

HA3515-DG Access Point

MA_1.3(1)B9P1

Web-based Configuration Guide

Document Version: V1.0 Date: 2023.12.11 Copyright © 2023 Ruijie Networks

Copyright

Ruijie Networks©2023

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.

Trademarks including Rujie Hetworks.

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

- Ruijie Networks Website: <u>https://www.ruijienetworks.com/</u>
- Technical Support Website: <u>https://ruijienetworks.com/support</u>
- Case Portal: <u>http://caseportal.ruijienetworks.com</u>
- Community: <u>http://community.ruijienetworks.com</u>
- Technical Support Email: <u>service rj@ruijienetworks.com</u>
- Skype: <u>service_rj@ruijienetworks.com</u>

Conventions

1. Signs

The symbols used in this document are described as follows:

✗ Caution

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

🕮 Note

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

Pre	face			I
1	Ove	erview of	Web-GUI	1
	1.1	Web-G	iUI	1
	1.2	jurable Functions on Web-GUI	1	
	1.3	rations before Web-GUI Connection	2	
	1.4	Prepa	ration for Web-GUI Connection	2
		1.4.1	Connection between the AP and the PC	2
		1.4.2	Configuring the IP Address of PC	3
	1.5	Web-G	iUI Login	4
		1.5.1	Open WWW Browser	4
		1.5.2	Measures for Certificate Error	5
		1.5.3	Entering Username and Password	6
2	Qui	ick Settin	gs	7
	2.1	Web-G	iUI Login	7
	2.2	Dashb	oard	7
	2.3	Config	juring Wireless SSIDs	8
	2.4	Config	juring RF Parameters	12
		2.4.1	Configuring RF Parameters on 2.4 GHz	13
		2.4.2	Configuring RF Parameters on 5 GHz	14
		2.4.3	Other Settings	15
	2.5	onal Instructions for Enterprises	16	
		2.5.1	Device Management	16
		2.5.2	Access Point Mode	16
		2.5.3	Routing Mode	17
3	Dev	vice Over	view	19
	3.1	Equipi	nent Overview	20
	3.2	Device	e Details	21
	3.3	Wi-Fi S	itatus	22
	3.4	Interfa	ace Information	22
4	Bas	sic Config	urations	23
	4.1	Basic l	Management	24
		4.1.1	WAN Settings (Routing Mode)	24
		4.1.2	LAN Settings (Routing Mode)	25
		4.1.3	IPv6 Settings	27
		4.1.4	Clients	28
		4.1.5	Mode Switching	32
	4.2	Wirele	ss Management	33
		4.2.1	Wireless Settings	33
		4.2.2	Configuring RF Parameters	33
		4.2.3	WPS	34
	4.3	Netwo	ork Management	35
		4.3.1	VLAN	35
	4.4	Behav	ior Management	36

Contents

	4.4.1	Access Control	36
	4.4.2	Security	38
	4.5 Diagno	ostics	40
	4.5.1	Network Tools	40
5	Advanced M	anagement	42
	5.1 User Is	solation	42
	5.2 IGMP	Snooping	43
	5.3 Accele	ration Settings	45
	5.4 DMZ (F	Routing Mode)	45
	5.5 Port M	lapping (Routing Mode)	46
	5.6 UPnP (Routing Mode)	47
	5.7 DNS Se	erver	48
	5.8 DHCP	(Routing Mode)	49
	5.9 Firewa	ll (Routing Mode)	50
6	System Man	agement	53
	6.1 NTP Se	ettings	53
	6.2 Port M	lanagement	53
	6.3 Login	Management	54
	6.3.1	Administrator Password	54
	6.3.2	Session Timeout	55
	6.3.3	Account Name	56
	6.4 Config	uration Management	56
	6.4.1	Restore	56
	6.4.2	Backup and Import	57
	6.5 Reset	Settings	60
	6.6 LED Se	ttings	60
	6.7 Web C	LI	62
	6.8 Systen	n Log	62
	6.9 Systen	n Upgrade	63
	6.9.1	Manual Upgrade	63
	6.9.2	G.hn Firmware Upgrade	65
	6.10 Reboo	t	65
	6.10.1	Reboot	65
	6.10.2	Scheduled Reboot	66
	6.11 Develo	oper Mode	67
7	Troubleshoo	ting	68
	7.1 Failing	to Connect to Web-GUI	68
	7.2 Failing	to Log into Web-GUI	68
	7.3 Comm	unication Failure	69
	7.4 About	Device Setup and Usage Support	69

1 Overview of Web-GUI

Description: This document is applicable only to HA3515-DG.

This chapter will provide an overview of Web-GUI from the following aspects:

- Web-GUI: The Web management system can be accessed through a WWW server (such as Google Chrome) to manage APs;
- Available Functions: This section briefly introduces the features that can be set via the Web-GUI, including SSID parameters, network configurations, security configuration, etc.;
- Preparation before Web-GUI Connection: This section introduces the materials required before connection and provides precautions;
- Preparation for Web-GUI Connection: This section introduces the connection between this device and the PC, the IP address setting and the Internet settings of the browser;
- Web-GUI Login: This section introduces the specific steps of Web login.
- Web-based management involves two parts: Web server and Web client. A web server is integrated into a device to receive and process requests sent from a client and returns the processing results. Generally, a Web client refers to a web browser like Firefox, Google Chrome, Safari.
- If the kernel version of the Microsoft Internet Explorer browser you are using is too low, the Web-GUI may experience slow response. Please roll back the interface or use other browsers. Google Chrome and Safari are recommended.

1.1 Web-GUI

This device can be configured through a WWW browser.

When logging into the Web-GUI, you can easily configure the AP without running commands in CLI (Command Line Interface). Almost all main functions can be set via Web-GUI.

1.2 Configurable Functions on Web-GUI

The main features that can be set via the Web-GUI are as follows:

- SSID Parameters: passwords, encryption modes, etc.
- 2. 4G/5G Parameter: channel, bandwidth, transmit power, etc.
- Network Configuration: WAN port, LAN, DHCP, etc.
- Security Configuration: black lists, white lists, user isolation, etc.
- AP Management: device upgrade, restart, etc.
- G.hn firmware upgrade.

1.3 Preparations before Web-GUI Connection

Materials	Description
	WWW Browser: Google Chrome, Firefox, Safari. Others: a PC with LAN port, or some other mobile terminal devices, such as laptops, iPads, mobile phones, etc.
Management	It is recommended that the resolution settings are 1280*1024, 1920*1080 and 1440*960. At other resolutions, the page fonts and formats may be misaligned and not beautiful enough. For example, due to the smaller screen of mobile phone terminals, the interface layout and format may be misaligned, unsightly, and other abnormalities.
Terminal	Due to the influence of WWW browsers, file uploads (updating program file versions, setting files) may fail. If it fails repeatedly, please try changing the WWW browser. We recommend Google Chrome, Firefox, and Safari. Internet Explorer or Microsoft Edge can also be used, but some functions may not be available, such as displaying English when the browser starts.
	If you perform "Save Settings", "Save File" or "Return" while updating the screen, it may not function properly. Please perform the above operations after the screen update is completed.
Ethernet Cable	UTP/STP Category 5e or higher is recommended.

Please prepare the following materials before connecting to Web-GUI:

1.4 Preparation for Web-GUI Connection

This section describes how to connect to the Web-GUI via the PC. The operations are:

- Form the connection between the AP and a PC •
- Set the IP address of the PC
- Set the Internet settings of a WWW browser

1.4.1 Connection between the AP and the PC

As shown in the figure below, the administrator can access the device through a browser and uses the WEB management system to configure the device.

The topology is shown as follows:



Use an Ethernet cable (RJ45) to connect this AP to the PC. Plug one end of the Ethernet cable connected to the PC into the LAN port of the AP until it clicks to the place.

- For unplugging the Ethernet cable, hold the plug, press down on the plastic clip at the top of the plug, and pull the plug from port.
- Do not use a cable other than an Ethernet cable to connect the AP and the PC, otherwise it may cause the device to work abnormally or burned out.

1.4.2 Configuring the IP Address of PC

Set the IP address of the PC to an IP address that can connect to the HA3515-DG. The IP address configured varies from the working modes of AP.

AP Mode:

Select "Use the following IP address" in the page, set the IP address to 192.168.110.X (the value of X ranges from 100 to 200) and set the DNS server to 192.168.110.1. For example, set the fixed IP to 192.168.110.100 and the DNS server to 192.168.110.1.

Internet Protocol Version 4 (TCP/IPv4) Properties							
General							
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.							
Obtain an IP address automatical	ly						
• Use the following IP address:							
IP address:	192 . 168 . 110 . 100						
Subnet mask:	255.255.255.0						
Default gateway:	192 . 168 . 110 . 1						
Obtain DNS server address autom	natically						
• Use the following DNS server add	resses:						
Preferred DNS server:	192 . 168 . 110 . 1						
Alternate DNS server:							
Validate settings upon exit Advanced							
OK Cancel							

Routing Mode:

Select "Obtain an IP address automatically" in the settings.

Internet I	Protocol Version 4 (TCP/IPv4) Pro	operties				×
Genera	Alternate Configuration					
You ca this ca for th	an get IP settings assigned auto apability. Otherwise, you need t e appropriate IP settings.	matically if yo o ask your ne	our ne twor	etwork su k adminis	upports strator	
0	Obtain an IP address automatica	lly				
	Jse the following IP address: —					
IP (address:					
Sut	onet mask:]	
Del	ault gateway:					
	Obtain DNS server address auto	matically				
	Jse the following DNS server add	tresses:				
Pre	ferred DNS server:					
Alt	ernate DNS server:					
	Validate settings upon exit			Advar	nced	
			OK		Cancel	

1.5 Web-GUI Login

This section introduces the operation method of logging into the Web-GUI. The specific steps are:

- Open a WWW browser
- What to do when a certificate error appears
- Enter username and password

1.5.1 Open WWW Browser

Open a WWW browser of your PC and enter the following IP address or website. The default URLs are http://192.168.110.1 or https://rjap.jp.

- It is recommended to use the default URL https://rjap.jp to access the Web.
- Both http:// and https:// are supported to be connected to the Web-GUI.
- If users access the Web from the WAN port of the AP, the default URL cannot be used. Please use the IP address of the AP to access the Web via the LAN port.
- If you want to check the IP of the WAN port IP, you can click "Basics"-> "WAN" in routing mode. In bridge mode, you can click "Basics" -> "External Network" to check.

- ✓ It is recommended to use Google Chrome, Firefox and Safari. When using other browsers to log into Web management, exceptions such as garbled characters or format errors may occur.
- ✓ In routing mode, if the "No WAN-Side Access" function is enabled and the whitelist IP is not configured, the AP's Web cannot be accessed through the WAN port. To address this issue, you can access the Web by connecting the SSID or via the LAN port, and then set the whitelist IP address.

1.5.2 Measures for Certificate Error

A WWW browser may display the following warning message indicating that there is a problem with this website's security certificate. In this case, please click "Continue to this website (not recommended)" to continue browsing.

8	There is a problem with this website's security certificate.
	The security certificate presented by this website was not issued by a trusted certificate authority. The security certificate presented by this website has expired or is not yet valid. The security certificate presented by this website was issued for a different website's address.
	Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
	We recommend that you close this webpage and do not continue to this website.
	Click here to close this webpage.
	Sontinue to this website (not recommended).
	More information

1.5.3 Entering Username and Password

Enter your username and password and click "Login".



Default username and password

Default Username / Password	Permission	
admin/admin	Super administrator owning all permissions.	

The initial password admin is only set for initial use. Since the security is very low, please set a new password after the following page pops up.

Ruijie									
윤Device Overview	Device Overview								
⊕Basics									
♥Wireless	Online Clients	0	Your management p security, change you	assword has low se ir management pas	ecurity. To ensure n ssword.	etwork			
⊘ [?] Network			 Administrator Pas 	ssword		?	6 at 0620		
MBehavior	Device Details		* Old Password		> _{>r} t				
⊖, Diagnostics	Model:	RG-HA3515-DG	* New Password		30 ¹⁶¹⁰ ×		MAC:	C4:70:AB:00:09:08	
Advanced	Hardware Ver:	V1	* Confirm Password		مجرخ		<u>}12719),</u>		
: System	Traffic Statistics			Save			6 560 00 ²⁰		
	Elapse Selection Q Last 24 Hours	 Last 7 Days 			- 20				
	Unit Selection MB								

✓ It is recommended to set a strong password. The length of a strong password should be more than 6 characters and formed by uppercase, lowercase and numbers.

2 Quick Settings

This chapter will introduce how to quickly configure the device, which includes:

- Web-GUI Login: Users can use the default password admin to log into the Web;
- Dashboard: The dashboard displays multiple system information to users;
- Configure wireless SSID: When the dual band is configured, up to 6 SSIDs can be set;
- Wireless RF Parameters: Users can not only set the parameters of 2. 4 GHz and 5 GHz, but also configure some items, such as the number of online terminals, signal switching and the interval for automatic signal switching;
- Additional Instructions for Enterprises: An introduction to device management, AP mode configuration and routing mode configurations are provided;

2.1 Web-GUI Login

Use the default password admin to log into the Web page

indea	
Welcome to use Ruijie RG-HA3515-DG	
Gigabit Dual-Band Wi-Fi 6 Router	
A Enter the device username	
Enter the device password	
Login	
Forget the account or password?	

Support Chrome, Firefox, Microsoft Edge browser	© 2000-2023 Ruijie Networks Co., Ltd
Official Website: https://w	/ww.ruijie.co.jp

2.2 Dashboard

When you log into the Web management system, the dashboard will be displayed. On the dashboard, you can see several system information.

Device Overview					
Online Clients	0		Status 🕑 : Online Uptime: 52Min 435 Systime: 2023-12-04 16:23:26		
Device Details					
Model: Hardware Ver:	RG-HA3515-DG V1	SN: Software Ver:	G3QH9XW002000 MA_1.3(1)89P1, Release(10212719), Revision(6a1bcbe15)/	MAC:	C4:70:AB:00:09:08
WiFi					
SSID 1 List		SSID 2 List		SSID 3 List	
Wi-Fi: Encrypted:	PR20-APART-2810 Yes	💮 Wi-Fi: Encrypte	SSID-SSID-C0908D_Wi-Fi5 d: Ves	↔ Wi-Fi: Encrypted:	SSID-SSID-C0908D-3 Yes
SSID 4 List		SSID 5 List		Guest Wi-Fi	
Wi-Fi: Encrypted:	SSID-SSID-C0908D-4 Yes	Wi-Fi: Encrypte	SSID-SSID-C0908D-5 d: Ves	WiFi: Encrypted:	SSID-SSID-C0908D-Guest Yes
Interface Details					
			WAN LAN LAN		

2.3 Configuring Wireless SSIDs

On the Web management system, you can configure wireless SSIDs. For a dual band integration, up to 6 SSIDs can be configured, of which one is specifically used for a guest network and the other five are universal.

Follow the following steps to configure wireless SSIDs:

Step 1: Click the "Wireless" in the left navigation bar (marked "1" in the figure);

Step 2: Click "Wi-Fi" (marked "2" in the figure), and then click "Wi-Fi Settings".

	Ruíjie			English 🗡 📑 Exit
	${}^{\mathcal{O}}_{\mathcal{O}^{2}}$ Device Overview \bigoplus Basics \checkmark		WI-Fi Settings Guest WI-Fi	
			1 Tip: Changing configuration requires a wireless restart and will force online clients to go offline.	0
1		^	Wi-Fi Settings	
2	Wi-Fi Radio	_	SSID List SSID 1 List V	
	WPS		Dual-Band Single SSID (The 2.4G and 5G bands use the same SSID.)	
	° [⊘] Network	~	5G Priority 📃 🔍	
	∰Behavior	×	WI-FI Switch	
	Spiagnostics	Ň	* SSID PR20-APART-2810	
	Advanced	Ň	Encryption WPA2-PSK(AES)(Recommend) V	
	-®- -®- System	Ť	* WI-FI Password	
			Hide SSID	
			Save	
	<pre>«Fold</pre>			

The configuration items are shown as follows:

Items Description		Default/Options	
SSID List	Select the SSID list to be configured. Up to 5 SSID lists can be configured with different SSID names at the same time.	Default: SSID 1 List Option: SSID 1 List to SSID 5 List.	
Dual-Band Single SSID	Choose whether to use the same SSID on 2.4GHz and 5Ghz. If it is disabled, you can configure different SSIDs on 2. 4GHz and 5GHz.	Default: Enabled (the same SSID is used for 2.4 GHz and 5 GHz) Option: Enabled/Disabled	
5G Priority	When 5G priority is enabled, it will give priority to guiding terminals to access the 5G channel. XIt is important to note that the 5G priority function will take effect throughout the entire machine. That is to say, after 5G priority is enabled on a SSID, it takes effect globally, even if it is not enabled on the rest of SSIDs.	Default: Disabled Option: Enabled/Disabled	
Wi-Fi Switch	If this switch is off, the SSID is turned off.	Default: SSID 1 list is enabled by default, and SSID 1 list to SSID 5 list is disabled by default.	
SSID	Set a SSID name.	Default: A random value on the device's sticker X The name cannot exceed 32 characters.	
Specify an authentication method.OPEN: It requires no password which means anyone can connect to the SSID.EncryptionWPA-PSK (TKIP): It is an earlier security protocol that evolves from the WEP (Wired Equivalent Privacy). Due to its low security, it is only suggested to be used on some early		Default: WPA2-PSK(AES) Options: WPA2 -PSK(AES) WPA3-SAE(AES) WPA2-PSK & WPA3-SAE (AES) Open (None) WAP-PSK & WPA2-PSK(AESTKIP)	

		•
	terminal devices that supports WPA.	WPA-PSK(TKIP)
	WPA2-PSK: It is a higher security protocol	
	based on the WPA-PSK. It is designed for home	
	users and small offices to protect their	
	networks.	
	WPA/WPA2-PSK: It is a mixed mode of WPA-PSK	
	and WPA2-PSK, and is backward-compatible,	
	which means it can be operated on terminals	
	that do not support WPA2.	
	WPA3-SAE: It is an overall improvement over its	
	iteration, WPA2. It provided more personalized	
	settings to deliver a higher security. But it only	
	can be used on the devices that support WPA3.	
	WPA2-PSK & WPA3-SAE : It is a mixed mode of	
	WPA2-PSK and WPA3- SAE, and is backward-	
	compatible, which means it can be operated on	
	terminals that do not support WPA3.	
	The length of a SSID password must be formed	
	by at least 8 characters. For security reasons,	Default: A random value printed on the
WI-FI Passworu	we recommend that you change the initial	device's sticker.
	password.	
	Sometimes for security reasons, you can hide	
	the SSID so that others cannot search for the	
	SSID name. However, when you search the SSID	Default: Disabled
Hide SSID	via your mobile phone, it can be found and	Option: Enchled (Dischled
	connected. When the SSID is hidden, the	
	terminals that have connected to it will not be	
	affected.	

When you disable "Dual-Band Single SSID", the following page is displayed. In this page, you can configure 2.4GHz and 5GHz bands separately.

Ruíjie		inglish \vee 🕒 Exit
음 Device Overview	Wi-Fi Settings Guest WI-Fi	
⊕ Basics	7 1 Tim Channing configuration requires a wireless restart and will force online clients to no offline.	0
Wi-Fi	Wi-Hi Settings	
Radio	SSID List v	
WPS	Dual-Band Single SSID (The 2.4G and 5G bands use the same SSID.)	
° Network	SG Switch C	
míBehavior	* \$\$ID PR20-APART-2810 * \$\$ID PR20-APART-2810-5G	
⊲ Diagnostics	Encryption WPA2-PSK/AES)(Recommend) V Encryption WPA2-PSK/AES)(Recommend)	
Advanced	* Wi-FI Password	
System	Hide SSID	
	Save	

When the SSID 2 list is configured, an additional item will be provided as shown in the red box in the figure below (Wi-Fi 5 Backup network):

Ruíjie		English 🗸 🕒 Exit
옭Device Overview	WLEI Sattings Great WLEI	
⊕ Basics ∨		0
↔ Wireless	The changing comparation requires a vinces resard and vin roce onnine cients to go onnine.	
Wi-Fi	Wi-Fi Settings	
Radio	SSID List V	
WPS	Dual-Band Single SSID (The 2.4G and 5G bands use the same SSID.)	
°S Network ∨	5G Priority 🔵 🖲	
∰Behavior ~	WI-FI Switch	
☉ Diagnostics ~	* SSID SSID-C0908D_WF-FI5	
△ Advanced	Encryption WPA2-PSK(AES)(Recommend) V	
:a− a− System ∨	* WI-FI Password	
	Hide SSID	
	WI-FI 5 Backup network 💽 💿	
«Fold	Save	

This item is only applicable to the SSID 2 list.

Items	Description	Defaults/Options
Utems Wi-Fi 5 Backup network	This AP is an 802.11ax (Wi-Fi 6) device. Although the 802.11ax standard supports being compatible with the 802.11ac (Wi-Fi 5), there are still a small number of laptops and other terminals that cannot be connected to the Wi-Fi 6 signal released by this device due to their old drives. When this feature is enabled, these terminal devices can be connected to the Wi-Fi 5 signal. But they will not be able to take advantage of the new features	Defaults/Options Default: Enabled Option: Enabled/Disabled
	brought by Wi-Fi 6 devices.	

Under the "Wi-Fi" menu, in addition to the "Wi-Fi Settings" tab page, there is also a "Guest Wi-Fi" tab page.

Ruíjie			
$\frac{9}{53}$ Device Overview		Wi-Fi Settings Guest Wi	-6
⊕ Basics	×	Tip: Chapping configure	ation requires a wireless restart and will force online clients to a
≎Wireless		The changing contigun	actor requires a wireless restart and will force online clients to g
Wi-Fi		Guest WiFi	
Radio		Dual-Band Single SSID	(The 2.4G and 5G bands use the same SSID.)
WPS		5G Priority	
₀ ^o Network	~	WI-FI Switch	
∰ Behavior	~	4.0010	
© Diagnostics	~	- 3510	
△Advanced	~	Encryption	WPA2-PSK(AES)(Recommend)
	~	* Wi-Fi Password	·····
		Hide SSID	
			Save

All the configurable items on this tab page are the same as the configurable items on the SSID 1 List~ SSID 5 List in "Wi-Fi Settings". The difference is that the signal emitted by this SSID is exclusively for guests. After they are associated with this SSID, they cannot access the local network in routing mode, but only the Internet.

2.4 Configuring RF Parameters

This feature can be configured for 2. 4 GHz and 5 GHz.

• The specific steps are:

Step 1: Click "Wireless" on the Web (marked "1" in the picture);

Step 2: Click "Radio" (marked "2" in the picture) to go to the setting page.

	Ruíjie		English 🗸 🕒 Đứt
	& Device Overview	Power & Radio	
•	⊕ Basics ~	You can manage 2.4G and 5G modules on this page.	
2	Wi-Fi	The terminal cannot be switched online	
	Radio	Period of Wireless Channel 24 H	
	WPS	2.4G Master Switch SG	Master Switch
	₀ ^o Network ∽	2.4G Channel Auto(CH1-11) V	5G Channel Auto(W52) V
	∰Behavior ~	Power High 100% \checkmark	Power High 100% 🗸
	ඁ©, Diagnostics ∽	2.4G Channel Width 20MHz V	hannel Width 20/40/80MHz \lor
	△ Advanced ~	802.11 Mode 802.11b/g/n/ax v	802.11 Mode 802.11a/n/ac/ax ~
	tan System ✓	WMM Switch 💽 🖲	WMM Switch 💽 🔍
		* Maximum access 15 * Ma	dmum access 15
		Save	
	« Fold		

2.4.1 Configuring RF Parameters on 2.4 GHz

Ruíjie				English 🗡 🗗 Exit
ಿ Device Overview	Power & Radio			
⊕ Basics ~				
ন্থWireless	You can manage 2.4G and 5G modules on this page.			
Wi-Fi	The terminal cannot be switched online 🗾			
Radio	Period of Wireless Channel 24 H 🔮			
WPS	2.4G Master Switch	5G Master Switch		
⊘ [⊙] Network ∨	2.4G Channel Auto(CH1-11) v	5G Channel	Auto(W52) v	
∰Behavior ~	Power High 100% v	Power	High 100% \sim	
ඁ© Diagnostics ∽	2.4G Channel Width 20MHz V	5G Channel Width	20/40/80MHz v	
Advanced ∨	802.11 Mode 802.11b/g/n/ax v	802.11 Mode	802.11a/n/ac/ax v	
System V	WMM Switch 🔵 🛛	WMM Switch	•	
	* Maximum access 15	* Maximum access	15	
	Save	-		

Items	Description	Defaults/Options		
2.4G Master Switch	Used to determine whether to release the 2.4 GHz signal. If is disabled, the 2. 4 GHz signal is not released.	Default: Enabled Options: Enabled/Disabled.		
2.4G Channel	Set the channel on 2. 4 GHz. You can choose a fixed channel, or choose to automatically select within the channel range 1-11 or the channel range 1-13.	Default: Auto (CH1-11). Options: Automatic(CH1-11),Auto(CH1-13), 1,2,3,4,5,6,7,8,9,10,11,12,13		
Power	Set the transmit power of 2. 4 GHz signal.	Default: High 100% Options: High 100%, Medium 60%, Low 40%		
2.4G Channel Width	Configure 2.4GHz bandwidth. You can choose a fixed bandwidth or an automatic bandwidth of 20/40MHz.	Default: 20 MHz Options: 20 MHz, 40 MHz, 20/40 MHz		
802.11 Mode	Set the wireless working mode of 2. 4 GHz.	Default: 802.11b/g/n/ax Options: 802.11b/g/n/ax, 802.11b/g/n, 802.11b/g		
WMM Switch	When it is enabled, the better quality of multimedia is provided. We recommend turning it on.	Default: Enabled Options: Enabled/Disabled.		
Maximum Access	Maximum number of terminals supported on 2.4GHz.	Default: 15 Options: 1-15		

2.4.2 Configuring RF Parameters on 5 GHz

Ruíjie			English \vee 🕞 Exit
ి Device Overview	Power & Radio		
⊕ Basics ∨	You can manage 2.4G and 5G modular on this page.		
Wi-Fi	The terminal cannot be switched online		
Radio	Period of Wireless Channel 24 H		
WPS	2.4G Master Switch	5G Master Switch	
°S Network ∨	2.4G Channel Auto(CH1-11) V	5G Channel Auto(W52) V	
∰Behavior ~	Power High 100%	Power High 100%	
Q. Diagnostics	2.4G Channel Width 20MHz ~	5G Channel Width 20/40/80MHz <>	
△ Advanced ∨	802.11 Mode 802.11b/g/n/ax V	802.11 Mode 802.11a/n/ac/ax 🗸	
System V	WMM Switch 💽 🛛	WMM Switch 💽 •	
	* Maximum access 15	* Maximum access 15	
	Save		

Items	Description	Defaults/Options
5G Master Switch	Used to determine whether to release the 5GHz signal. If is disabled, the 5GHz signal is not released.	Default: Enabled. Options: Enabled/Disabled.
5G Channel	Set the channel on 5GHz. You can choose a fixed channel, or choose to automatically select within the channel range 1-11 or the channel range 1-13.	Default: Auto (W52). Options: Auto (W52), Auto (W52+ W53), Auto (W52+W53+W56), 36,40,44,48,52,56,60,64,100,104,108, 112,116,120,124,128,132,136,140
Power	Set the transmit power of 5GHz signal.	Default: High 100% Options: High 100%, Medium 60%, Low 40%
5G Channel Width	Configure 5GHz bandwidth. You can choose a fixed bandwidth or an automatic bandwidth.	Default: 20/40/80MHz Options: 20MHz, 20/40MHz , 20/40/80MHz
802.11 Mode	Set the wireless working mode of 5 GHz signal.	Default: 802.11a/n/ac/ax Options: 802.11a/n/ac/ax, 802.11a/n/ac, 802.11a/n, 802.11a
WMM Switch	When it is enabled, the better quality of multimedia is provided. We recommend turning it on.	Default: Enabled. Options: Enabled/Disabled.
Maximum Access	Maximum number of terminals supported by 5GHz.	Default: 15 Options: 1-15

✓ It should be noted that if the 5G channel is set to a fixed channel, automatic bandwidth switching will be used by default, but in fact the underlying algorithm of the AP does not currently support automatic switching between 20/40/80MHz.

2.4.3 Other Settings

After the automatic channel and automatic bandwidth settings take effect, the device will scan the channel and bandwidth according to the set period and reselect the optimal channel and bandwidth.

Ruíjie		English \vee 🕒 Exit
중 Device Overview	Power & Radio	
⊕ Basics ~	You can manage 2.4G and 5G modules on this page.	
ি Wireless		
Wi-Fi		
Radio		
WPS	2.4G Master Switch C	
° [⊘] Network ∨	2.4G Channel Auto(CH1-11) V 5G Channel Auto(W52)	
∰Behavior ~	Power High 100% V Power High 100% V	
©₀ Diagnostics ~	2.4G Channel Width 20/Hz \checkmark 5G Channel Width 20/40/80MHz \checkmark	
△ Advanced ~	802.11 Mode 802.11b/g/n/ax \vee 802.11 Mode 802.11a/n/ac/ax \vee	
:≘ System ∨	WMM Switch 💽 🛛 WMM Switch 💽 🔍	
	* Maximum access 15 * Maximum access 15	
	Save	
«Fold		

Items	Description	Defaults/Options
The terminal cannot be	When a terminal is online, do not	Default: On.
switched online	switch the channel and the	Options: On/Off.
switched offine	bandwidth.	
	Set the time interval for automatic	
Devied of Wiveless Chapped	channel switching. The default	Default: 24 hours.
Period of wireless channel	setting is to automatically select	Options: 1-48 hours
	channels after each 24 hours.	

2.5 Additional Instructions for Enterprises

2.5.1 Device Management

In the left panel of the Web, eight menus are offered to you to manage the AP.

Ruíjie						English 🗡 🕞 Exit
윦 Device Overview	Device Overview					
⊕ Basics ~						
ି Wireless 🗸 ୪	Online Clients	0	Sta Upt	tus 🕑 : Online time: 51Min 39S		
<i>⊗</i> Network ~		-	Sys	time: 2023-12-04 16:22:22		
mißehavior ∽	Device Details					
୍ଦ୍ୱ Diagnostics 🛛 🗸	Model:	RG-HA3515-DG	SN:	G3QH9XW002000	MAC:	C4:70:AB:00:09:08
△ Advanced ∨	Hardware Ver:	V1	Software Ver:	MA_1.3(1)B9P1, Release(10212719),		
-e- -e- System				Revision(6a1bcbe15)/		
	WiFi					
	SSID 1 List		SSID 2 List		SSID 3 List	
	Wi-Fi: Encrypted:	PR20-APART-2810 Yes	Wi-Fi: Encrypted:	SSID-SSID-C0908D_WI-F 15 Yes	Wi-Fi: Encrypted:	SSID-SSID-C0908D-3 Yes
	SSID 4 List		SSID 5 List		Guest Wi-Fi	
<pre>«Fold</pre>	Wi-Fi:	SSID-SSID-C0908D-4 Yes	Wi-Fi: Encrypted:	SSID-SSID-C0908D-5 Yes	WiFi:	SSID-SSID-C0908D-Gues

2.5.2 Access Point Mode

The following page allows you to set the device to the bridge mode.

• The specific steps are as follows:

Step 1: Click "Basic " in the left panel (marked "1" in the picture);

Step 2: Click on "Work Mode " (marked "2" in the picture);

Step 3: Select "AP Mode" (bridge mode) (marked "3" in the picture).

	Ruíjie		English 🗸 🕞 Exit
1	Basics External Network	Work Mode The device is working in Bridge mode. The following Two modes are available: Router 3 Bridge	
	Clients	8ridge This mode allows you to establish a physical connection between a primary router and a secondary router, extending network coverage.	
2	Work Mode Image: Wireless Image: Wire	Work Mode Bridge Choose External Network to change the IP assignment mode. IP Address 192.168.30.2 4 Save	
	± System ✓		

In bridge mode, the management address of 192.168.110.1 has been set for the device. In bridge mode, if the AP is not connected to the upper-level network, the downstream client will not be able to obtain DHCP. In this case, the client can configure an IP in the same network segment as the management address to access the Web homepage through this management address.

2.5.3 Routing Mode

- In bridge mode, a terminal such as a mobile phone can obtain IP addresses from the uplink network of the AP. If there is no uplink network or the uplink network does not assign an IP address, the terminal may not be able to access to the network. To address this issue, you can set the IP address to 1 92.168.110.x on your mobile phone or wired terminal, and then access the Web management system via 192.168.110.1.
- In routing mode, a terminal such as a mobile phone can obtain an IP address in the network segment of 1 92.168.110.x by default. The terminal device can access the Web management system via 192.168.110.1 or http s:// rjap.jp. The configuration page of routing mode is shown as the following figure:

Ruíjie				English 🗠 🕞 Exit
🖧 Device Overview		Work Mode		
⊕ Basics		The device is working in	tridge mode. The following Two modes are available:	
External Network		Router	Bridge	
Clients		Router Router mode allow	s a connection between the router and an optical modem so as to provide Wi-Fi access.	
Work Mode		* IP Assignment	DHCP 🗸	
₩ireless	~		No username or password is required for DHCP clients.	
° [?] Network	×	IP Address	192.168.30.2	
☆ Behavior	~	Submask	255.255.0	
ඁ, Diagnostics	~	Gateway	192.168.30.1	
Advanced	~	DNS Server	192.168.5.28 172.30.44.20	
-a- -a- System	×		Save	

Items	Description	Defaults/Options
IP Assignment	Set the address assignment method of the AP to the terminal. DHCP and static IP are supported.	Default: DHCP Options: DHCP/Static IP

If DHCP is set, the address ranging from 192.168.110.100 to 192.168.110.200 will be assigned to the terminal, the default gateway is 1 92.168.110.1, and the default network mask is 255.255.255.0.

If you select the static IP, the setting page is shown as below:

Ruíjie		
Solution Device Overview	Work Mode	
⊕ Basics ^	The device is working in	Bridge mode. The following Two modes are available:
External Network	Router) Bridge
Clients	<i>i</i> Router Router mode allo	ws a connection between the router and an optical modem so as to provide Wi-Fi access.
Work Mode	* IP Assignment	Static IP 🗸
	* IP Address	Example: 1.1.1.1
° [⊘] Network ∨	* Submask	255 255 255 0
∰Behavior ~		
©₀ Diagnostics ∨	* Gateway	Example: 1.1.1.1
△ Advanced ~	* DNS Server	<u> </u>
-a- a- System		Save

«Fold

Items	Description	Defaults/Options
IP Assignment	Set an address allocation method of the AP to the terminal. DHCP and Static IP can be selected.	Default: DHCP Options: DHCP/Static IP ※ If you select the static IP, the AP will use the IP address configured by the user. In this case, users may need to configure their IP address to be in the same network segment as the AP to ensure they can log into the Web of AP again for configuration.
IP Address	Set an IP address for the AP.	Default : N/A
Submask	Set the subnet mask for the AP	Default : N/A
Gateway	Set the gateway address for the AP.	Default : N/A
DNS Server	Set the DNS server address for the AP.	Default: N/A

3 Device Overview

When users log into the Web management system, the device overview page is displayed. The overview page includes:

- Device Overview: Display the number of online users, network status and uptime.
- Device Details: Display the detailed information of the AP, such as its model, serial number, MAC address, hardware version, and software version information.
- WiFi: Display the detailed information of SSIDs, including SSID names, connection status, and encryption modes.
- Interface Details: You can check the connection status of a port by its color. When you move your mouse to the corresponding port, you can know the current rate of the port.

Ruíjie						English 🗸 🕞 Exit
A Device Overview	Device Overview					
⊕ Basics · · · · · · · · · · · · · · · · · · ·	Online Clients	0		Status 🗣 : Online Uptime: 01H 07Min 115 Systime: 2023-12-04 16:37:53		
mfBehavior ⊂ © Diagnostics ⊂ ⊖ Advanced ⊂ ± System ∽	Device Details Model: Hardware Ver: WiFi	RG-HA3515-DG V1	SN: Software Ver:	G30H9XW002000 MA_13()18941, Relate(10212719), Revision(G4 totale 15)/	MAC	C470A8.000908
	SSID 1 List WG-R: Encrypted: SSID 4 List	PR20-ABART-2810 Yes	SSID 2 List	SSID-SSID-COPORD_WI-FS R Yes	SSID 3 List	550-550-609080-3 Yes
	Wi-Fi: Encrypted: Interface Details	SSID-SSID-C0908D-4 Yea	💮 WI-FI: Encrypted	55D-55D-4098D-5 2: Yes	G W/FI: Encrypted:	SSID-SSID-C0908D-Guest Yes
< Fold	Connected Disconnected			NON LAN LAN		

3.1 Equipment Overview

Ruíjie								English 🗸 🕞 Exit
& Device Overview		Device Overview						
⊕ Basics	~	Online Clients	0		Status 🕑 : Uptime: 01	Online H 10Min 13S		
6 ⁹ Network	Ý				Systime: 20	023-12-04 16:40:55		
m∄Behavior	~	Device Details						
[©] Diagnostics	~	Model:	RG-HA3515-DG	SN:		G3QH9XW002000	MAC:	C4:70:AB:00:09:08
△ Advanced	Ý	naiuwale vel.	VI	Software ver.		Release(10212719), Revision(6a1bcbe15)/		
-a- System	Ŷ	WiFi						
		SSID 1 List		SSID 2 List			SSID 3 List	
		Wi-Fi: Encrypted:	PR20-APART-2810 Yes	WI-FI: Encry	pted:	SSID-SSID-C0908D_ Wi-Fi5 Yes	Wi-FI: Encrypted:	SSID-SSID-C0908D-3 Yes
«Fold				2010 F 11 -			6	

Items	Description
Online Clients	Display the number of current online wireless terminals.
Statuc	Display the status of Internet connection. Offline indicates that the Internet is
Status	not connected, and online means that the Internet is connected.
Uptime	Display the uptime of the device.
Systime	Displays the current time of the system.

The offline status may be caused by network disconnection, DNS or other firewalls. You can re-obtain the status by refreshing the interface. If it is still displayed as offline, check whether the network connection is normal.

3.2 Device Details

Ruíjie							English 🗸 🕞 Ex
&Device Overview		Device Overview					
Basics	Ň						
ି Wireless	Ý	Online Clients	0		Status 🕑 : Online Uptime: 01H 16Min 53S		
6 ^つ Network	~				Systime: 2023-12-04 16:47:35		
miBehavior	~	Device Details					
[©] ₀ Diagnostics	~	Model:	RG-HA3515-DG	SN:	G3QH9XW002000	MAC:	C4:70:AB:00:09:08
Advanced	~	Hardware Ver:	V1	Software Ver:	MA_1.3(1)B9P1, Release(10212719), Revision(6a1bcbe15)/		
-g- System	×	WiFi			Revision(our besc (5))		
		1					
		SSID 1 List		SSID 2 List		SSID 3 List	
		Wi-Fi: Encrypted:	PR20-APART-2810 Yes	Wi-Fi: Encryp	SSID-SSID-C0908D_ Wi-FIS ted: Yes	WI-FI: Encrypted:	SSID-SSID-C0908D-3 Yes
≪Fold						C	

Items	Description
Model	Display the device model.
Hardware Version	Display the hardware version. The initial version starts from V1.
SN	Displays the SN of the device. A SN is an unique identifier for the equipment
511	manufacturer to trace the product.
Software Version	Display the currently software version.
MAC	Display the MAC address of the device.

Click the "Basics" > "Clients" to view the terminal information connected to the AP. In this page, you also can view the IP addresses of clients.

	Ruíjie									English 🗸 🕞 Exit
	유 Device Overview		Clients	Blacklist/Whitelist						
1	Basics	^	6 Wirel	less Clients						
	External Network	¢	All 2	.4G 5G On	line Clients: 0				C Refresh	Advanced Search
2	Clients		Band	Username	MAC	IP Address	SSID	Uptime	Idle time	Action
	Work Mode		-	Xiaomi-13	BE:E1:3A:E6:74:02	-		00S	00S	Blacklist Rate
	ি Wireless	×	-	PC-4310fc	30:0D:9E:43:10:FC	-		00S	00S	Blacklist Rate
	6 ⁹ Network	Ň	-	-	9C:2B:A6:7C:8B:41	-		00S	00S	Blacklist Rate
	C Diagnostics	~	-	DESKTOP- 53MPELS	FC:45:96:55:DF:67	-		005	00S	Blacklist Rate
	Advanced	~	-	lly	18:1D:EA:5B:A6:62	-		00S	00S	Blacklist Rate
	:=- System	~	-	Galaxy-S10e	0E:BA:87:76:92:35	-		00S	00S	Blacklist Rate
			Total 6 20	D/page V	1 > Go to page	1				

3.3 Wi-Fi Status

This area displays the detailed information about currently available SSIDs, including the SSID status and encryption modes. The system can be configured with up to 5 general SSID lists and a guest SSID. When clients access the guest SSID in routing mode, they only can access the external Internet. The example below shows that only the SSID 1 list is enabled. The SSID 1 list name is PR20-APART-2810, and it is encrypted.

Basics Model: RG-HA3515-DG SN: G3QH9XW002000 MAC: C4:70-AB:00:09:08 Basics WiFi WiFi Metwork SSID 1 List SSID 1 List SSID 2 List SSID 2 List SSID 2 List SSID 4 List SSID 4 List SSID 4 List Solution SSID 4 List <	Ƴ 🕞 Exit
● Basics ✓ Minimum Minim	
☆ Wireless ✓ ☆ Network ✓ ☆ Network ✓ MBehavior ✓ SSID 1 List SSID 2 List SSID 4 List SSID 2 List SSID 7 SSID 2 List SSID 2 List SSID 4 List SSID 5 List SSID 4 List SSID 5 List Guest Wi-Fi Guest Wi-Fi	
^o Network SSID 1 List SSID 2 List SSID 3 List SSID 3 List MBehavior ^o Wi-Fi: PR20-APART-2810 ^o Wi-Fi: ^{SSID-SSID-C0908D_ ^o Wi-Fi: ^{SSID 4 List ^{SSID 5 List ^{SSID 4 List ^{SSID 5 List}}}}}</sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup></sup>	
MBehavior Vii Q Diagnostics Vii Q Diagnostics Vii Q Advanced Vii T System SSID 4 List SSID 5 List Guest Wi-Fi Guest Wi-Fi SSID 4 List	1
Q Diagnostics Image: Wirking the state of the state o	
Advanced ✓ System ✓ SSID 4 List SSID 5 List Guest Wi-Fi	
Esystem SSID 4 List SSID 5 List Guest Wi-Fi	
WI-FI: SSID-SSID-C0908D-4 WI-FI: SSID-SSID-C0908D-5 WIFI: SSID-SSID-C0908D-5 Encrypted: Yes Yes Encrypted: Yes Encrypted: Yes	ò
Interface Details	

3.4 Interface Information

This area displays the current wired port status. As shown in the following figure, the system has three wired ports. The ports in green indicate that they are enabled, and the ports in gray indicate that they are disabled. Based on port color, we can know that the first and third ports are enabled.

Ruíjie							English 🗸 🕒 Exit
윦Device Overview		SSID 1 List		SSID 2 List		SSID 3 List	
Basics	~	5510 1 654		5510 2 654		5510 5 2150	
ି Wireless	~	Wi-Fi: Encrypted:	PR20-APART-2810 Yes	Wi-Fi: Encrypted:	SSID-SSID-C0908D_ Wi-Fi5 Yes	Wi-Fi: Encrypted:	SSID-SSID-C0908D-3 Yes
ି ^୦ Network	Ŷ						
m∄Behavior	Ŷ	SSID 4 List		SSID 5 List		Guest Wi-Fi	
⊲ Diagnostics	~	Wi-Fi:	SSID-SSID-C0908D-4	Wi-Fi:	SSID-SSID-C0908D-5	WiFi:	SSID-SSID-C0908D-G
△Advanced	~	Encrypted:	Yes	Encrypted:	Yes	Encrypted:	uest Yes
System	~						
		Interface Details					
		Connected	ected	WAN	LAN LAN		
// Fold							

4 Basic Configurations

The content introduced in this chapter is suitable for users who are familiar with AP configurations. Users can optimize their networks via configuring the following features.

Ruíjie								English 🗸 🕞 Exit
욺Device Overview		Device Overview						
Basics	~	Device overview						
ି Wireless	Ý	Online Clients	0		Status 🕲 : Onlin Uptime: 01H 39	ne Min 15S		
∂ [⊘] Network	~				Systime: 2023-1	2-04 17:09:57		
míBehavior	~	Device Details						
[©] ₀ Diagnostics	~	Model:	RG-HA3515-DG	SN:	63	0002000XW002000	MAC:	C4:70:AB:00:09:08
Advanced	~	Hardware Ver:	V1	Software Ver:	MA Rel Rev	_1.3(1)B9P1, ease(10212719), vision(6a1bcbe15)/		
System	Ý	WiFi						
		SSID 1 List		SSID 2 List			SSID 3 List	
		Wi-Fi: Encrypted:	PR20-APART-2810 Yes	Wi-Fi: Encrypt	SS W ted: Ye	SID-SSID-C0908D_ fi-Fi5 ss	Wi-Fi: © Encrypted:	SSID-SSID-C0908D-3 Yes
«Fold				COD F LL L			6	

The main menus of basic configuration are shown as follows:

Menus	Description		
Pasies	Configure working modes, port features and blacklists and whitelists, and display		
Dasics	terminal information.		
Wireless	Configure the parameters of SSIDs and radios, and WPS function.		
Network	Configure and display the parameters of VLANs.		
Debovier	Configure the blacklists or whitelists of DNS/URL, port security and other security		
Denavior	features.		
Discreation	Use network tools such as ping, traceroute and DNS lookup to diagnose		
Diagnostics	networks.		

4.1 Basic Management

4.1.1 WAN Settings (Routing Mode)

In routing mode, you can connect to the Internet by modifying the IP assignment method of the WAN port.

• Click "Basics" -> "WAN" to enter the page to check the IP address of the WAN port.

Ruíjie			English 🗸 🕞 Exit
$^{P_{0}}_{\sim}$ Device Overview	WAN Settings		
⊕ Basics ^	 You can view ar 	nd manage WAN settings on this page.	0
LAN	* IP Assignment	рнср 🗸	
IPv6 Address		No username or password is required for DHCP clients.	
Clients Work Mode	IP Address	192.158.30.2	
	Gateway	192.168.30.1	
ć [?] Network ∨	DNS Server	192.168.5.28 172.30.44.20	
mîBehavior ∨		Save	
© Diagnostics			
Advanced V			
«Fold			

If you want to select another IP assignment method, you can click "IP Assignment" to change the assignment method. DHCP and static IP are available. For specific configuration steps, please refer to the section 2.5.3 "Routing Mode".

4.1.2 LAN Settings (Routing Mode)

In routing mode, you can change the default DHCP address pool settings in the LAN page.".

• Click "Basics" -> "LAN" to enter the setting page.

Ruíjie						English 🗸 🕞 Exit
Device Overview		LAN Settings				
Basics		When an AP is switched between Pouring	made and Pridge mode configurations on the	I AN side will be cleared. Please manually clear the sta	tic DHCP losco	0
WAN		When all AF is switched between Kouting	mode and bruge mode, comigurations on the	LAW side will be cleared. Flease manually clear the sta	luc Di ICF lease.	Ŷ
LAN		IP Address	Submask	Lease Time (Min)	DHCP Server	Action
IPv6 Address		192.168.110.1	255.255.255.0	1440	Enable	Edit
Clients						
Work Mode						
	~					
6 ⁹ Network	~					
m̂Behavior	~					
[©] ₀ Diagnostics	~					
Advanced	~					
-B- -B- System	~					

• Click "Edit" to enter the modification page.

Ruijie							English 🗸 🗗 Exit
$\overset{\circ}{\sim}_{\mathfrak{d}} Device$ Overview	LAN Settings						
⊕ Basics ^	When an AP is switched between	Edit			×	v clear the static DHCP lease.	0
WAN	IP Address	* IP Address	192.168.110.1	0		DHCP Server	Action
LAN IPv6 Address	192.168.110.1	* Submask	255.255.255.0			Enable	
Clients		DHCP Server	Enable	~			
Work Mode		* Lease Time (Min)	1440	Ø			
ି Wireless 🗸		* DHCP server starting address	192.168.110.100	ø			
©'Network		* DHCP server cutoff address	192.168.110.200	ø			
© Diagnostics		* Gateway	192.168.110.1	ø			
△Advanced		* DNS Server	192.168.110.1	ø			
a= a=System ∨							
«Fold				Cancel	ОК		

Items	Description	Defaults/Options	
IP Address	The gateway IP of DHCP server.	Default: 192.168.110.1	
Submask	The subnet mask of gateway IP of the DHCP server.	Default: 255.255.255.0	
DHCP Server	The switch of DHCP address pool. It is not recommended to disable it because when it is disabled, the terminal will not be assigned an IP address.	Default: Enabled Option: Enabled/Disabled/DHCP Relay	

	The lease time of the assigned IP. When the		
Looso Timo (Min)	lease expires, the IP will be reclaimed, and	Default: 1440 minutes (24 hours)	
Lease Time (Mill)	the terminal needs to reapply for an new IP	Option: 2-2880 minutes	
	address.		
DHCP server	Specify the start address of the IP address	Dofault: 192 168 110 100	
starting address	pool.	Default. 192.108.110.100	
DHCP server cutoff	Specify the end address of the IP address	Default: 102 168 110 200	
address	pool.	Default. 192.108.110.200	
Gateway	Specify the gateway address assigned to the	Default: 192 168 110 1	
Gateway	terminal.	Default. 192.108.110.1	
DNS Sonvor	Specify the DNS address assigned to the	Default: 102 168 110 1	
DIA2 261 A61	terminal.	Delault. 192.106.110.1	

In routing mode, if the WAN port is assigned an IP address in the range of 192.168.110.XX, the IP address of the DHCP address pool on the LAN side will be changed to an IP address in the range of 192.168.111.XX, and the gateway address is changed to 192.168.111.1, the start address to 192.168.111.100, and the end address to 192.168.111.200. The rest of configurations remain unchanged.

4.1.3 IPv6 Settings

Click "Basics" -> "IPv6 Address" to enter the IPv6 configuration page.

Ruijie		nglish 🗸 🕞 Exit
유 Device Overview	IPv6 Address	
Basics	Inable IPv6 to configure networking and address assigning. By default, IPv6 is supported in Bridge mode.	0
External Network	IPv6 Passthrough	
Clients	IPv6 Config Only IPv4 IPv6	
Work Mode		
ి Network		
∰Behavior ~		
△ Advanced ∨		
-a- a-System ∨		
«Fold		

The configuration items provided on the IPv6 configuration page are described in the following table:

Items	Description	Defaults/Options
	Configure whether to block IPv6 packets. When this feature	
IPv6	is enabled, IPv6 packets can be sent to wireless clients.	Default: Enabled.
Passthrough	$\%{\rm If}$ the devices on both sides have learned the other	Options: Enabled/Disabled.
	party's local link address, this function will not take effect.	
IPv6 Configuration	Configure whether the AP provides IPv6 services in routing mode. When "Only IPv4" option is selected, the AP only provides IPv4 addresses to clients. If the "IPv4&IPv6" option is selected, the AP will assign IPv4 and IPv6 addresses to clients.	Default: IPv4 &IP v6 Options: Only IPv4, IPv4&IPv6

In AP mode, IPv6 packets are transparently transmitted by default and will not be blocked.

Please note that if you select the IPv4&IPv6 option, faults may occur on a small number of APPs that do not support IPv6.

4.1.4 Clients

Click "Basics" -> "Clients" to display the current client list:

Ruíjie									English \vee 🕒 Exit
8 Device Overview	Clients	Blacklist /Whitelist							
⊕ Basics ^		Jaco Cliente							
WAN	All 2	2.4G 5G On	line Clients: 0					C Refres	Advanced Search
IPv6 Address	Band	Username	MAC	IP Address	SSID	Uptime	Idle time	Communication Mode TX Spe	Action
Clients Work Mode		Xiaomi-13	BE:E1:3A:E6:74:02	-		005	00S		Blacklist Rate
≎ Wireless ~	-	PC-4310fc	30:0D:9E:43:10:FC	-		00S	00S		Blacklist Rate
6 ⁹ Network	-	-	9C:2B:A6:7C:8B:41	-		00S	00S		Blacklist Rate
∰Behavior ~		DESKTOP- 53MPELS	FC:45:96:55:DF:67	-		00S	00S		Blacklist Rate
⊲ Diagnostics ∨		lly	18:1D:EA:5B:A6:62	-		00S	00S		Blacklist Rate
△Advanced	-	Galaxy-S10e	0E:BA:87:76:92:35			00S	00S		Blacklist Rate
System V	Total 6 2	10/page V	1 > Go to page 1						

«Fold

Items	Description					
Pand	If the client is a wireless client, it will be displayed here whether the client is currently					
Dallu	accessing the 2.4G signal or the 5G signal.					
Username	The host names of some clients, such as PC are displayed here.					
MAC	The MAC addresses of clients.					
IP Address	The IP address of clients.					
SSID	The SSID name associated with the terminal.					
Uptime	The online duration of the client.					
Idle Time	The duration of no activity or data transfer.					
Communication	Wi Eistandards, such as $802.11a/b/a/a/ac/ax$					
Mode	WI-FI standards, such as 602.11a/b/g/li/ac/ax.					
TX Speed (kbps)	If the client is a wireless client, its sending rate with the unit of Mbps will be displayed here.					
TX Speed (Kbps)	This value will be updated only by refreshing the page manually.					
RX (PKTS)	If the client is a wireless client, the number of packets it received will be displayed here.					
TX (PKTS)	If the client is a wireless client, the number of packets it sent will be displayed here.					
Signal Intensity	If the client is a wireless client, the signal intensity received by the AP from the client will be					
(dbm)	displayed here.					
PSSI (dbm)	If the client is a wireless client, its wireless signal strength will be displayed here. RSSI is					
	expressed as a negative number. The larger the number, the stronger the signal strength.					
Status	Whether the client is currently online.					
Access	This displays the client's connection type. The possible value displayed here is "wireless".					
Action	Here you can choose to conduct some simple operations on the client. There are two					
Action	management actions that can be performed: blacklisting and rate limiting.					
Pofrosh	The information on the page will not be updated dynamically. You can press this button to					
Nellesii	refresh the page to get the latest information.					
Advanced	If there are too many terminals displayed on the page, you can click the button to search a					

|--|

The descriptions of "Blacklist" and "Rate" in Action column are as follows:

• Click "Blacklist" and the following message will appear:

Ruíjie								English 🗸 🗗 Exit		
δ^2_{δ} Device Overview	Climite Placklist Mistali									
⊕ Basics ^	Wireless Clients	13 Blackist/Wnitelist								
WAN	Wireless Clients									
LAN	All 2.4G 5G	Online Clients: 1						Advanced Search		
IPv6 Address	Band Username	MAC	IP Address	SSID	Uptime	Idle time	Communication Mode TX Spe	Action		
Clients	nova 7 SE 56		192.168.110.101	SSID-PR20-APAR						
Work Mode	5G 35e57680de	92:2D:57:8D:07:10	Tip	×	065	00S	11ac 1	Blacklist Rate		
ିତ Wireless 🛛 👋	- Xiaomi-13	BE:E1:3A:E6:74:02	Client connection is in the bla want to add 92:2D:57:BD:07:10	cklist mode. Do you) to the blacklist?	00S	00S		Blacklist Rate		
ç [⊘] Network ∽	- PC-4310fc	30:0D:9E:43:10:FC	[Cancel OK	00S	005		Blacklist Rate		
∰Behavior [∨]		9C:2B:A6:7C:8B:41			00S	005		Blacklist Rate		
©, Diagnostics ∽	- DESKTOP- 53MPELS	FC:45:96:55:DF:67			00S	00S		Blacklist Rate		
Advanced ✓	- Ily	18:1D:EA:5B:A6:62			00S	00S		Blacklist Rate		
-a: System	- Galaxy-S10e	0E:BA:87:76:92:35			00S	00S		Blacklist Rate		
«Fold	Total 7 20/page 🗸	Go to page	1							

Clients added to the blacklist will not be able to access the AP. For the clients that are whitelisted or blacklisted, you can go to the "Blacklist/Whitelist " page to check the information.

• Click the "Blacklist/Whitelist", you can view the MAC of a client that is blacklisted.

Ruíjie				English 🗸 🕞 Exit
옭Device Overview		Cliente Risckliet Mbitaliet		
Basics		Blacklist Mode Whitelist Mode		
WAN		 All STAs except blacklisted STAs are allowed 	I to access WiFi.	0
IPv6 Address		Blacklist		+ Add 🗇 Delete Selected
Work Mode		Up to 32 members can be added.		
	~	MAC	Remarks	Action
° [⊘] Network	~	00:11:22:33:44:55		Edit Delete
míBehavior	~			
୍ତ୍ୱ Diagnostics	~			
Advanced	~			
System	~			
≪Fold				

• Click the "Edit" button on the Action column of a client to change the MAC address and the remarks.

Ruíjie					English 🗸 🗗 Exit
² ∂Device Overview	Clients Blacklist/Whitelist				
	Blacklist Mode Whitelit	it		×	
External Network					
IPv6 Address	All STAs except blacklisted STAs	* MAC	00:11:22:33:44:55		0
	Placklist	Remarks	test		
Work Mode	Diacklist				
₩ireless	Up to 32 members can be added.		Cancel	ОК	
2Notwork	MAL				Action
6 INCLINICK	00:11:22:33:44:55	5	test		Edit Delete
miBehavior					
© Diagnostics					
Advanced					
-e- System					
«Fold					

• Click "Delete" button in the "Action" column of client to remove the client from the blacklist so that it can connect to the AP normally.

Ruijie				English 🗸 🕞 Exit
🖧 Device Overview		Clients Blacklist/Whitelist		
Basics		Blacklist Mode		
External Network		 All STAs except blacklisted STAs are allowed to access WiFi. 		0
IPv6 Address Clients				
Work Mode		Blacklist		+ Add Delete selected
ି Wireless	~	Up to 32 members can be added.	Bemarks	Action
⊘ [?] Network	~	00:11:22:33:44:55	test	Edit Delete
miBehavior	~			
ି Diagnostics	~			
△ Advanced	~			
-a- -a-System	~			
« Fold				

• Click "Rate", and then the following configuration window will appear. In this configuration window, you can configure the uplink and downlink speeds of the clients.

Ruíjie										English 🗸 🗗 Exit
$\delta^{\frac{\Phi}{\delta}}_{\delta}$ Device Overview		Blacklist/Whitelist								
	W in	eless Clients		Rate		×				
External Network										
IPv6 Address	All	2.4G 5G 0	Online Clients: 0	* Upload speed limit	Idaas					
	Band	Username	M	0	kbps	v	SID	Uptime	Idle time	Action
Work Mode		Manager (1)	05-54-24	* Download speed limit	khos				000	
ି Wireless 🗸		XIaomi-13	BEIETISA	Ū.	kops			005	005	
2 Matwork		PC-4310fc	30:0D:9E					00S	005	Blacklist Rate
6 Network			9C:2B:A6		Cancel	ОК	J	005	005	Blacklist Rate
		DESKTOP- 53MPELS	FC:45:96:	55:DF:67				005	00S	Blacklist Rate
△Advanced		lly	18:1D:EA:	5B:A6:62				005	005	Blacklist Rate
-®= -®= System		Galaxy-S10e	0E:BA:87:	76:92:35				005	005	Blacklist Rate
	Total 6	20/page V	1 >	Go to page 1						
«Fold										

Items	Description	Defaults / options
Upload	Limit the uplink speed of the client. If it is set to 100 kbps, the	Default: 0, indicating no limit
speed limit	uplink speed of the client's network will not exceed 100 kbps.	on the uplink rate.
Download	Limit the downlink speed of the client. If it is set to 100 kbps, the	Default: 0, indicating no limit
speed limit	downlink speed of the client's network will not exceed 100 kbps.	on the downlink rate.

Blacklist/Whitelist

The blacklist and whitelist take effect only on wireless clients. Click the "Add" to add the specified a <u>MAC</u> address to the blacklist or whitelist. Wireless clients whose MAC address is added to the blacklist will not be able to access the AP. You can enter any characters such as "my mobile phone" in the Remark to help you identify the client. The operation of adding a MAC address to the whitelist is the same as that added to the blacklist. When a whitelist is configured, only the terminals with the listed MAC addresses can access the AP.

Ruíjie				English 🗸 📑 Exit
සී Device Overview		Clients Blacklist/Whitelist		
Basics		Blacklist Mode		
External Network		All STAs except blacklisted STAs are allowed to access V	NiFi.	0
Clients Work Mode		Blacklist		+ Add 💿 Delete Selected
🗟 Wireless	~	Up to 32 members can be added.		
ି Network	~	MAC	Remarks	Action
∰Behavior	~	00:11:22:33:44:55	my mobiel phone	Edit Delete
⊲ Diagnostics	~			
Advanced	~			
-a- -a- B- System	~			
«Fold				
Ruíjie				
------------------------	-------------------------------------------	------------------------------	-------------------------	
Device Overview	Clients Blacklist/Whitelist			
Basics ^	Blacklist Mode Whitelit	×		
External Network				
IPv6 Address	All STAs except blacklisted STAs * MA	C Example: 00:11:22:33:44:55	0	
	Blacklist	us	+ Add 🗇 Delete Selected	
Work Mode				
	Up to 32 members can be added.	Cancel		
6 ⁹ Network			Action	
mißehavior ∽	00:11:22:33:44:55	my mobiel phone	Edit Delete	
△Advanced				
-e- -e- System				
«Fold				

4.1.5 Mode Switching

Click "Basics" -> "Work Mode" to switch the working mode.

	Ruíjie	-		English 🗸 🕞 Exit
	Police Overview	3	Work Mode	
1	Basics	^	The device is working in Bridge mode. The following Two modes are available:	
	External Network		Router Bridge	
	IPv6 Address Clients		Bridge This mode allows you to establish a physical connection between a primary router and a secondary router, extending network coverage.	
2	Work Mode		Work Mode Bridge	
		~	Choose External Network to change the IP	
	୍ଦ ^ର Network	~	assignment mode.	
	m̂Behavior	~	IP Address 192.168.30.2	
	ඁ⊜, Diagnostics	~	Save	
	Advanced	~		
	-a- -a-System	×		
	<pre>«Fold</pre>			

4.2 Wireless Management

Click the "Wireless" -> "Wi-Fi" on the left panel to configure wireless parameters.

Ruíjie		English 🗸 🕞 Exit
Å Device Overview	Wi-Fi Settings Guest Wi-Fi	
⊕ Basics ∨	 Tip: Changing configuration requires a wireless restart and will force online clients to go offline. 	0
♥Wireless ^ Wi⊾Fi	Wi-Fi Settings	0
Radio	SSID List V	
WPS	Dual-Band Single SSID (The 2.4G and 5G bands use the same SSID.)	
°SNetwork ∨	5G Priority 🕖 🔍	
∰Behavior ∨	WI-FI Switch 💽	
⊲ Diagnostics ∨	* SSID PR20-APART-2810	
△ Advanced ~	Encryption WPA2-PSK(AES)(Recommend)	
-=- System V	* Wi-Fi Password	
	Hide SSID	
<pre>«Fold</pre>	Save	

4.2.1 Wireless Settings

The wireless management page is as shown as follows:

Ruijie		
[₽] _{6[°]8} Device Overview	WI-FI Settings Guest WI-FI	
⊕ Basics ∨	7 Tio: Changing configuration requires a wireless restart and will force online clients to go offline.	0
		U U
Wi-Fi	Wi-Fi Settings	
Radio	SSID List SSID 1 List V	
WPS	Dual-Band Single SSID (The 2.4G and 5G bands use the same SSID.)	
6 [⊘] Network ∨	5G Priority 🗾 🔍	
∰Behavior ~	WI-FI Switch	
ି୍କ Diagnostics	* SSID PR20-APART-2810	
△ Advanced ~	Encryption WPA2-PSK(AES)(Recommend) V	
÷e≓ System ∨	* WI-FI Password	
	Hide SSID	
	Save	
«Fold		

 \square The operations about wireless settings are detailed in Section 2.3 Configuring Wireless SSIDs.

4.2.2 Configuring RF Parameters

The configuration page of RF is shown as follows:

Bevice Overview	Dower & Padia				
Basics ∨	Power & Radio				
Wireless	 You can manage 2.4G and 	d 5G modules on this page.			
Wi-Fi	The terminal cannot be switch	ned online			
Radio	Period of Wireless Channel	24 H \varTheta			
WPS	2.4G Master Switch		5G Master Switch		
^o Network	2.4G Channel Auto	(CH1-11) v	5G Channel	Auto(W52) ~	
Behavior ~	Power High	100% ~	Power	High 100%	
Diagnostics	2.4G Channel Width 20MH	Hz v	5G Channel Width	20/40/80MHz ~	
Advanced	802.11 Mode 802.1	11b/q/n/ax v	802.11 Mode	802.11a/n/ac/ax v	
E System ~	WMM Switch	0	WMM Switch		
		-			
	* Maximum access 15		* Maximum access	15	
		Save			

4.2.3 WPS

Currently, WPS (Wi-Fi Protected Setup) can be configured only via the PBC (Push Button Configuration). Press and hold the WPS button for 2 seconds or click "WPS software key" to allow terminals that support WPS to access the AP without entering a password.

Ruíjie	English 🗸 🕞 Exit
$\frac{2}{\delta^2}$ Device Overview	WPS setting
⊕ Basics ∨	Winder connection can be activitized by exercise the WIC key of the device
	 At least one WinF is witch (24/3/56) in R parameter interface must be on; The corresponding WinF is SID must be on (24/3/56), and it cannot be hidden; The corresponding winF is SID must be on (24/3/56), and it cannot be hidden; The corresponding winF is side (swa2-sks and other actional exerction methods are waa-sks/waa2-sks;
Wi-Fi	Each time the WPS configuration is issued, the interval is at least 5 seconds.
Radio	WPS setting
WPS	WPS software key
$_{c}^{\diamond}$ Network	
∰Behavior ~	
Q Diagnostics	
△Advanced ~	
:e≕ System ∨	
<pre>«Fold</pre>	

4.3 Network Management

4.3.1 VLAN

After configuring the VLAN ID for wired ports and SSIDs, only packets with this VLAN tag can be forwarded.

Ruíjie				English \vee 🕒 Exit
Sevice Overview		VLAN		
⊕ Basics	~	VLAN setting for each LAN Port and WLAN. By default, all ports do not have VLAN tags.		
	~			
6 ⁹ Network		Port	VLAN ID	Action
VLAN		WAN		
mBehavior	~	LAN1	Please enter a positive integer, range format:1-4094	
©₀ Diagnostics	~	LAN2	Please enter a positive integer, range format:1-4094	
Advanced	~			
System	~	SSID-PR20-APART-2810 246 SSID 1 List	Please enter a positive integer, range format:1-4094	
		SSID-PR20-APART-2810	Please enter a positive integer, range format:1-4094	
		33 350 T Lak		
		Total 15 5/page 1 2 3 > Go to page 1		
«Fold				

Items	Description	Defaults / options
	Configure a VI ANI tag for the WANI port	Default: Untagged
WAIN	Configure a vean tag for the wan port.	Range : 1-4094
	Configure a VI ANI tag for the first I ANI port	Default: Untagged
LANT	configure a vean tag for the first ean port.	Range : 1-4094
	Configure a VI ANI tag for the second I ANI port	Default: Untagged
LAN Z	configure a vean tag for the second ean port.	Range : 1-4094
SCIDNOMON	Configure a VLAN tag for a specified SSID	Default: Untagged
2210777772	configure a versi tag for a specified SSID.	Range : 1-4094

4.4 Behavior Management

4.4.1 Access Control

You can restrict specific devices to access specific websites according to your needs. If you want to prevent a device from accessing a website, you can set the control type to blacklist. If you want a device to be able to access only specified websites, you can set the control type to whitelist.

• The specific operations are as follows:

Step 1: Click "Behavior" -> "Access Control"

Step 2: Click the "Add" to add a ACL.

1

Ruíjie								
음 Device Overview		ACL List					2	+ Add 🗇 Delete Selected
⊕ Basics	~	 Up to 64 rules can be added for a 	access control: 32 based on dor	main name and 32 on U	RL.			0
🐨 Wireless	~	-			Start and End			-
e [⊘] Network	~	Rule	Control Type	Effective Week	Time	Effective State	Remarks	Action
mißehavior	^				No Data			
Access Control		Total 0 10/page < 1	> Go to page 1					
Security								
୍କ Diagnostics	Ť							
Advanced	Ť							
: System	Ť							
«Fold								

Step 3: Then, enter the configuration page.

Ruíjie						English 🗡 🕞 Exit
Device Overview	ACL List					+ Add 💼 Delete Selected
⊕Basics	Jun to 64 miles can be added for	Add ACL		×		0
2 Network	Rule	Based on 🖗	DNS Server O URL Domain		Remarks	Action
		* MAC	Enter a MAC address.]		
Access Control	Total 0 10/page V K 1	* Domain Name List	×	0		
Security		Control Type	Blacklist \lor]		
⊖, Diagnostics		Effective State	Active ~			
Advanced		weekdays	Mon. Tue. Wed.	, 		
System			Thu. Fri. Sat. Sun.			
		Active Time	© Start Time © End Time			
		Remarks	Enter the purpose to add the ACL.			
				Cancel OK		
«Fold						

Items	Description	Defaults/Options
	Specify the rule to be based on DNS server or URL domain. The implementation principles of these two methods are different.	
Based on	Based on DNS server: When the rule is set to be filtered based on DNS, the system will resolve the DNS request of a client. If the request asks for the configured address, the rule will take effect. Based on URL domain: When the rule is set to be filtered based on URL domain, the system will resolve the URL visited by the client. If the URL accessed by the client is the configured URL, the rules will take effect.	Default: Based on DNS Server Options: Based on DNS Server or URL Domain
MAC	Specify the MAC address of the device to be controlled.	Default: N/A
Domain Name List	If the rule is based on the DNS address, you can enter a domain name list string to clarify the domain name to which the rule applies. A device in the blacklist cannot access the domain name even though its DNS addresses is matched. A device in the whitelist that matches this rule can only access the domain name configured. If you want the rule to match all URLs/addresses, enter * . If the rule is based on the domain names of URLs, you can enter the URL string to clarify the URL to which the rule applies. In this way,	Default: * * means matching all URLs and addresses.

	the devices in the blacklist that match this		
	rule cannot access the URL, and the devices in		
	the whitelist that match this rule can only		
	access the URL. If you want the rule to match		
	all URLs/ addresses , enter *.		
	Select whether to add the domain name of		
	the rule to the blacklist or whitelist.		
Control Turno	Blacklist: Devices are not allowed to access	Default: Blacklist	
control type	domain names in the blacklist.	Options: Blacklist/Whitelist	
	Whitelist: Devices are only allowed to access		
	domain names in the whitelist.		
Effective State	Make the rule active or inactive	Default: Active	
Effective State	Make the fulle active of mactive.	Options: Active/Inactive	
		Default: N/A	
Weekdays	select the day(s) of the week on which the rule	Option: Support to select any day in	
	will be enabled.	a week.	
Activo Timo	Select the time period for this rule to take		
Active fille	effect.	Default . N/A	
Bomarks	Notes can be added to identify the purpose of		
Remdrks	the rule.	Default : N/A	

Up to 64 rules can be configured, including 32 DNS-based rules and 32 URL-based rules.

4.4.2 Security

• Bridge Mode

If you do not want the terminals on LAN side to access the Web of the AP, you can click "Behavior" -> "Security" to enable "No LAN-side Access".

Ruíjie		
ကို Device Overview	Security	
⊕ Basics	O Security	
TWireless Twineless	No LAN-side Access	
⁹ Network	Save Save	
Yi Behavior		
Access Control		
Diagnostics		
Advanced		

Items	Description	Defaults /Options
No LAN side Assess	When it is enabled, the client cannot access the	Default: Disabled
NO LAN-SIDE ACCESS	device's Web from the LAN side.	Option: Enabled/Disabled

Routing Mode

In routing mode, apart from the security settings for accessing the WEB from the LAN side, you can also set the switch for accessing the WEB from the WAN side to prevent external access and attacks on the AP.

Ruíjie			
Device Overview		Security	
Basics	~	Y Users are allowed or forbidden to access the web from the LAN/WAN side or ping from the WAN side.	0
	~		Ű
° [⊘] Network	~	No LAN-Side Access	
míBehavior		No WAN Ping	
Access Control		No WAN-side Access	
Security		Whitelist +	
☉ Diagnostics	~	Save	
Advanced	ř		
:== System	~		
≪Fold			

Items	Description	Defaults /Options		
No LAN sido Accoss	When it is enabled, the client cannot access the	Default: Disabled		
NO LAN-SIDE ACCESS	device's Web from the LAN side.	Options: Enabled/Disabled		
	When it is enabled, the client cannot ping the	Default: Enabled		
NO WAN FING	device successfully from the WAN side.	Options: Enabled/Disabled		
No WAN side Access	When it is enabled, the client cannot access the	Default: Disabled		
NO WAN-SIDE ACCESS	Web from the WAN side.	Options: Enabled/Disabled		
Whitelist	In routing mode, if the "No WAN-side Access" is enabled, addresses in the whitelist can still access the device Web through the WAN port. The first address in the whitelist is still valid after reset.	Default: N/A Up to four IP addresses or IP address ranges can be configured.		

In routing mode, because the "No WAN-side Access" function is enabled by default, and no default IP address is configured on the "Whitelist", any IP address will not be able to access the AP from the WAN side.

"After the device is reset, the default IP address range stays unchanged, and WAN ping and WAN-side access are allowed." means that after setting the IP address or range, the AP can still retain it after restoring the factory settings.

4.5 Diagnostics

4.5.1 Network Tools

When the network disconnection occurs, you can use three diagnostic tools to check the network status: Ping, Traceroute, and DNS Lookup. Ping is generally used.

Ruíjie				
윤 Device Overview	Network Tools			
⊕ Basics ∨	 Network Tools 			
	Tool	Ping Traceroute	e 🔿 DNS Lookup)
_ି ଂ Network ଁ	* IP Address/Domain	www.google.com		
∰Behavior ~	* Count	4		
Q Diagnostics	* Packat Size	64		Butes
Network Tools	Tacket Size	04		bytes
△Advanced		Start		
∵a– System ∽	Result			
				d

«Fold

Items	Description	Defaults /Options		
	Specify an IDv4 address or a domain name	Default: <u>www.google.com</u>		
IP Address/Domain	used to be tested	Support modifying the IP		
	used to be tested.	address or the domain name.		
Count	Set the number of times to cond packets	Default: 4 times		
count	Set the humber of times to send packets.	Options: 1-50 times		
Docket Cine		Default: 64 bytes		
Packet Size	Set the size of the packet to be sent.	Options: 4-1472 bytes		

Trace Route:

Ruíjie			
🖧 Device Overview		Network Tools	
⊕ Basics	~	1 Network Tools	0
	×	Tool Ping • Traceroute ODNS Lookup	
₆ [⊘] Network	~	* IP Address/Domain www.google.com	
míBehavior	~	May THE 20	
Q Diagnostics			
Network Tools		Start Stop	
Advanced	~	Result	
-e- System	~		

Items	Description	Defaults/Options			
IP Address/Domain	Specify an IPv4 address or a domain name used to be tested.	Default: <u>www.google.com</u> Support modifying the IP address or the domain name.			
Max TTL	Specify the maximum value of TTLs for ICMP messages.	Default: 20 hops Options: 1~30 hops			

DNS Lookup:

Abevice Overview Basics Basics Wireless Network Tool Ping Traceroute DNS Lookup * P Address/Domain * P Address/Domain Www.google.com * P Address/Domain Result Result
Basis Wireless Network MiBehavior Network Tools Image: System
• Wireless ~ • Wireless ~ • Network ~ • Diagnostics • • Advanced ~ • System ~
P Address/Domain **P Address/Domain **P Address/Domain **********************************
MBehavior * IP Address/Domain Q Diagnostics * Network Tools Result Advanced *
Q Diagnostics Network Tools Advanced T System
Network Tools Result Advanced * Tables *
Advanced ∨ ∑System ∨
≣ System γ
«Fold

Items	Description	Defaults/Options
IP Address/Domain	Specify an IPv4 address or a domain name to be tested.	Default : <u>www.google.com</u> Support modifying the IP address or the domain name.

5 Advanced Management

5.1 User Isolation

User isolation feature can prevent users on a local Wi-Fi network from communicating with each other to ensure network security and block inadvertent data transmission. It can identify some special users that are allowed to communicate with each other via their usernames and MAC addresses. This feature is disabled by default. If you want to use it, please enable it manually.

Four working modes of user isolation:





Intra-SSID

Inter-SSID

LAN-SSID

Ruíjie		English 🗸 🕞 E
Device Overview		Isolation
⊕ Basics	~	
	~	Global Customize
° [⊙] Network	~	later SPD Jalatian
mißehavior	~	
୍ଦ୍ୱ Diagnostics	~	Save
Advanced		
Isolation		
IGMP Snooping		
Accelerated		
DMZ		
Port Mapping		
UPnP		
Local DNS		
CWMP/MACC		
DHCP		
«Fold		

Items	Description	Defaults/Options
Intra-SSID Isolation	Indicate the Intra-SSID isolation mode. When it is enabled, users connected to the same SSID cannot communicate with each other.	Default: Disabled Options: Enabled/Disabled
Inter-SSID Isolation	Indicate the Inter-SSID isolation mode. When it is enabled, users connected to the different SSIDs cannot communicate with each other.	Default: Disabled Options: Enabled/Disabled
Inter-LAN Isolation	Indicate the Inter-LAN isolation mode. When it	Default: Disabled

	is enabled, users connected to the different	Options: Enabled/Disabled
	LAN ports cannot communicate with each	
	other.	
	Indicate the LAN-SSID isolation mode. When it	
	is enabled, the traffic of the AP's LAN port will	
Isolation Between LAN	be separated from the that of the Wi-Fi	Default: Disabled
and SSID	network (SSID), so that users connected to the	Options: Enabled/Disabled
	LAN port and users connected to the SSID	
	cannot communicate with each other.	

5.2 IGMP Snooping

If Internet Group Management Protocol (IGMP) snooping is enabled in your network environment, it can help to control the broadcast of IGMP messages to avoid affecting other terminals. By default, the IGMP snooping is enabled on the device.



Items	Description	Defaults/Options
	Indicate the switch of enabling or disabling the	
	IGMP Snooping. When it is disabled, IGMP	Default: Enabled
IGMP Snooping	messages can be broadcasted in the LAN. When	Default. Ellabled.
	it is enabled, IGMP messages cannot be	Options: Enabled/Disabled
	broadcasted in the LAN network.	
	When IGMP Snooping is enabled, specify its	
	mode. There are two modes available:	
	Blocking Mode: In this mode, IGMP messages are	Default: Blocking Mode
Mode	blocked in the LAN by default. Only when a client	Options: Blocking Mode/Standard
	joins a broadcast group can the corresponding	mode
	IGMP message be sent to the LAN port where the	
	client is located.	

	Standard Mode: In this mode, IGMP messages are broadcasted to all LAN ports by default. Only when a client joins a certain broadcast group can the corresponding IGMP message be sent to the LAN port where the client is located, instead of broadcasting to all LAN ports.	
IGMP LAN to LAN Multicast	Generally speaking, the IGMP source messages come from the WAN port. By default, IGMP source messages on the LAN port will not be affected by IGMP Snooping function. But with its feature enabled, IGMP Snooping also takes effect on the IGMP source messages from the LAN ports.	Default: Disabled. Options: Enabled/Disabled

5.3 Acceleration Settings

When the hardware acceleration is enabled, the overall performance of the device will be improved, but some software functions will be affected.

Ruíjie		English 🗸 🕞 Exit
2 Device Overview		Accelerate
⊕ Basics	~	Note: After hardware acceleration is enabled, the system performance will be improved, but some software functions will be affected. For example, in mesh scenarios, communication exceptions may occur after multiple terminal
₩ireless	~	V roaming.
° [?] Network	~	Hardware speedup 🕥
m̃Behavior	~	Save
୍ଦ୍ୱ Diagnostics	~	
Advanced		
Isolation		
IGMP Snooping		
Accelerated		
Local DNS		
CWMP/MACC		
📳 System	~	
«Fold		

5.4 DMZ (Routing Mode)

If you set up a server on an internal network, such as an FTP server, and want to access the server from an external network, you can use the DMZ function to specify the host on the internal network to enable all ports to be accessed from the external network.

Ruijie			English 🗸 🕞 Exit
Police Overview	DMZ Rule Co	nfig	
Basics			
	The Broadb	nd Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer. sible only in router mode.	0
6 ⁹ Network	Because the	firewall is enabled by default, the DMZ function will be disabled. To use the DMZ function, ensure that the IPv4 firewall function is disabled.	
m∄Behavior	DMZ 💽		
[©] ₀ Diagnostics	* Dest IP Address	Example: 1.1.1.1	
Advanced	Save		
Isolation			
IGMP Snooping			
Accelerated			
DMZ			
Port Mapping			
UPnP			
Local DNS			
«Fold			
Ite	ms	Description Defaults/Optio	ons
DMZ		Enable or disable DMZ function. Only when it is Default: Disabled.	

	enabled can the IP address of the host be	Options: Enabled/Disabled
	configured.	
Destination IP Address	After the DMZ function is enabled, specify the IP address of the DMZ host in the internal network. After configuration, AP will use the IP address of	Default: N/A Specify the IPv4 address of the DMZ bost
	WAN port as the external IP address by default .	DWZ HOSt.

5.5 Port Mapping (Routing Mode)

Normally, the host of an internal network cannot be accessed from an external network. However, if the port mapping is enabled, users can access the host from the external network.

Port mapping maps the host IP address n port of an external network to a device in the local area network to provide corresponding services. When a user accesses the port of this IP, the server automatically maps the request to the device in the local area network.

Click "Advanced" - > "Port Mapping" to go to setting page.

Ruíjie			English 🗸 🗗 Exit
$^{\circ}_{\delta \circ}$ Device Overview		Port Mapping List	+ Add 🗇 Delete Selected
Basics	~		
	~	Note: You need to re-compute port mapping after changing the work mode of the networking type (dynamic in / static in K= / broadband internet). This part is visible only in router mode.	0
ି Network	~	Because the firewall is enabled by default, the port mapping function will be disabled. To use the port mapping function, ensure that the IPv4 firewall function is disabled.	sabled.
m̃Behavior	~	Name Protocol Internal IP Address Internal Port External Port	Action
⊲ Diagnostics	~	No Data	
Advanced		Total 0 20/page > < 1 > Go to page 1	
Isolation			
IGMP Snooping			
Accelerated			
DMZ			
Port Mapping			
UPnP			
Local DNS			
≪ Fold			

Click "Add" to add a port mapping entry.

Ruíjie							
Device Overview	Port Mapping List				_	+ A	dd 🍈 Delete Selected
Basics	I tott mapping not	Add		\times			
중 Wireless	Note: You need to re-configure port ma This part is visible only in router mode.	* Nama	Diana antar Nama		P <=> broadband	Internet).	0
ି Network	Because the firewall is enabled by defau	Deste cel			ensure that the IPv		
míBehavior	Name	* Futernal Dart /Dange	ICP		l Port	External Port	Action
⊖ Diagnostics		* External Port/Kange	C				
Advanced	Total 0 20/page 🗸 🤇 1 🗦	* Internal IP Address	Enter internal server IP				
Isolation		 Internal Port/Range 		e			
IGMP Snooping							
Accelerated			Cancel	ОК			
DMZ							

Items	Description	Defaults/Options
Name	Set a rule name.	Default: N/A
Protocol	Specify a protocol	Default: TCP
		Options: TCP and UDP
	Specify the port number to be mapped to the	
Extornal Port/Pango	external network.	Default: N/A
External Port/Range	By default, the IPv4 address of the external	Port Number Range: 1-65535
	network is the IP address the WAN port.	
Internal IP Address	Specify the IPv4 address to be mapped to the	Default · N/A
Internal IF Address	external network.	
	Specify the port number to be mapped to the	Default: N/A
Internal Port/Range	internal network.	Port Number Range: 1-65535

✓ It should be noted that after changing the working mode or network type (such as changing the dynamic IP to the static IP), you need to reconfigure the port mapping.

5.6 UPnP (Routing Mode)

The main function of UPnP (Universal Plug and Play) is to automatically install and configure a network device. With the UPnP, devices can share resources within the LAN.

Ruijie			English 🗸 🕞 Exit
${}_{\delta}^{P}$ Device Overview		UPnP	
Basics	~	 It is a new laterest verticeal strengtwine communication between divisor. If the dwise is in Division stack, DS Lite or MAR 5, LIReB is not supported. 	
	~	It is a new interfact policity amend a improving communication between devices in the device is in the single-stack, Do-title or work -t, On in is not supported. This part is visible only in router mode.	
୍ଦ ^ର Network	~	UPnP:	
∰Behavior	~	Save	
	~		
OAdvanced			
Isolation			
IGMP Snooping			
Accelerated			
DMZ			
Port Mapping			
UPnP			
Local DNS			
«Fold			

5.7 DNS Server

If you want to use a specific DNS server, you can set it on this page. Usually the DNS server address used by the AP is automatically obtained from its uplink network.

Ruíjie		English ∨ ⊕Exit
$\frac{9}{\delta^2\delta} Device$ Overview		DNS Server
Basics	\sim	
	~	Configuring the local DNS server is optional. By default, the device obtains the IP address of the DNS server from uplinked devices.
ି Network	~	DNS Server
∰ Behavior	~	Save
Diagnostics	~	
~ Diagnostics		
Advanced		
Isolation		
IGMP Snooping		
Accelerated		
DMZ		
Port Mapping		
UPnP		
Local DNS		
«Fold		

Items	Description	Defaults/Options
		Default: Disabled.
DNS Sever	When it is enabled, you can specify the local DNS	By default, the DNS address is
	server address for the AP, so that the AP will not	not specified, but automatically
	use the address automatically obtained from its	obtained from its uplink
	uplink network.	network.
		Options: Enabled/Disabled

Ruíjie	English 🗸 🕞 Exit
$\mathcal{S}_{\mathfrak{d}}^{\mathbb{P}}$ Device Overview	DNS Server
⊕ Basics ∨	
© Wireless	Configuring the local DNS server is optional. By default, the device obtains the IP address of the DNS server from uplinked devices.
• •••••••••••	DNS Server
6 [℃] Network ~	* Local DNS server
∰Behavior ~	
	Save
~ Diagnostics	
△ Advanced ^	
Isolation	
IGMP Snooping	
Accelerated	
DMZ	
Port Mapping	
UPnP	
Local DNS	
«Fold	

After it is enabled, you can enter the DNS server address.

Items	Description	Defaults/Options
Local DNS Server	Manually specify the address of DNS Server.	Default: N/A. The DNS server address is automatically assigned by the uplink network .

✓ It should be noted that before configuration, please ensure that the DNS Server to be configured is working normally, otherwise it may fail to access the Internet.

5.8 DHCP (Routing Mode)

Assign a fixed IP address to the downstream client by adding its MAC address. (Up to 20 clients can be added.)

Ruíjie					English ∨ ⊖Exit
6 [™] Network	~	Static Address Pool			+ Add 🗇 Delete Selected
୍ଦ୍ର Diagnostics	~	<i>i</i> Enter the MAC information of the downli This part is visible only in router mode.	ink terminal to assign a fixed IP address to the terminal. Up	to 20 members can be added.	
Advanced		МАС	IP Address	Remarks	Action
Isolation		00:11:22:33:44:55	192.168.110.120	1	Edit Delete
IGMP Snooping Accelerated		Total 1 10/page < 1 >	Go to page 1		
DMZ					
Port Mapping					
UPnP					
Local DNS					
CWMP/MACC					
DHCP					
Firewall					
System	~				
≪ Fold					

Items	Description
MAC	Display the client's MAC address.
IP Address	Display the assigned IP address.
Pomarka	Display the note for the MAC address. You can enter any description such as "my
Refficience	mobile phone".
Action	Two management actions can be performed, including modification and deletion.

The description of "Edit" and "Delete" in the Action column:

• Click "Edit" to modify the client's MAC address, assigned IP and the remark.

Ruijie							
MiBehavior ~	Static Address Pool	5.19			×	1	
© Diagnostics ∨	Enter the MAC information of the do This part is visible only in router moc	Edit			^	added.	
	□ MAC	* MAC	00:11:22:33:44:55			emarks	Action
Isolation	00:11:22:33:44:55	* IP Address	192.168.110.120			1	Edit Delete
IGMP Snooping		Remarks	1				
Accelerated	Total 1 10/page 🗸 🧹 1 🔿						
DMZ							
Port Mapping				Cancel	ОК		
UPnP							
Local DNS							
CWMP/MACC							
Firewall							
÷e= System ∨							
<pre>«Fold</pre>							

• Click "Delete" to delete the assigned IP. After the AP is connected again, a random IP address is obtained.

Ruijie				
©" INEtWORK ·	Static Address Pool	minal to assign a fixed IP address to the terminal. Up to 20	members can be added	
Solution Construction Construct	This part is visible only in router mode.			
Advanced ^	МАС	IP Address	Remarks	Action
Isolation	00:11:22:33:44:55	192.168.110.120	1	Edit Delete
IGMP Snooping Accelerated	Total 1 10/page v K 1 > Go	Are you sure you want to delete the entry?	×	
DMZ		Cancel	ж	
Port Mapping				
UPnP				
Local DNS				
CWMP/MACC				
DHCP				
Firewall				
System V				
«Fold				

5.9 Firewall (Routing Mode)

A firewall is a network security device or software used to monitor and control network traffic to protect the network from suffering unauthorized access, malicious attacks, and data leaks. Firewalls filter network traffic by restricting access to specific IP addresses, ports or protocols through rules or implementing access control policies to block potential threats.

With the firewall feature, the AP restricts access to the ports based on its IPv4 or IPv6 TCP and UDP protocols.

Ruijie				English 🗸 🕒
	~	Firewall		
°S Network	~	1 This part is visible only in router mode.		
míBehavior	~	SPI Firewall mode Only IPv4 Only IPv6 OIPv4 & IPv6	O Disable	
୍ଦ୍ର Diagnostics	~	* IPv4 TCP Internal Port/Range default	0	
Advanced		* IPv4 TCP External Port/Range 137-139,445,1243,2049,12345,273	0	
Isolation		* IPv4 UDP Internal Port/Range default	Θ	
IGMP Snooping Accelerated		* IPv4 UDP External Port/Range 137-139,445,2049,31789,31791	0	
DMZ Port Mapping		* IPv6 TCP Internal Port/Range default	0	
UPnP		* IPv6 TCP External Port/Range 137-139,445,1243,2049,12345,273	θ	
Local DNS		* IPv6 UDP Internal Port/Range default	0	
DHCP		* IPv6 UDP External Port/Range 137-139,445,2049,31789,31791	θ	
Firewall		Save		
-e- System	~]
«Fold				

Items	Description	Defaults/Options	
SPI Firewall Mode	Four options are available: Only IPv4, IPv4 & IPv6, Only IPv6, Disabled.	Default: IPv4 & IPv6	
IPv4 TCP Internal Port/Range	The internal port range of IPv4 TCP is from 1 to 65535. You can specify a single port (X) or a port range (X-Y). If multiple items are configured, separated them by commas (,).	It is recommended to specify the default configuration, which is to select all ports.	
IPv4 TCP External Port/Range	The external port range of IPv4 TCP is from 1 to 65535. You can specify a single port (X) or a port range (X-Y). If multiple items are configured, separated the by commas (,).	It is recommended to specify the following ports that are frequently attacked: 137-139, 445, 1243, 2049, 12345, 27374, 31785	
IPv4 UDP Internal Port/Range	The internal port range of IPv4 UDP is from 1 to 65535. You can specify a single port (X) or a port range (X-Y). If multiple items are configured, separated them by commas (,).	It is recommended to select the default configuration, which is to select all ports.	
IPv4 UDP External Port/Range	The external port range of IPv4 UDP is from 1 to 65535. You can specify a single port (X) or a port range (X-Y). If multiple items are configured, separated them by commas (,).	It is recommended to specify the following ports that are frequently attacked: 137-139, 445, 2049, 31789, 31791	
IPv6 TCP Internal Port/Range	The internal port range of IPv6 TCP is from 1 to 65535. You can specify a single port (X) or a port range (X-Y). If multiple items are configured, separated them by commas (,).	It is recommended to select the default configuration, which is to select all ports.	
IPv6 TCP External Port/Range	The external port range of IPv6 TCP is from 1 to 65535. You can specify a single port (X)	It is recommended to specify the following ports that are	

	or a port range (X-Y). If multiple items are	frequently attacked:		
	configured, separated them by commas	137-139, 445, 1243, 2049, 12345,		
	(,).	27374, 31785		
	The internal port range of IPv6 UDP is			
	from 1 to 65535. You can specify a single	It is recommended to select the		
IPv6 UDP Internal Port/Range	port (X) or a port range (X-Y). If multiple	default configuration, which i		
	items are configured, separated them by	to select all ports.		
	commas (,).			
	The external port range of IPv6 UDP is	It is recommended to select the		
	from 1 to 65535. You can specify a single	following ports that are		
IPv6 UDP External Port/Range	port (X) or a port range (X-Y). If multiple	frequently attacked:		
	items are configured, separated them by	137-139,445,2049,31789,31791		
	commas (,).			

6 System Management

6.1 NTP Settings

Network Time Protocol (NTP) is a protocol used to synchronize the clocks of devices on a network. NTP is designed to ensure that the consistency and accuracy of clicks of devices on the network.

Ruíjie						English 🗡 🕞 Exit
[₽] Device Overview	NTP Setting					
⊕ Basics ∨	NTP function	٠ ٢				
	* NTP Server Name	p nict in				
⊘ ^o Network ∨	t Confirmation time	panetip				
∰Behavior ~	* Confirmation time 24	nour				
©₀ Diagnostics ∽	Time Zone (G	TM 09:00) Tokyo, Osaka, Sapporo				
△Advanced ∨	Time 🕒 :	2023-12-04 21:15:57	Current Time			
:말:System ^		Save				
NTP Setting						
Port Management						
Login						
Restore						
Reset Configuration						
LED						
Web CLI						
System Log ≪Fold						

Items	Description	Defaults
NTP function	Enable or disable NTP function.	Default: Enabled.
NTP Server Name	Specify the domain name of the NTP server.	Default: ntp.nict.jp
Confirmation Time	Specify the synchronization period.	Default: 24 hours
Time Zone	Specify the time zone.	Default: (GTM 09:00) Tokyo, Osaka, Sapporo
Time	Display the current time.	Default: Current time.

6.2 Port Management

This function is designed to manage the physical attributes of the WAN port and two LAN ports. Currently, a WAN port cannot be set to a G.hn port. The LAN port supports shutdown and rate negotiation (Auto/100Mbps/1000Mbps).

Ruíjie					English 🗡 🕒 Exit
్లి Device Overview	Port Management				
⊕ Basics ∨		we want of the second	2		
	Please contirm before	modifying, if the setting is wrong, the communic	ation may fail.		
2 Natwork	ID	Port	Speed	Status	Action
6. Network	1	WAN	1816/1682M	Enable	Edit
∰Behavior ~	2	LAN 1	Auto	Enable	Edit
©₀ Diagnostics ∨		14112			
△Advanced	3	LAN 2	Auto	Enable	Edit
i∰ System^	L				
NTP Setting					
Port Management					
Login					
Restore					
Reset Configuration					
LED					
Web CLI					
System Log					
«Fold					

6.3 Login Management

6.3.1 Administrator Password

In order to improve system security and make information interaction more secure, please click "System" -> "Login"-> "Login Password" to change the default password.

Ruíjie			English 🗸 🕞 Eat
$\frac{\circ}{\delta \ \delta}$ Device Overview	Login Password Login Tim	neout Login Name	
⊕ Basics ~	Administrator Passwo	rd	0
⇔ Wireless			U
° [⊘] Network ∽	* Old Password	775	
∭Behavior	* New Password	بېرې مېرې	
Diagnostics	* Confirm Password	* **	
		Save	
Advanced	L		
System ^			
NTP Setting			
Port Management			
Login			
Restore			
Reset Configuration			
LED			
Web CLI			
System Log ≪Fold			

Items	Description	Defaults/Options
Old Password	Enter the original password: admin	Default: admin

New Password	Enter a new password.	Default: N/A
Confirm Password	Enter the password you set for confirmation.	Default: N/A

6.3.2 Session Timeout

In this page, you can set the Web session timeout. After the timeout is configured, Web will automatically log out when it is in standby state for a long time.

Ruíjie		
and Device Overview	Login Password Login Timeout Login Name	
⊕ Basics ∨	Session Timeout	٦
♥Wireless	Session Switch	1
6 ^o Network	* Session Timeout 300 S	
∭Behavior ~		
୍ଦ୍ର Diagnostics ଁ		
△ Advanced		_
System ^		
NTP Setting		
Port Management		
Login		
Restore		
Reset Configuration		
LED		
Web CLI		
«Fold		

Items	Description	Defaults/Options
Session Switch	Enable or disable the login timeout function.	Default: Enabled. Options: Enabled/Disabled
Session Timeout	When the session timeout is enabled, specify the time value. If no operation is performed on the Web management system for the time that exceeds the configured time, the system will be logged out.	Default: 300 seconds Options: 300-7200 seconds

6.3.3 Account Name

By default, the account name is admin. You can change the account name in the following page.

Ruíjie	English 🗸 [Exit
🖧 Device Overview	Login Password Login Timeout Login Name	
⊕ Basics ∨	() Account	٦
♥ Wireless	* Original administrator account	1
$^{\circ}$ Network $^{\vee}$	* New administrator account	
í∬Behavior ~		
Q Diagnostics ✓	Save	
△ Advanced ~		
System		
NTP Setting		
Port Management		
Login		
Restore		
Reset Configuration		
LED		
Web CLI		
System Log ≪Fold		

6.4 Configuration Management

6.4.1 Restore

If you need to restore the system, please click "System" -> "Restore" to restore the device.

Ruijie	Ēr	nglish 🗠 🕒 Exit
A Device Overview	Restore Backup & Import	
⊕ Basics ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	Restoring factory settings will delete all current configurations.	0
₩ireless	✓ Factory Model currently allocated ✓	
° Network	Restore	
∰ Behavior ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		
☉ Diagnostics	×	
△Advanced ~	×	
System 🔿		
NTP Setting		
Port Management		
Login		
Restore		
Reset Configuration		
LED		
Web CLI		
System Log «Fold		

6.4.2 Backup and Import

• If you want to keep the current configuration settings after restore the system, please click "Restore" -> "Backup & Import" -> "Export" to export the current configuration file of the device.

Ruíjie		English 🗸 🕞 Exit
and Device Overview	Restore Backup & Import	
⊕ Basics ∨	If the target version is much later than the current version, some configuration may be missing.	0
ି Wireless ଁ	It is recommended to choose Restore before importing the setup. The device will be rebooted automatically after the importing.	÷
_ି ଂ Network ଁ	Backup Setup	
mißehavior ∽		
ඁ©, Diagnostics ∽		
△ Advanced ~	rite raui Prease select a me. Browse import	
訾 System へ		
NTP Setting Port Management		
Login		
Restore		
Reset Configuration		
Web CLI		
System Log ≪Fold		

• After the device is restored, if you want to reuse the previous configurations, please click "Browse" in the Import Setup page to select the previous configuration file.

Ruíjie		English 🗸 🕞 Exit
🖧 Device Overview	Restore Backup & Import	
⊕ Basics ∨	If the target version is much later than the current version, some configuration may be missing.	0
	Backup Setup	-
6 ⁹ Network ∽	Backup Setup Export	
mîBehavior ∨	Import Setup	
⊖, Diagnostics ∨		
△Advanced ~	The fault Pricase select a file. Drowse import	
System ^		
NTP Setting		
Port Management Login		
Restore		
Reset Configuration		
LED		
Web CLI		
System Log 《Fold		

• Click "Import" to import the previous configurations. Then, click "OK" to confirm the operation.

Ruijie	English ~	∕ 🕞 Exit
and Device Overview	Restore Backup & Import	
⊕ Basics ~	f the target version is much later than the current version, some configuration may be missing.	0
♥Wireless	It is recommended to choose Restore before importing the setup. The device will be rebooted automatically after the importing.	Ŭ
₆ ⁰ Network [∨]	васкир Setup	
miBehavior ∽	Backup Setup	
🔍 Diagnostics 🛛 👋	Tip ×	
△Advanced ~	File Path rgcall_config.text Browse Image: Path Prove you sure you want to import the setup and then the device will be rebooted automatically?	
	Cancel	
NTP Setting		
Port Management		
Login		
Restore		
Reset Configuration		
LED		
Web CLI		
System Log «Fold		

• Load the configurations. Please wait.

Ruíjie		English \vee 🕒 Exit
¢ ² Network ∽	Restore Backup & Import	
∰Behavior ~	If the target version is much later than the current version, some configuration may be missing. It is recommended to choose Restore before importing the setup. The device will be rebooted automatically after the importing.	?
©, Diagnostics 👋	Backup Setup	
△Advanced	Backup Setup Export	
	Import Setup	
NTP Setting	File Path Disarce celect a file Persuan Import	
Port Management	Loading	
Login		
Restore		
Reset Configuration		
LED		
Web CLI		
System Log		
Upgrade		
Reboot		
Development Mode		
<pre>«Fold</pre>		

• After the configuration is completed, the device will restart. Please wait.

Ruíjie		English \vee 🕞 Exit
_େ ି Network	Restore Backup & Import	
mißehavior ∽	If the target version is much later than the current version, some configuration may be missing. It is recommended to choose Restore before importing the setup. The device will be rebooted automatically after the importing.	0
୍ଦ୍ୱ Diagnostics 🗸 🗸	Backup Setup	
	Backup Setup Export	
	Import Setup	
NTP Setting	File Path Please select a file. Browse Import	
Port Management	Restoring	
Restore		
Reset Configuration		
LED		
Web CLI		
System Log		
Upgrade		
Development Mode		
«Fold		

• After the restart is complete, log in to the Web system again.

Program	
Circleit Duck Rend Wi Fi & Deuter	
Enter the device username Enter the device password	
Login	
Forget the account or password?	
Support Chrome, Firefox, Microsoft Edge browser © 2000-2023 Ruijie Networks Co., Lto Official Website: https://www.ruijie.co.jp	ł

 \square The related operations of device login have been described in detail in Section 2.1.

6.5 Reset Settings

In this page, you can determine whether the reset button can be used or not. It is enabled by default.

Ruijie	English ~	Exit
c° Network	Reset Configuration	
☆ Behavior ~	1 Reset Configuration	0
₀, Diagnostics ∨	Reset Button Status 📃	
△ Advanced	Save	
System ^		
NTP Setting		
Port Management		
Login		
Restore		
Reset Configuration		
LED		
Web CLI		
System Log		
Upgrade		
Reboot		
Development Mode		
«Fold		

6.6 LED Settings

In this page, you can enable or disable LEDs. Also, you can schedule the LED to be enabled or disabled at a specific time period.

Ruijie	English	∼ 🕞 Exit
c^{9} Network	LED Status Control	
☆ Behavior ~	You can change the status of all LEDs on this page.	0
₀, Diagnostics ∨	LED O Enable 🔿 Disable 🔿 Customize	
△ Advanced	Save	
System ^		
NTP Setting		
Port Management		
Login		
Restore		
Reset Configuration		
LED		
Web CLI		
System Log		
Upgrade		
Reboot		
Development Mode		
«Fold		

• If you want to LEDs to light at a scheduled time, follow the following steps:

Step 1: Click "Customize".

Step 2: Click the "Add" button to go to the setting page.

Ruíjie					English 🗡 🕞 Exi
$_{c}^{\mathcal{P}}$ Network	LED Status Control				
∰ Behavior Ý	You can change the status of all LEDs on this page.				?
୍ଦ୍ୱ Diagnostics ଁ	LED Enable Disable Customize				
△Advanced	Status	Day		Time	Action
∰ System ^			No Data		
NTP Setting					
Port Management					2 + Add
Login	Save				
Restore					
Reset Configuration					
LED					
Web CI I					
System Log					
Upgrada					
Debaat					
Report					
Vevelopment Mode					
<pre>«Fold</pre>					

Ruíjie

₆ ?Network ∽	LED Status Control		
mBehavior ∼	You can change the status of all LEDs on this page	Add a Rule ×	0
् Diagnostics ४	LED Enable Disable OCustomize	LED 💽	
	Status	* Day _ Mon Tue Wedme	Action
		Thu. Fri. Sat. Sun.	
NTP Setting		Start Time 00 v : 00 v	+ Add
Port Management	Save	Find Times 24	- 400
Login			
Restore			
Reset Configuration		Cancel	
Web CLI			
System Log			
Upgrade			
Reboot			
Development Mode			
«Fold			

Items	Description	Defaults/Options
	If the switch is in on state, it means that the	
	LEDs will turn on in the specified time period.	Default: Enabled
	If the switch is in off state, the LEDs will turn	Option: Enabled/Disabled
	off in the specified time period.	
Dav	Specify the day(c) of a week	Default: N/A
Day	specify the day(s) of a week.	Options: Any day of the week.
		Default: 00:00
Start Time	Specify the start time on the day of a week.	Drop down the selection box to
		select a start time.
End Time	Charify the and time on the day of a weak	Default: 24:00
End Time	specify the end time on the day of a week.	Drop down the selection box to

select an end time.

6.7 Web CLI

You can run rgcall commands in the page to deliver configurations.

Ruíjie	English 🗸 🕒 Exit
c^{9} Network	Web CLI
m Behavior ~	You can use this page to send commands to the device for execution and display the relevant execution results,
Q Diagnostics ∨	* Execute command
△Advanced ~	Start execution
system ^	results of enforcement
NTP Setting	
Port Management	
Login	
Restore	
Reset Configuration	
LED	
Web CLI	
System Log	
Upgrade	
Reboot	
Development Mode	
<pre>«Fold</pre>	

6.8 System Log

Checking system logs is a way for locating fault causes.

When a large number of logs are available, you can enter key words, log types, modules or dates to figure out the logs you need for locating fault causes.

Ruíjie						English 🗡 🕞 Exit
₆ ? Network	System Log					
mîBehavior ∽	👔 You can view system log	gs on this page. You ca	n also Download Log Package.			
୍ଦ୍ୱ Diagnostics ଁ				Please enter key words Please	ase select a type 🗸 Please select a module 🗸 🗎 2023-12-05	a
△Advanced ∨	Data	Turne	Madula		Betwile	
System ^	2023-12-05 11:26:36	log	System Log	user operation: info	Details	
NTP Setting	2023-12-05 11:26:34	log	Login module	login sucess!		
Port Management	2023-12-05 11:11:36	log	System Log	user operation: info		
Restore	2023-12-05 11:11:35	log	Login module	login sucess!		
Reset Configuration	2023-12-05 10:50:13	log	System Log	log storage success		
LED	2023-12-05 09:49:13	log	System Log	log storage success		
System Log	2023-12-05 08:48:13	log	System Log	log storage success		
Upgrade	2023-12-05 07:47:12	log	System Log	log storage success		
Reboot	2023-12-05 06:46:12	log	System Log	log storage success		
Development Mode	2023-12-05 05:45:12	log	System Log	log storage success		

6.9 System Upgrade

6.9.1 Manual Upgrade

Click "System" -> "Upgrade" to manually upgrade the software version of the device Step 1: Click the "File" button to select an upgrade file.

Ruíjie		English 🗸 🕒 Exit
₆ [⊙] Network ∽	Local Upgrade Ghn Upgrade	
mîBehavior ∨	Local Upgrade Please do not refresh the page or close the browser.	0
୍ଦ୍ୱ Diagnostics 🗸 🗸	Please ensure that there are no special characters in the upgrade file name, such as space , %, ¥ ,etc.	
△Advanced ~	Model RG-HA3515-DG	
뺥 System ^	Current Version MA_1.3(1)B9P1, Release(10212719), Revision(6a1bcbe15)/	
NTP Setting	File Path Please select a file. Upload	
Port Management		
Login		
Restore		
Reset Configuration		
LED		
Web CLI		
System Log		
Upgrade		
Reboot		
Development Mode		
«Fold		

Step 2: After selecting the upgrade file, click the "Upload" button to start downloading the software to the device.

Ruijie	Eng	
ç ⁹ Network ∽	Local Upgrade G.hn Upgrade	
mißehavior ∨	Local Upgrade Please do not refresh the page or close the browser. Please ensure but have are no spacial characters in the upgrade file name such as space % ¥ etc.	0
©₀ Diagnostics ∨		
△Advanced ~		
System ^	Current Version MA_1.3(1)B9P1, Release(10212/19), Revision(6a1bcbe15)/	
NTP Setting	File Path MA_1.3(1)B9P1_HA351! Browse Upload	
Port Management		
Login		
Reset Configuration		
LED		
Web CLI		
System Log		
Upgrade		
Reboot		
«Fold		

Step 3: Click " OK " to start the upgrade process.

0

Please wait patiently during the upgrade process.

Ruíjie	
° ² Network ∽	Local Upgrade G-hn Upgrade
∰ Behavior ~	Local Upgrade Please do not refresh the page or close the browser. Please do not refresh the page or close the browser. (2) Please do not refresh the page or close the browser. (2) Please do not refresh the page or close the browser. (3) Please do not refresh the page or close the browser. (4) Please do not refresh the page or close the browser. (5) Please do not refresh the page or close the browser. (5) Please do not refresh the page or close the browser. (5) Please do not refresh the page or close the browser. (6) Please do not refresh the page or close the browser. (7) Please do not refresh the page or close the browser. (7) Please do not refresh the page or close the browser. (7) Please do not refresh the page or close the browser. (7) Please do not refresh the page or close the browser. (7) Please do not refresh the page or close the browser. (7) Please do not refresh the page or close the browser. (7) Please do not refresh the page or close the browser. (7) Please do not refresh the page or close the browser. (7) Please do not refresh the page or close the browser. (7) Please do not refresh the page or close the browser. (7) Please do not refresh the page or close the browser. (7) Please do not refresh the page or close the browser. (7) Please do not refresh the page or close the browser. (7) Please do not refresh the page or close the browser. (7) Please do not refresh the page or close the browser. (7) Please do not refresh the page or close the browser. (7) Please do not refresh the page or close the browser. (7) Please do not refresh the page or close the page or close the browser. (7) Please do not refresh the page or close the browser. (7) Please do not refresh the page or close the browser. (7) Please do not refresh the page or close the browser. (7) Please do not refresh the page or close the browser. (8) Please do not refresh the page or close the browser. (8) Please do not refresh the page or close the browser. (8) Please do no
🔍 Diagnostics 🛛 🗸	rease ставие настояте аге но зречая навачеся и иле иријаче не завле, зична зраче, л, + ,еч.
△Advanced ~	Model RG-HA3515-DG
	Current Version MA_1.3(1)89P1, Release(10212719), Revision(6a1bcbe15)/
NTP Setting	File Path MA_1.3(1)B9P1_HA351! Browse Upload
Port Management	Upgrading
Login	
Restore	
Reset Configuration	
LED	
Web CLI	
System Log	
Upgrade	
Reboot	
Development Mode	
<pre>«Fold</pre>	

Step 4: After the upgrade is successful, you will return to the login interface. Please use the password to log into the Web management system again, and check the software version in "Device Details" to confirm whether the upgrade is successful.

Ruíjie								English 🗸 🔂 Exit
⁹ _{6⁶6} Device Overview		Device Overview						
⊕ Basics	~	Online Clients	0		Status 😧 : Online			
₀ [⊙] Network	v	0			Systime: 2023-12-05 12:03:09			
ាាំBehavior	×	Device Details						
© Diagnostics	ž	Model: Hardware Ver	RG-HA3515-DG	SN:	G3QH9XW002000	MAC:		C4:70:AB:00:09:08
System	Ŭ,			Solution Col.	Revision(6a1bcbe15)/			
		WiFi						
		SSID 1 List		SSID 2 List		SSID 3 Lis	st	
		Wi-Fi: Encrypted:	SSID-PR20-APART-2810 Yes	Wi-Fi: Encrypte	SSID-SSID-C0908D_Wi-Fi5 ed: Yes	((•	Wi-Fi: Encrypted:	SSID-SSID-C0908D-3 Yes
		SSID 4 List		SSID 5 List		Guest Wi	-Fi	
			SSID-SSID-C0908D-4 Yes	Wi-Fi: Encrypte	SSID-SSID-C0908D-5 ed: Yes	((•	WiFi: Encrypted:	SSID-SSID-C0908D-Guest Yes
«Fold		Interface Details						

6.9.2 G.hn Firmware Upgrade

G.hn firmware can be upgraded separately. The upgrade of G.hn firmware is perfumed by the main program.

Ruíjie	English 🗸 🔂 Exit			
m∄Behavior ∨				
© Diagnostics ∨	Local Upgrade G.hn Upgrade			
△Advanced ∨	G.hn Upgrade This page is used to upgrade G.hn firmware. Please ensure that there are no special characters in the upgrade file name, such as space , %, ¥ ,etc.			
System ∧	System Model G.hn-GNT			
NTP Setting	G.hn Hardware Version 1_0			
Port Management	G.hn Software Version G.hn-GNT-v7 8 r590+22 cvs,Release(202308101121)			
Login				
Restore	G.hn SN_G3QH9XW002000			
Reset Configuration	File Path Please select a file. Browse Upload			
LED				
Web CLI				
System Log				
Upgrade				
Reboot				
Development Mode				
« Fold				

6.10Reboot

6.10.1 Reboot

You can click "System" -> "Reboot" to reboot the AP remotely.

If you want to reboot the device directly, click "Reboot" on the page.

Ruíjie	English 🗸	🕞 Exit
m̃Behavior ∨	Reboot Scheduled Reboot	
©₀ Diagnostics ∨	Reboot	
△ Advanced ~	Please keep the device powered on during reboot.)
System ^	Reboot	
NTP Setting		
Port Management		
Restore		
Reset Configuration		
LED		
Web CLI		
System Log		
Upgrade		
Development Mode		
«Fold		

6.10.2 Scheduled Reboot

In this page, you can schedule the reboot of the AP to take effect at a specific time in a day of a week.

Ruíjie	English 🗸 🕞 Đư
míBehavior	
	Reboot Scheduled Reboot
Advanced	Scheduled Reboot It is recommended to schedule a reboot on a network idle time, such as 2 A.M. Rebooted schedule will not work until time is set by NTP server.
System	Scheduled Reboot
NTP Setting	* Day 🗌 Mon. 🗌 Tue. 🗹 Wed.
Port Management	Thu. Fri. Sat. Sun.
Login	
Restore	Time 03 v: 42 v
Reset Configuration	Save
LED	
Web CLI	
System Log	
Upgrade	
Reboot	
Development Mode	
<pre>«Fold</pre>	

Items	Description	Defaults/Options
Scheduled	Enable or disable the scheduled reboot	Default: Disabled.
Reboot	function.	Option: Enabled/Disabled
Day	Specify the day of a week to restart the device.	Default: Any day of the week.
Time	Set the checific time to restart the device	Default: A specific time between 3 a.m and 4
nine	Set the specific time to restart the device.	a.m.

6.11 Developer Mode

With the developer mode enabled, you can log in to the device console through SSH to configure the device.

Ruíjie	English 🗸 🕞 Exit
∰Behavior ∨	
© Diagnostics ∨	Development Mode
△Advanced ~	👔 Development mode allows engineers to enter console over SSH to change and deliver configuration. It will be disabled automatically after reboot.
System ^	Development Mode (It is recommended to be disabled after use to prevent others from using it.)
NTP Setting	Save
Port Management	
Login	
Restore	
Reset Configuration	
LED	
Web CLI	
System Log	
Upgrade	
Reboot	
Development Mode	
«Fold	
7 Troubleshooting

This chapter mainly introduces countermeasures when you encounter problems that you cannot solve.

7.1 Failing to Connect to Web-GUI

When you cannot connect to the Web-GUI, please confirm the following points:

(1) Check the connection between the AP and your PC.

Please refer to section 1.4 "Preparation for Web-GUI Connection" to confirm whether the connection is correct.

(2) Check whether the AP works in routing mode and the PC accesses the AP through the LAN port.

When the AP works in routing mode, the PC cannot access the AP via a WAN port, because the WAN port is a G.hn port. By default, the PC accesses the AP via the LAN port.

- (3) Check whether the PC can ping the AP.
- (4) Check whether your browser can display the Web-GUI interface correctly.

The Web-GUI of HA3515-DG supports Google Chrome, Firefox, Safari and some browsers based on IE kernel. It is strongly recommended that you use Google Chrome to access the Web-GUI again.

7.2 Failing to Log into Web-GUI

If you cannot log in to the Web-GUI, please check the following points:

(1) Check whether the username and password are correct.

Please log in again with the correct username and password. Default username/password: admin/admin.

(2) Forget the password.

If you forget the login password, you can use a slender needle to press the Reset button on the AP panel to restore the device to factory settings.

(3) Check whether the browser you use can display the Web-GUI interface normally.

The Web-GUI of HA3515-DG supports Google Chrome, Firefox, Safari and some browsers based on IE kernel. It is strongly recommended that you use Google Chrome to access the Web-GUI again.

7.3 Communication Failure

When the device connects normally but cannot communicate normally, please check the following things:

(1) Check device status:

When the IP address of WAN port is set to be obtained automatically via DHCP, you can check the interface status by checking whether the AP automatically obtains an IP address or DNS address. If the address cannot be obtained, the WAN cannot be connected (no Internet service is provided). Please check whether the DHCP server is reachable or whether the IP+ MAC binding have been configured.

(2) Blacklist and Whitelist

Only clients in the whitelist are allowed to access the Web-GUI. If the device cannot communicate normally, check whether the device has been listed in the whitelist. If not, please add the device to the whitelist. Also, check whether the device has been added to the blacklist by mistake.

For details, please refer to section 4.4.1 "Access Control".

7.4 About Device Setup and Usage Support

If you need to analyze the cause of a fault or collect usage status, please refer to section 6.8 "System Log". And provide the saved logs to your service provider for support.