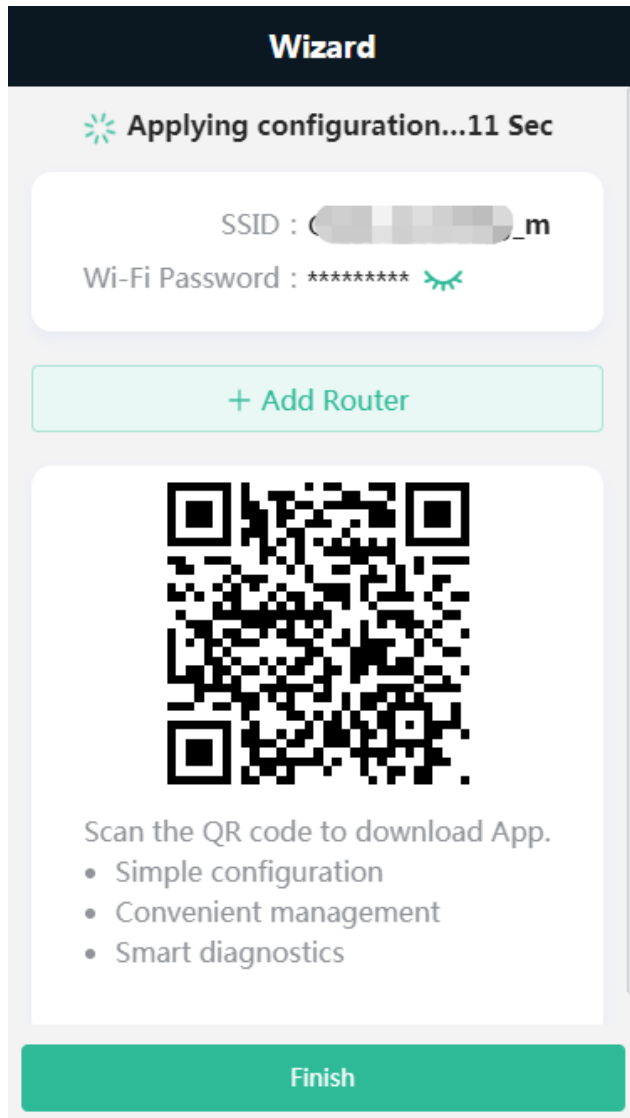
Figure 2-2-18 WiFi Settings



2.2.4 Finish

After the configuration is delivered, click **Finish** to enter the homepage.

Figure 2-2-19 Finish



Note: For a new device which is configured via a mobile client, the automatically pop-up page does not display **Finish**.

Click **Add Router**.

Figure 2-2-20 Add Router

Wizard

You can set up a seamless roaming network without cables by mesh networking.

1 Place the second router 2 meters away from the first router and power on the second router.

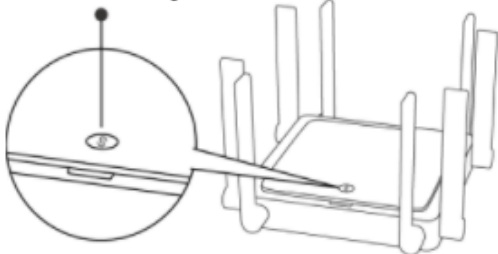
The system LED of the second router starts to blink. Wait for 2 to 3 minutes until the LED turns solid on.

2 Press the Mesh Networking button on the first router.

The mesh networking LED on both routers blinks green slowly for about 2 minutes. When both LEDs stop blinking and turn solid green, mesh networking succeeds.

Diagram:


Mesh Networking Button



3 Place the second router where you want to have Wi-Fi coverage and then power on the router.

Wait for 3 to 5 minutes until the mesh networking LED turns solid on. The second router will stop broadcasting SSID @Ruijie-sXXXX. You can access the Internet by connecting to the new Wi-Fi network.

Diagram:



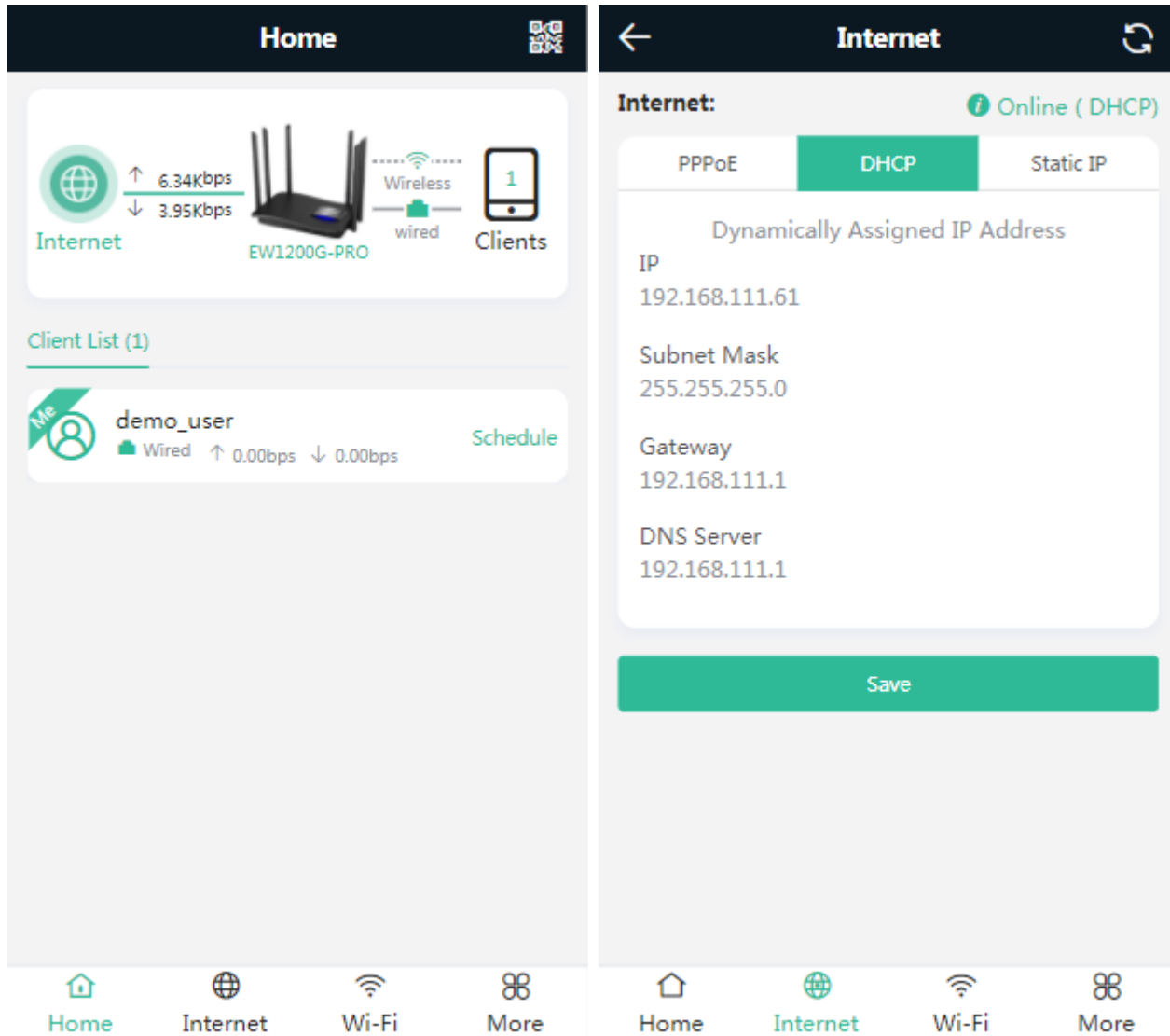
Finish

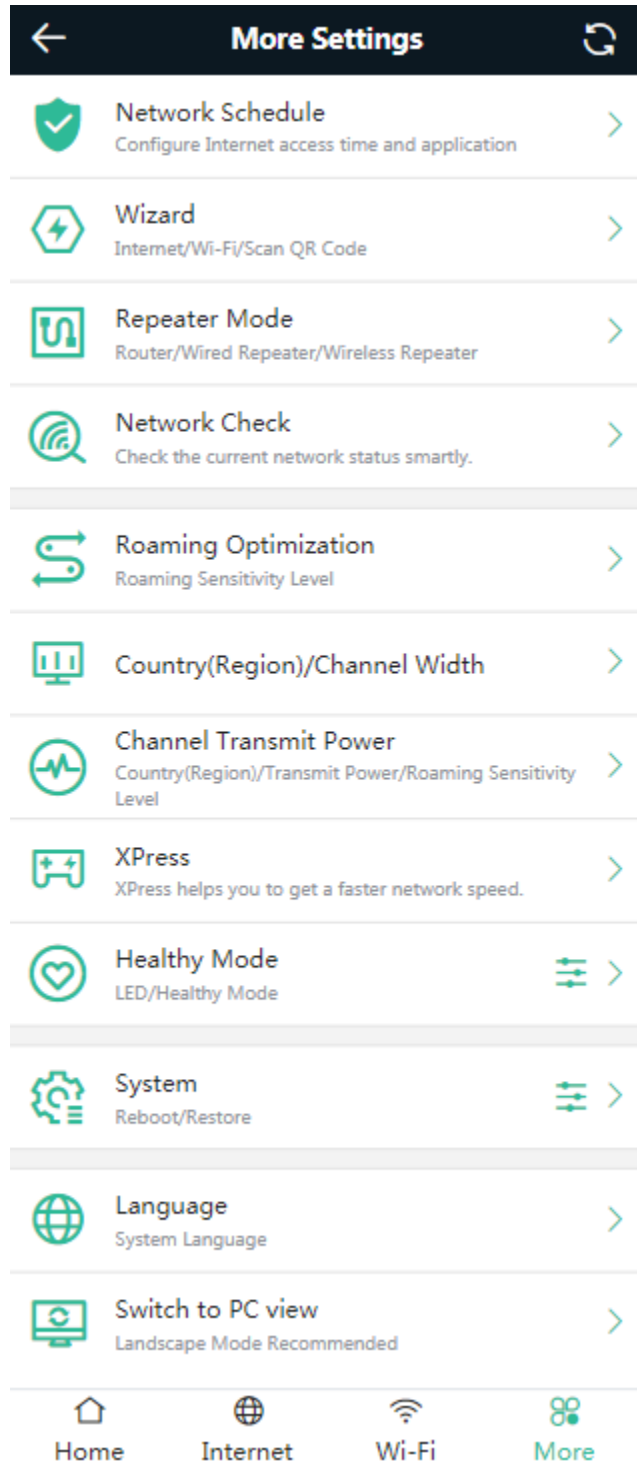
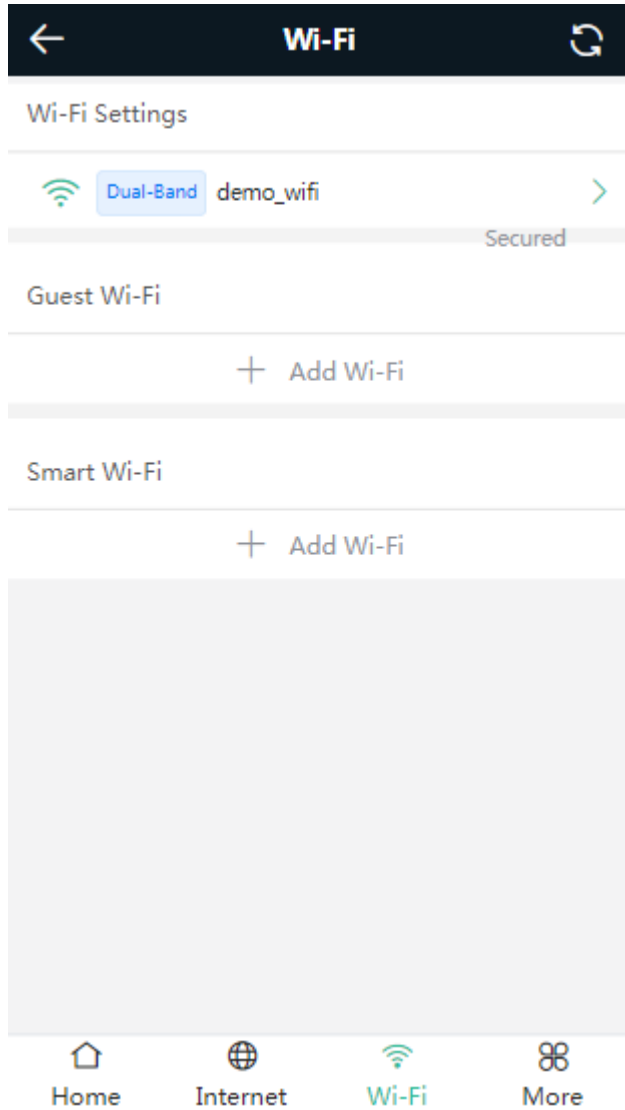
2.3 GUI

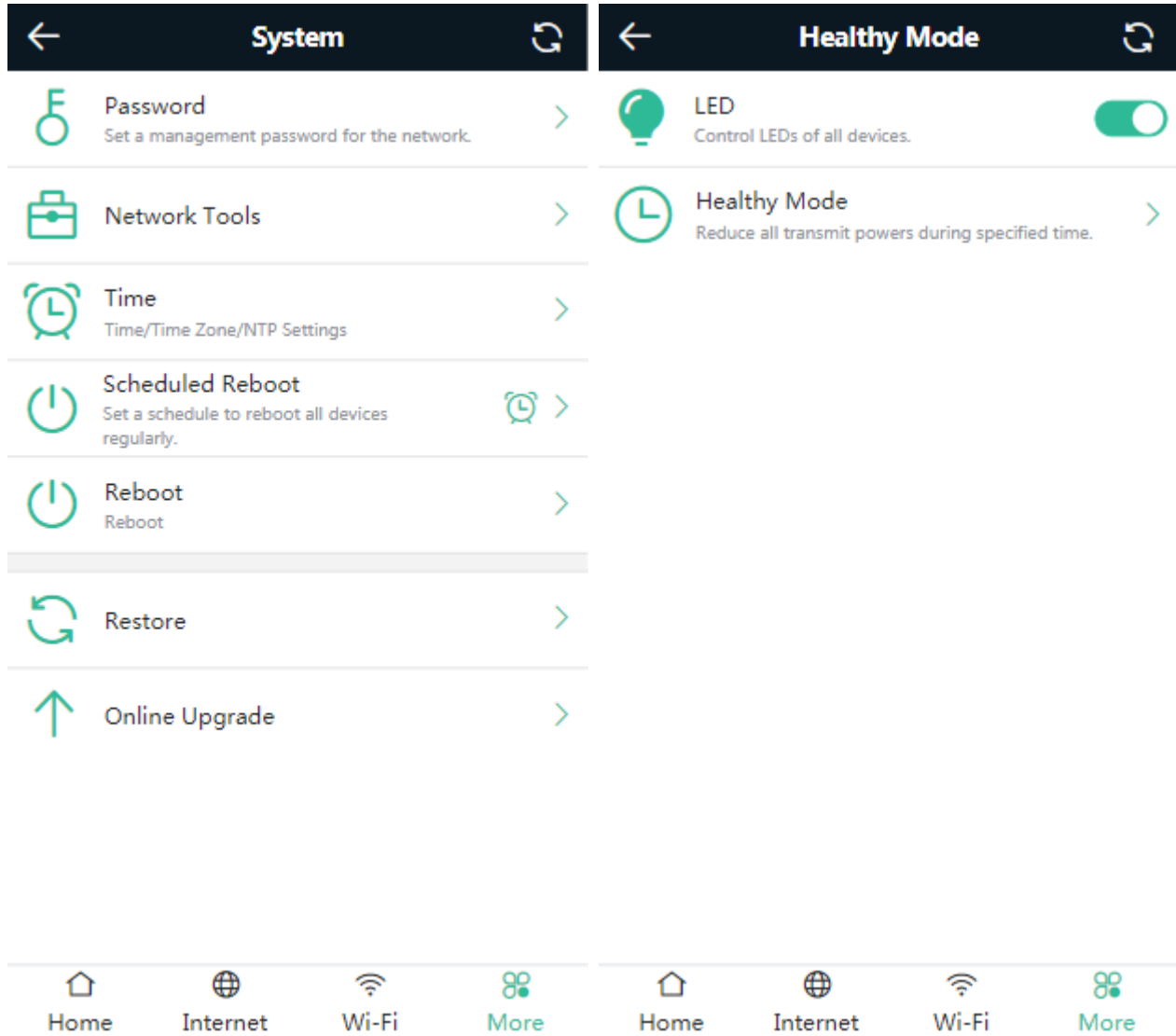
2.3.1 Phone-Based GUI

The system switches between the phone-based GUI and PC-based GUI according to the screen width and browser type. The phone-based GUI is more concise.

Figure 2-3-1 Phone-Based GUI







2.3.2 PC-Based GUI

Click **Pro** in the upper right corner of phone-based GUI to switch over to the PC-based GUI. The PC-based GUI provides more configuration items. For details, see [eWeb Configuration](#).

Figure 2-3-2 PC-Based GUI

 Home  Clients  Internet  Wi-Fi  More English   

 Internet ↑ 7.22Kbps ↓ 7.38Kbps  EW1200G-PRO Wireless wired  Clients



Device Details





Model: EW [redacted] Hostname: [redacted] [?](#)
SN: G1 [redacted] MAC: 00:74: [redacted]
Duration: 5 hours 6 minutes 18 seconds Systemtime: 2021-07-15 20:54:16
Hardware Ver: 1.00 Software Ver: ReyeeO [redacted]

Wi-Fi

 Primary Wi-Fi: demo_wifi  Guest Wi-Fi: Security: Yes Security: No

Interface Details

 Connected  Disconnected

 WAN  LAN3  LAN2  LAN1

192.168.111.61 192.168.110.1

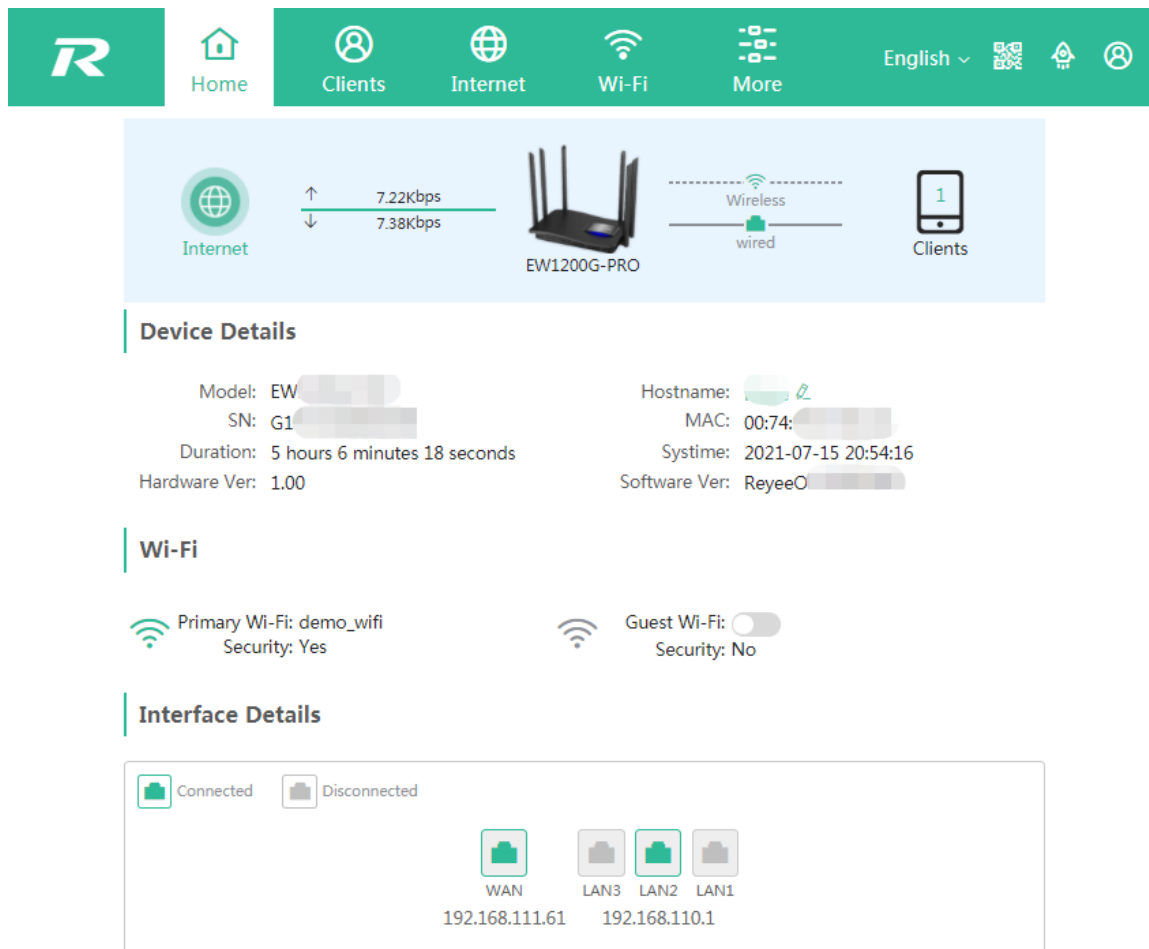
3 eWeb Configuration

This chapter introduces the features on the PC-based GUI.

3.1 Overview

The **Overview** page displays the device details, WiFi and interface details.

Figure 3-1 Overview



3.2 Clients

The **Clients** module allows you to bind the static IP, manage blocked time and block WLAN clients.

Figure 3-2-1 Online Clients

Clients

The client list includes online clients and blocked clients. The client going offline will not disappear immediately. Instead, the client will stay in the list for three more minutes.

Clients

Search by IP/MAC/Username Refresh Blocked Time Management Blocked WLAN Clients Management

Username/Type	IP/MAC	Current Rate	Blocked Time	Action
R12225 Wired	192.168.111.127 54:bf:64:5c:dc:49	Up:2.48Kbps Down:3.48Kbps	Not Set (No time is blocked.) + Add Blocked Time	Wired Client
MI9-Mr 5G	192.168.111.251 a8:9c:ed:92:6f:e2	Up:5.73Kbps Down:4.31Kbps	Not Set (No time is blocked.) + Add Blocked Time	Block
- 5G	0.0.0.0 62:ee:b7:96:cf:b6	Up:0.00bps Down:0.00bps	Not Set (No time is blocked.) + Add Blocked Time	Block
- Blocked	06:64:9C:87:6D:A 5	--	Failed to access the Internet.	Unblock

1 / 10/page Total 4

Blocked Time Management

Figure 3-2-2 Blocked Time Management

Blocked Time Management

Blocked Time List + Add Delete Selected

Set a time to prevent clients accessing the Internet. Up to 32 entries can be added.

<input type="checkbox"/>	Blocked Time	Blocked MAC	Remark	Action
<input type="checkbox"/>	23:34-23:59 Sunday	c8:5b:76:94:00:3c	R03605_mewe b	Edit Delete
<input type="checkbox"/>	00:00-23:59 Saturday Sunday	70:3c:69:9f:88:e7	X_meweb	Edit Delete

1 / 10/page Total 2

Add Rule

Figure 3-2-3 Add Rule

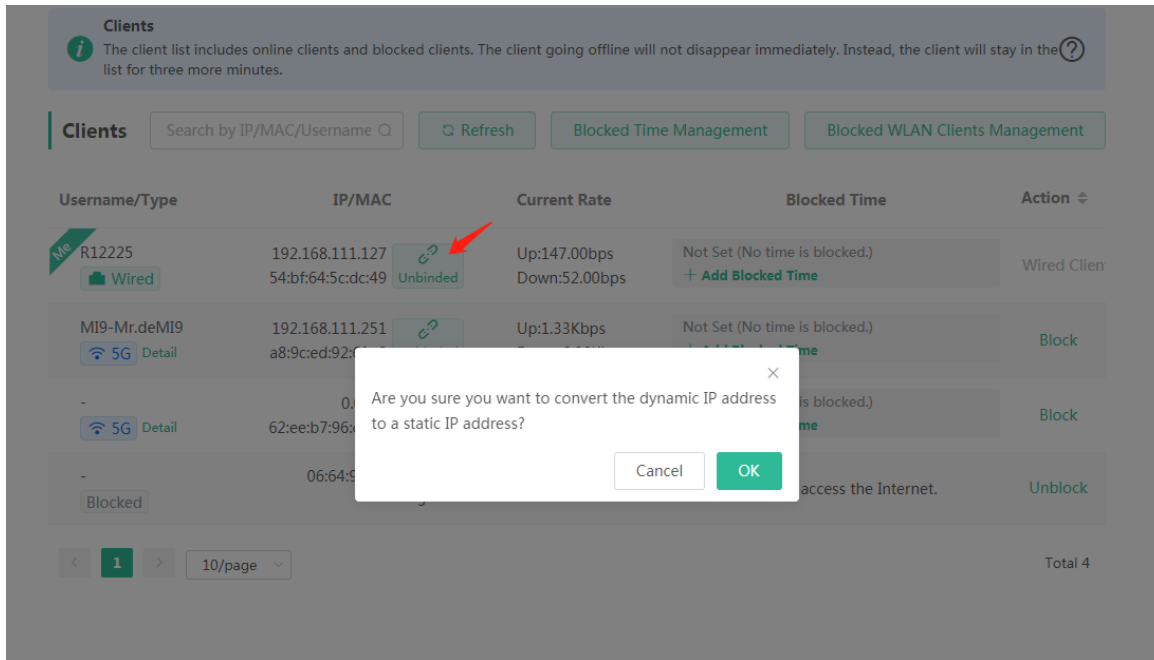
Add Rule



Blocked Time	<input type="text" value="Custom"/>
* Date	<input type="text" value="Please Select Day"/>
* Time	<input type="text" value="🕒 17:59"/> - <input type="text" value="🕒 18:59"/>
* Blocked MAC	<input type="text" value="Enter a MAC address."/>
Remark	<input type="text" value="Enter the ACL purpose."/>

Bind the Static IP Address

Figure 3-2-4 Bind Static IP Address

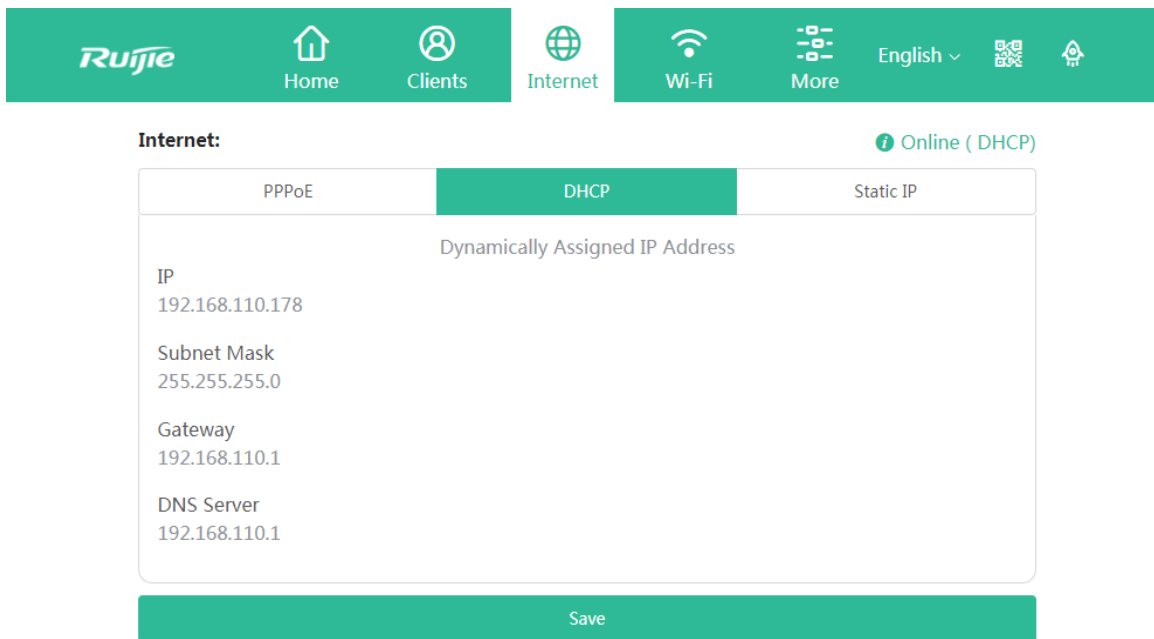


You can convert a dynamic IP address to a static IP address by clicking **Unbinded**. In the displayed dialog box, configure settings and click **OK**.

3.3 Internet

The **Internet** module allows you to select an IP assignment mode.

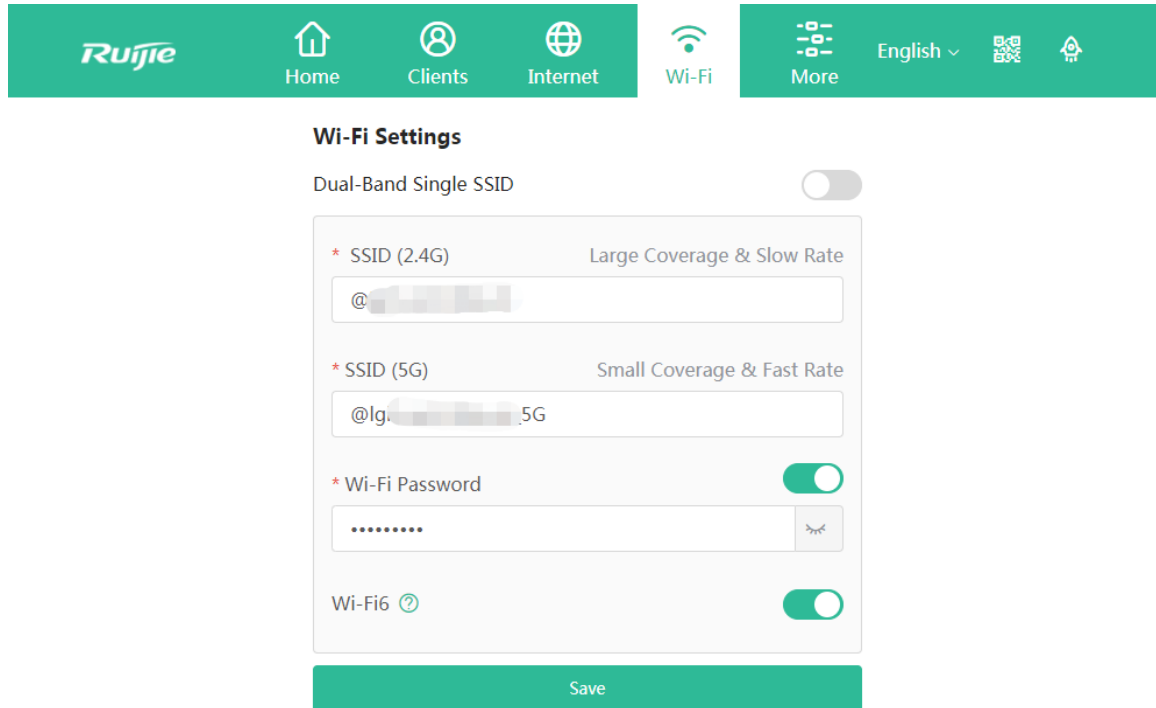
Figure 3-3-1 Internet



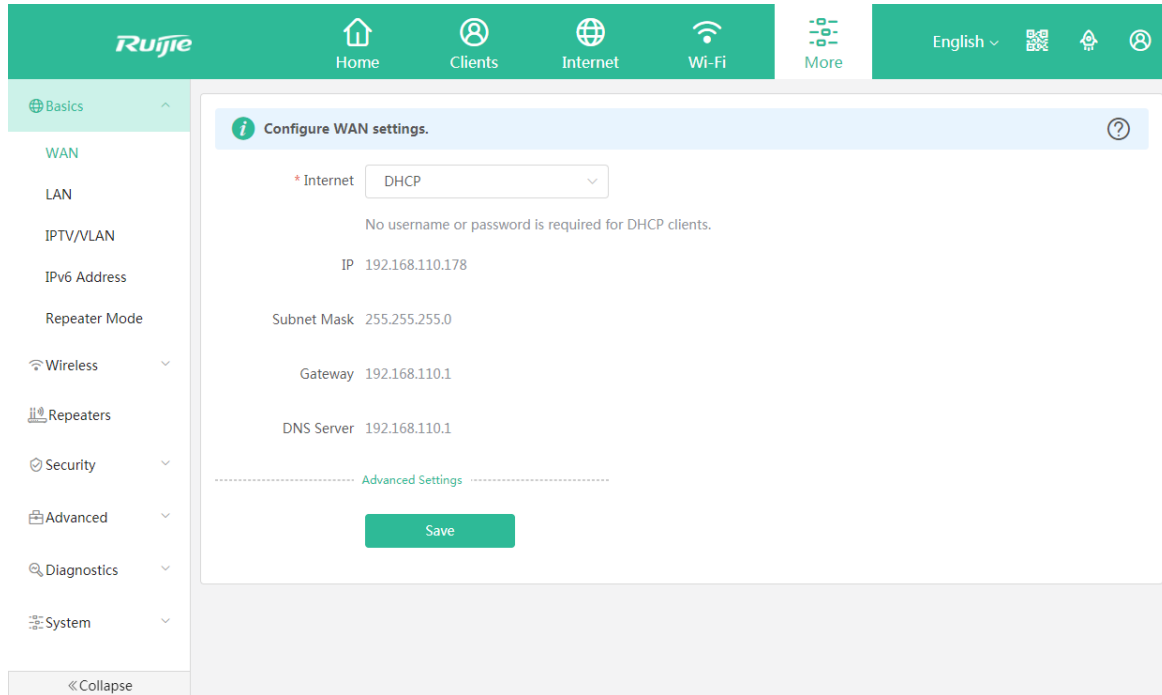
3.4 WiFi

The WiFi module allows you to configure WiFi settings.

Figure 3-4-1 WiFi Settings



3.5 More



3.5.1 Basics

3.5.1.1 WAN

The **WAN** module allows you to configure WAN settings. There are three IP assignment modes available: **Static IP Address**, **DHCP** and **PPPoE**.

Figure 3-5-1 WAN Settings

Configure WAN settings.
?

* Internet DHCP

No username or password is required for DHCP clients.

IP 192.168.110.178

Subnet Mask 255.255.255.0

Gateway 192.168.110.1

DNS Server 192.168.110.1

----- Advanced Settings -----

* MTU 1500

* MAC c0:b8:e6:fe:cd:4c

802.1Q Tag

Save



3.5.1.2 LAN

The LAN module contains LAN Settings, DHCP Clients, Static IP Addresses and DNS Proxy.

3.5.1.2.1 LAN Settings

The LAN module allows you to set the IP address of the LAN port and DHCP status.

Figure 3-5-2 LAN Settings

 LAN Settings 

* IP

* Subnet Mask

Remark

* MAC

DHCP Server

* Start

* IP Count

* Lease Time(Min)

3.5.1.2.2 DHCP Clients

The **DHCP Clients** page displays DHCP clients.

Figure 3-5-3 DHCP Clients

View DHCP clients.

DHCP Clients

Up to **300** IP-MAC bindings can be added.

<input type="checkbox"/>	No.	Hostname	IP	MAC	Remaining Lease Time(Min)	Status
<input type="checkbox"/>	1	EW1200G-PRO-876DAA	192.168.111.61	00:74:9c:87:6d:aa	23	Convert to Static IP
<input type="checkbox"/>	2	EW1200-96CFB3	192.168.111.94	64:ee:b7:96:cf:b3	30	Convert to Static IP
<input type="checkbox"/>	3	R12225	192.168.111.127	54:bf:64:5c:dc:49	29	Convert to Static IP

< 1 >

Total 3

Click **Convert to Static IP** in the **Action** column to convert a DHCP-assigned IP address to a static IP address. Alternatively, select DHCP-assigned IP addresses and click **Batch Convert** to convert more than one IP address.

3.5.1.2.3 Static IP Addresses

The **Static IP Addresses** module allows you to add, delete and edit static IP addresses.

Figure 3-5-4 Static IP Addresses

Static IP Address List

Static IP Address List

Up to **300** entries can be added.

<input type="checkbox"/>	No.	IP	MAC	Action
<input type="checkbox"/>	1	192.168.111.220	70:3c:69:9f:88:e7	Edit Delete

< 1 >

Total 1

Click **Add** to add a static IP address manually. In the displayed dialog box, configure settings and click **OK**.

Figure 3-5-5 Add Static IP Address

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. It contains two required input fields:

- * IP: A text input field containing the example "Example: 1.1.1.1".
- * MAC: A text input field containing the example "Example: 00:11:22:33:44:55".

 At the bottom right of the dialog, there are two buttons: "Cancel" and "OK".

3.5.1.2.4 DNS Proxy

The **DNS Proxy** module allows you to configure DNS proxy settings.

Figure 3-5-6 DNS Proxy

The screenshot displays the DNS Proxy configuration interface. At the top, there is a light blue information banner with an 'i' icon and a question mark icon, containing the text: "DNS proxy is not required. The device will obtain the DNS server address from the uplink device by default." Below the banner, there is an "Enable" label next to a green toggle switch that is currently turned on. Underneath, there is a required input field labeled "* DNS Server" with the placeholder text "Please enter a DNS server address." At the bottom of the configuration area, there is a green "Save" button.

3.5.1.1 IPTV/VLAN

The **IPTV/VLAN Settings** module allows you to configure IPTV/VLAN settings.

Figure 3-5-7 IPTV/VLAN

i IPTV/VLAN settings.

IPTV/VLAN

* Mode

* LAN1

* LAN2

* LAN3

Internet VLAN 802.1Q Tag

3.5.1.2 IPv6 Address

The **WAN Settings** module allows you to configure WANv6 settings.

Figure 3-5-7 IPv6 Address

IPv6 Address

- 1. When IPv6 is enabled, the MTU of IPv4 WAN port must be greater than 1280.
- 2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to UNTAG and set the other VLANs to Not Join.

Enable

WAN Settings LAN Settings DHCPv6 Clients

WAN_V6

* Internet

No username or password is required for DHCP clients.

IPv6 Address

IPv6 Prefix

Gateway

DNS Server

NAT66

The **LAN Settings** module allows you to configure LANv6 settings.

Figure 3-5-8 LAN Settings

IPv6 Address

- 1. When IPv6 is enabled, the MTU of IPv4 WAN port must be greater than 1280.
- 2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to UNTAG and set the other VLANs to Not Join.

Enable

WAN Settings LAN Settings DHCPv6 Clients

IPv6 Assignment Auto ?

IPv6 Address/Prefix 0:0::2

Length

Advanced Settings

Subnet Prefix Name Default ?

Subnet Prefix Length 64 ?

Subnet ID 0 ?

* Lease Time(Min) 30 ?

DNS Server Example: 0:0::2, each separated by a comma.

Save

The **DHCPv6 Clients** module allows you to configure DHCPv6 clients.

Figure 3-5-9 DHCPv6 Clients

IPv6 Address

- 1. When IPv6 is enabled, the MTU of IPv4 WAN port must be greater than 1280.
- 2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to UNTAG and set the other VLANs to Not Join.

Enable

WAN Settings LAN Settings DHCPv6 Clients

DHCPv6 Clients
You can view the DHCPv6 clients information on this page.

DHCPv6 Clients

Search by DUID

No.	Hostname	IPv6 Address	Remaining Lease Time(Min)	DUID
-----	----------	--------------	---------------------------	------

No Data

< **1** > 10/page

Total 0

3.5.1.3 Repeater

The **Repeater** module displays the current mode and the other available modes.

Figure 3-5-10 Router Mode

The device is working in **Router** mode. The following three modes are available:

Router Wired Repeater Wireless Repeater

Switch the device over to the wired repeater mode.

Figure 3-5-11 Wired Repeater

The device is working in **Router** mode. The following three modes are available:

Router **Wired Repeater** Wireless Repeater

i This mode allows you to establish a wired connection between a primary router and a secondary router, extending network coverage.
Cable Connection: Please connect the WAN port of the local router to the LAN port of the primary router.

Wired Repeater

Status **Cable Plugged**
IP Address: 192.168.110.178

* Local Router SSID

Password

Switch the device over to the wireless repeater mode.

Figure 3-5-12 Wireless Repeater

The device is working in **Router** mode. The following three modes are available:

Router Wired Repeater **Wireless Repeater**

i

- This mode allows you to establish a wireless connection between a primary router and a secondary router, extending network coverage.
- The local router will work as a secondary router.
- It is recommended to select a 5G Wi-Fi of the primary router.

Please unplug the cable to avoid loops.

Wireless Repeater

* Primary Router SSID

Select a target Wi-Fi.

Figure 3-5-13 Wi-Fi List



5G Wi-Fi List Select a target Wi-Fi.

Q SSID 5G Re-scan

SSID	BSSSID	Security	Channel	RSSI
IPC-10	c0:b8:e6:88:34:6e	WPA2PSK	44	-34 dBm High
@@@你好 _TPYY_5G_plus_5 G	02:d0:f6:15:39:59	OPEN	48	-41 dBm High
@Ruijie- s2201_5G	32:0d:9e:97:22:03	WPA2PSK	52	-42 dBm High
@Ruijie- s8858_5G	02:88:88:98:88:5a	OPEN	48	-43 dBm High
@@@你好	80:8f:1d:18:71:26	WPA2PSK	48	-45 dBm

Set a new Wi-Fi password (optional).

Figure 3-5-14 Wi-Fi Password

The device is working in **Router** mode. The following three modes are available:

Router Wired Repeater **Wireless Repeater**

i

- This mode allows you to establish a wireless connection between a primary router and a secondary router, extending network coverage.
- The local router will work as a secondary router.
- It is recommended to select a 5G Wi-Fi of the primary router.

Please unplug the cable to avoid loops.

Wireless Repeater

* Primary Router SSID **IPC-10**

* Password

Local Router Wi-Fi **New Wi-Fi**
 Same as Primary Router Wi-Fi

* SSID(2.4G)

* SSID(5G)

Password


3.5.2 Wireless

3.5.2.1 WiFi

3.5.2.1.1 WiFi Settings

The **WiFi Settings** module allows you to configure the primary WiFi.

Figure 3-5-15 WiFi Settings

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



Wi-Fi Settings

Dual-Band Single (The 2.4G and 5G bands use the same SSID.)

SSID

* SSID

Security

* Wi-Fi Password 

[Collapse](#)

Wireless Schedule

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

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

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

XPress (The client will experience faster speed.)

Wi-Fi6 (802.11ax High-Speed Wireless Connectivity.) 


3.5.2.1.2 Guest WiFi

The guest WiFi is disabled by default. You can enable guest WiFi on this page or homepage.

AP isolation is enabled by default and cannot be edited.

Set a schedule, and the guest WiFi will be enabled only during this period time. When the time expires, the guest WiFi will be disabled.

Figure 3-5-16 Guest WiFi

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




Guest Wi-Fi

Enable

Save

Enable the guest Wi-Fi.

Figure 3-5-17 Enable Guest WiFi

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



Guest Wi-Fi

Enable

Dual-Band Single (The 2.4G and 5G bands use the same SSID.)

SSID

* SSID

Security

[Collapse](#)

Wireless Schedule

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

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

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

XPress (The client will experience faster speed.)



Wi-Fi6 (802.11ax High-Speed Wireless Connectivity.) 

Save

3.5.2.1.3 Smart WiFi

The Smart WiFi module allows to configure the smart WiFi.

Figure 3-5-18 Smart WiFi

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

Smart Wi-Fi

Enable

Dual-Band Single (The 2.4G and 5G bands use the same SSID.)

SSID

* SSID(2.4G)

* SSID(5G)

Security

----- Collapse -----

Wireless Schedule

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

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

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



XPress (The client will experience faster speed.)

Wi-Fi6 (802.11ax High-Speed Wireless Connectivity.) 

3.5.2.1.4 Healthy Mode

The **Healthy Mode** module allows you to enable health mode and set a schedule.

Figure 3-5-19 Healthy Mode

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

Healthy Mode

Enable

Wireless Schedule

* Date

* Time +

3.5.2.2 Blocked Clients

The **Blocked Clients** module allows you to add, edit or delete blocked clients.

Click **Delete** in the **Action** column to delete a blocked client. Alternatively, select target clients and click **Delete Selected** to delete more than one blocked clients.

Figure 3-5-20 Blocked Clients

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

Blocked WLAN Clients

Up to 64 members can be added.

<input type="checkbox"/>	MAC	Remark	Action
<input type="checkbox"/>	06:64:9C:87:6D:A5	-	Edit Delete
<input type="checkbox"/>	62:EE:B7:96:CF:B5	ZGB	Edit Delete

< **1** > Total 2

Click **Add** to add a blocked Clients. In the displayed dialog box, configure settings and click **OK**.

Figure 3-5-21 Add Blocked Client

Add ×

* MAC

Remark

The **Allowed WLAN Clients** mode only allows the whitelisted wireless clients to access Wi-Fi.

Click **Delete Selected** to delete the blocked clients in batches. Alternatively, click **Delete** in the **Action** column to delete more than one whitelisted clients.

Figure 3-5-22 Allowed WLAN Client

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

Allowed WLAN Clients + Add

Up to **64** members can be added. *Note: If the whitelist contains no clients, all clients will be allowed to access Wi-Fi.*

<input type="checkbox"/>	MAC	Remark	Action
<input type="checkbox"/>	62:EE:B7:96:CF:B6	-	Edit Delete
<input type="checkbox"/>	54:BF:64:5C:DC:46	R12225	Edit Delete

< **1** > 10/page Total 2

Click **Add** to manually add MAC address to the **Allowed WLAN Clients**.

Figure 3-5-23 Manually Add WLAN Client

Add



* MAC

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

Remark

Cancel

OK

3.5.2.3 Radio Frequency

The **Radio Frequency** module allows you to configure channel width, transmit power and roaming sensitivity.

Figure 3-5-24 Radio Frequency

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

Radio Frequency

Country/Region

2.4G Channel Width

5G Channel Width

The settings are valid for only **current device**

2.4G Channel

5G Channel

Transmit Power Auto Lower Low Medium High

Transmit Power Auto Lower Low Medium High

Roaming Sensitivity Low 20% 40% 60% 80% High

Roaming Sensitivity Low 20% 40% 60% 80% High

Save

3.5.3 Repeater

The **Repeater** module allows you to view repeaters in the network and upgrade and delete them.

Figure 3-5-25 Repeater List

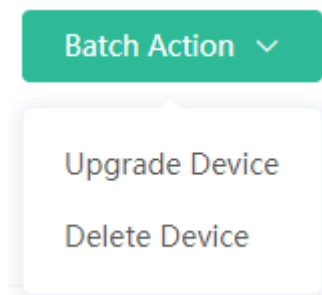
<input type="checkbox"/>	Action	Hostname	IP	MAC	Status	Model	Uplink Info	Clients	Software Ver	SN	Channel
<input type="checkbox"/>	Manage Reboot	EW1200PRO	192.168.111.61	00:74:9C:87:6D:AA	Online	EW1200G-PRO	Wired Detail	0	ReyeeOS 1.51.1620	G1PD3QN000688	auto-3,64
<input type="checkbox"/>	Manage Reboot	老款百兆	192.168.111.94	64:EE:87:96:CF:B3	Online	EW1200	5G Detail	0	EW_3.0(1)B11P50.Release(08140502)	G1PT3QH00044A	auto-9,56

A. The Repeater module supports **Advanced Search** and **List Filter** features.

B. Batch Action

You can tick list items and click **Batch Action**. The following drop-down list will appear:

Figure 3-5-26 Batch Action



Upgrade Device: An upgraded version is obtained from the cloud. When the device list contains an upgradable version, you can upgrade the devices in batches.

Delete Device: You can delete any offline device.

3.5.4 Security

3.5.4.1 ARP List

The **ARP List** page displays ARP entries and supports ARP binding.

Figure 3-5-27 ARP List



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



Enable ARP guard and configure IP-MAC binding to improve network security.

ARP Guard

Enable

Only the devices configured with IP-MAC binding are allowed to access the Internet.

ARP List

Search by IP/MAC



+ Add

🗑️ Delete Selected

Up to **64** IP-MAC bindings can be added.

<input type="checkbox"/>	No.	MAC	IP	Type	Action
<input type="checkbox"/>	1	c8:5b:76:94:00:3c	192.168.110.136	Dynamic	Bind
<input type="checkbox"/>	2	00:74:9c:87:65:bb	192.168.110.1	Dynamic	Bind
<input type="checkbox"/>	3	54:bf:64:5c:dc:49	192.168.111.127	Dynamic	Bind
<input type="checkbox"/>	4	64:ee:b7:96:cf:b3	192.168.111.94	Dynamic	Bind
<input type="checkbox"/>	5	00:74:9c:87:6d:aa	192.168.111.61	Dynamic	Bind

Total 5

10/page



1



Go to page

1

Click **Bind** in the **Action** column to set ARP entries to static ARP binding.

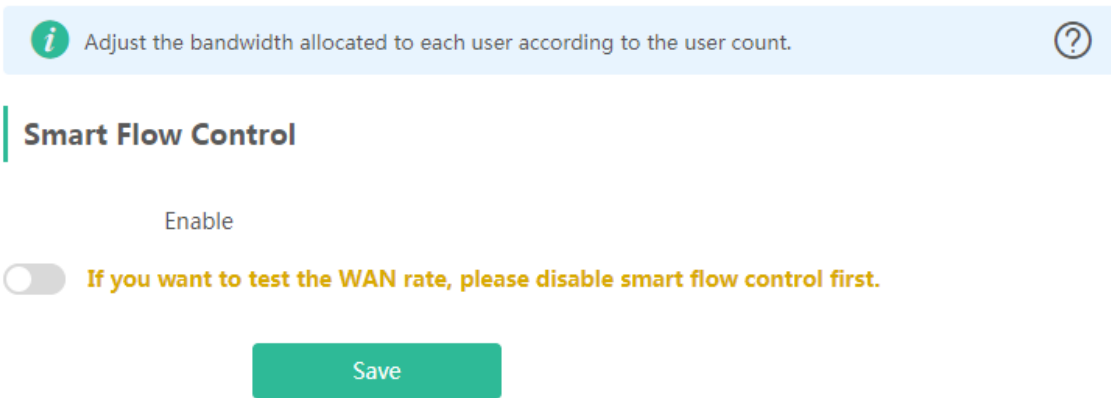
3.5.5 Advanced

3.5.5.1 Flow Control

3.5.5.1.1 Smart Flow Control

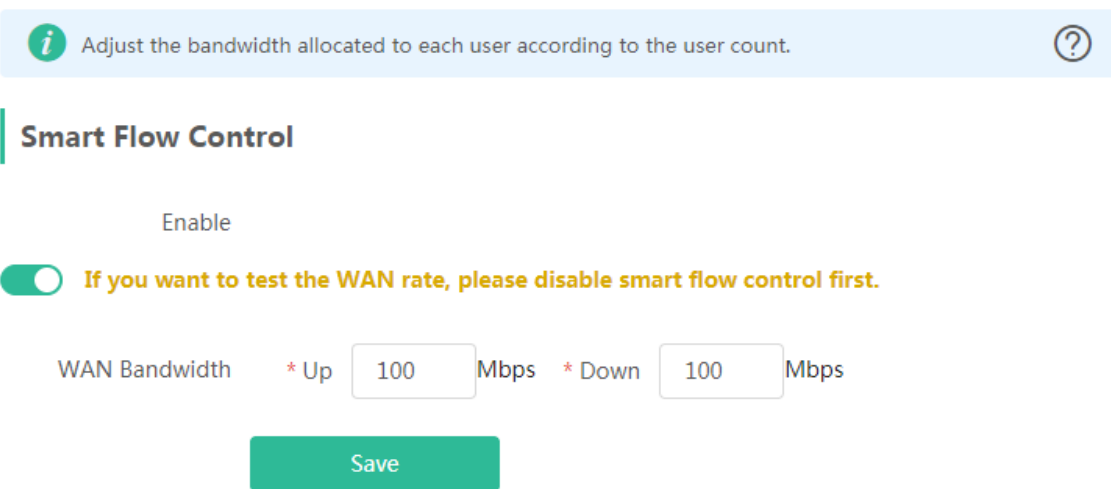
The **Smart Flow Control** module allows you to configure smart flow control.

Figure 3-5-28 Smart Flow Control



Enable **Smart Flow Control**.

Figure 3-5-29 Enable Smart Flow Control



If there is more than one WAN port, **WAN Bandwidth** settings of each port will be displayed accordingly.

3.5.5.1.2 Custom Policy

The **Custom Policy** module allows you to add, delete and edit custom flow control policies.

Figure 3-5-30 Custom Flow Control Policy

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

Policy List + Add + Delete Selected

Up to 30 entries can be added.

<input type="checkbox"/>	Policy Name	IP/IP Range	Bandwidth Type	Uplink Rate	Downlink Rate	Interface	Status	Effective State	Action
<input type="checkbox"/>	test	192.168.1 11.1- 192.168.1 11.10	Shared	CIR 1000 Kbps PIR 2000 Kbps	CIR 1000 Kbps PIR 2000 Kbps	WAN	Disable ●	Inactive ●	Edit Delete

Click **Add** to add a custom flow control policy.

Figure 3-5-31 Add Flow Control Policy

Add ×

* Policy Name

* IP/IP Range

Bandwidth Type

Uplink Rate * CIR * PIR Kbps

Downlink Rate * CIR * PIR Kbps

Status

Cancel OK

3.5.5.2 Port Mapping

3.5.5.2.1 Port Mapping

The **Port Mapping** module allows you to configure port mapping.

Figure 3-5-32 Port Mapping List

Port Mapping

Port Mapping List + Add Delete Selected

Up to 50 entries can be added.

<input type="checkbox"/>	Name	Protocol	External IP Address	External Port	Internal IP Address	Internal Port	Action
<input type="checkbox"/>	test	TCP	192.168.110.178	8888	192.168.111.188	80	Edit Delete

< 1 > 10/page Total 1

Click **Add** to add a port mapping policy. In the displayed dialog box, configure settings and click **OK**.

Figure 3-5-33 Add Port Mapping Policy

Add



* Name

Preferred Server

Protocol

External IP Address 192.168.110.178

* External Port/Range

* Internal IP Address

* Internal Port/Range

Cancel

OK

3.5.5.2.2 NAT-DMZ

The **NAT-DMZ** module allows you to configure the mapping of the device.

Figure 3-5-34 NAT-DMZ Rule List

NAT-DMZ ⓘ

Enable

* Dest IP Address

Save

3.5.5.3 Dynamic DNS

The **Dynamic DNS** page allows you to configure the dynamic DNS.

3.5.5.3.1 Peanut Shell NAT

It is recommended to use WeChat or Peanut Shell to scan the QR code.

Figure 3-5-35 Peanut Shell NAT


Peanut Shell NAT ⓘ It is recommended to use WeChat or Peanut Shell to scan the QR code.

Peanut Shell NAT

Enable

Save

Service Status Online

Scan to Login 

3.5.5.3.2 No-IP DNS

Figure 3-5-36 No-IP DNS

i No-IP DNS

No-IP DNS

* Username [Register](#)

* Password

Domain [?](#)

Log In

Delete

Link Status -

Domain -

3.5.5.4 UPnP Settings

The **UPnP Settings** module allows you to configure the UPnP list.

Figure 3-5-37 UPnP Settings

i UPnP (**Universal Plug and Play**) is a new Internet protocol aimed at improving communication between devices. **i**

UPnP List

Enable

Protocol	App	Client IP Address	Internal Port	External Port
No UPnP Device				

3.5.5.5 Local DNS

The **Local DNS** module allows you to configure a local DNS server.

Figure 3-5-38 Local DNS

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

Local DNS server

Save

3.5.5.6 Reyee Mesh

Figure 3-5-39 Reyee Mesh

i After Reyee Mesh is enabled, the new router will join the network automatically when being connected to the LAN port of the device. And then you can press the key for Reyee Mesh pairing. After Reyee Mesh is disabled, the bridged slave router will still be connected.

Reyee Mesh

Enable

Save

3.5.5.7 Hardware Acceleration

The **Hardware Acceleration** module allows you to enable hardware acceleration to improve network speed.

Figure 3-5-40 Hardware Acceleration

i After Hardware Acceleration is enabled, the Internet access speed will be improved and clients will not be rate-limited.

Hardware Acceleration

Enable

Save

3.5.5.8 Other Settings

Figure 3-5-41 Other Settings

i Other Settings

Other Settings

Enable RIP&RIPng

Enable Advanced ?
Security

Disable ICMPv6 Error
Messages

- Destination Unreachable
- Datagram Too Big
- Time Exceeded
- Parameter Problem

Save

3.5.6 Diagnostics

3.5.6.1 Network Check

Figure 3-5-42 Network Check

i Network Check



Start

Click **Start**, and click **OK** in the confirmation box. After the test finishes, the result will be displayed.

Figure 3-5-43 Result

i Network Check ?

Recheck

100%

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

If any problem occurs, the result will be displayed as follows:

Figure 3-5-44 Issue & Advice

Network Check

Recheck

100%

WAN/LAN Cable

Check WAN Cable

Result : The WAN cable is unplugged. Internet access may fail.

Advice : Please verify that the device is plugged into the WAN port properly and check the cable and plug.

Check LAN Cable

Result : OK

Please fix the problem by taking the suggested action.

3.5.6.2 Alarms

The **Alarms** module allows you to view and manage alarms in the network.

Figure 3-5-45 Alarms

View and manage alarms.

Alarm List

View Unfollowed Alarm

Expand	Alarms	Suggestion	Action
>	There is more than one wireless controller in the network.	Please power off the extra wireless controller.	Delete Unfollow
>	A MAC address conflict or loop error occurs.	Please troubleshoot the MAC address conflict or loop error.	Delete Unfollow
>	The LAN IP address is already in use.	Please check the LAN IP address. If it is a static IP address, please change the IP address.	Delete Unfollow

<

1

>

10/page

Total 3

Click **Unfollow** in the **Action** column to unfollow an alarm. In the confirmation box, click **OK**.

Figure 3-5-46 Unfollow Alarm

Are you sure you want to delete the alarm? ✕

1. If you want to unfollow the alarm, please click **Unfollow** on the right.
2. If you delete an unhandled alarm, the alarm will appear again later.
3. You can delete a handled alarm. The system will automatically delete an alarm not appearing again over a period of time.

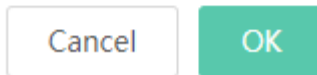


Click **View Unfollowed Alarm**, and you can view and follow the alarm again.

Figure 3-5-47 Re-follow Alarm

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

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



Click **View Unfollowed Alarm**, and you can view the following page.

Figure 3-5-48 View Unfollowed Alarm

View Unfollowed Alarm



The port is operating at 10Mbps.

[Re-follow](#)

Cancel

Click **Re-follow**, and you can view the following page.

Figure 3-5-49 Re-follow

Are you sure you want to follow the alarm again? ×

1. After being re-followed, an alarm will appear again.
2. You can click [Unfollow](#) to unfollow the alarm.

Cancel

3.5.6.3 Network Tools

The **Network Tools** module provides the following network tools to detect the network status: **Ping**, **Traceroute**, and **DNS Lookup**.

Figure 3-5-50 Ping Test and Result

i Network Tools ?

Tool Ping Traceroute DNS Lookup

* IP Address/Domain

* Ping Count

* Packet Size Bytes

```
PING www.baidu.com (14.215.177.39): 64 data bytes
72 bytes from 14.215.177.39: seq=0 ttl=49 time=17.442 ms
72 bytes from 14.215.177.39: seq=1 ttl=49 time=17.240 ms
72 bytes from 14.215.177.39: seq=2 ttl=49 time=16.964 ms
72 bytes from 14.215.177.39: seq=3 ttl=49 time=17.755 ms

--- www.baidu.com ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 16.964/17.350/17.755 ms
```

Figure 3-5-51 Traceroute Test and Result

Network Tools ?

Tool Ping Traceroute DNS Lookup

* IP Address/Domain

* Max TTL

```
tracert to www.baidu.com (14.215.177.39), 20 hops max,
46 byte packets
 1 192.168.110.1 (192.168.110.1) 0.990 ms 0.945 ms 0.629
ms
 2 172.30.111.1 (172.30.111.1) 2.369 ms 2.046 ms 2.209 ms
 3 172.30.255.33 (172.30.255.33) 1.457 ms 1.255 ms 1.189
ms
 4 172.30.255.146 (172.30.255.146) 0.903 ms 0.878 ms
0.960 ms
 5 172.30.255.150 (172.30.255.150) 1.275 ms 1.231 ms
1.179 ms
 6 172.30.255.33 (172.30.255.33) 1.632 ms 1.572 ms 1.887
ms
```

DNS lookup test interface and result

Figure 3-5-52 DNS Lookup Test and Result

i Network Tools ?

Tool Ping Traceroute DNS Lookup

* IP Address/Domain

```
Server:      127.0.0.1
Address: 127.0.0.1#53

Name:   www.baidu.com
www.baidu.com canonical name = www.a.shifen.com
Name:   www.a.shifen.com
Address 1: 14.215.177.38
Address 2: 14.215.177.39
www.baidu.com canonical name = www.a.shifen.com
```

3.5.6.4 Packet Capture

The **Packet Capture** module allows you to perform packet capture and download the result for troubleshooting.

Figure 3-5-53 Packet Capture

i Packet Capture ?

Interface

Protocol

IP Address

File Size Limit Available Memory **71.45 M**

Packet Count Limit

Start

Specify an IP address and click **Start**.

Figure 3-5-54 Start Packet Capture

i Packet Capture ?

Interface

Protocol

IP Address

File Size Limit Available Memory **71.45 M**

Packet Count Limit

PCAP file Capturing... **32.11K** **i**

*** Capturing**

After a few seconds, click **Stop**.

Figure 3-5-55 Stop Packet Capture

i Packet Capture
?

Interface

Protocol

IP Address

File Size Limit Available Memory **71.45 M**

Packet Count Limit

File Size: **113.23K**
 Captured on: **2021-05-14 10:13:01**

PCAP file [Click to download the PCAP file.](#) i

[Click to delete the file.](#)

Start
Stop

As shown in the preceding figure, click to delete the file, and click to download the packet capture result in the PCAP format.

3.5.7 System

3.5.7.1 System Time

The **System Time** module allows you to set the system time. The system time is synchronized with the NTP server by default.

Select a time zone and set at least one NTP server, and click **Save**.

Figure 3-5-56 Synchronized with NTP Server



Configure and view system time



Current Time 2021-05-14 10:17:45

[Edit](#)* Time Zone (GMT+8:00)Asia/Shanghai * 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](#)

Alternatively, Click **Edit**, select a data and a time and click **OK**.

Figure 3-5-57 Manually Set Time

Edit



* Time

3.5.7.2 Login

The **Login** module contains **Login Password** and **Session Timeout** settings.

3.5.7.2.1 Login Password

The **Login Password** module allows you to set the device's login password. You need to log into the system again after changing the password.

Figure 3-5-58 Login Password

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

* Old Password



* New Password

* Confirm Password

3.5.7.2.2 Session Timeout

The **Session Timeout** module allows you to set the session timeout period for login to the eWeb management system.

Figure 3-5-59 Session Timeout

 **Session Timeout**

* Session Timeout seconds



Save

3.5.7.3 Management

3.5.7.3.1 Backup & Import

The **Backup & Import** module allows you to import a configuration file and apply the imported settings. It can also import the configuration file, and restore the import configuration.

Figure 3-5-60 Backup & Import

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

Backup Profile

Backup Profile Backup



Import Profile

File Path Browse Import

3.5.7.3.2 Reset

The **Reset** module allows you to reset the device to factory settings. The module provides the Reset all routers option only when there is any repeater.

Figure 3-5-61 Reset

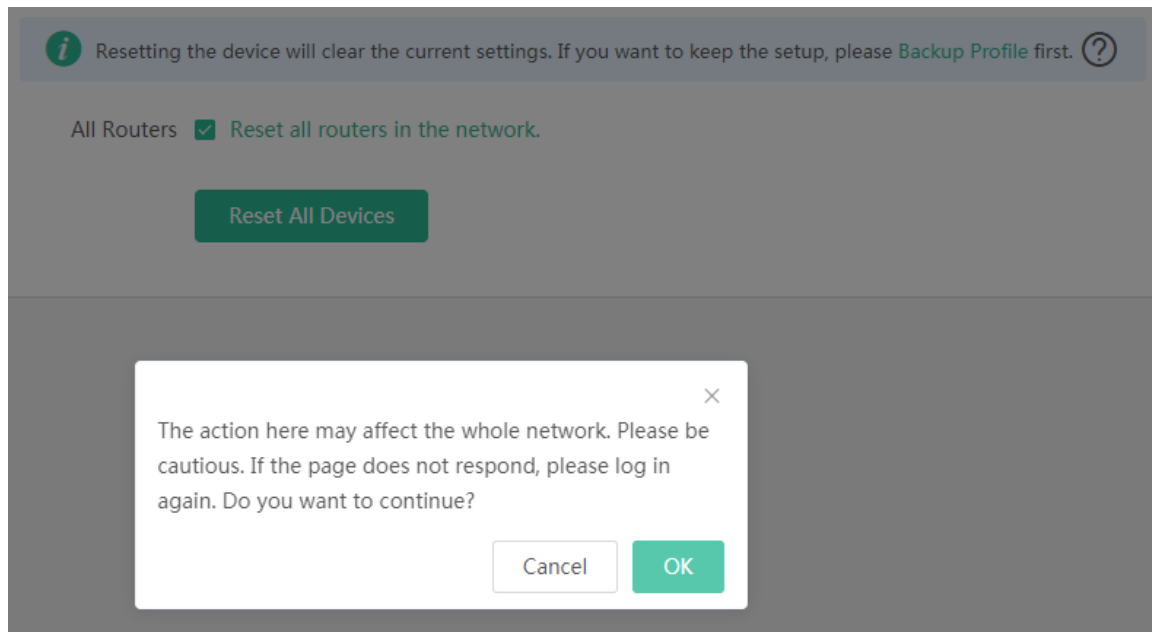
 Resetting the device will clear the current settings. If you want to keep the setup, please [Backup Profile](#) first. 

All Routers [Reset all routers in the network.](#)

Reset All Devices

Please exercise caution if you want to restore the factory settings.

Figure 3-5-62 Confirm Restore



Click **OK** to restore all default values. This function is recommended when the network configuration is incorrect or the network environment is changed.


3.5.7.4 Upgrade

Both online upgrade and local upgrade are available

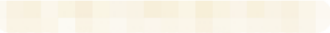
3.5.7.4.1 Online Upgrade

This page allows you to perform online upgrade. If any upgradeable “online version” is available in the network, the page displays the information of the upgradable version.

Figure 3-5-63 Online Upgrade

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

Current Version ReyeeOS 

New Version ReyeeOS 

- Description
1. 
 2. 

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


[Upgrade Now](#)

Auto Upgrade Auto upgrade the device when a new version appears.

Click **Upgrade Now**. The device downloads the upgrade package from the network, and upgrades the current version. The upgrade operation retains configuration of the current device. Alternatively, you can select **Download File** to the local device and import the upgrade package on the [Local Upgrade](#) page.

If there is no available new version, the device displays a prompt indicating that the current version is the latest.

Figure 3-5-64 Latest Version

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


Current Version  the latest version.)

Auto Upgrade Auto upgrade the device when a new version appears.

3.5.7.4.2 Local Upgrade

Click **Browse** to select an upgrade package, and click **Upload**. After uploading and checking the package, the device displays the upgrade package information and a prompt asking for upgrade confirmation. Click **OK** to start the upgrade.

Figure 3-5-65 Local Upgrade

 Please do not refresh the page or close the browser. 

Model X32-PRO

Current Version ReyeeO 

Development (It is recommended to be disabled after use.)
Mode


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

File Path

3.5.7.5 LED

The **LED** module allows you to enable LED.

Figure 3-5-66 LED

 **LED Status Control**
Control the LED status of **All Equipment**.

Enable



3.5.7.6 Reboot

Both immediate reboot and scheduled reboot are available.

3.5.7.6.1 Reboot

The **Reboot** module allows you to reboot the device immediately. The module provides the Reset all routers option only when there is any repeater.

Figure 3-5-67 Reboot

 Please keep the device powered on during reboot. 

All Routers Reboot all routers in the network.


Reboot All Device

Click **Reboot**, and click **OK** in the confirmation box. The device is rebooted and you need to log into the eWeb management system again after the reboot. Do not refresh the page or close the browser during the reboot. After the device is successfully rebooted and the eWeb service becomes available, you will be redirected to the login page of the eWeb management system.

3.5.7.6.2 Scheduled Reboot

The **Scheduled Reboot** module allows you to reboot the device at a scheduled time.

Figure 3-5-68 Scheduled Reboot

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

Enable

Day Mon Tue Wed Thu Fri Sat Sun

Time 03 : 00

Save

Enable scheduled reboot, select the time and click **Save**.

4 FAQs

Q1: I failed to log into the eWeb management system. What can I do?

Perform the following steps:

- (1) Check that the network cable is properly connected to the LAN port of the device and the corresponding LED indicator blinks or is steady on.
- (2) Before accessing the configuration GUI, set the IP assignment mode to **Obtain an IP address automatically** (recommended), so that the server with DHCP enabled can automatically assign an IP address to the PC. To designate a static IP address to the PC, set the IP address of the PC in the same network segment as the IP address of the management interface. For example, if the default IP address of the management interface is 192.168.110.1 and the subnet mask is 255.255.255.0, set the IP address of the PC to 192.168.110.X (X is any integer ranging from 2 to 254), and the subnet mask is 255.255.255.0.
- (3) Run the **ping** command to test the connectivity between the PC and the device.
- (4) If the login failure persists, restore the device to factory settings.

Q2: What can I do if I forget my username and password? How to restore the factory settings?

To restore the factory settings, power on the device, and press and hold the **Reset** button for 5s or more. The device will restart and restore the factory settings. Upon the restoration, you can access 192.168.110.1 and immediately log in to the eWeb management system.

Q3: The subnet mask value needs to be specified to divide the address range for certain functions. What are the common subnet mask values?

A subnet mask is a 32-bit binary address that is used to differentiate between the network address and host address. The subnet and the quantity of hosts in the subnet vary with the subnet mask.

Common subnet mask values include 8 (default subnet mask 255.0.0.0 for class A networks), 16 (default subnet mask 255.255.0.0 for class B networks), 24 (default subnet mask 255.255.255.0 for class C networks), and 32 (default subnet mask 255.255.255.255 for a single IP address).