Industrial Indoor WiFi6 Wireless AP

User Manual

Document Version: 03

Issue Date: 06/08/2023

Industrial Ethernet Communication Solution Expert **3onedata Co., Ltd.**

Trademark statement

3onedata, 3onedata and 3One data® are the registered trademark owned by 3onedata Co., Ltd. And other trademarks mentioned in this manual belong to their corresponding companies.

Note

Purchased product, service or features should be constrained by 3onedata commercial contracts and clauses. The whole or part product, service or features described in this document may beyond purchasing or using range. 3onedata won't make any statement or warranty for this document content unless any other appointment exists.

Due to product version upgrading or other reason, this document content will be upgraded periodically. Unless other appointment exists, this document only for usage guide, all statement, information and suggestion in this document won't constitute any warranty.

3onedata

Make network communication more reliable

Please scan our QR code for more details

Embedded Industrial Ethernet Switch Modules

Embedded Serial Device Server Modules

Industry-specialized Products

(Rail Transit, Power, Smart City, Pipe Gallery…)

3onedata

Make network communication more reliable

Honor·Quality·Service

Layer 2 (Unmanaged) Managed Industrial Ethernet Switch

Layer 3 Managed Industrial Ethernet Switch

Industrial PoE Switch

BlueEyes pro

BlueEyes Pro Management Software

VSP Virtual Serial Port Management Software

SNMP Management Software

Modbus Gateway

Serial Device Server

Media Converter

CAN Device Server

Interface Converter

Industrial Wireless Products

3onedata Co., Ltd.

Headquarter address:	3/B, Zone 1, Baiwangxin High Technology Industrial park, Nanshan District, Shenzhen, 518108 China
Technology support:	support@3onedata.com
Service hotline:	+86-400-880-4496
E-mail:	sales@3onedata.com
Fax:	+86-0755-26703485
Website:	http://www.3onedata.com

Preface

The user manual has introduced the network management method of wireless AP product.

Applicable Products

The software version of this manual is V3.1500.0B2023040838R3458H00000, and the applicable product models are shown in the following table. This manual is continuously optimized and updated, which is consistent with the latest software version. Therefore, the manual may contain some functions that are not supported by the products you purchased. Please refer to the products you actually purchased.

Number	Available Models	Specification
1	IAP3300-2E-4GT1GP-2LVI V1.0.0	2 2.4G/5G combined antenna interfaces + 4 Gigabit RJ45 ports (LAN) + 1 Gigabit PoE RJ45 port (LAN/WAN), 1 12~48VDC power input
2	IAP3500-2E-1GT1GS-LV V1.0.0	2 2.4G/5G dual-frequency antenna interfaces + 1 Gigabit SFP slot + 1 Gigabit copper port, and 1 9~24VDC power input
3	IAP3600Exi-2225-2GS4GT-P12_48 V1.0.0	2 2.4G antenna interfaces + 2 5G antenna interfaces + 2 Gigabit SFP slots + 4 Gigabit copper ports, 1 12~48VDC power input (12~24VDC safety input)
4	IAP3600Exi-2225-2GS4GT-SMA-P12_48 V1.0.0	2 2.4G antenna SMA interfaces + 2 5G antenna SMA interfaces + 2 Gigabit SFP slots + 4 Gigabit copper ports, 1 12~48VDC power input (12~24VDC safety input)
5	IAP3300L-2E-4GT1GP-2LVI V1.0.0	2 2.4G/5G combined antenna interfaces + 4 Gigabit RJ45 ports(LAN) + 1 Gigabit PoE RJ45 port (LAN/WAN), 1 12~48VDC power input
6	IAP3300-2E-4GT1GP-2LVI	2 2.4G/5G combined antenna interfaces + 4 Gigabit RJ45 port (LAN) + 1 Gigabit PoE RJ45

Number	Available Models	Specification
	V1.0.0	port (LAN/WAN), 1 12~48VDC power input
7	IAP3600S-2225-2GT-PD V1.0.0	2 2.4G antenna interfaces + 2 5G antenna interfaces + 1 Gigabit RJ45 port (LAN) + 1 Gigabit PoE RJ45 port (LAN/WAN)

Audience

This manual applies to the following engineers:

- Network administrators
- Technical support engineers
- Network engineer

Port Convention

The port number in this manual is only an example, and does not represent the actual port with this number on the device. In actual use, the port number existing on the device shall prevail.

Text Format Convention

Format	Description
" "	Words with “” represent the interface words. Such as: “Port No.”.
>	Multi-level path is separated by ">". Such as opening the local connection path description: Open "Control Panel> Network Connection> Local Area Connection".
Light Blue Font	It represents the words clicked to achieve hyperlink. The font color is as follows: ‘Light Blue’.
About this chapter	The section ‘about this chapter’ provide links to various sections of this chapter, as well as links to the Principles Operations Section of this chapter.

Symbols

Format	Description
⚠Notice	Remind the announcements in the operation, improper operation may result in data loss or equipment damage.

Format	Description
⚠ Warning	Pay attention to the notes on the mark, improper operation may cause personal injury.
📄 Note	Make a necessary supplementary instruction for operation description.
🔑 Key	Configuration, operation, or tips for device usage.
💡 Tips	Pay attention to the operation or information to ensure success device configuration or normal working.

Revision Record

Version No.	Date	Revision note
01	08/09/2022	Product release
02	04/27/2023	Software upgrade
03	2023-06-08	Add Ring configuration and fiber port VLAN functions

Contents

PREFACE 1
CONTENTS I
1 LOG IN THE WEB INTERFACE 1
1.1 SYSTEM REQUIREMENTS FOR WEB BROWSING 1
1.2 SETTING IP ADDRESS OF PC 1
1.2.1 Wired Access Mode 1
1.2.2 Wireless Access Mode 2
1.3 LOG IN THE WEB CONFIGURATION INTERFACE 3
2 HOME PAGE 5
3 MODE SETTING 1
3.1 ROUTE 2
3.1.1 WAN Settings 3
3.1.2 LAN Settings 5
3.1.3 WiFi1 6
3.1.4 WiFi2 9
3.1.5 Finish 12
3.2 AP 13
3.2.1 LAN Settings 13
3.2.2 WiFi1 15
3.2.3 WiFi2 18
3.2.4 Finish 21
3.3 BRIDGE 22
3.3.1 Connection Mode 23
3.3.2 LAN Settings 24
3.3.3 Connection Settings 25
3.3.4 WiFi1 27
3.3.5 WiFi2 29
3.3.6 Finish 30
3.4 CLIENT 31
3.4.1 Connection Mode 32
3.4.2 WAN Settings 33
3.4.3 LAN Settings 36
3.4.4 Connection Settings 37
3.4.5 Finish 40

3.5 DUAL-LINK MODE 41
3.5.1 Connection Mode 42
3.5.2 WAN Settings 43
3.5.3 LAN Settings 46
3.5.4 Connection Settings.... 47
4 STATUS CENTER 54
4.1 SYSTEM STATUS 54
4.2 NETWORK STATUS 55
4.3 DEVICE STATISTICS 56
4.4 ARP TABLE 56
4.5 DEVICE STATISTICS 57
4.6 ROUTE TABLE 58
5 NETWORK SETTING 59
5.1 LAN SETTINGS 59
5.1.1 LAN Settings 1 59
5.1.2 LAN Settings 2 61
5.2 WAN SETTINGS....64
5.3 WIRELESS SETTINGS-AP 67
5.3.1 RF 1 Configuration.... 67
5.3.2 RF 2 Configuration.... 70
5.3.3 Advanced Configuration 74
5.3.4 WMM Configuration.... 76
5.4 WIRELESS SETTINGS-CLIENT 79
5.4.1 RF Configuration 79
5.5 RING CONFIGURATION 87
5.6 OPTICAL VLAN 90
5.7 WIRELESS PROBE 91
5.8 AC MANAGEMENT 92
5.9 QOS CONFIG....94
5.9.1 QoS Strategy.... 94
5.9.2 QoS Whitelist 95
5.10 SNMP MANAGEMENT....96
5.11 QOS MANAGEMENT....97
5.11.1 QoS Whitelist 98
5.12 AP ROAMING CONTROL 99
5.13 ROAMING AGENT 100
6 WIRELESS CLIENT.... 101
6.1 USERS....101
6.2 USER EVENT 103
7 FIREWALL 105
7.1 IP FILTER....105
7.2 MAC FILTER....106
7.3 URL FILTER....108

7.4 PORT FORWARD 109
7.5 PORT REDIRECTION 110
7.6 ARP BINDING 111
7.7 DMZ SETTINGS 112
8 SYSTEM TOOLS 114
8.1 NETWORK DETECTION 114
8.2 USER SETTINGS 115
8.3 DEVICE ALIAS 116
8.4 TIME SETTINGS 117
8.5 TIMED RESTART 118
8.6 ACCESS SETTINGS 118
8.7 SYSTEM UPGRADING 119
8.8 CONFIG UPDATE 120
8.9 SYSTEM MANAGEMENT 121
8.10 SYSTEM LOG 122
8.11 LOG MANAGE 124
9 DIAGNOSTIC TOOLS 125
9.1 PING TEST 125
9.2 ROUTE TRACKING 126
10 FAQ 127
11 MAINTENANCE AND SERVICE 130
11.1 INTERNET SERVICE 130
11.2 SERVICE HOTLINE 130
11.3 PRODUCT REPAIR OR REPLACEMENT 131

1 Log in the Web Interface

1.1 System Requirements for WEB Browsing

While logging into the WEB of this device, the system should meet the following conditions.

Hardware and software	System requirements
CPU	Above Pentium 586
Memory	Above 128MB
Resolution	Above 1024x768
Color	256 color or above
Browser	Internet Explorer 8.0 or above
Operating system	Windows XP/7/8/10

1.2 Setting IP Address of PC

1.2.1 Wired Access Mode

The default management network address of the device as follows:

IP Settings	Default Value
IP Address	192.168.1.254
Subnet mask	255.255.255.0

When configuring a device through the Web:

- Please confirm the computer has installed and enabled Ethernet network card.
- Before conducting remote configuration, please confirm the route between

computer and device is reachable.

- Before making a local configuration, make sure that the IP address of the computer and the serial server are on the same subnet.

Note:
While configuring the device for the first time, if it's the local configuration mode, first confirm the network segment of current PC is 1.

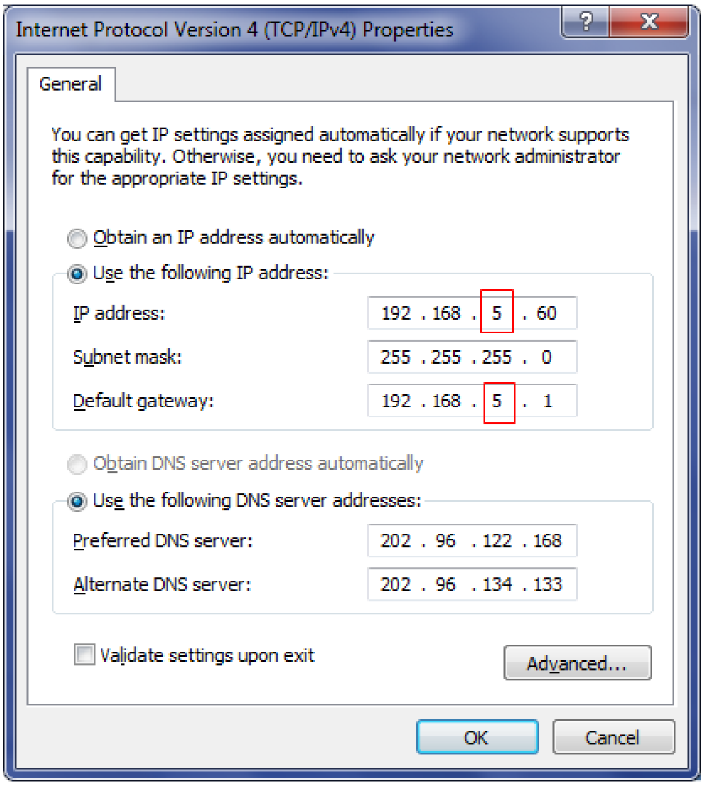
Eg: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

Operation Steps

Amendment steps as follow:

Step 1 Open "Control Panel> Network Connection> Local Area Connection> Properties> Internet Protocol Version 4 (TCP / IPv4)> Properties".

Step 2 Change the selected "5" in red frame of the picture below to "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 automatically

● Use the following IP address:

IP address: 192 . 168 . 5 . 60

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 5 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 202 . 96 . 122 . 168

Alternate DNS server: 202 . 96 . 134 . 133

□ Validate settings upon exit

Step 3 Click “OK”, IP address is modified successfully.

Step 4 End.

1.2.2 Wireless Access Mode

The default management network address of the device as follows:

IP Settings	Default Value
IP Address	192.168.1.254
Subnet mask	255.255.255.0

When configuring a device through the Web:

- Please confirm the computer has installed and enabled wireless network card.
- Place the computer on wireless network range of the device.
- Please confirm the IP address of computer is in the same subnet to the device.

⚠Notice

Do not use a proxy server for device IP addresses or network segments

Set the IP address of computer in the same subnet to the device IP address.

Operation Steps

Operation steps of wireless connection as follows.

Notes

This manual takes the wireless network settings function of Windows 7 system for example.

Step 1 Click wireless icon “📶" on the lower right corner of the computer, pop up the wireless list box.

Step 2 Choose the device wireless network name in the wireless list box, click "Connect" button.

Note:

The default wireless network name of the device contains frequency band and part of MAC address information, no encryption.

Step 3 End. After successful connection, wireless network displays "Connected".

1.3 Log in the Web Configuration Interface

Operation Steps

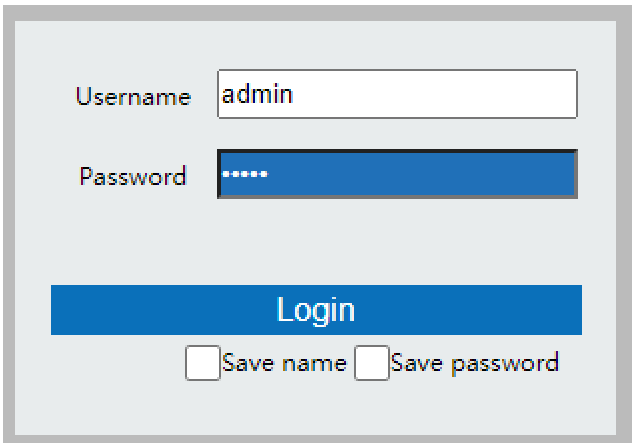
Login in the web configuration interface as follow:

Step 1 Run the computer browser.

Step 2 Enter the address of the device "http://192.168.1.254" in the address bar of the browser.

Step 3 Click the “Enter” key.

Step 4 Pop-up dialog box as shown below, enter the user name and password in the login window.



Username admin

Password •••••

Note:

The default username and password are “admin”; please strictly distinguish capital and small letter while entering.

Step 5 Click "Login".

Step 6 End.

After login in successfully, user can configure relative parameters and information according to demands.

Notes

After logging in to the device, user can modify the device IP address for convenient usage; if there is no interface operation within 10 minutes, user will need to log in to the device again.

2 Home page

Function Description

On the "Home page" page, user can check the following information:

- System resource utilization;
- Basic information;
- Equipment information;
- Wireless information/Bridge information;
- Extranet information/network information/bridge status;
- WiFi real-time flow (KB/s)

Notes

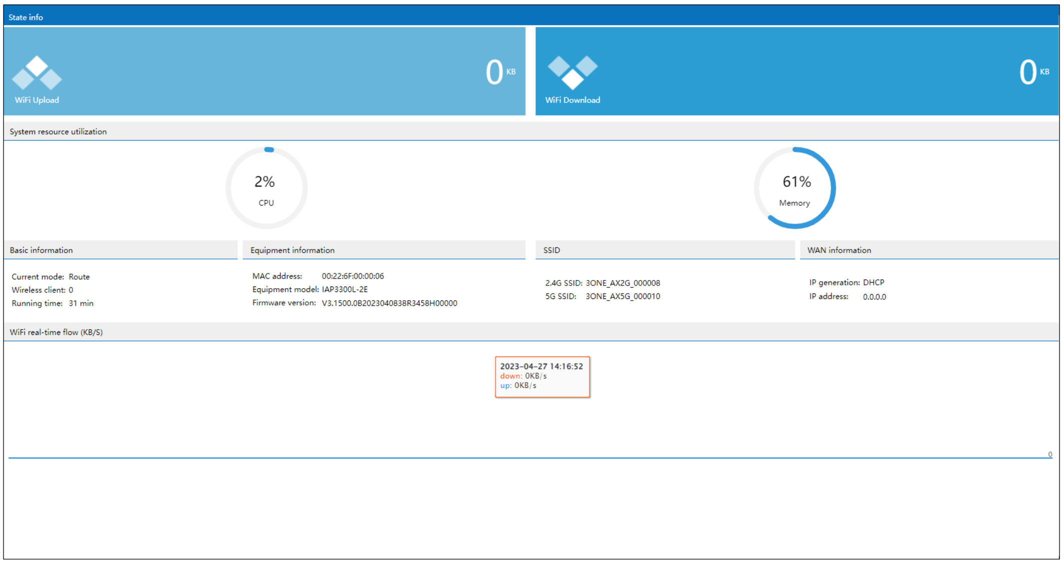
- In AP/ routing mode, displays "Wireless Information"; In bridge/client mode, displays “bridge state”.
- In routing mode, displays "Extranet Information"; In AP mode, displays “Network Information”; In bridge/client mode, displays “bridge state”.

Operation Path

On the navigation bar, select "Home page".

Interface Description

Home page interface as follows:



State info

WiFi Upload 0 KB

WiFi Download 0 KB

System resource utilization

2% CPU

61% Memory

Basic information

Current mode: Route
Wireless client: 0
Running time: 31 min

Equipment information

MAC address: 00:22:6F:00:00:06
Equipment model: IAP3300L-2E
Firmware version: V3.1500.0B2023040838R3458H00000

SSID

2.4G SSID: 3ONE_AX2G_000008
5G SSID: 3ONE_AX5G_000010

WAN information

IP generation: DHCP
IP address: 0.0.0.0

WiFi real-time flow (KB/S)

2023-04-27 14:16:52
down: 0KB/s
up: 0KB/s

Main elements configuration description of Home page interface:

Interface Element	Description
Total WIFI upload	**Total upload area** Note: WiFi upload traffic statistics.
Total WIFI download	**Total download area** Note: WiFi download traffic statistics.
System resource utilization	**Resource utilization column**
CPU (%)	The usage rate of device CPU.
Memory (%)	The usage rate of device memory. Note: The performance of the device would be affected if the application consumes too much memory.
Basic information	**Basic information column**
Current mode	Current operation mode of the device.
Wireless client	Wireless client connection number.
Running time	The device running time after power on.
Device information	**Equipment information column**
MAC Address	Device MAC address.
Equipment model	Equipment model name.
Firmware version	Device firmware version.
SSID	**SSID column** Note: In AP/ routing mode, displays "Wireless Information".
2.4G	2.4G wireless network name.
5G	5G wireless network name.

Interface Element	Description
Bridge information	**Bridge information column** Note: In bridge/client mode, displays “bridge information”.
SSID	Display the name of the connected SSID
BSSID	Display the information of the connected BSSID.
WAN information	**WAN information column** Note: In Routing/Wireless NAT mode, "WAN Information” would display.
IP generation	Access mode of the device WAN IP address.
IP address	IP addresses of the device WAN.
WAN information	**Network information bar** Note: In AP mode, "Network Information” displays.
IP Access Method	Access mode of the device intranet IP address.
IP Address	IP addresses of the device intranet.
WiFi real-time flow (KB/s)	**WiFi real-time flow (KB/s) column.**
WiFi real-time flow (KB/s)	WiFi real-time flow monitoring view. ● Upload: the blue line represents device’s rate changes of wireless upload traffic. ● Download: the orange line represents device’s rate changes of wireless download traffic.

3 Mode Setting

Function Description

On the "Mode Setting" page, user can select the working mode according to the site needs, and then complete the mode setting step by step according to the guidance.

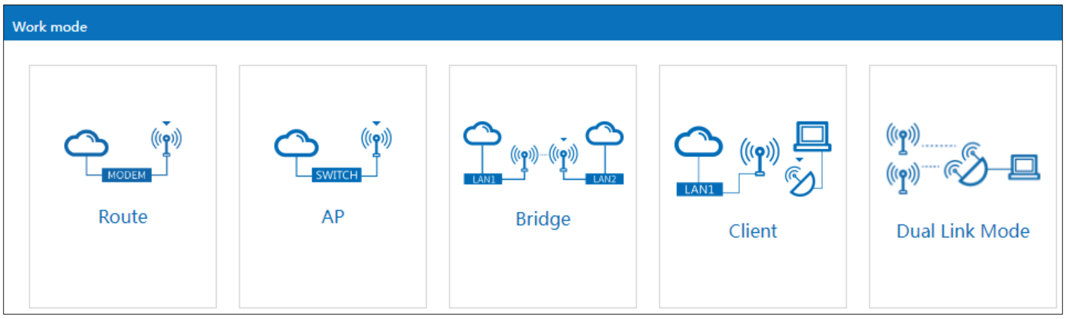
- Route;
- AP;
- Bridge;
- Client;
- Dual Link Mode.

Operation Path

Click: "Work Mode".

Interface Description

Work mode interface as follows:



Main elements configuration description of mode settings interface:

Interface Element	Description
Route	Under the route mode, the device WAN port can be connected to WAN via PPPoE dial-up, static IP and dynamic acquisition;

Interface Element	Description
	the LAN port can be connected to LAN and provides wireless access point. Note: When the data is transmitted from one subnet to another subnet or WAN, it can be accomplished via the device route function.
AP	Under the AP mode, the device can be used as a wireless access point, the equivalent of the wireless switch.
Bridge	Under the bridge mode, the device will convert received wireless signal to cable signal and wireless signal.
Client	Under the client mode, the device will convert received wireless signal to cable signal.
Dual-link	Under the dual-link mode, the device will convert received wireless signal to cable signal, support dual link client that can realize dual-band seamless roaming.

3.1 Route

Under the route mode, the device WAN port can be connected to the WAN via PPPoE dial-up, static IP and dynamic acquisition. Under this mode, LAN port and wireless signal are in the same VLAN, the LAN port defaults to enable DHCP server function.

PPPoE (PPP Over Ethernet) carries PPP (Point to Point Protocol) on the Ethernet. It is a technology that provides access services for hosts on the Ethernet through a remote access device, and can control and charge each accessed host.

The quick configuration of route mode mainly includes five configuration links:

- WAN settings
- LAN settings
- WiFi1
- WiFi2
- Finish

3.1.1 WAN Settings

Function Description

On the "WAN Settings" page of route mode, WAN port can be connected to WAN via three methods:

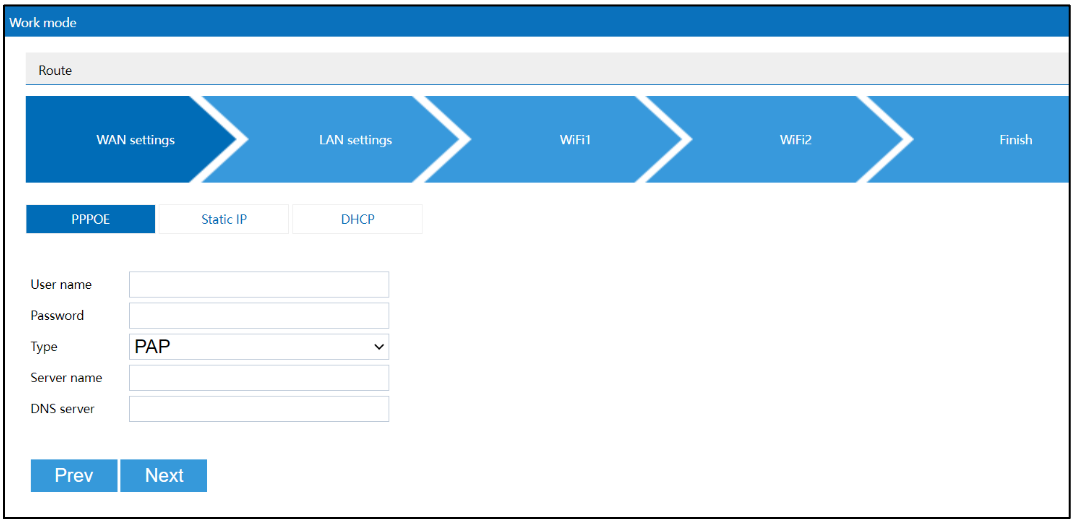
- PPPoE;
- Static IP;
- DHCP;

Operation Path

Please open in order: "Work mode > Route".

Interface Description 1: PPPoE

PPPoE interface as follows:



User name
Password
Type PAP
Server name
DNS server

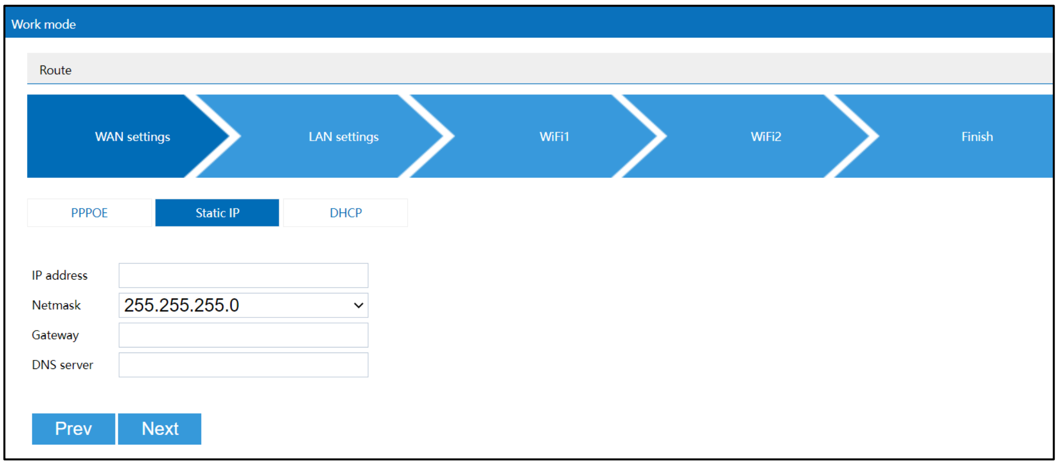
The main element configuration description of PPPoE interface:

Interface Element	Description
PPPoE	PPPoE tab, it supports PPPoE to achieve Internet access.
Username	User name of PPPoE connection. Note: User name, password and service name are provided by network provider.
Password	Password of PPPoE connection. Note: User name, password and service name are provided by network provider.
Type	The type of PPPoE dialing: ● PAP: Password Authentication Protocol, which sends user name or password over the network; ● CHAP: Challenge Handshake Authentication Protocol, it

Interface Element	Description
	only transmits user name; ● PAP/CHAP: uses Password Authentication Protocol or Challenge Handshake Authentication Protocol.
Server name	Server name, not fill if network provider doesn't supply. Note: User name, password and service name are provided by network provider.
DNS server	The DNS server address provided by network provider or extranet.

Interface Description 2: Static IP

Static IP interface as follows:



IP address

Netmask 255.255.255.0

Gateway

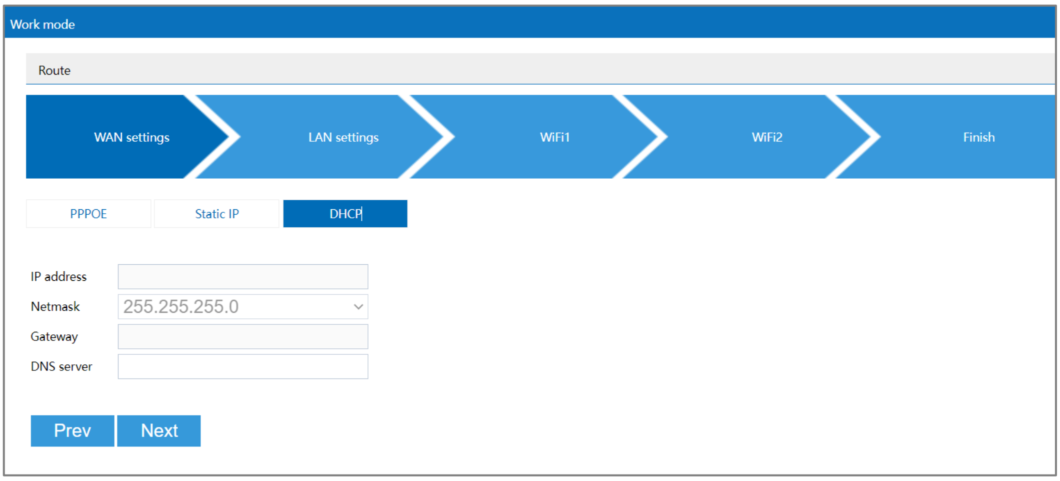
DNS server

The main element configuration description of static IP interface:

Interface Element	Description
Static IP	Static IP tab, network information configuration of device WAN port.
IP Address	The fixed IP address provided by network provider or extranet.
Netmask	Drop-down list of netmask.
Gateway	The default gateway address provided by network provider or extranet.
DNS server	The DNS server address provided by network provider or extranet.

Interface Description 3: DHCP

DHCP interface as follows:



IP address:
Netmask: 255.255.255.0
Gateway:
DNS server:

Main elements configuration description of DHCP interface:

Interface Element	Description
DHCP	In the dynamic acquisition tab, the network information of the device WAN port is automatically obtained. Note: The device automatically acquires the network address information distributed by network provider or WAN.
IP Address	IP address automatically distributed by network provider or WAN.
Netmask	The subnet mask automatically distributed by network provider or WAN.
Gateway	Gateway address automatically distributed by network provider or WAN.
DNS server	DNS server address. Note: The priority level of manually setting DNS server address is higher than the one of automatically acquired DNS server address.

3.1.2 LAN Settings

Function Description

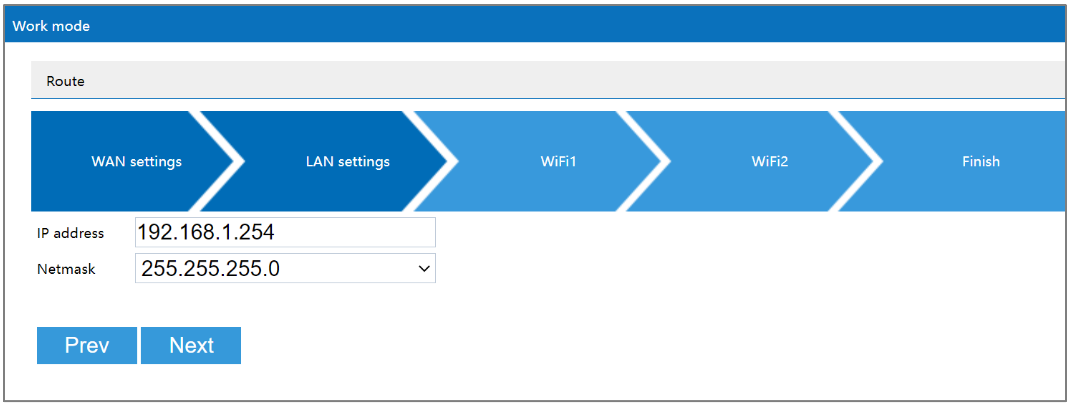
On the "LAN Settings" page of route mode, user can configure the IP address and subnet mask of LAN.

Operation Path

Please open in order: "Work mode > Route".

Interface Description

LAN settings interface as follows:



IP address 192.168.1.254

Netmask 255.255.255.0

The main element configuration description of LAN settings interface:

Interface Element	Description
IP Address	IP address information of LAN.
Netmask	Drop-down list of netmask.

3.1.3 WiFi1

Function Description

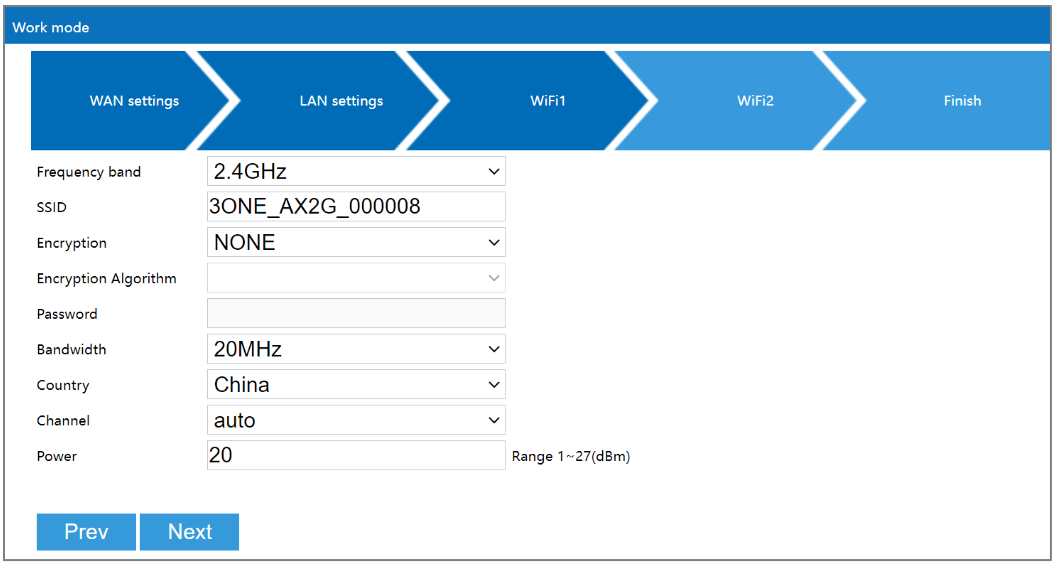
On the "WiFi1" page of route mode, user can set the wireless parameters of RF1.

Operation Path

Please open in order: "Work mode > Route".

Interface Description

The WiFi1 interface as follows:



Frequency band 2.4GHz

SSID 3ONE_AX2G_000008

Encryption NONE

Encryption Algorithm

Password

Bandwidth 20MHz

Country China

Channel auto

Power 20 Range 1~27(dBm)

Main elements configuration descriptions of WiFi1 interface:

Interface Element	Description
Frequency band	The wireless frequency band corresponding to the current wireless setting, the options are as follows: ● 2.4GHz
SSID	SSID name of wireless network, it supports 1-32 characters.
Encryption	Encryption mode of wireless network, options as follows: ● No encryption; ● WPA2: WiFi Protected Access II suits for the individual or average family network. It adopts pre-shared key mode and supports TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) encryption modes. ● WPA/WPA2: mixed mode of WPA and WPA2, it uses WPA or WPA2 encryption algorithm. ● WPA3: the third version of Wi-Fi protected access, with further security improvements over WPA2, longer encryption keys, and SAE authentication. ● WPA2/WPA3: mixed mode of WPA2 and WPA3, it uses WPA2 or WPA3 encryption algorithm. Note: WPA2/WPA3 only supports personal edition and doesn't support enterprise edition currently. Other encryption algorithms are supported by both of them.
Encryption algorithm	Encryption algorithm of wireless network, options as follows: ● AES (CCMP): advanced encryption standard; ● TKIP/AES: the key integrates 2113 protocol or advanced encryption standard temporarily. Note: When the encryption method is WPA2/WPA3 and WPA3, only AES (CCMP) encryption algorithm is supported.
Password	Password of wireless network, it supports 8-63 characters. Note: Wireless password doesn’t support blanks. It represents no encryption for wireless network if no password is filled in.
Bandwidth	Wireless network channel bandwidth, options are as follows: ● 20MHz (default); ● 40MHz.
Country	Applied countries and regions. Options are as follows: ● China; ● USA. Note: Different country opens different channels.
Channel	Working channel of wireless network, default "auto" self-adaptation, options as follows: ● Auto: channel self-adaptation;

Interface Element	Description
	• 1: main frequency band 2412Hz, frequency range 2401~2423Hz; • 2: main frequency band 2417Hz, frequency range 2406~2428Hz; • 3: main frequency band 2422Hz, frequency range 2411~2433Hz; • 4: main frequency band 2427Hz, frequency range 2416~2438Hz; • 5: main frequency band 2432Hz, frequency range 2421~2443Hz; • 6: main frequency band 2437Hz, frequency range 2426~2448Hz; • 7: main frequency band 2442Hz, frequency range 2431~2453Hz; • 8: main frequency band 2447Hz, frequency range 2436~2458Hz; • 9: main frequency band 2452Hz, frequency range 2441~2463Hz; • 10: main frequency band 2457Hz, frequency range 2446~2468Hz; • 11: main frequency band 2462Hz, frequency range 2451~2473Hz; • 12: main frequency band 2467Hz, frequency range 2456~2478Hz, this frequency band is not open in America, so it's temporarily unavailable; • 13: main frequency band 2472Hz, frequency range 2461~2483Hz, this frequency band is not open in America, so it's temporarily unavailable; Note: • Different frequency bands and countries support different options. • In order to improve the network performance, please choose unused channel in the device working environment.
Power	Transmission power of device wireless signal. Note: • Greater the transmitted power, better the transmittability, longer the transmission range, but stronger the interference; • Different device may has different transmitted power range.

3.1.4 WiFi2

Function Description

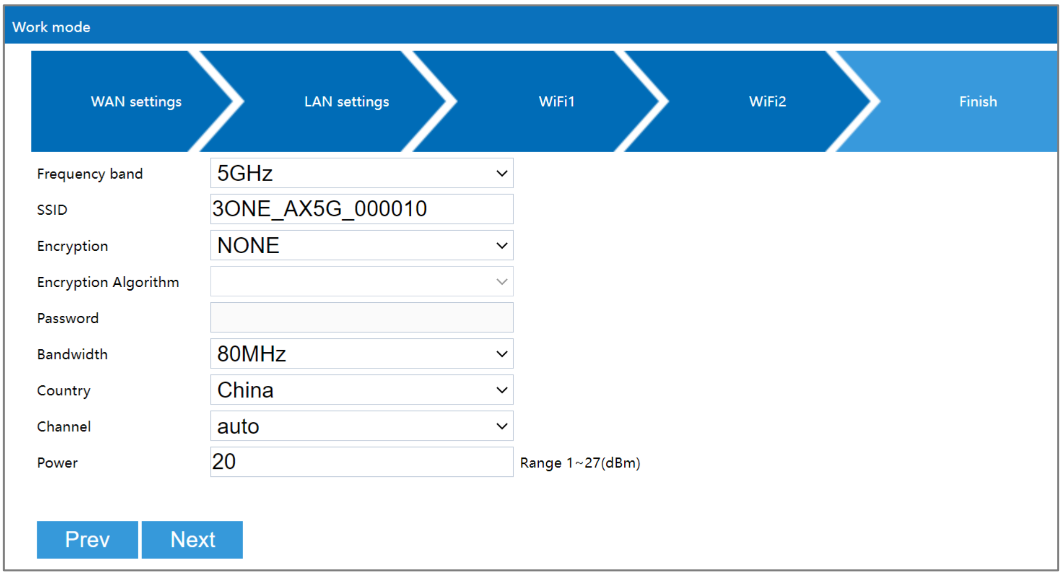
On the "WiFi2" page of route mode, user can set the wireless parameters of RF2.

Operation Path

Please open in order: "Work mode > Route".

Interface Description

The WiFi2 interface as follows:



Frequency band 5GHz

SSID 3ONE_AX5G_000010

Encryption NONE

Encryption Algorithm

Password

Bandwidth 80MHz

Country China

Channel auto

Power 20 Range 1~27(dBm)

Main elements configuration descriptions of WiFi2 interface:

Interface Element	Description
Frequency band	The wireless frequency band corresponding to the current wireless setting, the options are as follows: ● 5GHz
SSID	SSID name of wireless network, it supports 1-32 characters.
Encryption	Encryption mode of wireless network, options as follows: ● No encryption; ● WPA2: WiFi Protected Access II suits for the individual or average family network. It adopts pre-shared key mode and supports TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) encryption modes. ● WPA/WPA2: mixed mode of WPA and WPA2, it uses WPA or WPA2 encryption algorithm. ● WPA3: the third version of Wi-Fi protected access, with further security improvements over WPA2, longer

Interface Element	Description
	encryption keys, and SAE authentication. ● WPA2/WPA3: mixed mode of WPA2 and WPA3, it uses WPA2 or WPA3 encryption algorithm. Note: WPA2/WPA3 only supports personal edition and doesn't support enterprise edition currently. Other encryption algorithms are supported by both of them.
Encryption algorithm	Encryption algorithm of wireless network, options as follows: ● AES (CCMP): advanced encryption standard; ● TKIP/AES: the key integrates 2113 protocol or advanced encryption standard temporarily. Note: When the encryption method is WPA2/WPA3 and WPA3, only AES (CCMP) encryption algorithm is supported.
Password	Password of wireless network, it supports 8-63 characters. Note: Wireless password doesn’t support blanks. It represents no encryption for wireless network if no password is filled in.
Bandwidth	Channel bandwidth of wireless network, it defaults to 80MHz, options as follows: ● 20MHz; ● 40MHz; ● 80MHz.
Country	Applied countries and regions. Options are as follows: ● China; ● USA. Note: Different country opens different channels.
Channel	Working channel of wireless network, default "auto" self-adaptation, options as follows: ● Auto: channel self-adaptation; ● 36: main frequency band 5180Hz, frequency range 5170~5190Hz; ● 40: main frequency band 5200Hz， frequency range 5190~5210Hz； ● 44: main frequency band 5220Hz, frequency range 5210~5230Hz; ● 48: main frequency band 5230Hz, frequency range 5210~5250Hz; ● 52: main frequency band 5260Hz, frequency range 5250~5270Hz; ● 56: main frequency band 5280Hz, frequency range 5270~5290Hz;

Interface Element	Description
	• 60: main frequency band 5300Hz, frequency range 5290~5310Hz; • 64: main frequency band 5320Hz, frequency range 5310~5330Hz; • 100: main frequency band 5500Hz, frequency range 5490~5510Hz, this frequency band is not open in China, so it's temporarily unavailable; • 104: main frequency band 5520Hz, frequency range 5510~5530Hz, this frequency band is not open in China, so it's temporarily unavailable; • 108: main frequency band 5540Hz, frequency range 5530~5550Hz, this frequency band is not open in China, so it's temporarily unavailable; • 112: main frequency band 5560Hz, frequency range 5550~5570Hz, this frequency band is not open in China, so it's temporarily unavailable; • 116: main frequency band 5580Hz, frequency range 5570~5590Hz, this frequency band is not open in China, so it's temporarily unavailable; • 120: main frequency band 5600Hz, frequency range 5590~5610Hz, this frequency band is not open in China, so it's temporarily unavailable; • 124: main frequency band 5620Hz, frequency range 5610~5630Hz, this frequency band is not open in China, so it's temporarily unavailable; • 128: main frequency band 5640Hz, frequency range 5630~5650Hz, this frequency band is not open in China, so it's temporarily unavailable; • 132: main frequency band 5660Hz, frequency range 5650~5670Hz, this frequency band is not open in China, so it's temporarily unavailable; • 136: main frequency band 5680Hz, frequency range 5670~5690Hz, this frequency band is not open in China, so it's temporarily unavailable; • 140: main frequency band 5700Hz, frequency range 5690~5710Hz, this frequency band is not open in China, so it's temporarily unavailable; • 144: main frequency band 5720Hz, frequency range 5710~5730Hz, this frequency band is not open in China, so it's temporarily unavailable; • 149: main frequency band 5745Hz, frequency range

Interface Element	Description
	5735~5755Hz; • 153: main frequency band 5765Hz, frequency range 5755~5775Hz; • 157: main frequency band 5785Hz, frequency range 5775~5795Hz; • 161: main frequency band 5805Hz, frequency range 5795~5815Hz; • 165: main frequency band 5825Hz, frequency range 5815~5835Hz; Note: • Different frequency bands and countries support different options. • In order to improve the network performance, please choose unused channel in the device working environment.
Power	Transmission power of device wireless signal. Note: • Greater the transmitted power, better the transmittability, longer the transmission range, but stronger the interference; • Different device may has different transmitted power range.

3.1.5 Finish

Function Description

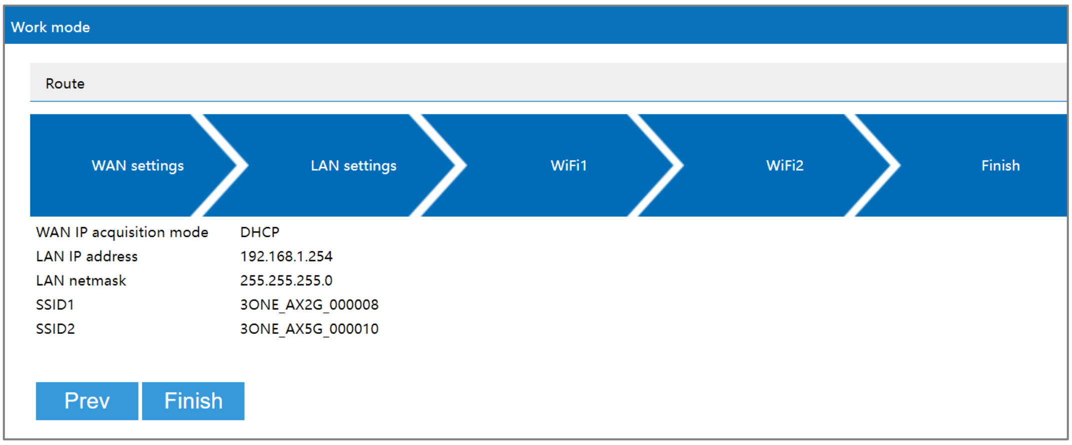
On the "Finish" page of route mode, user can check the main parameters of wireless route mode.

Operation Path

Please open in order: "Work mode > Route".

Interface Description

Finish interface as follows:



WAN IP acquisition mode	DHCP
LAN IP address	192.168.1.254
LAN netmask	255.255.255.0
SSID1	3ONE_AX2G_000008
SSID2	3ONE_AX5G_000010

The main element configuration description of finish interface:

Interface Element	Description
WAN IP acquisition mode	• PPPoE • Static IP • DHCP
LAN IP address	IP address information of LAN.
LAN netmask	Subnet masks information of LAN.
SSID1	SSID name of wireless 1 network.
SSID2	SSID name of wireless 2 network.

3.2 AP

Under AP mode, the device can be used as a wireless access point, the equivalent of the wireless switch. Under the mode, WAN port, LAN port and wireless signal are all in the same VLAN; LAN port is static IP, DHCP server defaults to closed.

The rapid configuration of AP mode mainly includes four configuration links:

- LAN settings
- WiFi1
- WiFi2
- Finish

3.2.1 LAN Settings

Function Description

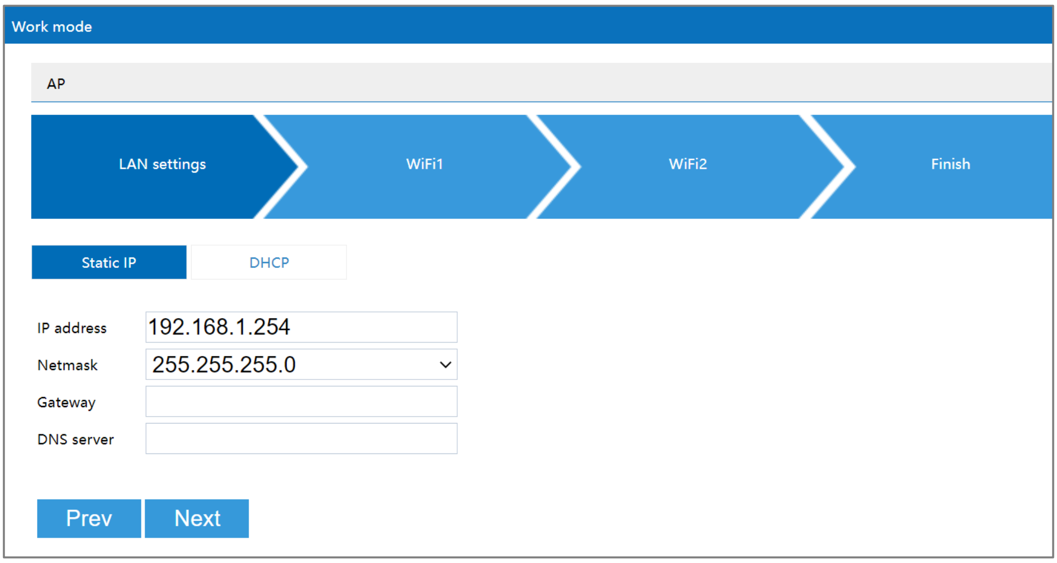
On the "LAN settings" page of AP mode, user can configure the IP address and subnet mask information of LAN.

Operation Path

Please open in order: "Work mode > AP".

Interface description 1: Static IP

Static IP interface as follows:



IP address: 192.168.1.254

Netmask: 255.255.255.0

Gateway:

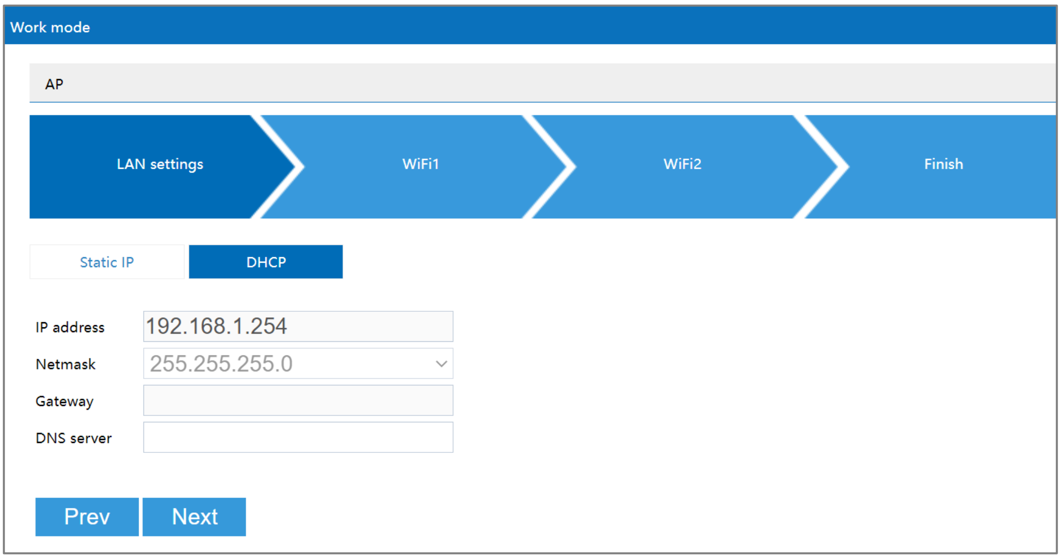
DNS server:

The main element configuration description of static IP interface:

Interface Element	Description
Static IP	Static IP tab.
IP Address	IP address information of LAN.
Netmask	Drop-down list of netmask.
Gateway	Default gateway address of LAN.
DNS Server	DNS server address.

Interface Description 2: DHCP

DHCP interface as follows:



Work mode

AP

IP address 192.168.1.254

Netmask 255.255.255.0

Gateway

DNS server

Main elements configuration description of DHCP interface:

Interface Element	Description
DHCP	DHCP tab.
IP Address	Dynamic acquisition of IP addresses information of LAN.
Netmask	Automatic acquisition of subnet masks information of LAN.
Gateway	Automatically acquired default gateway address.
DNS server	DNS server address. Note: The priority level of manually setting DNS server address is higher than the one of automatically acquired DNS server address.

3.2.2 WiFi1

Function Description

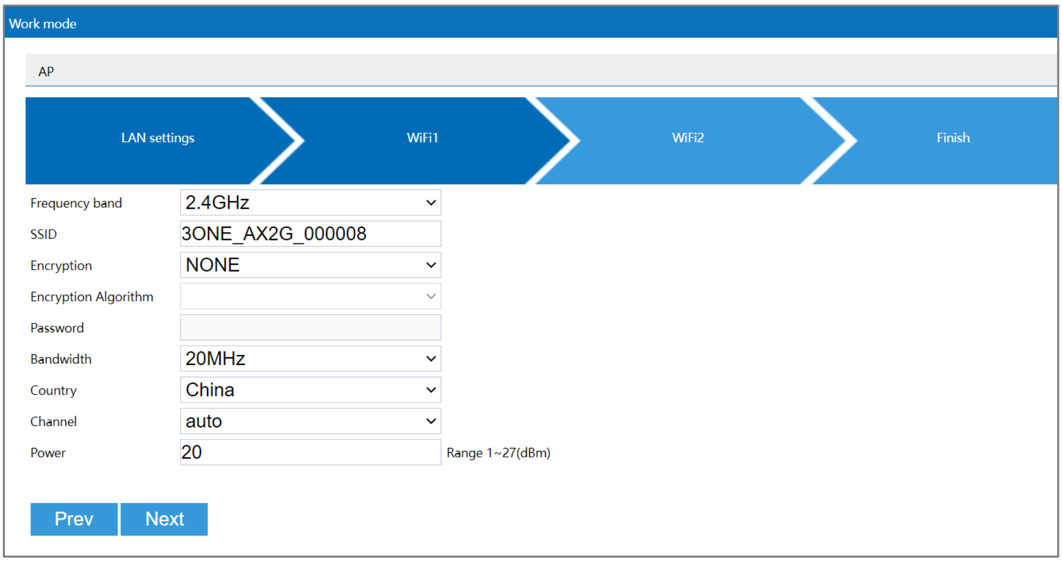
On the "WiFi1" page of AP mode, user can configure the wireless parameters of RF1.

Operation Path

Please open in order: "Work mode > AP".

Interface Description

The WiFi1 interface as follows:



Work mode

AP

Frequency band: 2.4GHz

SSID: 3ONE_AX2G_000008

Encryption: NONE

Encryption Algorithm:

Password:

Bandwidth: 20MHz

Country: China

Channel: auto

Power: 20 Range 1~27(dBm)

Main elements configuration descriptions of WiFi1 interface:

Interface Element	Description
Frequency band	The wireless frequency band corresponding to the current wireless setting, the options are as follows: ● 2.4GHz
SSID	SSID name of wireless network, it supports 1-32 characters.
Encryption	Encryption mode of wireless network, options as follows: ● No encryption; ● WPA2: WiFi Protected Access II suits for the individual or average family network. It adopts pre-shared key mode and supports TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) encryption modes. ● WPA/WPA2: mixed mode of WPA and WPA2, it uses WPA or WPA2 encryption algorithm. ● WPA3: the third version of Wi-Fi protected access, with further security improvements over WPA2, longer encryption keys, and SAE authentication. ● WPA2/WPA3: mixed mode of WPA2 and WPA3, it uses WPA2 or WPA3 encryption algorithm. Note: WPA2/WPA3 only supports personal edition and doesn't support enterprise edition currently. Other encryption algorithms are supported by both of them.
Encryption algorithm	Encryption algorithm of wireless network, options as follows: ● AES (CCMP): advanced encryption standard; ● TKIP/AES: the key integrates 2113 protocol or advanced encryption standard temporarily. Note: When the encryption method is WPA2/WPA3 and WPA3, only AES

Interface Element	Description
	(CCMP) encryption algorithm is supported.
Password	Password of wireless network, it supports 8-63 characters. Note: Wireless password doesn't support blanks. It represents no encryption for wireless network if no password is filled in.
Bandwidth	Wireless network channel bandwidth, options are as follows: ● 20MHz (default); ● 40MHz.
Country	Applied countries and regions of wireless network, options are as follows: ● China; ● USA. Note: Different country opens different channels.
Channel	Working channel of wireless network, default "auto" self-adaptation, options as follows: ● Auto: channel self-adaptation; ● 1: main frequency band 2412Hz, frequency range 2401~2423Hz; ● 2: main frequency band 2417Hz, frequency range 2406~2428Hz; ● 3: main frequency band 2422Hz, frequency range 2411~2433Hz; ● 4: main frequency band 2427Hz, frequency range 2416~2438Hz; ● 5: main frequency band 2432Hz, frequency range 2421~2443Hz; ● 6: main frequency band 2437Hz, frequency range 2426~2448Hz; ● 7: main frequency band 2442Hz, frequency range 2431~2453Hz; ● 8: main frequency band 2447Hz, frequency range 2436~2458Hz; ● 9: main frequency band 2452Hz, frequency range 2441~2463Hz; ● 10: main frequency band 2457Hz, frequency range 2446~2468Hz; ● 11: main frequency band 2462Hz, frequency range 2451~2473Hz; ● 12: main frequency band 2467Hz, frequency range 2456~2478Hz, this frequency band is not open in

Interface Element	Description
	America, so it's temporarily unavailable; • 13: main frequency band 2472Hz, frequency range 2461~2483Hz, this frequency band is not open in America, so it's temporarily unavailable; Note: • Different frequency bands and countries support different options. • In order to improve the network performance, please choose unused channel in the device working environment.
Power	Transmission power of device wireless signal. Note: • Greater the transmitted power, better the transmittability, longer the transmission range, but stronger the interference; • Different device may has different transmitted power range.

3.2.3 WiFi2

Function Description

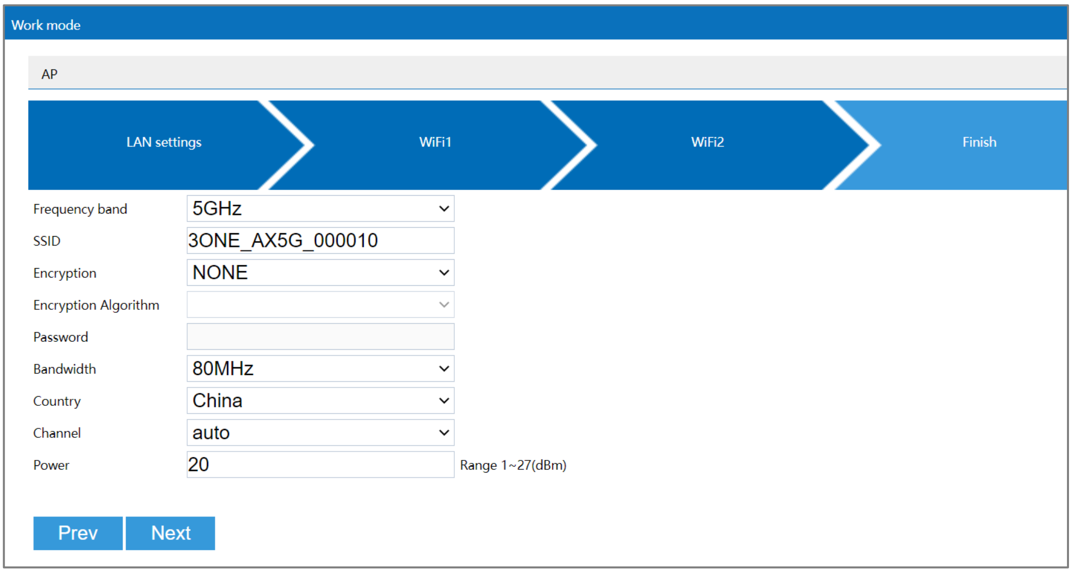
On the "WiFi2" page of AP mode, user can configure the wireless parameters of RF2.

Operation Path

Please open in order: "Work mode > AP".

Interface Description

The WiFi2 interface as follows:



Frequency band: 5GHz
SSID: 3ONE_AX5G_000010
Encryption: NONE
Encryption Algorithm:
Password:
Bandwidth: 80MHz
Country: China
Channel: auto
Power: 20 Range 1~27(dBm)

Main elements configuration descriptions of WiFi2 interface:

Interface Element	Description
Frequency band	The wireless frequency band corresponding to the current wireless setting, the options are as follows: • 5GHz
SSID	SSID name of wireless network, it supports 1-32 characters.
Encryption	Encryption mode of wireless network, options as follows: • No encryption; • WPA2: WiFi Protected Access II suits for the individual or average family network. It adopts pre-shared key mode and supports TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) encryption modes. • WPA/WPA2: mixed mode of WPA and WPA2, it uses WPA or WPA2 encryption algorithm. • WPA3: the third version of Wi-Fi protected access, with further security improvements over WPA2, longer encryption keys, and SAE authentication. • WPA2/WPA3: mixed mode of WPA2 and WPA3, it uses WPA2 or WPA3 encryption algorithm. Note: WPA2/WPA3 only supports personal edition and doesn't support enterprise edition currently. Other encryption algorithms are supported by both of them.
Encryption algorithm	Encryption algorithm of wireless network, options as follows: • AES (CCMP): advanced encryption standard; • TKIP/AES: the key integrates 2113 protocol or advanced encryption standard temporarily. Note: When the encryption method is WPA2/WPA3 and WPA3, only AES (CCMP) encryption algorithm is supported.
Password	Password of wireless network, it supports 8-63 characters. Note: Wireless password doesn’t support blanks. It represents no encryption for wireless network if no password is filled in.
Bandwidth	Channel bandwidth of wireless network, it defaults to 80MHz, options as follows: • 20MHz; • 40MHz; • 80MHz.
Country	Applied countries and regions. Options are as follows: • China; • USA. Note: Different country opens different channels.

Interface Element	Description
Channel	Working channel of wireless network, default "auto" self-adaptation, options as follows: ● Auto: channel self-adaptation; ● 36: main frequency band 5180Hz, frequency range 5170~5190Hz; ● 40: main frequency band 5200Hz， frequency range 5190~5210Hz； ● 44: main frequency band 5220Hz, frequency range 5210~5230Hz; ● 48: main frequency band 5230Hz, frequency range 5210~5250Hz; ● 52: main frequency band 5260Hz, frequency range 5250~5270Hz; ● 56: main frequency band 5280Hz, frequency range 5270~5290Hz; ● 60: main frequency band 5300Hz, frequency range 5290~5310Hz; ● 64: main frequency band 5320Hz, frequency range 5310~5330Hz; ● 100: main frequency band 5500Hz, frequency range 5490~5510Hz, this frequency band is not open in China, so it's temporarily unavailable; ● 104: main frequency band 5520Hz, frequency range 5510~5530Hz, this frequency band is not open in China, so it's temporarily unavailable; ● 108: main frequency band 5540Hz, frequency range 5530~5550Hz, this frequency band is not open in China, so it's temporarily unavailable; ● 112: main frequency band 5560Hz, frequency range 5550~5570Hz, this frequency band is not open in China, so it's temporarily unavailable; ● 116: main frequency band 5580Hz, frequency range 5570~5590Hz, this frequency band is not open in China, so it's temporarily unavailable; ● 120: main frequency band 5600Hz, frequency range 5590~5610Hz, this frequency band is not open in China, so it's temporarily unavailable; ● 124: main frequency band 5620Hz, frequency range 5610~5630Hz, this frequency band is not open in China, so it's temporarily unavailable; ● 128: main frequency band 5640Hz, frequency range

Interface Element	Description
	5630~5650Hz, this frequency band is not open in China, so it's temporarily unavailable; • 132: main frequency band 5660Hz, frequency range 5650~5670Hz, this frequency band is not open in China, so it's temporarily unavailable; • 136: main frequency band 5680Hz, frequency range 5670~5690Hz, this frequency band is not open in China, so it's temporarily unavailable; • 140: main frequency band 5700Hz, frequency range 5690~5710Hz, this frequency band is not open in China, so it's temporarily unavailable; • 144: main frequency band 5720Hz, frequency range 5710~5730Hz, this frequency band is not open in China, so it's temporarily unavailable; • 149: main frequency band 5745Hz, frequency range 5735~5755Hz; • 153: main frequency band 5765Hz, frequency range 5755~5775Hz; • 157: main frequency band 5785Hz, frequency range 5775~5795Hz; • 161: main frequency band 5805Hz, frequency range 5795~5815Hz; • 165: main frequency band 5825Hz, frequency range 5815~5835Hz; Note: • Different frequency bands and countries support different options. • In order to improve the network performance, please choose unused channel in the device working environment.
Power	Transmission power of device wireless signal. Note: • Greater the transmitted power, better the transmittability, longer the transmission range, but stronger the interference; • Different device may has different transmitted power range.

3.2.4 Finish

Function Description

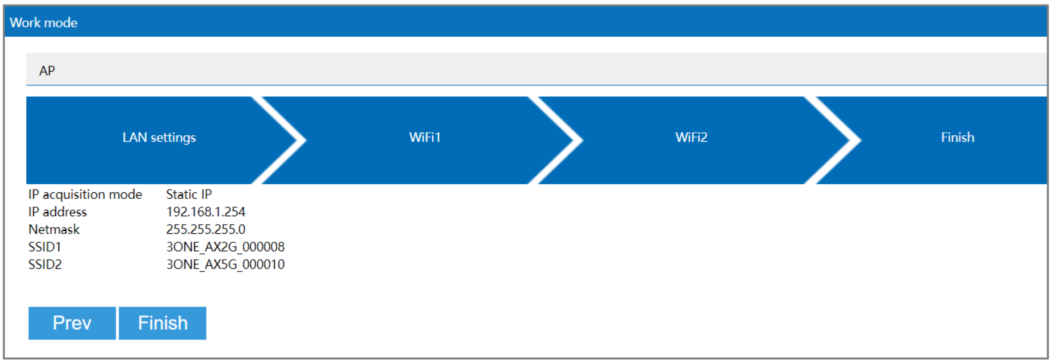
On the "Finish" page of AP mode, user can check the main parameters of AP mode.

Operation Path

Please open in order: "Work mode > AP".

Interface Description

Finish interface as follows:



Work mode

AP

IP acquisition mode Static IP
IP address 192.168.1.254
Netmask 255.255.255.0
SSID1 3ONE_AX2G_000008
SSID2 3ONE_AX5G_000010

The main element configuration description of finish interface:

Interface Element	Description
IP Acquisition Method	● Static IP ● DHCP
IP Address	IP address information of LAN.
Netmask	Subnet masks information of LAN.
SSID1	SSID name of wireless 1 network.
SSID2	SSID name of wireless 2 network.

3.3 Bridge

Under the bridge mode, the device will convert received wireless signal to cable signal and a wireless access point signal. Under the mode, WAN port, LAN port and wireless signal are all in the same VLAN, DHCP server defaults to closed.

⚠Notice

When WDS (Wireless Distribution System) wireless bridging is used for bridging connection, WDS function should be supported and turned on in the parent Wireless network.

The rapid configuration of bridge mode mainly includes six configuration links:

- Connection Mode
- LAN settings
- Connection Settings

- WiFi1
- WiFi2
- Finish

3.3.1 Connection Mode

Function Description

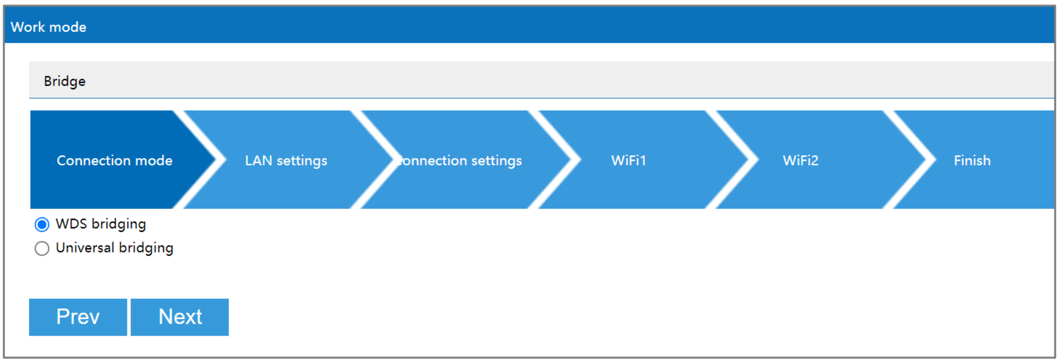
On the "Connection Mode" page of Bridge mode, user can choose universal bridging or WDS bridging.

Operation Path

Please open in order: "Work mode > Bridge".

Interface Description

The connection mode interface as follows:



The main element configuration description of connection mode interface:

Interface Element	Description
WDS bridging	WDS (Wireless Distribution System) bridging is adopted. Note: In WDS bridging mode, the transmitted data is transparently transmitted. WDS bridging is recommended if the device WDS of the same brand or each supplier are compatible.
Universal bridging	Universal bridging is adopted. Note: In the universal bridging mode, the forwarding data is forwarded through the device agent, which is compatible with all kinds of supplier devices. However, the proxy forwarding mechanism hides the MAC address of the real wireless client, which is not suitable for the network environment with strict requirements on MAC address.

3.3.2 LAN Settings

Function Description

On the "LAN settings" page of bridge mode, user can configure the IP address and subnet mask of LAN.

Notes

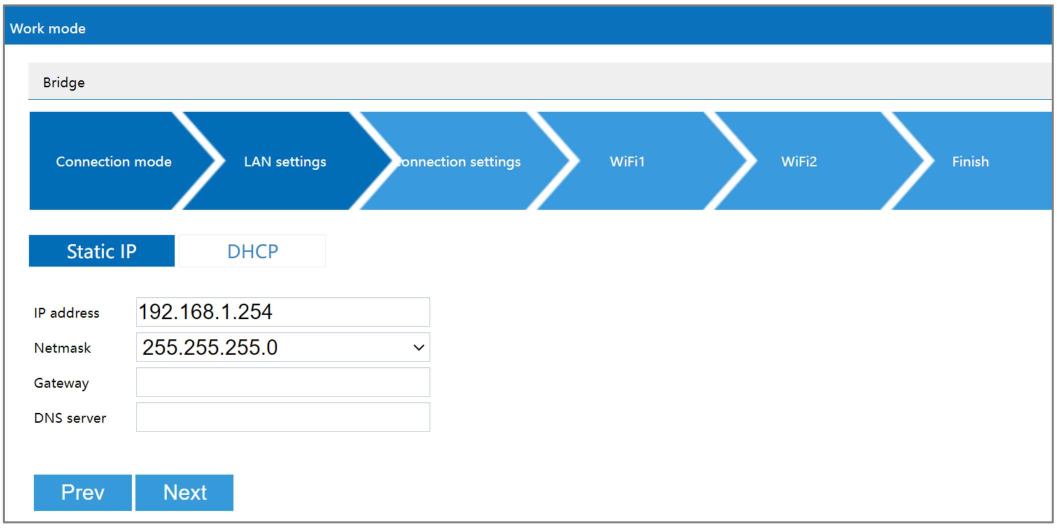
- In universal bridging mode, supports "static IP".
- In WDS bridging mode, supports "static IP" and "DHCP".

Operation Path

Please open in order: "Work mode > Bridge".

Interface description 1: Static IP

Static IP interface as follows:



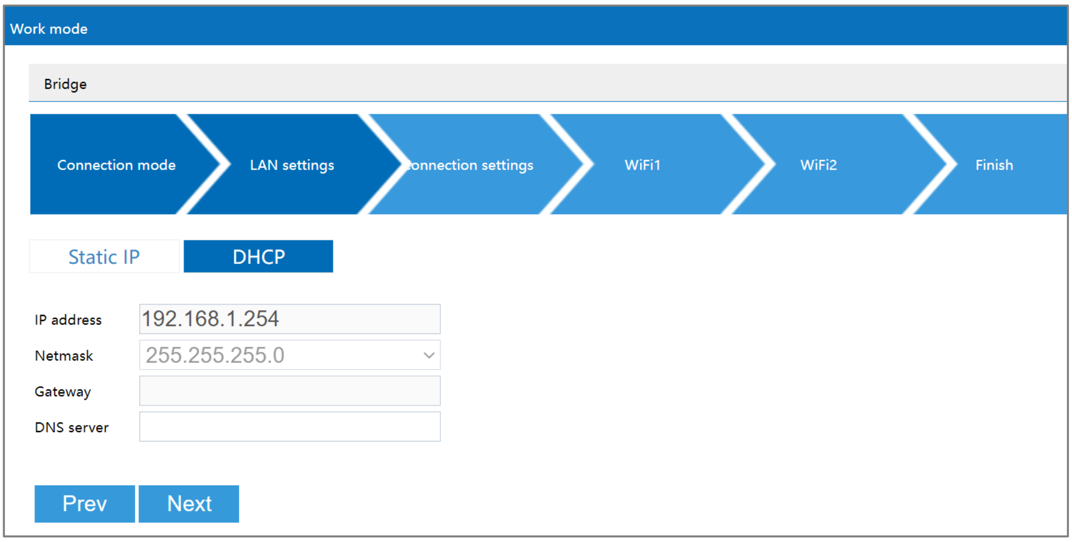
IP address: 192.168.1.254
Netmask: 255.255.255.0
Gateway:
DNS server:

The main element configuration description of static IP interface:

Interface Element	Description
Static IP	Static IP tab.
IP Address	IP address information of LAN.
Netmask	Drop-down list of netmask.
Gateway	Default gateway address of LAN.
DNS server	DNS server address.

Interface Description 2: DHCP

DHCP interface as follows:



IP address 192.168.1.254

Netmask 255.255.255.0

Gateway

DNS server

Main elements configuration description of DHCP interface:

Interface Element	Description
DHCP	DHCP tab.
IP Address	Dynamic acquisition of IP addresses information of LAN.
Netmask	Automatic acquisition of subnet masks information of LAN.
Gateway	Automatically acquired default gateway address.
DNS server	DNS server address. Note: The priority level of manually setting DNS server address is higher than the one of automatically acquired DNS server address.

3.3.3 Connection Settings

Function Description

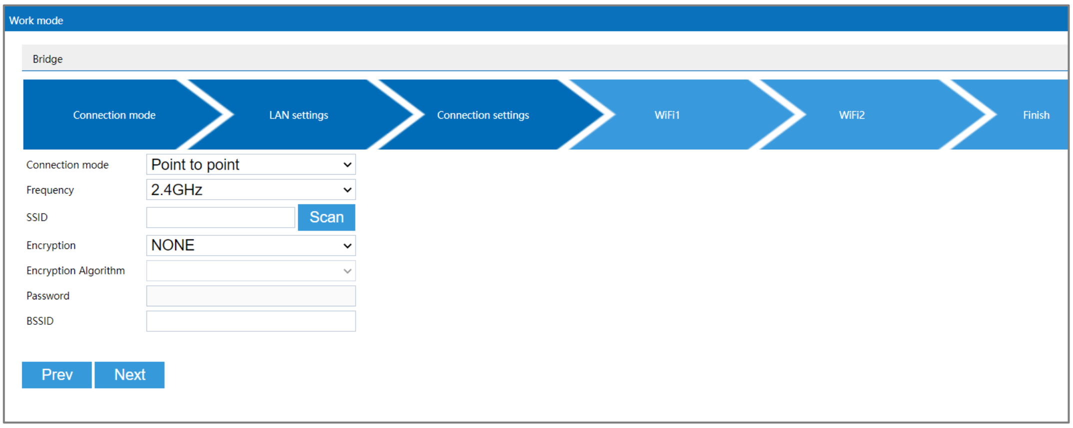
On the "Connection Setting" page of Bridge mode, user can configure the parameters of bridging superior wireless network.

Operation Path

Please open in order: "Work mode > Bridge".

Interface Description

Connection setting interface as follows:



Connection mode: Point to point
Frequency: 2.4GHz
SSID:
Encryption: NONE
Encryption Algorithm:
Password:
BSSID:

The main element configuration description of connection setting interface:

Interface Element	Description
Connection mode	Connection mode of the device and opposite terminal wireless device, options as follows: ● Point to point: it's used for connecting the appointed wireless device; ● Roam: Switching among wireless devices with the same SSID.
Roaming signal threshold	Textbox of roaming signal threshold. ● When the signal strength RSSI falls below this threshold, roaming will be triggered. ● When the signal strength RSSI is higher than this threshold, roaming will not be triggered. Note: This input box is displayed only when connection mode is selected as roaming.
Frequency	Scanning frequency band. Options are as follows: ● 2.4GHz ● 5GHz
SSID	SSID name of the opposite device wireless network. Note: User can add the wireless device for bridge via scan button.
Encryption	Encryption mode of opposite device wireless network, options as follows: ● No encryption; ● WPA2: WiFi Protected Access II suits for the individual or average family network. It adopts pre-shared key mode and supports TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) encryption modes. ● WPA/WPA2: mixed mode of WPA and WPA2, it uses WPA or WPA2 encryption algorithm. ● WPA3: the third version of Wi-Fi protected access, with

Interface Element	Description
	further security improvements over WPA2, longer encryption keys, and SAE authentication. ● WPA2/WPA3: mixed mode of WPA2 and WPA3, it uses WPA2 or WPA3 encryption algorithm. Note: WPA2/WPA3 only supports personal edition and doesn't support enterprise edition currently. Other encryption algorithms are supported by both of them.
Encryption algorithm	Wireless network encryption algorithm of the opposite device, options as follows: ● AES (CCMP): advanced encryption standard; ● TKIP/AES: the key integrates 2113 protocol or advanced encryption standard temporarily. Note: When the encryption method is WPA2/WPA3 and WPA3, only AES (CCMP) encryption algorithm is supported.
Password	Password of opposite device wireless network.
BSSID	MAC address of opposite device wireless network. Note: This input box is displayed only when “connection mode” is selected as “point to point”.

3.3.4 WiFi1

Function Description

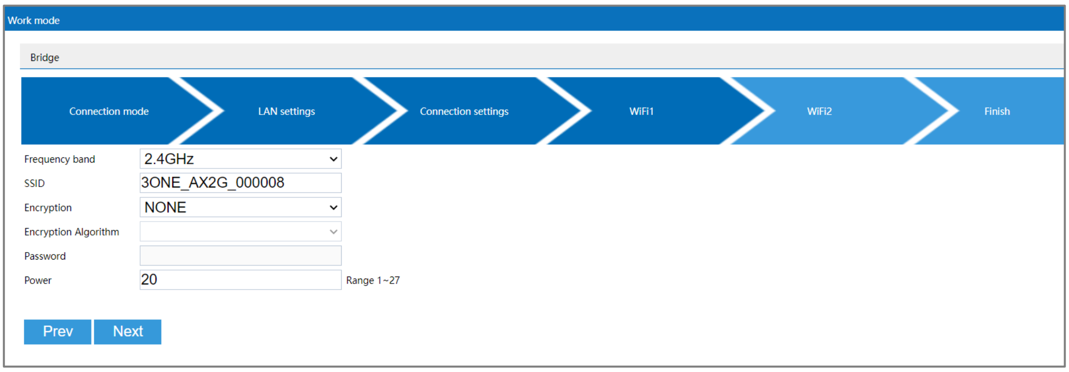
On the "WiFi1" page of bridge mode, user can configure the wireless parameters of RF1.

Operation Path

Please open in order: "Work mode > Bridge".

Interface Description

The WiFi1 interface as follows:



Frequency band: 2.4GHz

SSID: 3ONE_AX2G_000008

Encryption: NONE

Encryption Algorithm:

Password:

Power: 20 Range 1~27

Main elements configuration descriptions of WiFi1 interface:

Interface Element	Description
Frequency band	The wireless frequency band used by the bridging corresponding to the current wireless setting.
SSID	SSID name of wireless network, it supports 1-32 characters.
Encryption	Encryption mode of wireless network, options as follows: • No encryption; • WPA2: WiFi Protected Access II suits for the individual or average family network. It adopts pre-shared key mode and supports TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) encryption modes. • WPA/WPA2: mixed mode of WPA and WPA2, it uses WPA or WPA2 encryption algorithm. • WPA3: the third version of Wi-Fi protected access, with further security improvements over WPA2, longer encryption keys, and SAE authentication. • WPA2/WPA3: mixed mode of WPA2 and WPA3, it uses WPA2 or WPA3 encryption algorithm. Note: WPA2/WPA3 only supports personal edition and doesn't support enterprise edition currently. Other encryption algorithms are supported by both of them.
Encryption algorithm	Encryption algorithm of wireless network, options as follows: • AES (CCMP): advanced encryption standard; • TKIP/AES: the key integrates 2113 protocol or advanced encryption standard temporarily. Note: When the encryption method is WPA2/WPA3 and WPA3, only AES (CCMP) encryption algorithm is supported.
Password	Password of wireless network, it supports 8-63 characters. Note: Wireless password doesn’t support blanks. It represents no encryption for wireless network if no password is filled in.
Power	Transmission power of device wireless signal.

Interface Element	Description
	Note: • Greater the transmitted power, better the transmittability, longer the transmission range, but stronger the interference; • Different device may has different transmitted power range.

3.3.5 WiFi2

Function Description

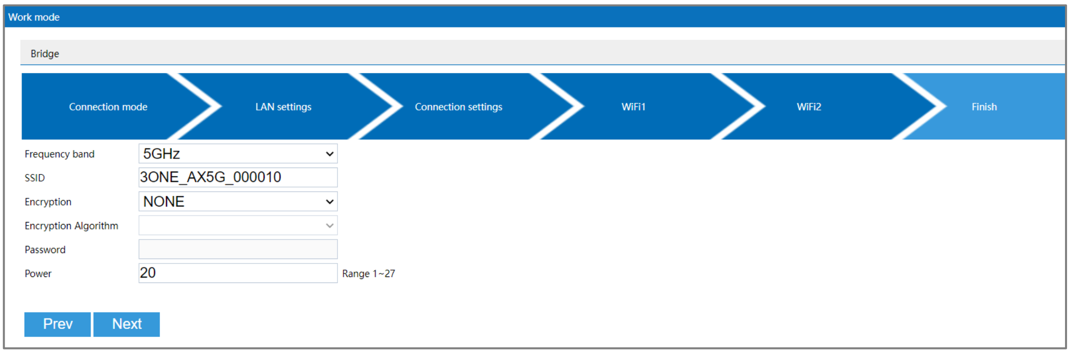
On the "WiFi2" page of bridge mode, user can configure the wireless parameters of RF2.

Operation Path

Please open in order: "Work mode > Bridge".

Interface Description

The WiFi2 interface as follows:



Frequency band: 5GHz
SSID: 3ONE_AX5G_000010
Encryption: NONE
Encryption Algorithm:
Password:
Power: 20 Range 1~27

Main elements configuration descriptions of WiFi2 interface:

Interface Element	Description
Frequency band	• The wireless frequency band used by the bridging corresponding to the current wireless setting.
SSID	SSID name of wireless network, it supports 1-32 characters.
Encryption	Encryption mode of wireless network, options as follows: • No encryption; • WPA2: WiFi Protected Access II suits for the individual or average family network. It adopts pre-shared key mode and supports TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) encryption modes. • WPA/WPA2: mixed mode of WPA and WPA2, it uses WPA or WPA2 encryption algorithm.

Interface Element	Description
	● WPA3: the third version of Wi-Fi protected access, with further security improvements over WPA2, longer encryption keys, and SAE authentication. ● WPA2/WPA3: mixed mode of WPA2 and WPA3, it uses WPA2 or WPA3 encryption algorithm. Note: WPA2/WPA3 only supports personal edition and doesn't support enterprise edition currently. Other encryption algorithms are supported by both of them.
Encryption algorithm	Encryption algorithm of wireless network, options as follows: ● AES (CCMP): advanced encryption standard; ● TKIP/AES: the key integrates 2113 protocol or advanced encryption standard temporarily. Note: When the encryption method is WPA2/WPA3 and WPA3, only AES (CCMP) encryption algorithm is supported.
Password	Password of wireless network, it supports 8-63 characters. Note: Wireless password doesn’t support blanks. It represents no encryption for wireless network if no password is filled in.
Power	Transmission power of device wireless signal. Note: ● Greater the transmitted power, better the transmittability, longer the transmission range, but stronger the interference; ● Different device may has different transmitted power range.

3.3.6 Finish

Function Description

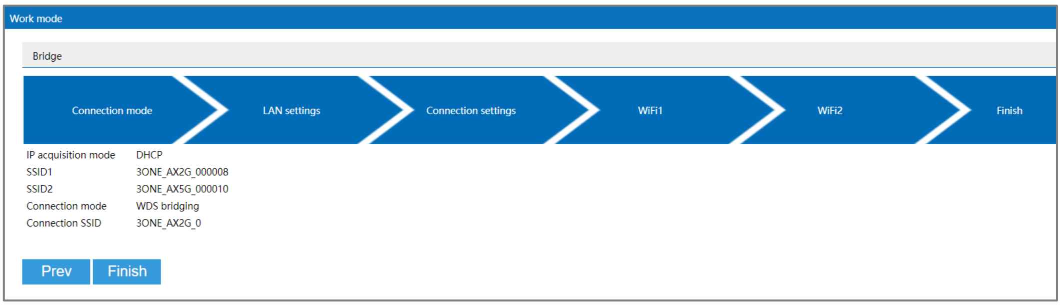
On the "Finish" page of bridge mode, user can check the main parameters of bridge mode.

Operation Path

Please open in order: "Work Mode > Bridge".

Interface Description

Finish interface as follows:



IP acquisition mode DHCP
SSID1 3ONE_AX2G_000008
SSID2 3ONE_AX5G_000010
Connection mode WDS bridging
Connection SSID 3ONE_AX2G_0

The main element configuration description of finish interface:

Interface Element	Description
IP Acquisition Mode	IP address acquisition mode ● Static IP ● DHCP
IP Address	IP address information of LAN.
Netmask	Subnet masks information of LAN.
SSID1	SSID name of wireless 1 network.
SSID2	SSID name of wireless 2 network.
Connection mode	Display Wireless bridging Method.
Connection SSID	Display the SSID name of the opposite end of the bridge.

3.4 Client

Under the client mode, the device will convert received wireless signal to cable signal.

- Under WDS bridging and universal bridging in this mode, WAN port, LAN port and wireless signal are all in the same VLAN, and DHCP server is disabled by default.
- In the wireless NAT mode of this mode, the wireless signal is connected to the external network, the WAN port and LAN port are in the internal network, and the DHCP server is enabled by default.

Notice

There are three client connection modes: WDS (Wireless Distribution System), universal bridging and wireless NAT. When WDS bridging is used, the superior wireless network device needs to support and enable the WDS function.

The client mode mainly has five configuration links:

- Connection Mode
- WAN settings

  Note:
  External network settings are only supported when the connection mode is "Wireless NAT".
- LAN settings
- Connection Settings

- Finish

Following is the explanation of those configuration links.

3.4.1 Connection Mode

Function Description

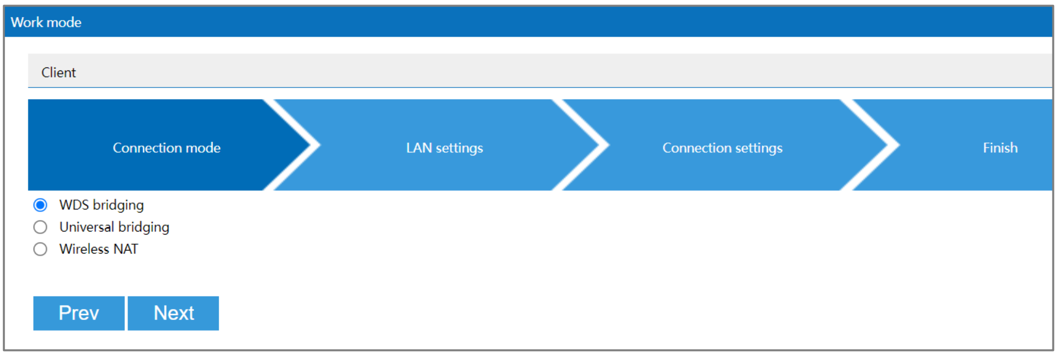
On the "Connection Mode" page of client mode, user can choose universal bridging, WDS bridging and wireless NAT.

Operation Path

Please open in order: "Work mode > Client".

Interface Description

The connection mode interface as follows:



● WDS bridging
○ Universal bridging
○ Wireless NAT

The main element configuration description of connection mode interface:

Interface Element	Description
WDS bridging	The client connection adopts WDS (wireless distribution system) wireless distribution system bridging mode. Note: In WDS bridging mode, the transmitted data is transparently transmitted. WDS bridging is recommended if the device WDS of the same brand or each supplier are compatible.
Universal bridging	The client connection adopts universal bridge mode. Note: In the universal bridging mode, the forwarding data is forwarded through the device agent, which is compatible with all kinds of supplier devices. However, the proxy forwarding mechanism hides the MAC address of the real wireless client, which is not suitable for the network environment with strict requirements on MAC address.
Wireless NAT	Wireless NAT (Network Address Translation) is adopted for connection. Note: Under the wireless NAT connection mode, the device wireless can connect to the external network via PPPoE dial-up, static IP and dynamic acquisition; the LAN port can be connected to LAN.

3.4.2 WAN Settings

Function Description

⚠Notice

External network settings are only supported when the connection mode is "Wireless NAT".

On the "WAN Settings" page of client mode (wireless NAT), Wireless can be connected to WAN via three methods:

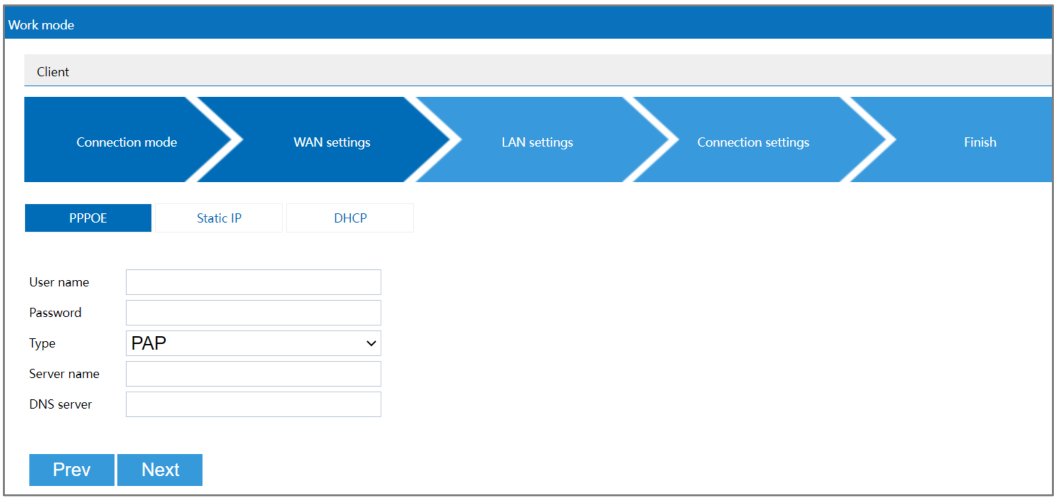
- PPPoE;
- Static IP;
- DHCP.

Operation Path

Please open in order: "Work mode > Client".

Interface Description 1: PPPoE

PPPoE interface as follows:



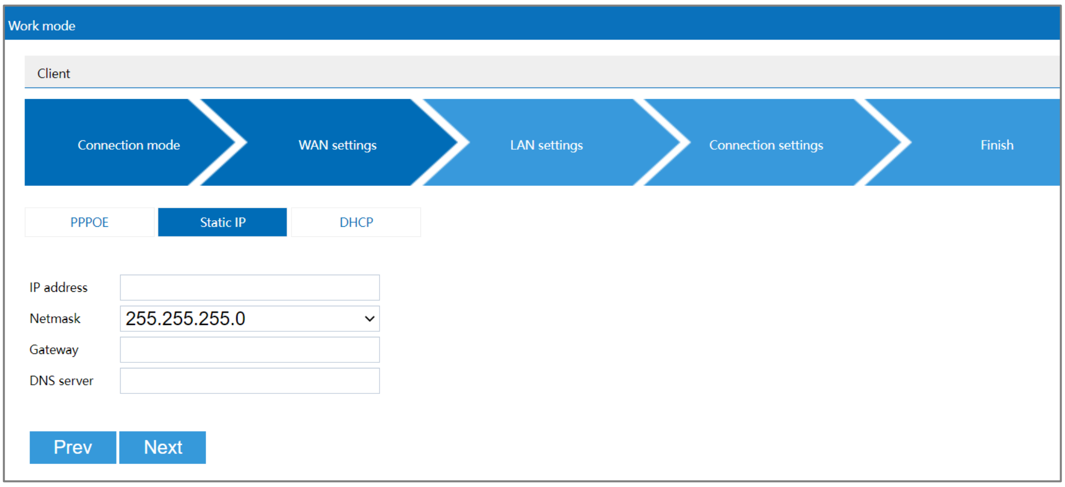
The main element configuration description of PPPoE interface:

Interface Element	Description
PPPoE	Click the "PPPoE Dialing" button to dial through the point-to-point protocol on Ethernet to realize Internet access.
User name	User name of PPPoE connection. Note:

Interface Element	Description
	User name, password and service name are provided by network provider.
Password	Password of PPPoE connection. Note: User name, password and service name are provided by network provider.
Type	The type of PPPoE dialing: ● PAP: Password Authentication Protocol, which sends user name or password over the network; ● CHAP: Challenge Handshake Authentication Protocol, it only transmits user name; ● PAP/CHAP: uses Password Authentication Protocol or Challenge Handshake Authentication Protocol.
Server name	Server name, not fill if network provider doesn't supply. Note: User name, password and service name are provided by network provider.
DNS server	The DNS server address provided by network provider or extranet.

Interface Description 2: Static IP

Static IP interface as follows:



IP address

Netmask 255.255.255.0

Gateway

DNS server

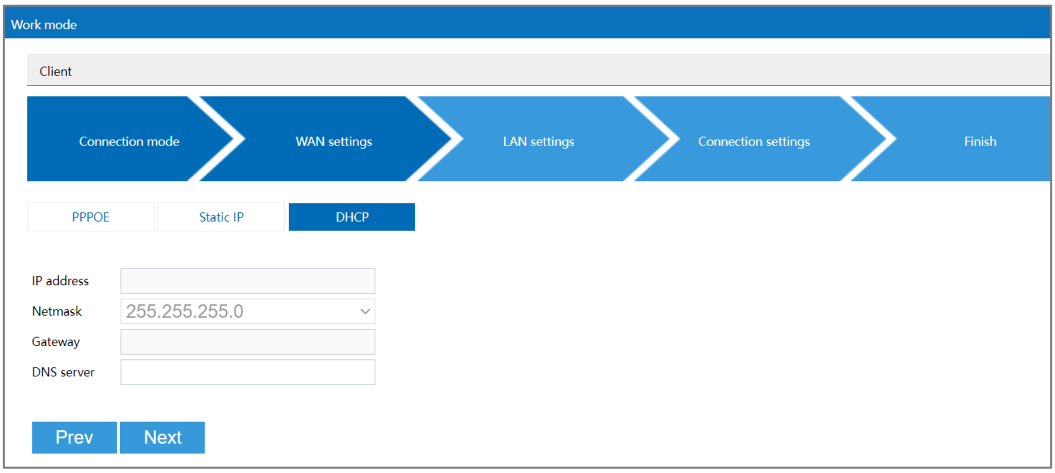
The main element configuration description of static IP interface:

Interface Element	Description
Static IP	Click the "static IP" button to configure the extranet network information of the device.
IP Address	The fixed IP address provided by network provider or extranet.

Interface Element	Description
Netmask	The subnet mask provided by network provider or LAN.
Gateway	The default gateway address provided by network provider or extranet.
DNS server	The DNS server address provided by network provider or extranet.

Interface Description 3: DHCP

DHCP interface as follows:


Work mode

Client

IP address

Netmask 255.255.255.0

Gateway

DNS server

Main elements configuration description of DHCP interface:

Interface Element	Description
DHCP	Click the "dynamic acquisition" button to automatically acquire the WAN port network information of the device. Note: The device automatically acquires the network address information distributed by network provider or WAN.
IP Address	IP address automatically distributed by network provider or WAN.
Netmask	The subnet mask automatically distributed by network provider or WAN.
Gateway	Gateway address automatically distributed by network provider or WAN.
DNS server	DNS server address. Note: The priority level of manually setting DNS server address is higher than the one of automatically acquired DNS server address.

3.4.3 LAN Settings

Function Description

On the "LAN settings" page of client mode, user can configure the IP address and subnet mask information of LAN.

Notes

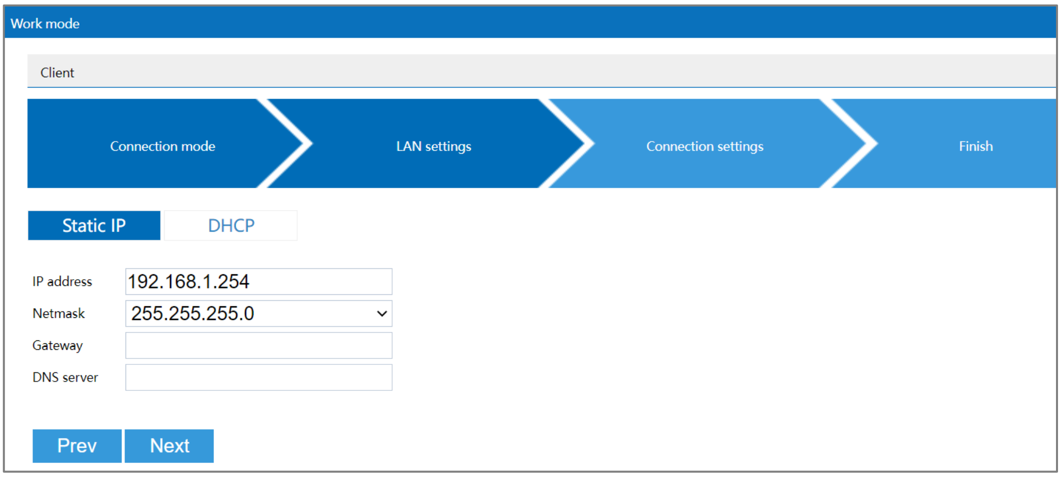
- In universal bridging and wireless NAT mode, "static IP” is supported.
- In WDS bridging mode, supports "static IP" and "DHCP".

Operation Path

Please open in order: "Work mode > Client".

Interface description 1: Static IP

Static IP interface as follows:



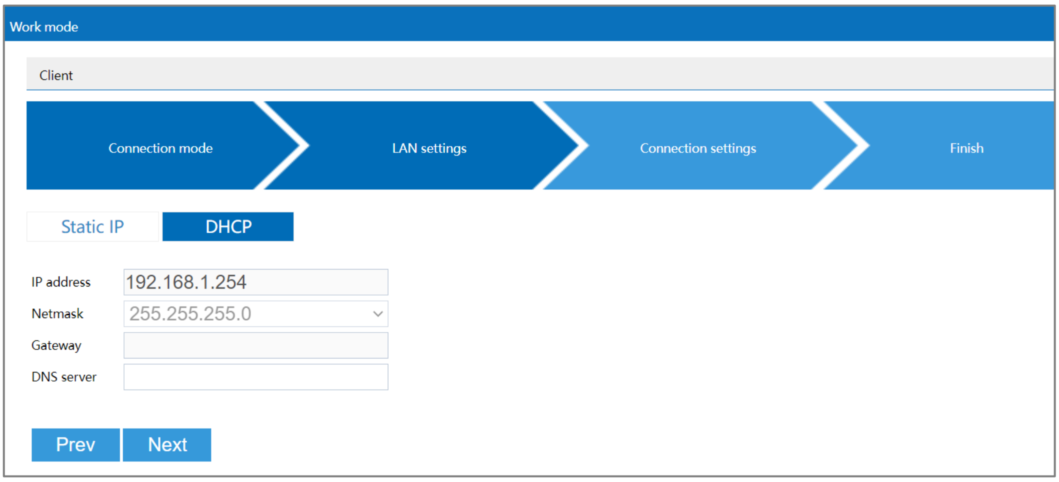
IP address 192.168.1.254
Netmask 255.255.255.0
Gateway
DNS server

The main element configuration description of static IP interface:

Interface Element	Description
Static IP	Static IP tab.
IP Address	IP address information of LAN.
Netmask	Drop-down list of netmask.
Gateway	Default gateway address of LAN.
DNS server	DNS server address.

Interface Description 2: DHCP

DHCP interface as follows:



Work mode

Client

IP address: 192.168.1.254

Netmask: 255.255.255.0

Gateway:

DNS server:

Main elements configuration description of DHCP interface:

Interface Element	Description
DHCP	DHCP tab.
IP Address	Dynamic acquisition of IP addresses information of LAN.
Netmask	Drop-down list of netmask.
Gateway	Automatically acquired default gateway address.
DNS server	DNS server address. Note: The priority level of manually setting DNS server address is higher than the one of automatically acquired DNS server address.

3.4.4 Connection Settings

Function Description

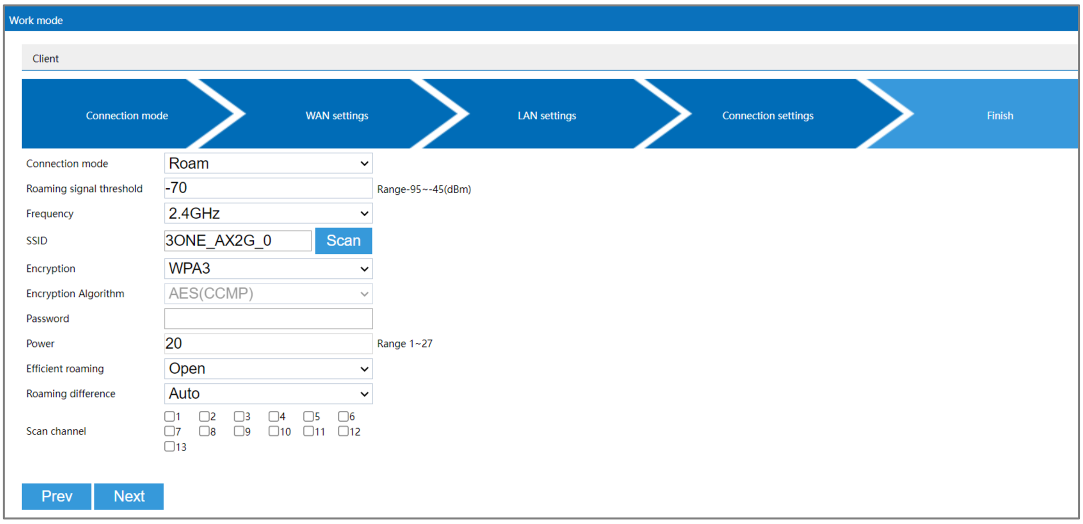
On the "Connection Setting" page of Client mode, user can configure the parameters of bridging superior wireless network.

Operation Path

Please open in order: "Work mode > Client".

Interface Description

The interface of connection setting is as follows:



Connection mode	Roam
Roaming signal threshold	-70 Range-95~-45(dBm)
Frequency	2.4GHz
SSID	3ONE_AX2G_0
Encryption	WPA3
Encryption Algorithm	AES(CCMP)
Password	
Power	20 Range 1~27
Efficient roaming	Open
Roaming difference	Auto
Scan channel	□1 □2 □3 □4 □5 □6 □7 □8 □9 □10 □11 □12 □13

The main element configuration description of connection setting interface:

Interface Element	Description
Connection mode	Connection mode of the device and opposite terminal wireless device, options as follows: • Point to point: it's used for connecting the appointed wireless device; • Roam: Switching among wireless devices with the same SSID.
Roaming signal threshold	Textbox of roaming signal threshold. • When the signal strength RSSI falls below this threshold, roaming will be triggered. • When the signal strength RSSI is higher than this threshold, roaming will not be triggered. Note: This input box is displayed only when connection mode is selected as roaming.
Frequency	Scanning frequency band. Options are as follows: • 2.4GHz • 5GHz
SSID	SSID name of the opposite device wireless network. Note: User can add the wireless device for bridge via scan button.
Encryption	Encryption mode of opposite device wireless network, options as follows: • No encryption; • WPA2: WiFi Protected Access II suits for the individual or average family network. It adopts pre-shared key mode and supports TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) encryption modes.

Interface Element	Description
	• WPA/WPA2: mixed mode of WPA and WPA2, it uses WPA or WPA2 encryption algorithm. • WPA3: the third version of Wi-Fi protected access, with further security improvements over WPA2, longer encryption keys, and SAE authentication. • WPA2/WPA3: mixed mode of WPA2 and WPA3, it uses WPA2 or WPA3 encryption algorithm. Note: WPA2/WPA3 only supports personal edition and doesn't support enterprise edition currently. Other encryption algorithms are supported by both of them.
Encryption algorithm	Wireless network encryption algorithm of the opposite device, options as follows: • AES (CCMP): advanced encryption standard; • TKIP/AES: the key integrates 2113 protocol or advanced encryption standard temporarily. Note: When the encryption method is WPA2/WPA3 and WPA3, only AES (CCMP) encryption algorithm is supported.
Password	Password of opposite device wireless network.
BSSID	MAC address of opposite device wireless network. Note: This item is displayed when the connection mode is "Point-to-Point" connection.
Power	Transmission power of device wireless signal. Note: • Greater the transmitted power, better the transmittability, longer the transmission range, but stronger the interference; • Different device may has different transmitted power range.
Efficient roaming	The switch of efficient roaming function Efficient roaming is a roaming acceleration technology independently developed by our company. Ordinary roaming requires all-channel scanning, while efficient roaming specifies any channels for scanning, and which has optimized the roaming strategy and greatly shortened the roaming time. Note: Efficient roaming can only be enabled when the"Roaming" is selected as the "Connection Mode".
Roaming RSSI difference	Roaming RSSI difference of efficient roaming function. The default is the dynamic value calculated automatically, or you can select a fixed value in the drop-down list (range: 5-20). • When the signal strength RSSI difference between the new AP and the current associated AP is higher than

Interface Element	Description
	this threshold, roaming is triggered; - When the RSSI difference between the signal strength of the new AP and the current associated AP is lower than this threshold, roaming will not be triggered; Note: This drop-down box is displayed only when efficient roaming is enabled.
Scan channel	High-priority scan channels under efficient roaming function. No channel is checked by default, that is, there is no priority channel, and all channels are scanned in sequence. When some channels are checked, the designated channel is scanned first, and if no stable signal can be scanned in the designated channel, other channels will be scanned. Note: This item is displayed only when "efficient roaming" is enabled.

3.4.5 Finish

Function Description

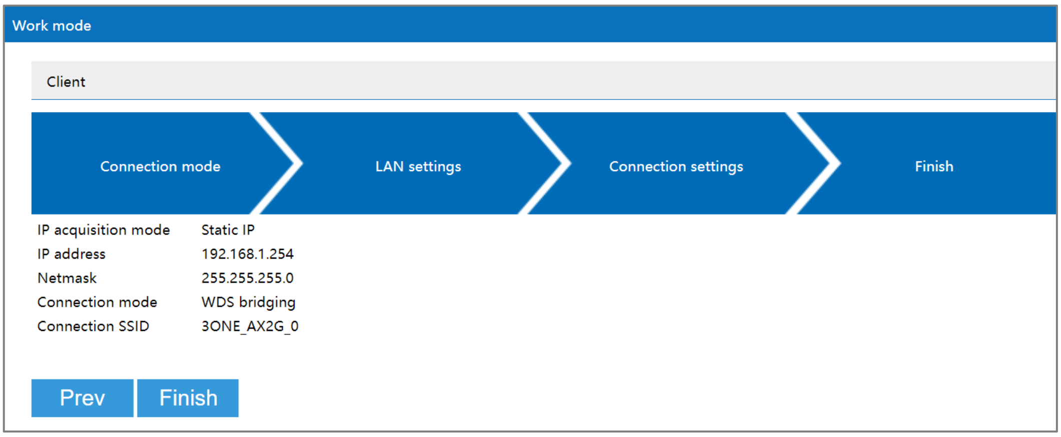
On the "Finish" page of client mode, user can check the main parameters of client.

Operation Path

Please open in order: "Work mode > Client".

Interface Description

Finish interface as follows:



IP acquisition mode Static IP
IP address 192.168.1.254
Netmask 255.255.255.0
Connection mode WDS bridging
Connection SSID 3ONE_AX2G_0

The main element configuration description of finish interface:

Interface Element	Description
IP acquisition mode/WAN IP acquisition mode	- PPPoE - Static IP

Interface Element	Description
	• DHCP
IP Address/LAN IP Address	IP address information of LAN.
Netmask/LAN Netmask	Subnet masks information of LAN.
Connection mode	Display Wireless bridging Method.
Connect SSID	Display the SSID name of the opposite end of the bridge.

3.5 Dual-link Mode

Notes

Only dual-frequency devices support dual link mode, and single-frequency devices do not support dual link mode.

In dual-link mode, dual-link client is supported, and dual-frequency seamless roaming and link backup are supported.

The principle of dual-frequency seamless roaming is using two wireless bands to complete the roaming action at the same time, the two bands can be 2.4G+5G, or dual-5G. The two frequency bands are respectively associated with different BSSIDs, one of which is the main frequency band and responsible for data communication with AP; The other band, which acts as a backup, scans when the signal strength is below the threshold and connects to a better source automatically if it is found. This process is the same as that of single frequency roaming. When the communication quality of the primary frequency band is significantly reduced and the signal strength of the backup frequency band is strong enough, the backup frequency band will be switched to the primary frequency band, and take over the data communication with AP, while the original primary frequency band will be converted to the backup frequency band. When switching between the primary and backup frequency bands, both frequency bands are in the state of associated AP without the process of disconnecting and reassociating AP, so seamless roaming can be achieved.

Dual link mode mainly has five configuration links:

- Connection Mode

- WAN settings

  Note:

  External network settings are only supported when the connection mode is "Wireless NAT".
- LAN settings
- Connection Settings
- Finish

Following is the explanation of those configuration links.

3.5.1 Connection Mode

Function Description

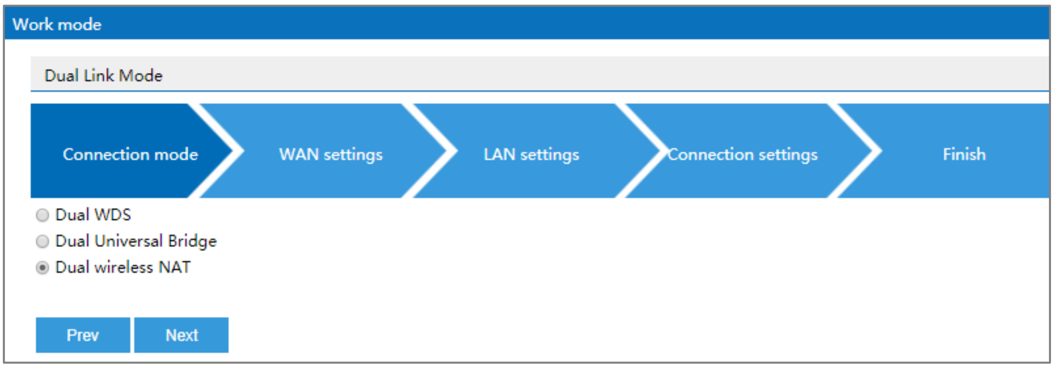
On the "Connection Mode" page of dual-link mode, user can choose dual WDS, dual universal bridging and dual wireless NAT.

Operation Path

Please open in order: “Mode Settings > Dual-link Mode".

Interface Description

The connection mode interface as follows:



The main element configuration description of connection mode interface:

Interface Element	Description
Dual WDS	The connection mode adopts the bridge mode of dual WDS (wireless distribution system). This mode is mainly used for realizing seamless roaming. Note: In dual WDS mode, the transmitted data is transparently transmitted. WDS bridging is recommended if the device WDS of the same brand or each supplier are compatible.
Dual Universal Bridging	The connection mode adopts dual universal bridging. This mode is mainly used for realizing seamless roaming. Note: In the universal bridging mode, the forwarding data is forwarded through the device agent, which is compatible with all kinds of supplier devices. However, the proxy forwarding mechanism hides

Interface Element	Description
	the MAC address of the real wireless client, which is not suitable for the network environment with strict requirements on MAC address.
Dual Wireless NAT	Wireless NAT (Network Address Translation) is adopted for connection. Note: Under the wireless NAT connection mode, the device wireless can connect to the external network via PPPoE dial-up, static IP and dynamic acquisition; the LAN port can be connected to LAN.

3.5.2 WAN Settings

Function Description

⚠Notice

Only dual wireless NAT mode supports external network settings.

On the "WAN Settings" page of dual link mode (dual wireless NAT), wireless can connect to the WAN in three modes:

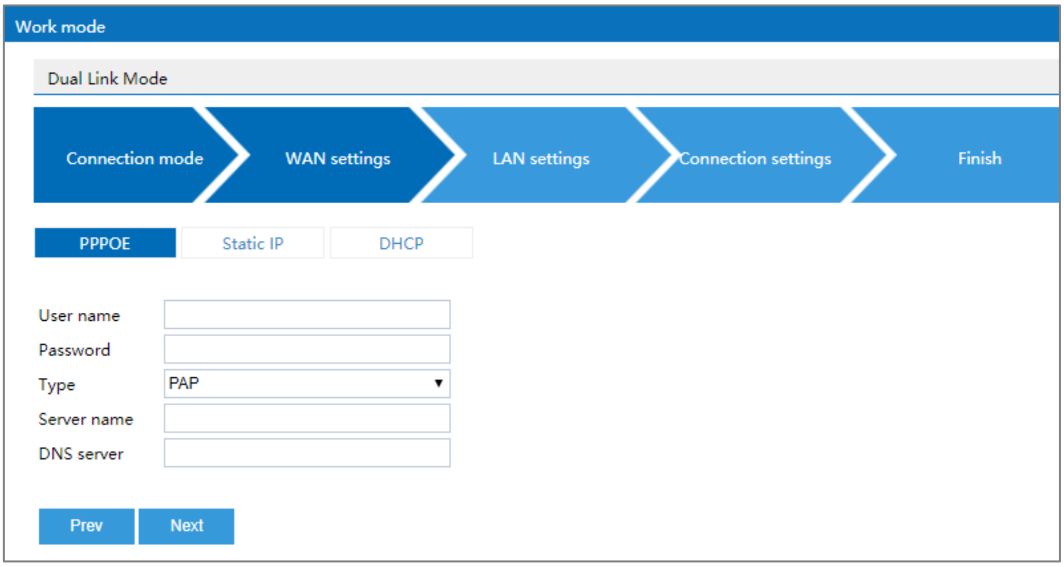
- PPPoE;
- Static IP;
- DHCP.

Operation Path

Please open in order: “Mode Settings > Dual-link Mode".

Interface Description 1: PPPoE

PPPoE interface as follows:



User name

Password

Type PAP

Server name

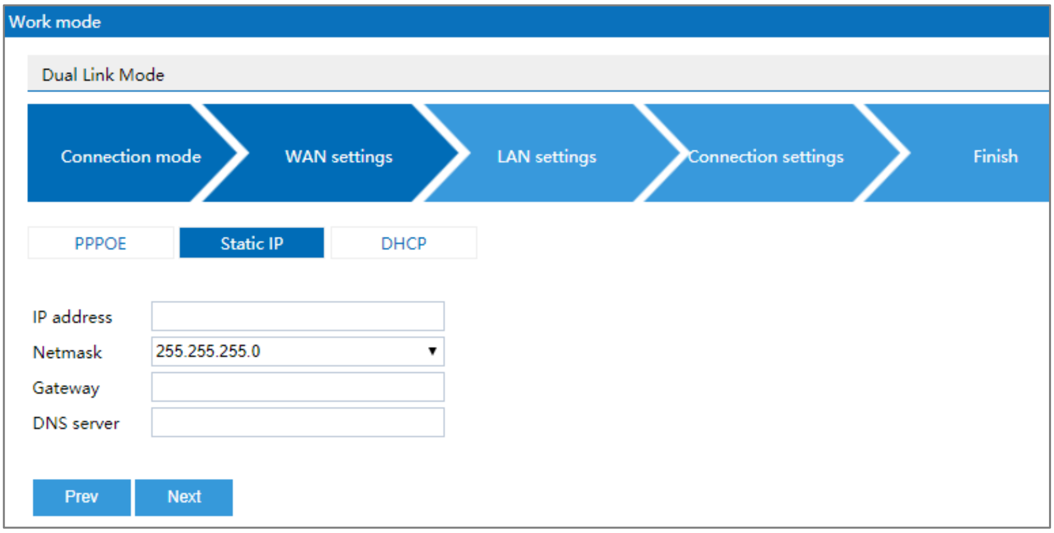
DNS server

The main element configuration description of PPPoE interface:

Interface Element	Description
PPPoE	Click the "PPPoE Dialing" button to dial through the point-to-point protocol on Ethernet to realize Internet access.
Username	User name of PPPoE connection. Note: User name, password and service name are provided by network provider.
Password	Password of PPPoE connection. Note: User name, password and service name are provided by network provider.
Type	The type of PPPoE dialing: ● PAP: Password Authentication Protocol, which sends user name or password over the network; ● CHAP: Challenge Handshake Authentication Protocol, it only transmits user name; ● PAP/CHAP: uses Password Authentication Protocol or Challenge Handshake Authentication Protocol.
Server Name	Server name, not fill if network provider doesn't supply. Note: User name, password and service name are provided by network provider.
DNS Server	The DNS server address provided by network provider or extranet.

Interface Description 2: Static IP

Static IP interface as follows:



IP address

Netmask 255.255.255.0

Gateway

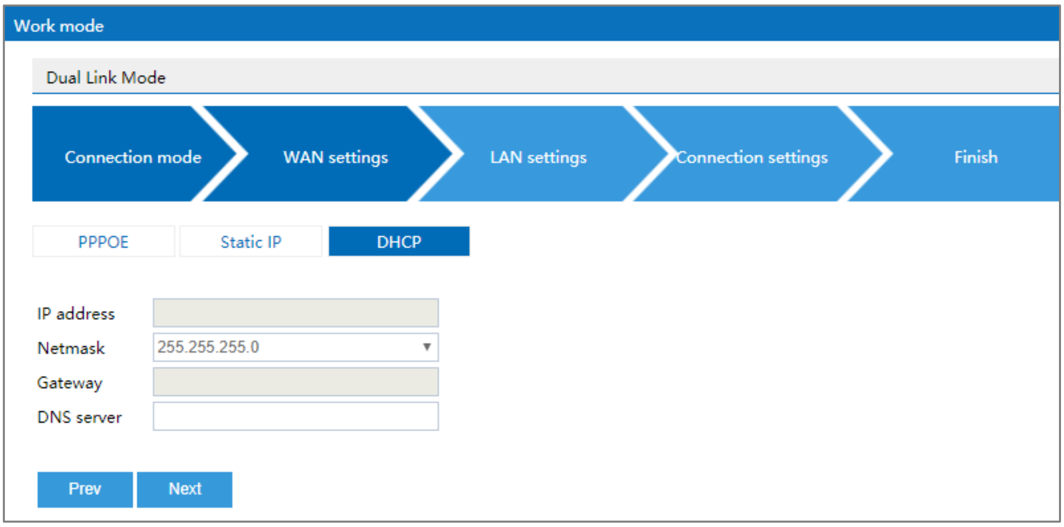
DNS server

The main element configuration description of static IP interface:

Interface Element	Description
Static IP	Click the "static IP" button to configure the extranet network information of the device.
IP Address	The fixed IP address provided by network provider or extranet.
Netmask	Drop-down list of netmask.
Gateway	The default gateway address provided by network provider or extranet.
DNS server	The DNS server address provided by network provider or extranet.

Interface Description 3: DHCP

DHCP interface as follows:



IP address
Netmask 255.255.255.0
Gateway
DNS server

Main elements configuration description of DHCP interface:

Interface Element	Description
DHCP	Click the "dynamic acquisition" button to automatically acquire the WAN port network information of the device. Note: The device automatically acquires the network address information distributed by network provider or WAN.
IP Address	IP address automatically distributed by network provider or WAN.
Netmask	Drop-down list of netmask.
Gateway	Gateway address automatically distributed by network provider or WAN.

Interface Element	Description
DNS server	DNS server address. Note: The priority level of manually setting DNS server address is higher than the one of automatically acquired DNS server address.

3.5.3 LAN Settings

Function Description

On the "Intranet Settings" page of dual-link mode, user can configure the IP address and subnet mask information of LAN.

Note

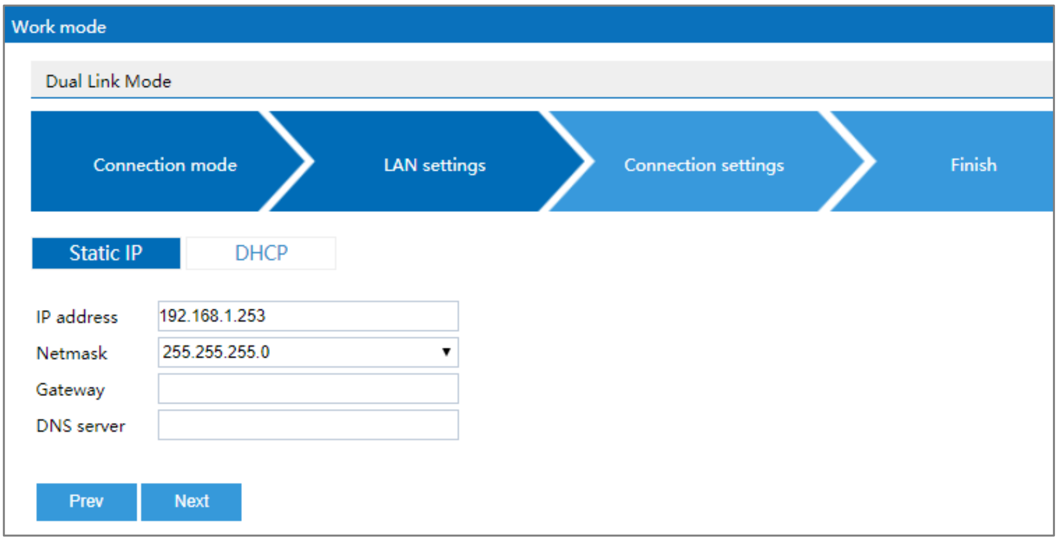
- In dual universal bridging and dual wireless NAT mode, "Static IP” is supported.
- In WDS bridging mode, supports "static IP" and "DHCP".

Operation Path

Please open in order: “Mode Settings > Dual-link Mode".

Interface description 1: Static IP

Static IP interface as follows:



IP address 192.168.1.253
Netmask 255.255.255.0
Gateway
DNS server

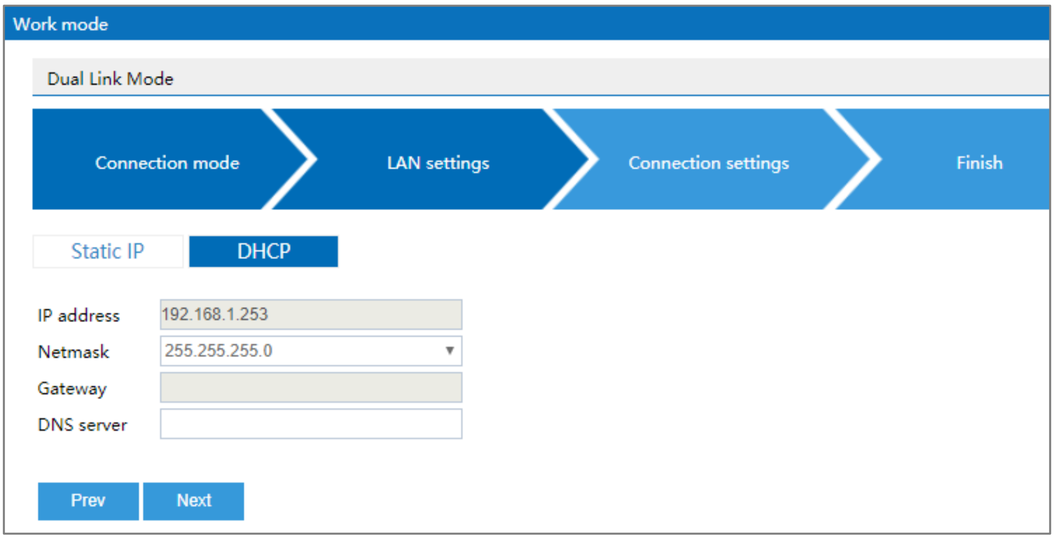
The main element configuration description of static IP interface:

Interface Element	Description
Static IP	Static IP tab.
IP Address	IP address information of LAN.

Interface Element	Description
Netmask	Drop-down list of netmask.
Gateway	Default gateway address of LAN.
DNS server	DNS server address.

Interface Description 2: DHCP

DHCP interface as follows:



IP address 192.168.1.253
Netmask 255.255.255.0
Gateway
DNS server

Main elements configuration description of DHCP interface:

Interface Element	Description
DHCP	DHCP tab.
IP Address	Dynamic acquisition of IP addresses information of LAN.
Netmask	Drop-down list of netmask.
Gateway	Automatically acquired default gateway address.
DNS server	DNS server address. Note: The priority level of manually setting DNS server address is higher than the one of automatically acquired DNS server address.

3.5.4 Connection Settings

Function Description

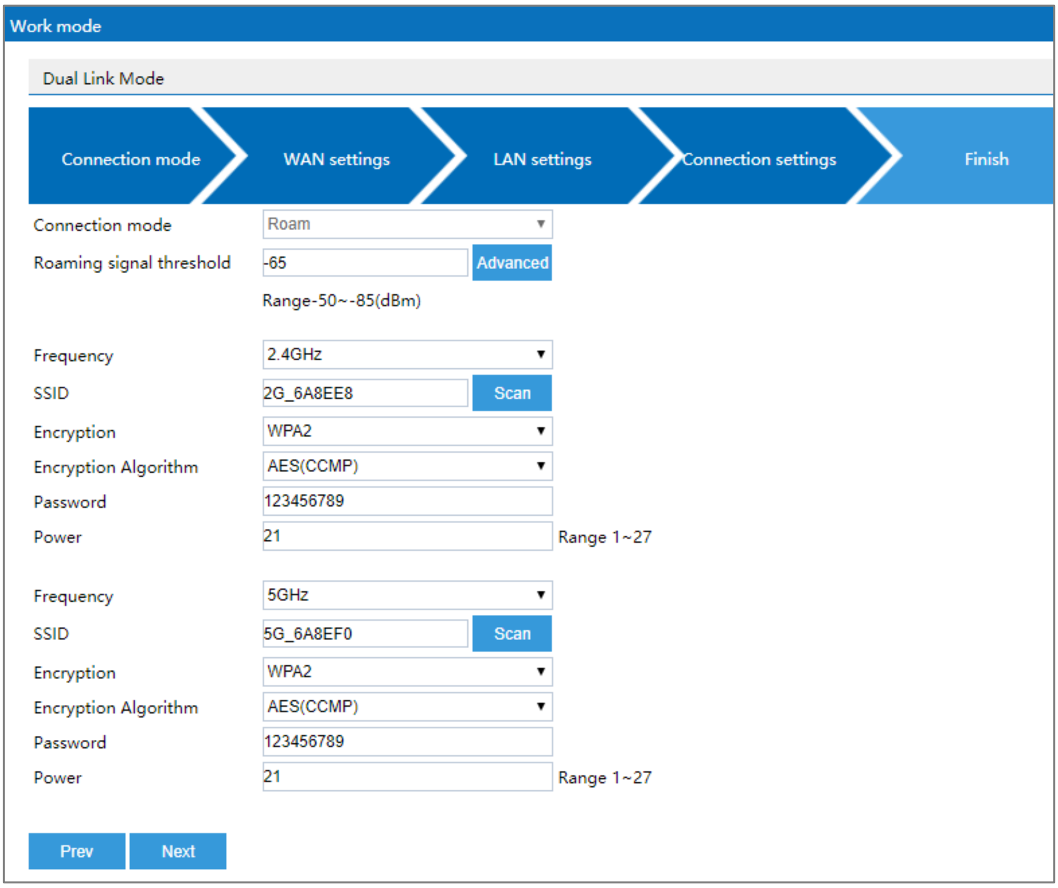
On the "Connection Settings" page of dual-link mode, user can configure the parameters of bridging superior wireless network.

Operation Path

Please open in order: “Mode Settings > Dual-link Mode".

Interface Description

The interface of dual-link connection setting is as follows:



Work mode

Dual Link Mode

Connection mode: Roam

Roaming signal threshold: -65 Advanced

Range-50~-85(dBm)

Frequency: 2.4GHz

SSID: 2G_6A8EE8 Scan

Encryption: WPA2

Encryption Algorithm: AES(CCMP)

Password: 123456789

Power: 21 Range 1~27

Frequency: 5GHz

SSID: 5G_6A8EF0 Scan

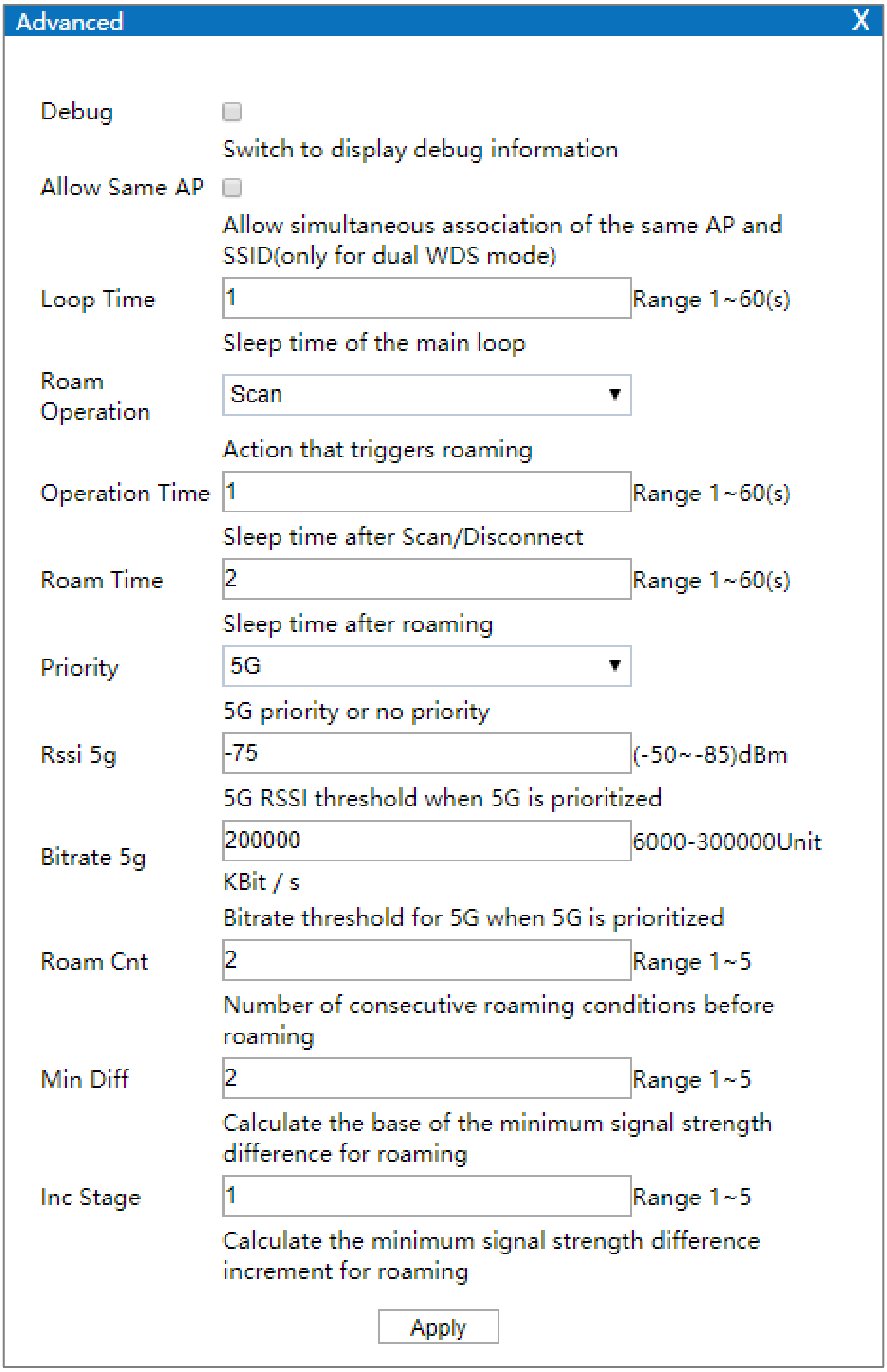
Encryption: WPA2

Encryption Algorithm: AES(CCMP)

Password: 123456789

Power: 21 Range 1~27

The settings interface of “Advanced” button is as follows:



Advanced X

Debug □
Switch to display debug information

Allow Same AP □
Allow simultaneous association of the same AP and SSID(only for dual WDS mode)

Loop Time: 1 Range 1~60(s)
Sleep time of the main loop

Roam Operation: Scan
Action that triggers roaming

Operation Time: 1 Range 1~60(s)
Sleep time after Scan/Disconnect

Roam Time: 2 Range 1~60(s)
Sleep time after roaming

Priority: 5G
5G priority or no priority

Rssi 5g: -75 (-50~-85)dBm
5G RSSI threshold when 5G is prioritized

Bitrate 5g: 200000 6000-300000Unit KBit / s
Bitrate threshold for 5G when 5G is prioritized

Roam Cnt: 2 Range 1~5
Number of consecutive roaming conditions before roaming

Min Diff: 2 Range 1~5
Calculate the base of the minimum signal strength difference for roaming

Inc Stage: 1 Range 1~5
Calculate the minimum signal strength difference increment for roaming

The main element configuration description of connection setting interface:

Interface Element	Description
Connection Mode	The default mode of connection between the device and the wireless device on the other side is roaming: seamless switching between wireless devices with two SSIDs that are not in use.
Roaming Signal	The roaming signal threshold of the backup frequency band for

Interface Element	Description
Threshold	scanning is -70 by default. When the roaming threshold of the backup band is lower than this value, it will scan.
Advanced	**Click the "Advanced" button to pop up the Advanced configuration bar**
Debug	Debug information switch, default is off: • I: Open, the system debugging information will be constantly printed in the log; • 0: Close, the system debugging information is not printed in the log;
Allow Same AP	The same SSID of the same AP is allowed to be associated at the same time, and it is only used in dual WDS mode.
Loop Time	The sleep time of the main loop of the dual-band seamless roaming is 1 second by default.
Roam Operation	The drop-down list of backup band roaming operation, the options are as follows: • Scan • Disconnect
Operation Time	The sleep time after Scan/Disconnect the backup frequency band is 2 seconds by default.
Roam Time	The sleep time after switching the primary and secondary frequency band is 2 seconds by default.
Priority	Priority setting, options: • 5G: 5G first; • None: no priority Note: • 2.4G+5G displays this item, and the default is 5G first. • Dual 2G or dual 5G does not display this item.
Rssi 5g	In the case of 5G priority, the signal strength threshold of 5G roaming. The default is -75. This parameter needs to be smaller than the roaming signal threshold. Note: Only 2.4G+5G displays this item, and it can be configured when 5G is preferred; Dual 2G or dual 5G does not display this item.
Bitrate 5g	In the case of 5G priority, the connection rate threshold of 5G roaming is 200000 by default. Note: Only 2.4G+5G displays this item, and it can be configured when 5G is preferred; Dual 2G or dual 5G does not display this item.
Roam Cnt	The default number of times that the roaming conditions are

Interface Element	Description
	satisfied continuously is 3 times, that is, the primary and standby switching will only be carried out if the roaming conditions are satisfied for 3 consecutive times in the backup frequency band.
Min Diff	The cardinality for calculating the minimum difference of roaming signal strength is 2 by default.
Inc Stage	Calculate the increment value of the minimum difference value of roaming signal strength, the default is 2.
RF 1 Configuration	**RF 1 Configuration Area**
Frequency	Scanning frequency band 1. Options are as follows: ● 2.4GHz ● 5GHz
SSID	SSID name of the opposite device wireless network 1. Note: User can add the wireless device for bridge via scan button.
Encryption	Encryption mode of the opposite device wireless network 1, options as follows: ● No encryption; ● WPA2: WiFi Protected Access II suits for the individual or average family network. It adopts pre-shared key mode and supports TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) encryption modes. ● WPA/WPA2: mixed mode of WPA and WPA2, it uses WPA or WPA2 encryption algorithm. ● WPA3: the third version of Wi-Fi protected access, with further security improvements over WPA2, longer encryption keys, and SAE authentication. ● WPA2/WPA3: mixed mode of WPA2 and WPA3, it uses WPA2 or WPA3 encryption algorithm. Note: WPA2/WPA3 only supports personal edition and doesn't support enterprise edition currently. Other encryption algorithms are supported by both of them.
Encryption Algorithm	Wireless network encryption algorithm of the opposite device, options as follows: ● AES (CCMP): advanced encryption standard; ● TKIP/AES: the key integrates 2113 protocol or advanced encryption standard temporarily. Note: When the encryption method is WPA2/WPA3 and WPA3, only AES

Interface Element	Description
	(CCMP) encryption algorithm is supported.
Password	Password of opposite device wireless network 1.
Power	Transmission power of device wireless signal 1. Note: • Greater the transmitted power, better the transmittability, longer the transmission range, but stronger the interference; • Different device may has different transmitted power range.
RF 2 Configuration	**RF 2 Configuration Area**
Frequency	Scanning frequency band 2. Options are as follows: • 2.4GHz • 5GHz
SSID	SSID name of the opposite device wireless network 2. Note: User can add the wireless device for bridge via scan button.
Encryption	Encryption mode of opposite device wireless network, options as follows: • No encryption; • WPA2: WiFi Protected Access II suits for the individual or average family network. It adopts pre-shared key mode and supports TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) encryption modes. • WPA/WPA2: mixed mode of WPA and WPA2, it uses WPA or WPA2 encryption algorithm. • WPA3: the third version of Wi-Fi protected access, with further security improvements over WPA2, longer encryption keys, and SAE authentication. • WPA2/WPA3: mixed mode of WPA2 and WPA3, it uses WPA2 or WPA3 encryption algorithm. Note: WPA2/WPA3 only supports personal edition and doesn't support enterprise edition currently. Other encryption algorithms are supported by both of them.
Encryption Algorithm	Wireless network encryption algorithm of the opposite device, options as follows: • AES (CCMP): advanced encryption standard; • TKIP/AES: the key integrates 2113 protocol or advanced encryption standard temporarily. Note: When the encryption method is WPA2/WPA3 and WPA3, only AES (CCMP) encryption algorithm is supported.

Interface Element	Description
Password	Password of the opposite device wireless network 2.
Power	Transmission power of device wireless signal 2. Note: • Greater the transmitted power, better the transmittability, longer the transmission range, but stronger the interference; • Different device may has different transmitted power range.

4 Status Center

In the status center, you can view system status, network status, wireless status, device statistics, ARP table and routing table.

4.1 System Status

Function Description

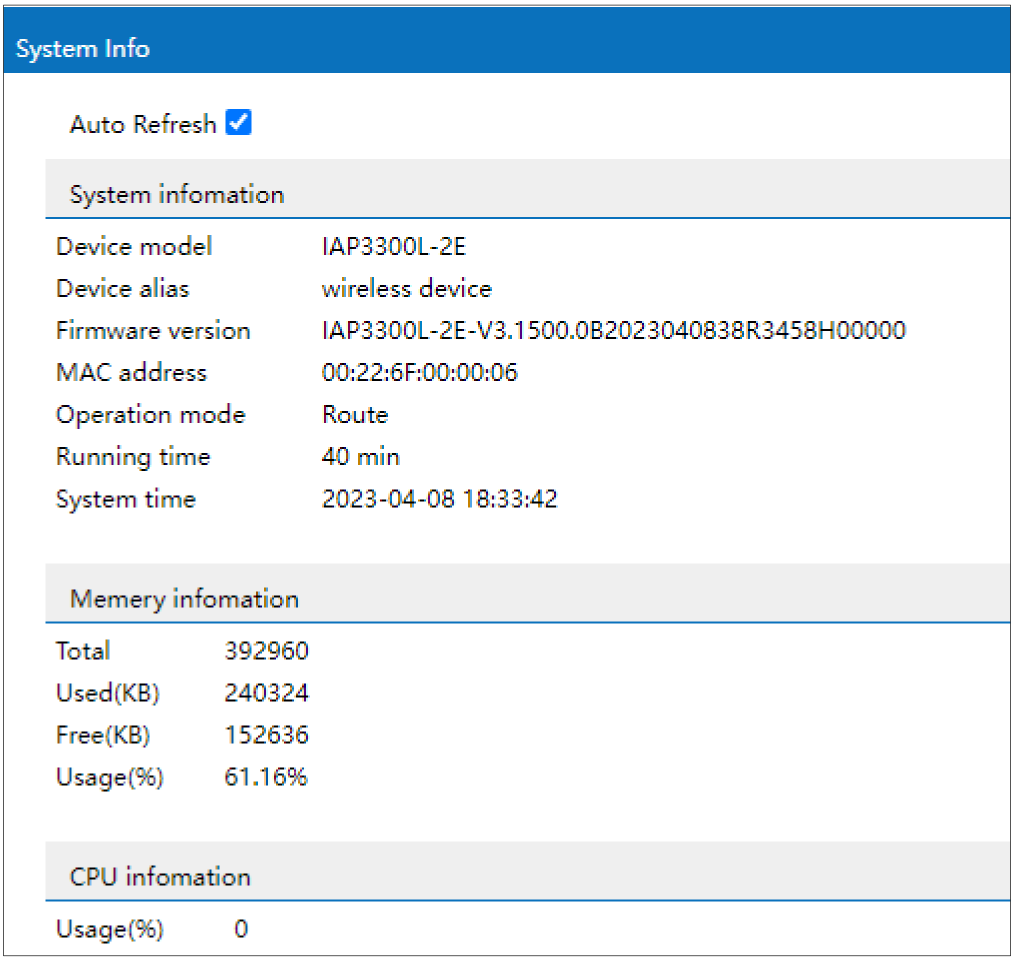
In the system status, you can view system information, memory information and CPU information.

Operation Path

Please open: Status Center > System Status.

Interface Description

System status interface as follows:



System Info

Auto Refresh ☑

System infomation

Device model	IAP3300L-2E
Device alias	wireless device
Firmware version	IAP3300L-2E-V3.1500.0B2023040838R3458H00000
MAC address	00:22:6F:00:00:06
Operation mode	Route
Running time	40 min
System time	2023-04-08 18:33:42

Memery infomation

Total	392960
Used(KB)	240324
Free(KB)	152636
Usage(%)	61.16%

CPU infomation

Usage(%)	0

4.2 Network Status

Function Description

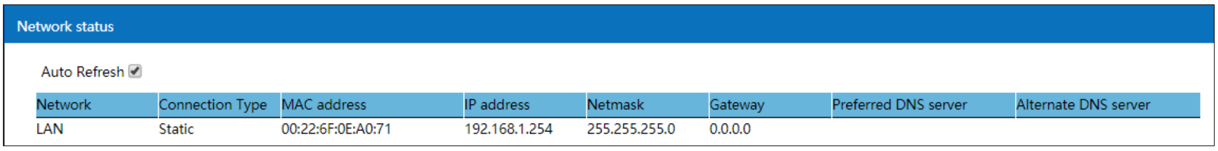
In the network status, you can view the wireless network parameters of the radio frequency of this device.

Operation Path

Please open: Status Center > Network Status.

Interface Description

The network status interface is as follows:



Network status

Auto Refresh ☑

Network	Connection Type	MAC address	IP address	Netmask	Gateway	Preferred DNS server	Alternate DNS server
LAN	Static	00:22:6F:0E:A0:71	192.168.1.254	255.255.255.0	0.0.0.0		

4.3 Device Statistics

Function Description

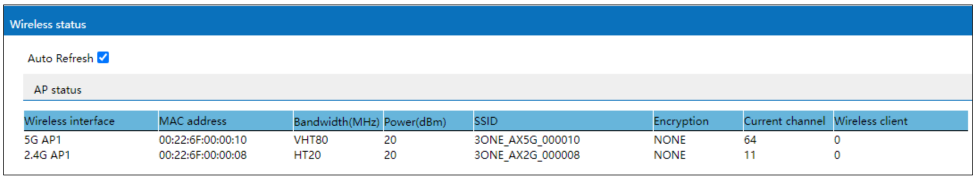
In device statistics, you can view the information statistics of data sent and received by this device.

Operation Path

Please open: Status Center > Device Statistics.

Interface Description

The device statistics interface is as follows:



Wireless status

Auto Refresh ☑

AP status

Wireless interface	MAC address	Bandwidth(MHz)	Power(dBm)	SSID	Encryption	Current channel	Wireless client
5G AP1	00:22:6F:00:00:10	VHT80	20	3ONE_AX5G_000010	NONE	64	0
2.4G AP1	00:22:6F:00:00:08	HT20	20	3ONE_AX2G_000008	NONE	11	0

4.4 ARP Table

Function Description

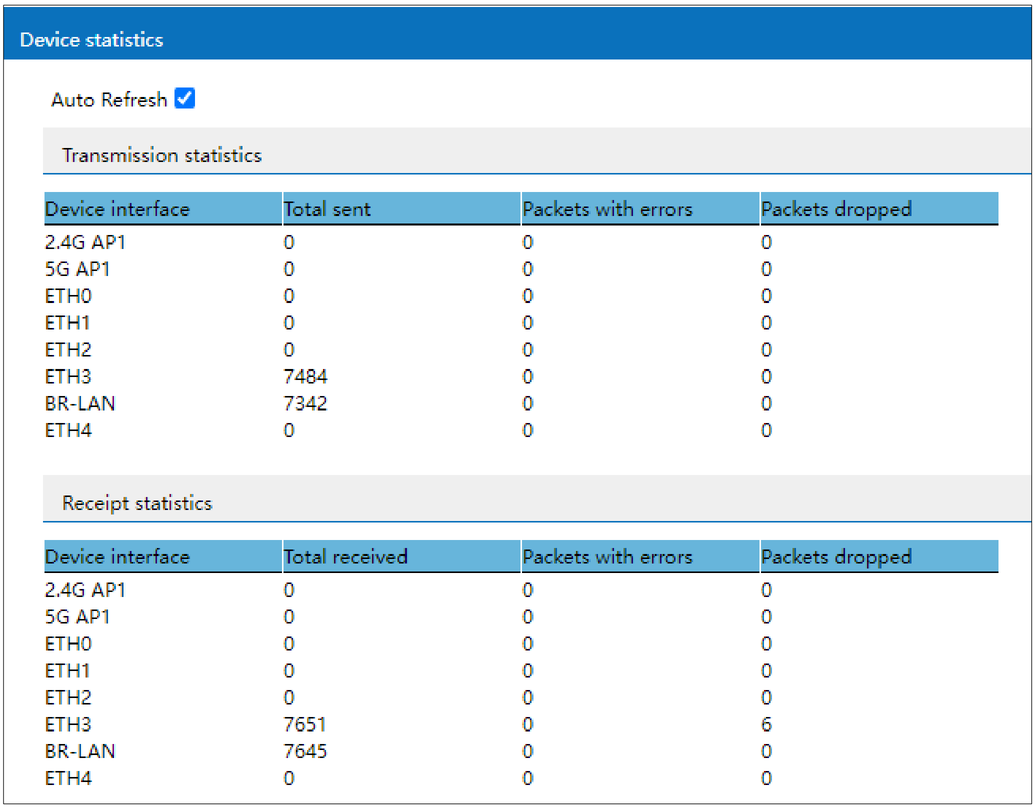
In ARP table, you can view the IP address and MAC information detected in the same LAN.

Operation Path

Please open: Status Center > ARP Table.

Interface Description

ARP table interface is as follows:



Device statistics

Auto Refresh ☑

Transmission statistics

Device interface	Total sent	Packets with errors	Packets dropped
2.4G AP1	0	0	0
5G AP1	0	0	0
ETH0	0	0	0
ETH1	0	0	0
ETH2	0	0	0
ETH3	7484	0	0
BR-LAN	7342	0	0
ETH4	0	0	0

Receipt statistics

Device interface	Total received	Packets with errors	Packets dropped
2.4G AP1	0	0	0
5G AP1	0	0	0
ETH0	0	0	0
ETH1	0	0	0
ETH2	0	0	0
ETH3	7651	0	6
BR-LAN	7645	0	0
ETH4	0	0	0

4.5 Device Statistics

Function Description

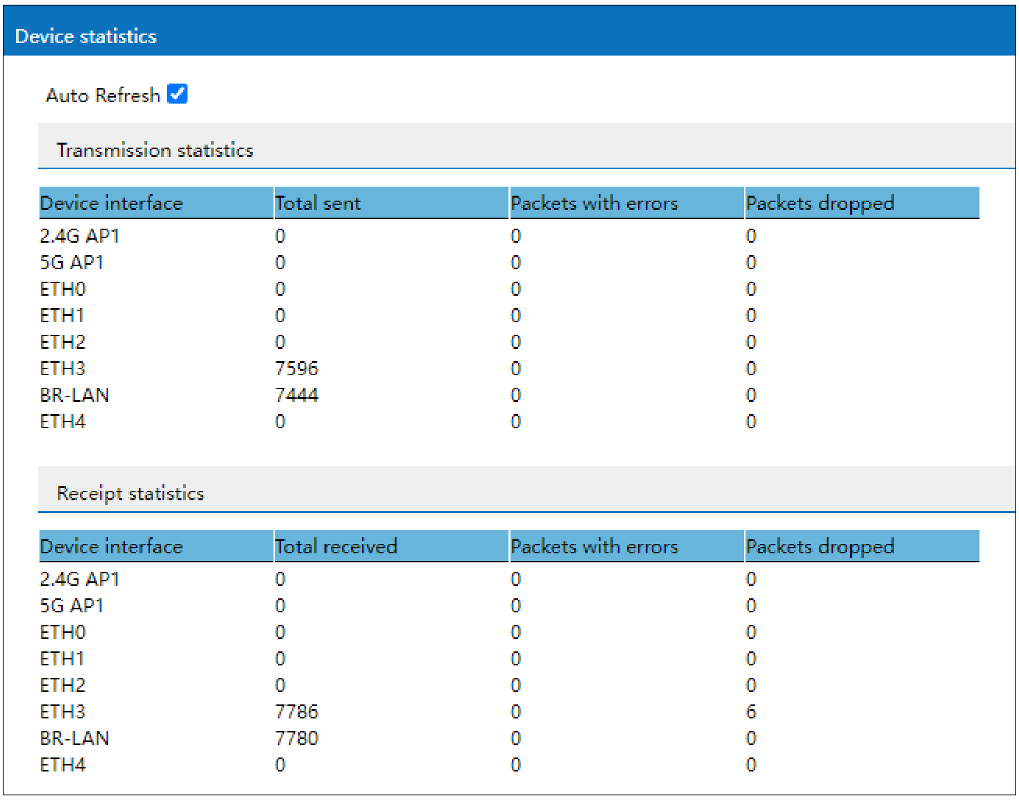
In device statistics, you can view the information statistics of data sent and received by this device.

Operation Path

Please open: Status Center > Device Statistics.

Interface Description

The device statistics interface is as follows:



Device statistics

Auto Refresh ☑

Transmission statistics

Device interface	Total sent	Packets with errors	Packets dropped
2.4G AP1	0	0	0
5G AP1	0	0	0
ETH0	0	0	0
ETH1	0	0	0
ETH2	0	0	0
ETH3	7596	0	0
BR-LAN	7444	0	0
ETH4	0	0	0

Receipt statistics

Device interface	Total received	Packets with errors	Packets dropped
2.4G AP1	0	0	0
5G AP1	0	0	0
ETH0	0	0	0
ETH1	0	0	0
ETH2	0	0	0
ETH3	7786	0	6
BR-LAN	7780	0	0
ETH4	0	0	0

4.6 Route Table

Function Description

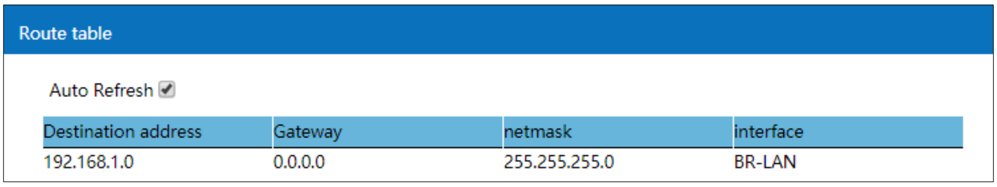
In the route table, you can view the destination address and interface of data forwarding.

Operation Path

Please open: Status Center > Route Table.

Interface Description

The route table interface is as follows:



Route table

Auto Refresh ☑

Destination address	Gateway	netmask	interface
192.168.1.0	0.0.0.0	255.255.255.0	BR-LAN

5 Network Setting

5.1 LAN Settings

Intranet settings are slightly different in different modes and different connection modes, which are introduced separately below.

- LAN settings 1
  - Route;
  - Universal bridging in bridge/client mode;
  - Wireless NAT of Client Mode.
- LAN Settings 2

  Intranet settings in other modes.

5.1.1 LAN Settings 1

Function Description

Under the universal bridge of route mode, bridge/client mode, and under the wireless NAT of client mode, the static intranet IP address and DHCP server parameters can be set on the "Intranet Settings" page of network settings, here:

- In routing mode, the DHCP server function is enabled by default.
- In the bridge/client mode, when the connection mode is universal bridge, the DHCP server function is disabled by default.
- In the client mode, when the connection mode is wireless NAT, the DHCP server function is enabled by default.

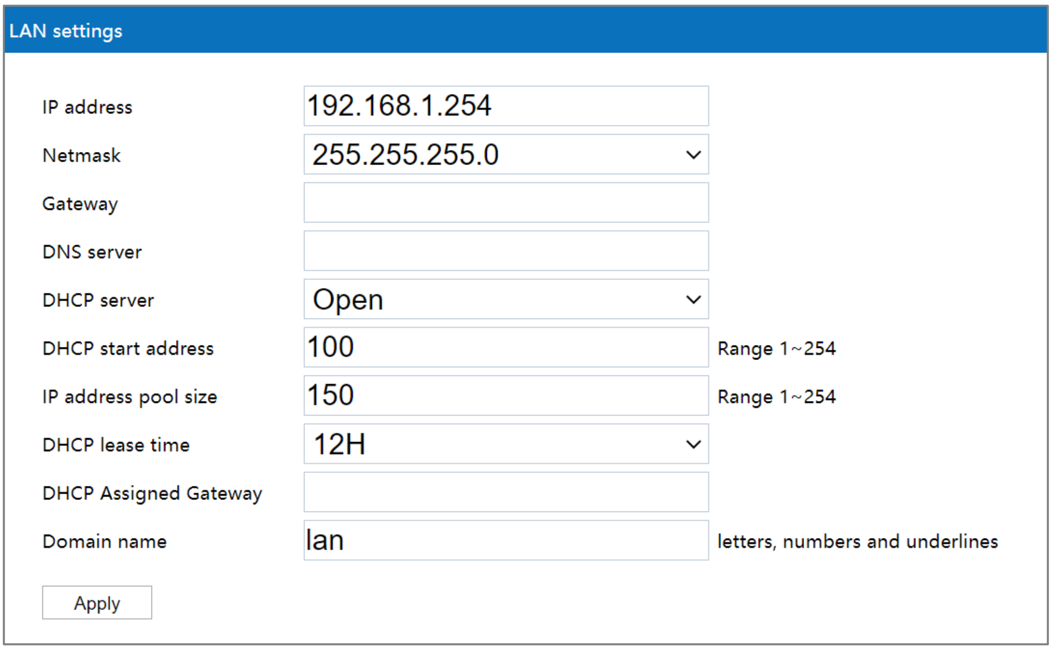
DHCP (Dynamic Host Configuration Protocol) is a LAN protocol which uses UDP protocol to allocate IP address to internal network automatically and improve IP address utilization. Client in network environment can acquire dynamic IP address, Gateway address, DNS server address and other information from DHCP server.

Operation Path

Please open in order: "Network Settings > LAN Settings".

Interface Description

LAN settings interface as follows:



LAN settings

IP address	192.168.1.254	
Netmask	255.255.255.0	
Gateway		
DNS server		
DHCP server	Open	
DHCP start address	100	Range 1~254
IP address pool size	150	Range 1~254
DHCP lease time	12H	
DHCP Assigned Gateway		
Domain name	lan	letters, numbers and underlines

The main element configuration description of LAN settings interface:

Interface Element	Description
IP Address	IP address of the device LAN port.
Netmask	Drop-down list of netmask.
Gateway	Default gateway address of LAN.
DNS server	DNS server address.
DHCP Server	The drop-down list of DHCP server. The options are as follows: • Disable; • Enable.
DHCP start address	The minimum IP address host number allocated by DHCP address pool. Value range is 1-254.
IP address pool size	The maximum IP address number allocated by DHCP address pool. Value range is 1-254.
DHCP lease time	Valid time of IP address distributed by DHCP address pool, it defaults to 12 hours. Drop-down list of time unit, options as follows: • 30m; • 1 hour;

Interface Element	Description
	- 6h; - 12h; - 1 day; - 3 days; - 7 days.
DHCP assigned gateway	DHCP assigns gateway IP address.
Domain name	DHCP domain name is composed of letter, number and underline; it supports 0-32 valid characters.

5.1.2 LAN Settings 2

Function Description

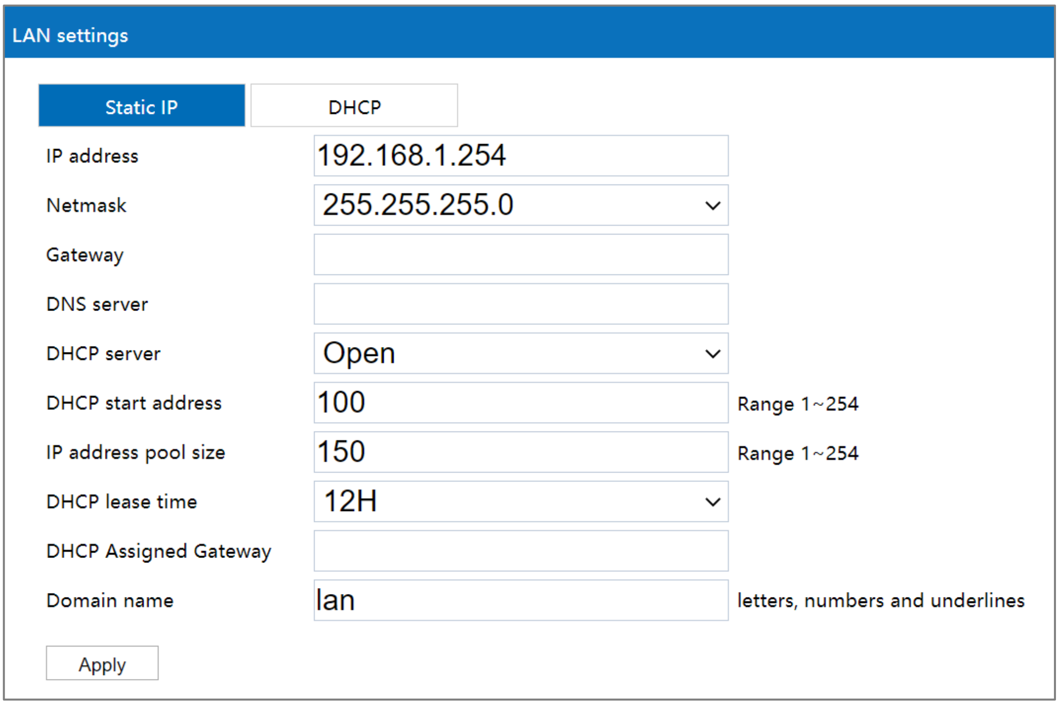
On the “Intranet Settings” page of other modes, static IP and dynamic access are supported in setting intranet IP. The DHCP server is disabled by default.

Operation Path

Please open in order: "Network Settings > LAN Settings".

Interface description 1: Static IP

Static IP interface as follows:



LAN settings

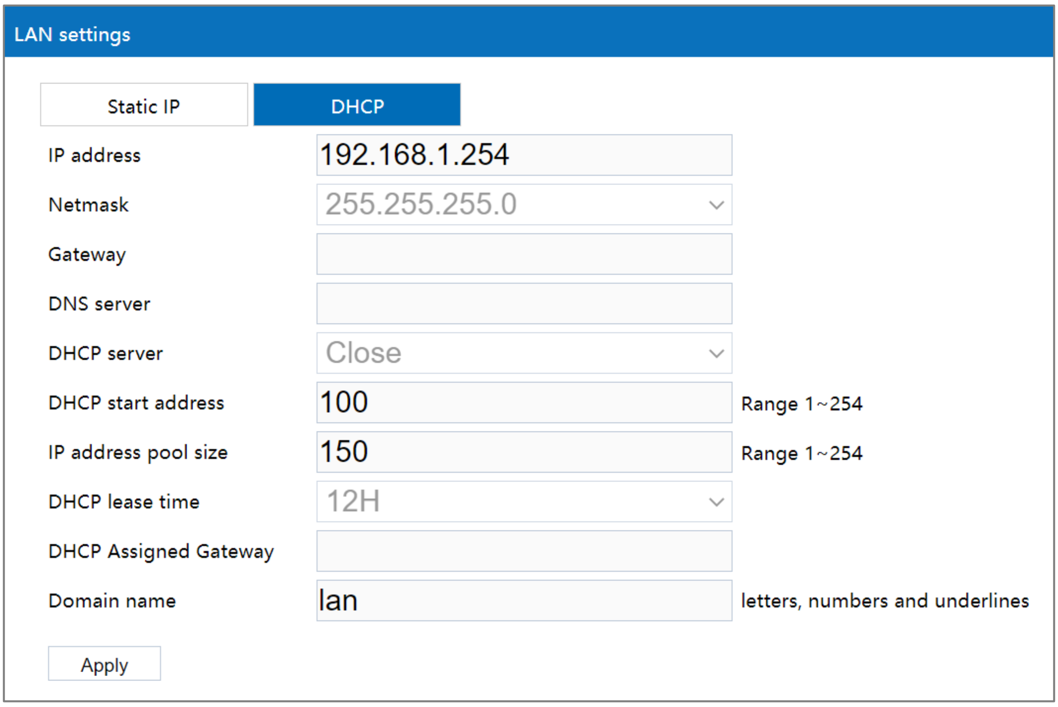
IP address	192.168.1.254	
Netmask	255.255.255.0	
Gateway		
DNS server		
DHCP server	Open	
DHCP start address	100	Range 1~254
IP address pool size	150	Range 1~254
DHCP lease time	12H	
DHCP Assigned Gateway		
Domain name	lan	letters, numbers and underlines

The main element configuration description of static IP interface:

Interface Element	Description
IP Address	IP address of the device LAN port.
Netmask	Drop-down list of netmask.
Gateway	Default gateway address of LAN.
DNS server	DNS server address.
DHCP Server	The drop-down list of DHCP server. The options are as follows: ● Disable; ● Enable.
DHCP start address	The minimum IP address host number allocated by DHCP address pool. Value range is 1-255.
IP address pool size	The maximum IP address number allocated by DHCP address pool. Value range is 1-255.
DHCP lease time	Valid time of IP address distributed by DHCP address pool, it defaults to 12 hours. Drop-down list of time unit, options as follows: ● 30m; ● 1 hour; ● 6h; ● 12h; ● 1 day; ● 3 days; ● 7 days.
DHCP assigned gateway	DHCP assigns gateway IP address
Domain name	DHCP domain name is composed of letter, number and underline; it supports 0-32 valid characters.

Interface Description 2: DHCP

DHCP interface as follows:



IP address: 192.168.1.254

Netmask: 255.255.255.0

Gateway:

DNS server:

DHCP server: Close

DHCP start address: 100 Range 1~254

IP address pool size: 150 Range 1~254

DHCP lease time: 12H

DHCP Assigned Gateway:

Domain name: lan letters, numbers and underlines

Main elements configuration description of DHCP interface:

Interface Element	Description
IP Address	The IP address of the device LAN port would be automatically acquired.
Netmask	Drop-down list of netmask.
Gateway	Default gateway address of LAN.
DNS server	DNS server address.
DHCP Server	• The drop-down list of DHCP server. The options are as follows: • Disable; • Enable.
DHCP start address	The minimum IP address host number allocated by DHCP address pool. Value range is 1-255.
IP address pool size	The maximum IP address number allocated by DHCP address pool. Value range is 1-255.
DHCP lease time	Valid time of IP address distributed by DHCP address pool, it defaults to 12 hours. Drop-down list of time unit, options as follows: • 30m; • 1 hour; • 6h; • 12h; • 1 day;

Interface Element	Description
	• 3 days; • 7 days.
DHCP assigned gateway	DHCP assigns gateway IP address.
Domain name	DHCP domain name is composed of letter, number and underline; it supports 0-32 valid characters.

5.2 WAN Settings

Function Description

On the "WAN settings" page of network, user can configure three connection modes between WAN port and WAN:

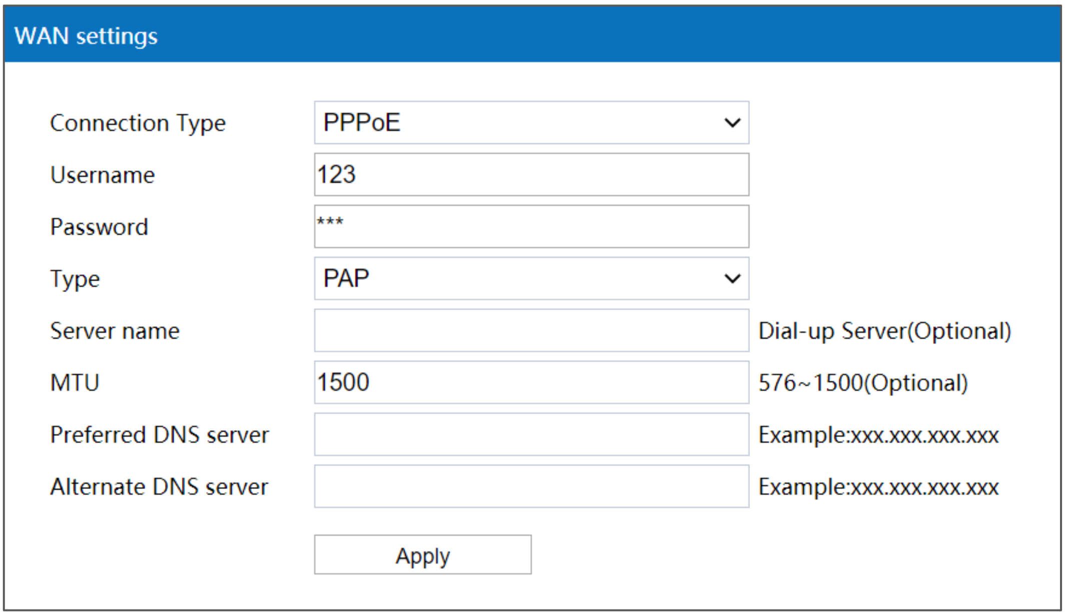
- PPPoE;
- Static IP;
- DHCP.

Operation Path

Please open in order: "Network > WAN settings".

Interface Description 1: PPPoE

PPPoE interface as follows:


WAN settings

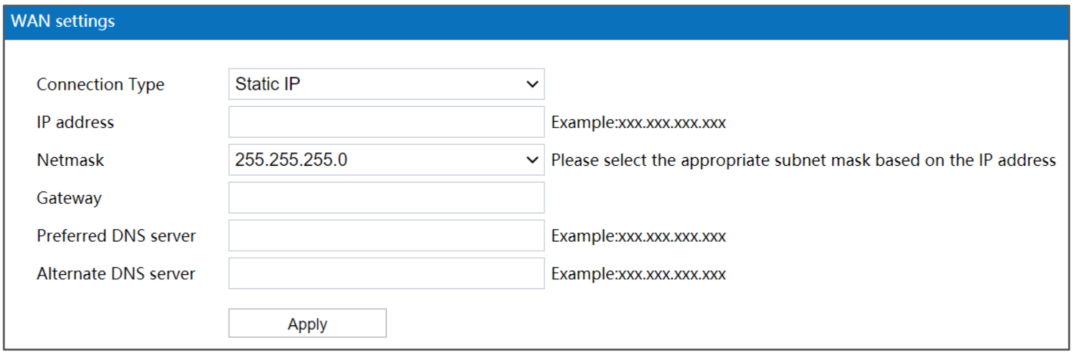
Connection Type	PPPoE	
Username	123	
Password	***	
Type	PAP	
Server name		Dial-up Server(Optional)
MTU	1500	576~1500(Optional)
Preferred DNS server		Example:xxx.xxx.xxx.xxx
Alternate DNS server		Example:xxx.xxx.xxx.xxx

The main element configuration description of PPPoE interface:

Interface Element	Description
PPPoE	PPPoE tab, it supports PPPoE to achieve Internet access.
Username	User name of PPPoE connection. Note: User name, password and service name are provided by network provider.
Password	Password of PPPoE connection. Note: User name, password and service name are provided by network provider.
Type	The type of PPPoE dialing: ● PAP: Password Authentication Protocol, which sends user name or password over the network; ● CHAP: Challenge Handshake Authentication Protocol, it only transmits user name; ● PAP/CHAP: uses Password Authentication Protocol or Challenge Handshake Authentication Protocol.
Server name	Dial-up server name, not fill if network provider doesn't supply. Note: User name, password and service name are provided by network provider.
MTU	The maximum length of a single message that can get through in PPPoE protocol dialing, with a value range of 576-1500 bytes. Note: • MTU (Maximum Transmission Unit), the device will divide the data packet into multiple small packets if the maximum length of single message exceeds the given MTU value; so reasonable setting can optimize network speed; • MTU value is recommended to be same to the one of superior router.
Preferred DNS server	Address of primary DNS server.
Alternate DNS server	Address of backup DNS server. Note: ● The priority level of primary DNS server address is higher than the one of backup DNS server address; ● The priority level of manually setting DNS server address is higher than the one of automatically acquired DNS server address.

Interface Description 2: Static IP

Static IP interface as follows:



WAN settings

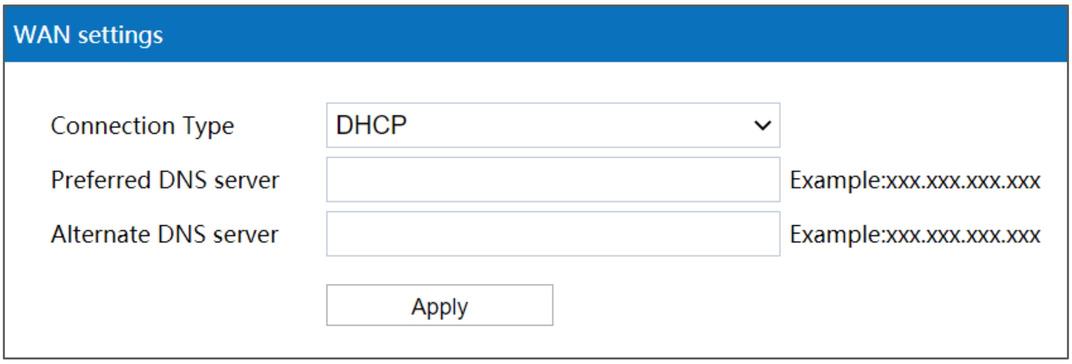
Connection Type	Static IP	
IP address		Example:xxx.xxx.xxx.xxx
Netmask	255.255.255.0	Please select the appropriate subnet mask based on the IP address
Gateway		
Preferred DNS server		Example:xxx.xxx.xxx.xxx
Alternate DNS server		Example:xxx.xxx.xxx.xxx

The main element configuration description of static IP interface:

Interface Element	Description
Connection type	Static IP tab, network information configuration of device WAN.
IP Address	The fixed IP address provided by network provider or extranet.
Netmask	Drop-down list of netmask.
Gateway	The default gateway address provided by network provider or extranet.
Preferred DNS server	Address of primary DNS server.
Alternate DNS server	Backup DNS server address, DNS server address offered by network provider or WAN. Note: ● The priority level of primary DNS server address is higher than the one of backup DNS server address; ● The priority level of manually setting DNS server address is higher than the one of automatically acquired DNS server address.

Interface Description 3: DHCP

DHCP interface as follows:



WAN settings

Connection Type	DHCP	
Preferred DNS server		Example:xxx.xxx.xxx.xxx
Alternate DNS server		Example:xxx.xxx.xxx.xxx

Main elements configuration description of DHCP interface:

Interface Element	Description
Connection type	In the dynamic acquisition tab, the WAN network information of the device is automatically obtained. Note: The device automatically acquires the network address information distributed by network provider or WAN.
Preferred DNS server	Address of primary DNS server.
Alternate DNS server	Address of backup DNS server. Note: ● The priority level of primary DNS server address is higher than the one of backup DNS server address; ● The priority level of manually setting DNS server address is higher than the one of automatically acquired DNS server address.

5.3 Wireless Settings-AP

Notes

The wireless setting page is different in different working modes:

- Routing, AP mode, factory default mode: only the "Wireless Settings -AP" page is displayed.
- Bridge Mode: The “Wireless Settings-AP” page and the “Wireless Settings-Client” page are displayed.
- Client mode: only the “Wireless Settings-Client” page is displayed.

5.3.1 RF 1 Configuration

Function Description

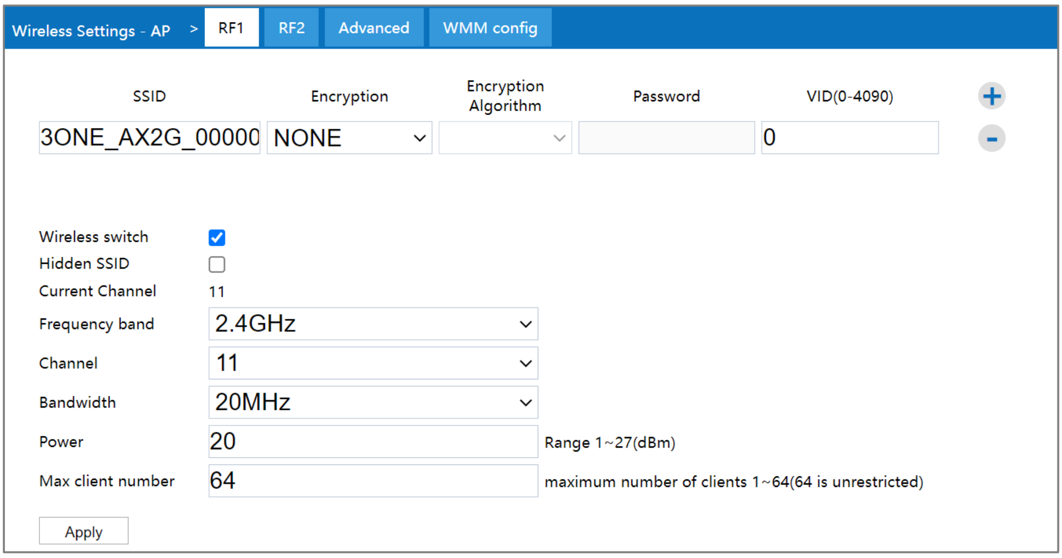
On the "RF 1 Configuration" page of wireless settings, user can configure relative parameters of RF 1 wireless network, such as wireless switch, hidden SSID, new SSID, channel, bandwidth, max client number and other wireless configuration.

Operation Path

Please open in order: "Network > Wireless Settings-AP > RF1".

Interface Description

The RF 1 configuration interface as follows:



Wireless Settings - AP > RF1 | RF2 | Advanced | WMM config

SSID	Encryption	Encryption Algorithm	Password	VID(0-4090)
3ONE_AX2G_00000	NONE			0

Wireless switch ☑

Hidden SSID □

Current Channel 11

Frequency band 2.4GHz

Channel 11

Bandwidth 20MHz

Power 20 Range 1~27(dBm)

Max client number 64 maximum number of clients 1~64(64 is unrestricted)

Apply

The main element configuration description of RF1 configuration interface:

Interface Element	Description
SSID	SSID name of wireless network, it supports 1-32 characters.
Encryption	Encryption mode of wireless network, options as follows: ● NONE; ● WPA2: WiFi Protected Access II suits for the individual or average family network. It adopts pre-shared key mode and supports TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) encryption modes. ● WPA/WPA2: mixed mode of WPA and WPA2, it uses WPA or WPA2 encryption algorithm. ● WPA3: the third version of Wi-Fi protected access, with further security improvements over WPA2, longer encryption keys, and SAE authentication. ● WPA2/WPA3: mixed mode of WPA2 and WPA3, it uses WPA2 or WPA3 encryption algorithm. Note: WPA2/WPA3 only supports personal edition and doesn't support enterprise edition currently. Other encryption algorithms are supported by both of them.
Encryption algorithm	Encryption algorithm of wireless network, options as follows: ● AES (CCMP): advanced encryption standard; ● TKIP/AES: the key integrates 2113 protocol or advanced encryption standard temporarily. Note: When the encryption method is WPA2/WPA3 and WPA3, only AES (CCMP) encryption algorithm is supported.
Password	Password of wireless network, it supports 8-63 valid characters.
VID	Wireless network VLAN ID.

Interface Element	Description
	Note: VID configuration is supported only in AP mode and bridge mode using WDS bridging.
Wireless switch	Wireless Network function enable checkbox, check to enable wireless network function.
Hidden SSID	Hidden SSID function enable checkbox, check to enable hidden SSID function. SSID name of the device wireless signal will be hidden and displayed as unnamed network. Please enter the SSID name of wireless signal manually while connecting hidden wireless signal.
Current channel	The working channel of current wireless network.
Frequency band	The wireless frequency band corresponding to the current wireless setting, the options are as follows: • 2.4GHz
Channel	Working channel of 2.4G wireless network, options as follows: • Auto: channel self-adaptation; • 1: main frequency band 2412Hz, frequency range 2401~2423Hz; • 2: main frequency band 2417Hz, frequency range 2406~2428Hz; • 3: main frequency band 2422Hz, frequency range 2411~2433Hz; • 4: main frequency band 2427Hz, frequency range 2416~2438Hz; • 5: main frequency band 2432Hz, frequency range 2421~2443Hz; • 6: main frequency band 2437Hz, frequency range 2426~2448Hz; • 7: main frequency band 2442Hz, frequency range 2431~2453Hz; • 8: main frequency band 2447Hz, frequency range 2436~2458Hz; • 9: main frequency band 2452Hz, frequency range 2441~2463Hz; • 10: main frequency band 2457Hz, frequency range 2446~2468Hz; • 11: main frequency band 2462Hz, frequency range 2451~2473Hz; • 12: main frequency band 2467Hz, frequency range 2456~2478Hz, this frequency band is not open in

Interface Element	Description
	America, so it's temporarily unavailable; - 13: main frequency band 2472Hz, frequency range 2461~2483Hz, this frequency band is not open in America, so it's temporarily unavailable; Note: - In order to improve the network performance, please choose unused channel in the device working environment. - Different frequency bands and countries support different channel options.
Bandwidth	Channel bandwidth of wireless network, it defaults to 20MHz, options as follows: - 20MHz; - 40MHz. Note: 40MHz bandwidth binds two 20MHz bandwidth channels together to gain the throughput capacity more than twice of the 20MHz bandwidth.
Power	Transmission power of device wireless signal. Note: - Greater the transmitted power, better the transmittability, longer the transmission range, but stronger the interference; - Different device may has different transmitted power range.
Max client number	Maximum client number of the device wireless signal, value range 1-64, when the value is 64, it represents the unlimited connected clients number.

5.3.2 RF 2 Configuration

Function Description

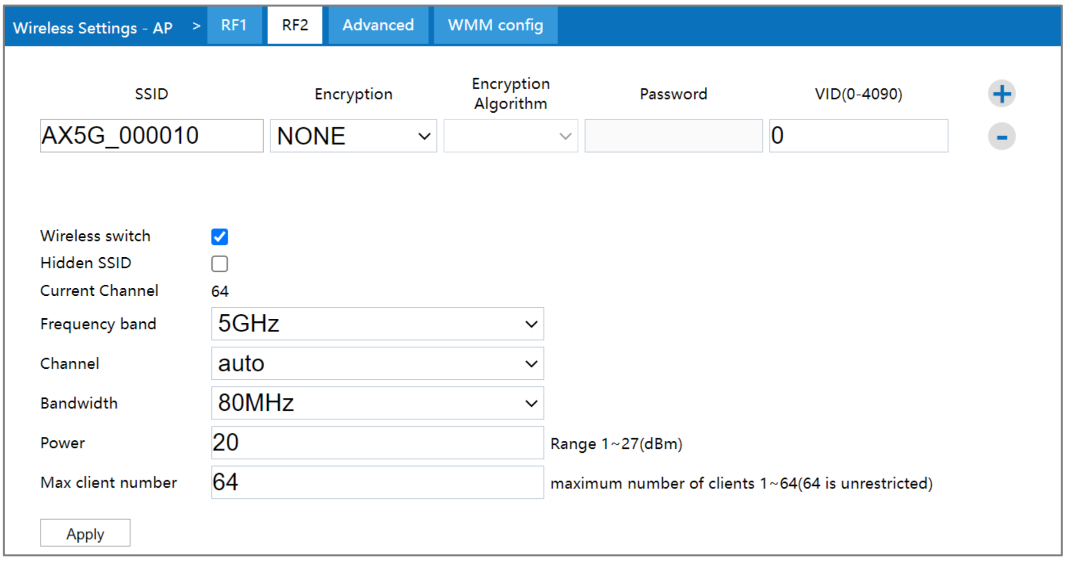
On the "RF 2 Configuration" page of wireless settings, user can configure relative parameters of RF 2 wireless network, such as wireless switch, hidden SSID, new SSID, channel, bandwidth, max client number and other wireless configuration.

Operation Path

Please open in order: "Network > Wireless Settings-AP > RF2".

Interface Description

The RF 2 configuration interface as follows:



SSID	Encryption	Encryption Algorithm	Password	VID(0-4090)
AX5G_000010	NONE			0

Wireless switch ☑
Hidden SSID □
Current Channel 64
Frequency band 5GHz
Channel auto
Bandwidth 80MHz
Power 20 Range 1~27(dBm)
Max client number 64 maximum number of clients 1~64(64 is unrestricted)

The main element configuration description of RF 2 configuration interface:

Interface Element	Description
SSID	SSID name of wireless network, it supports 1-32 characters.
Encryption	Encryption mode of wireless network, options as follows: • NONE; • WPA2: WiFi Protected Access II suits for the individual or average family network. It adopts pre-shared key mode and supports TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) encryption modes. • WPA/WPA2: mixed mode of WPA and WPA2, it uses WPA or WPA2 encryption algorithm. • WPA3: the third version of Wi-Fi protected access, with further security improvements over WPA2, longer encryption keys, and SAE authentication. • WPA2/WPA3: mixed mode of WPA2 and WPA3, it uses WPA2 or WPA3 encryption algorithm. Note: WPA2/WPA3 only supports personal edition and doesn't support enterprise edition currently. Other encryption algorithms are supported by both of them.
Encryption algorithm	Encryption algorithm of wireless network, options as follows: • AES (CCMP): advanced encryption standard; • TKIP/AES: the key integrates 2113 protocol or advanced encryption standard temporarily. Note: When the encryption method is WPA2/WPA3 and WPA3, only AES (CCMP) encryption algorithm is supported.
Password	Password of wireless network, it supports 8-63 valid characters.

Interface Element	Description
VID	Wireless network VLAN ID. Note: VID configuration is supported only in AP mode.
Wireless switch	Wireless Network function enable checkbox, check to enable wireless network function.
Hidden SSID	Hidden SSID function enable checkbox, check to enable hidden SSID function. SSID name of the device wireless signal will be hidden and displayed as unnamed network. Please enter the SSID name of wireless signal manually while connecting hidden wireless signal.
Current channel	The working channel of current wireless network.
Frequency band	The wireless frequency band corresponding to the current wireless setting, the options are as follows: ● 5GHz
Channel	Working channel of 5G wireless network, options as follows: ● Auto: channel self-adaptation; ● 36: main frequency band 5180Hz, frequency range 5170~5190Hz; ● 40: main frequency band 5200Hz， frequency range 5190~5210Hz； ● 44: main frequency band 5220Hz, frequency range 5210~5230Hz; ● 48: main frequency band 5230Hz, frequency range 5210~5250Hz; ● 52: main frequency band 5260Hz, frequency range 5250~5270Hz; ● 56: main frequency band 5280Hz, frequency range 5270~5290Hz; ● 60: main frequency band 5300Hz, frequency range 5290~5310Hz; ● 64: main frequency band 5320Hz, frequency range 5310~5330Hz; ● 100: main frequency band 5500Hz, frequency range 5490~5510Hz, this frequency band is not open in China, so it's temporarily unavailable; ● 104: main frequency band 5520Hz, frequency range 5510~5530Hz, this frequency band is not open in China, so it's temporarily unavailable; ● 108: main frequency band 5540Hz, frequency range 5530~5550Hz, this frequency band is not open in China,

Interface Element	Description
	so it's temporarily unavailable; ● 112: main frequency band 5560Hz, frequency range 5550~5570Hz, this frequency band is not open in China, so it's temporarily unavailable; ● 116: main frequency band 5580Hz, frequency range 5570~5590Hz, this frequency band is not open in China, so it's temporarily unavailable; ● 120: main frequency band 5600Hz, frequency range 5590~5610Hz, this frequency band is not open in China, so it's temporarily unavailable; ● 124: main frequency band 5620Hz, frequency range 5610~5630Hz, this frequency band is not open in China, so it's temporarily unavailable; ● 128: main frequency band 5640Hz, frequency range 5630~5650Hz, this frequency band is not open in China, so it's temporarily unavailable; ● 132: main frequency band 5660Hz, frequency range 5650~5670Hz, this frequency band is not open in China, so it's temporarily unavailable; ● 136: main frequency band 5680Hz, frequency range 5670~5690Hz, this frequency band is not open in China, so it's temporarily unavailable; ● 140: main frequency band 5700Hz, frequency range 5690~5710Hz, this frequency band is not open in China, so it's temporarily unavailable; ● 144: main frequency band 5720Hz, frequency range 5710~5730Hz, this frequency band is not open in China, so it's temporarily unavailable; ● 149: main frequency band 5745Hz, frequency range 5735~5755Hz; ● 153: main frequency band 5765Hz, frequency range 5755~5775Hz; ● 157: main frequency band 5785Hz, frequency range 5775~5795Hz; ● 161: main frequency band 5805Hz, frequency range 5795~5815Hz; ● 165: main frequency band 5825Hz, frequency range 5815~5835Hz. Note: ● In order to improve the network performance, please choose unused channel in the device working environment.

Interface Element	Description
	- Different frequency bands and countries support different channel options.
Bandwidth	Channel bandwidth of wireless network, it defaults to 80MHz, options as follows: - 20MHz; - 40MHz; - 80MHz.
Power	Transmission power of device wireless signal. Note: - Greater the transmitted power, better the transmittability, longer the transmission range, but stronger the interference; - Different device may has different transmitted power range.
Max client number	Maximum client number of the device wireless signal, value range 1-64, when the value is 64, it represents the unlimited connected clients number.

5.3.3 Advanced Configuration

Function Description

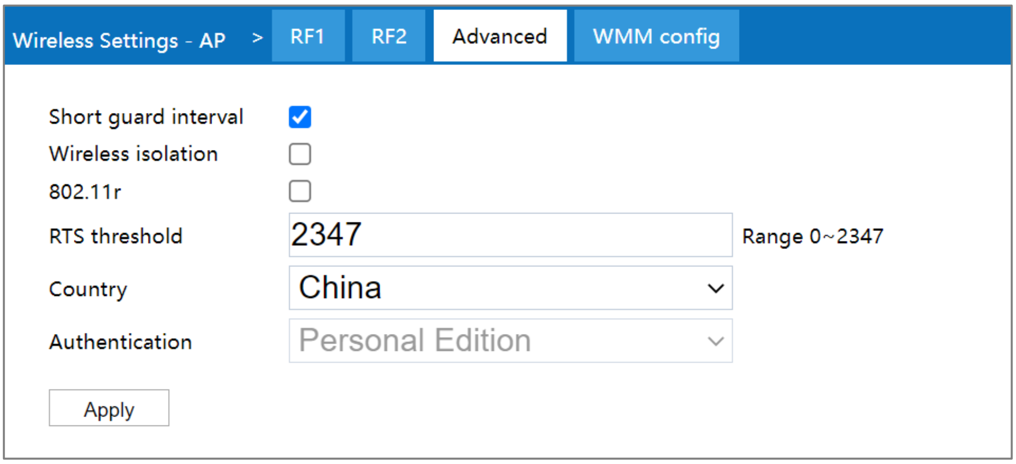
On the "Advanced" page of wireless settings, user can enable short GI, wireless isolate, RTS and other functions.

Operation Path

Please open in order: "Network > Wireless settings-AP > Advanced".

Interface Description

The advanced configuration interface as follows:



Short guard interval ☑

Wireless isolation □

802.11r □

RTS threshold 2347 Range 0~2347

Country China

Authentication Personal Edition

The main element configuration description of advanced interface:

Interface Element	Description
Short Guard Interval	Short GI (Short Guard Interval) checkbox: ● Check: enabling the function can reduce the gap between two data packets to 400ns, and improve the data transmission speed. ● Uncheck: after disabling the function, the transmission interval of data packet defaults to 800ns. Note: Under high signal strength and low latency, this function can be enabled to improve nearly 10% handling capacity.
WDS	WDS (Wireless Distribution System), this function is used for bridging multiple WLAN. Note: Please enable WDS function while bridging the device with other wireless devices.
Wireless isolatation	Wireless user isolation, it's used for isolating the wireless clients connected to the device wireless network with same SSID, defaults to disabled. Note: After enabling the wireless isolation function, two wireless clients connected to the same SSID can't mutually access, and this function can further enhance the wireless network security.
80211r	802.11r check box, check it to enable the fast roaming function. Note: 802.11r configuration is supported only in AP mode.
RTS threshold	Data packet RTS (Request to Send) threshold, value range 0-2347, defaults to 2347. ● RTS threshold = 0: it needs to detect whether there exists collision only if the data packet is sent out; AP will send RTS signal; ● 0 < RTS threshold < 2347: when the length of data packet surpasses RTS threshold, the device wireless terminal will send RTS signal to avoid signal conflict; ● RTS threshold = 2347: the device wireless terminal won't send RTS signal. Note: ● As for the wireless nodes in different wireless detection range of AP range, collision will occur when the nodes send out signals; RTS function can avoid the collision. ● The device will send RTS to destination station for negotiation when the length of data packet surpasses RTS threshold. After receiving RTS frame, the wireless station will send a CTS (Clear

Interface Element	Description
	to Send) frame to the device, which represents the two can conduct wireless communication.
Country	Applied countries and regions. Options are as follows: ● China ● USA Note: Different country opens different channels.
Authentication	Authentication mode of wireless network, options as follows: ● Personal edition: wireless network WPA/WPA2/WPA3 uses WPA/WPA2-PSK/ WPA3-SAE encryption method and pre-shared key. Personal edition is suitable for personal and home users; ● Enterprise edition: wireless network WPA/WPA2/WPA3 uses WPA-802.1X/WPA2-802.1X/WPA3-802.1X encryption method. It is necessary to install Radius server to authenticate, and suitable for enterprise users with high security requirements. Note: Authentication mode can be configured after the wireless network is encrypted, WAP2/WAP3 encryption mode does not support enterprise authentication mode for the time being.
Radius Server IP	IP address of RADIUS (Remote Authentication Dial In User Service) sever. Note: The item will display as a text input box when the wireless network authentication method is enterprise edition.
Radius Server port	The authentication port number of the RADIUS server, value range is 1-65535. Note: The item will display as a text input box when the wireless network authentication method is enterprise edition.
RADIUS Shared key	Shared key of RADIUS server. Note: The item will display as a text input box when the wireless network authentication method is enterprise edition.

5.3.4 WMM Configuration

802.11 network provides wireless access services based on competition, but different application requirements have different requirements on the network, and the original network cannot provide access services of different quality for different applications, so it’s unable to meet the needs of practical applications. IEEE 802.11e adds QoS features to WLAN system based on 802.11 protocol, which has been standardized for a long time. In this process, the Wi-Fi organization defines WMM (Wi-Fi Multimedia) standard in order to ensure interoperability between devices provided QoS by different WLAN vendors. The WMM standard enables WLAN networks to provide QoS services. WMM is a wireless QoS protocol, which is used to ensure that high-priority messages have the priority of sending, so as to ensure the better quality of voice, video and other applications in wireless networks.

Function Description

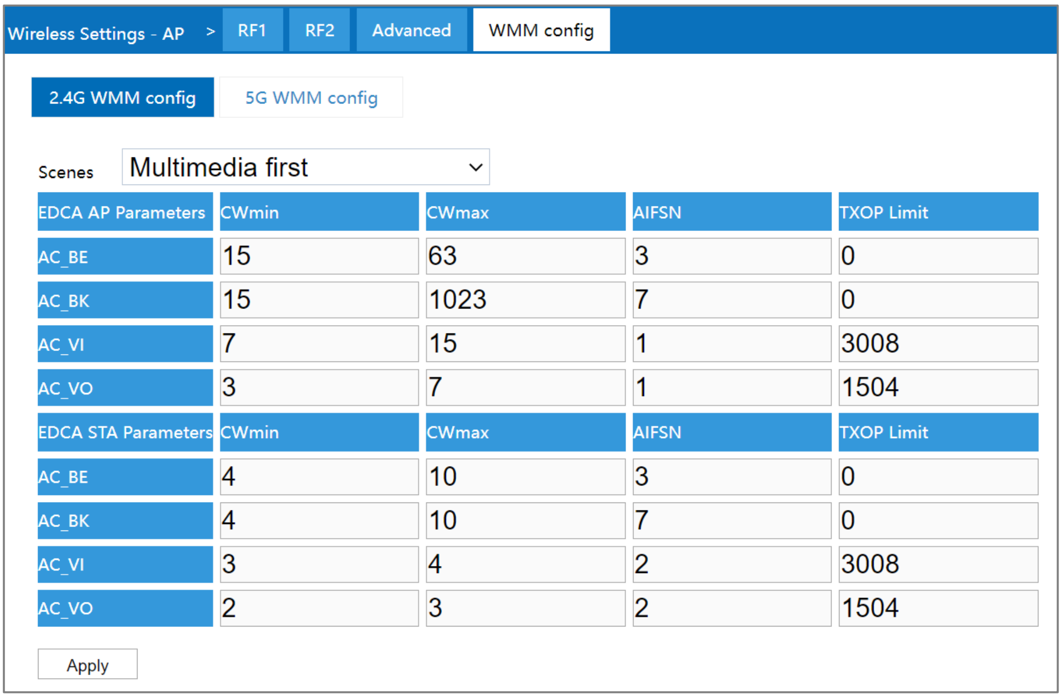
On the "WMM Settings" page of wireless settings, user can configure the relevant parameters of WMM.

Operation Path

Please open in order: "Network Settings> Wireless Settings-AP > WMM Configuration".

Interface Description

WMM configuration interface is as follows:



Scenes: Multimedia first

EDCA AP Parameters	CWmin	CWmax	AIFSN	TXOP Limit
AC_BE	15	63	3	0
AC_BK	15	1023	7	0
AC_VI	7	15	1	3008
AC_VO	3	7	1	1504

EDCA STA Parameters	CWmin	CWmax	AIFSN	TXOP Limit
AC_BE	4	10	3	0
AC_BK	4	10	7	0
AC_VI	3	4	2	3008
AC_VO	2	3	2	1504

The main element configuration description of WMM configuration interface:

Interface Element	Description
WMM Configuration Tab	● 2.4G WMM Configuration ● 5G WMM Configuration Note: Display the current frequency band configuration of RF 1 and RF 2.
Scene	WMM scene settings, options: ● No priority; ● Multimedia First;

Interface Element	Description
	- User-defined. Note: - The default scenario is no priority. At this time, data stream and video voice stream have the same priority, and no one has the priority. - After selecting WMM function, the device can process the data packet with priority level, improving the data transmission performance of WMM and ensuring the service quality of voice, video and other services with high real-time requirements. - To select user-defined functions, users need to set their own parameters.
EDCA AP Parameters	WMM priority queue, options are as follows: - AC_BE (best effort streaming); - AC_BK (background streaming); - AC_VI (video streaming); - AC_VO (voice streaming);
EDCA STA Parameters	EDCA (Enhanced Distributed Channel Access) parameters of terminal device (Workstation STA) supporting 802.11 standard.
CWmin	Minimum competition window, available values: 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023, 2047, 4095, 8191, 16383, 32767
CWmax	Maximum contention window, available values: 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023, 2047, 4095, 8191, 16383, 32767. Note: The value of the maximum contention window must be greater than that of the minimum contention window.
AIFSN	AIFSN, Arbitration Inter Frame Spacing Number WMM can configure different idle waiting time for different AC. The larger the value of AIFSN, the longer the idle waiting time of users will be. Value range is 1-255.
TXOP Limit	Transmission Opportunity Limit The maximum length of time the user can occupy the channel after a successful competition The larger this value is, the longer the user can occupy the channel at a time. If it is 0, only one message can be sent after occupying the channel at a time. Note: The value of this parameter must be positive and modification is not recommended.

5.4 Wireless Settings-Client

Notes

The wireless setting page is different in different working modes:

- Routing, AP mode: only the "Wireless Settings -AP" page is displayed.
- Bridge Mode: The “Wireless Settings-AP” page and the “Wireless Settings-Client” page are displayed.
- Client mode: only the “Wireless Settings-Client” page is displayed.

5.4.1 RF Configuration

Notes

The configuration parameters on the RF configuration page are different in different connection modes and authentication modes.

Function Description

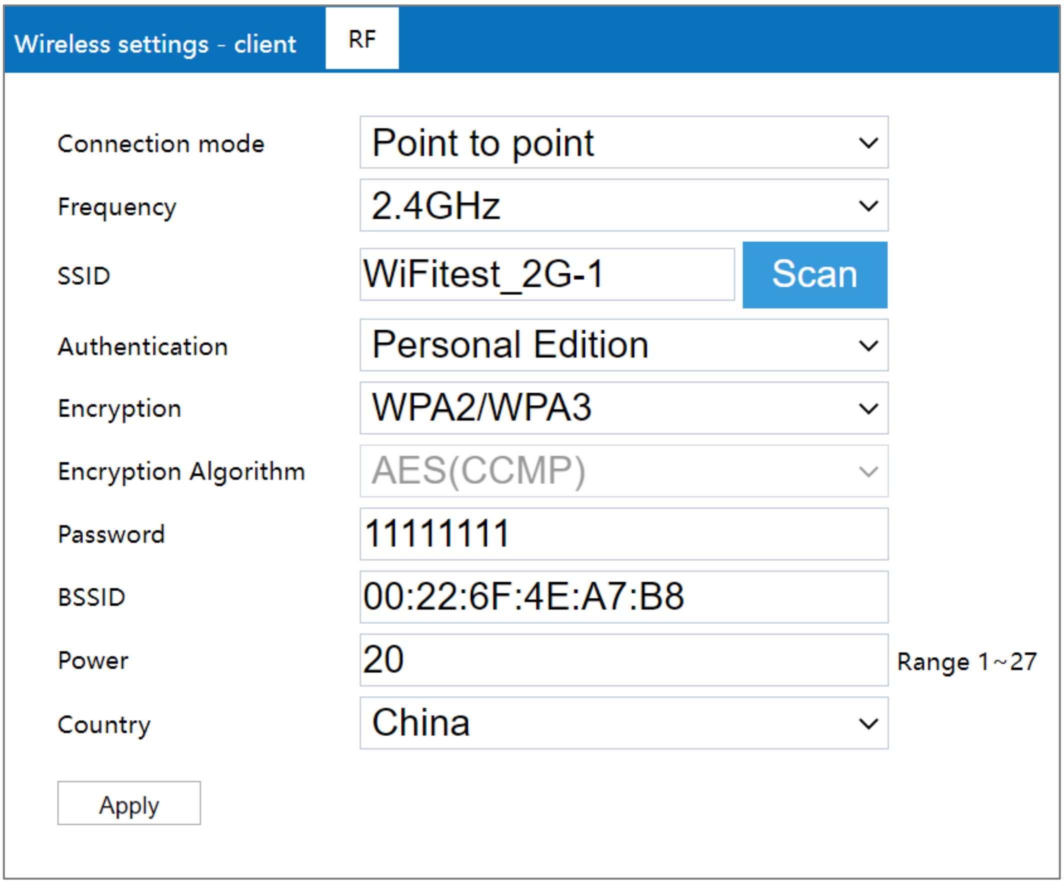
On the "Wireless Settings-Client-RF” page, user can configure the superior wireless network parameters of RF bridge.

Operation Path

Please open in order: "Network settings > Wireless Settings-Client > RF".

Interface Description 1: Personal Authentication Method

The RF - Personal Edition authentication method interface as follows:



Wireless settings - client | RF

Connection mode: Point to point

Frequency: 2.4GHz

SSID: WiFitest_2G-1

Authentication: Personal Edition

Encryption: WPA2/WPA3

Encryption Algorithm: AES(CCMP)

Password: 11111111

BSSID: 00:22:6F:4E:A7:B8

Power: 20 Range 1~27

Country: China

The main element configuration description of RF-Personal Edition authentication method interface:

Interface Element	Description
Connection mode	Connection mode of the device and opposite terminal wireless device, options as follows: • Point to point: it's used for connecting the appointed wireless device; • Roam: Switching among wireless devices with the same SSID. Note: In the bridge mode, it supports the switching between point-to-point and roaming modes.
Roaming signal threshold	Textbox of roaming signal threshold. • When the signal strength RSSI falls below this threshold, roaming will be triggered. • When the signal strength RSSI is higher than this threshold, roaming will not be triggered. Note: This input box is displayed only when connection mode is selected as roaming.
Frequency	Scanning frequency band. Options are as follows: • 2.4GHz

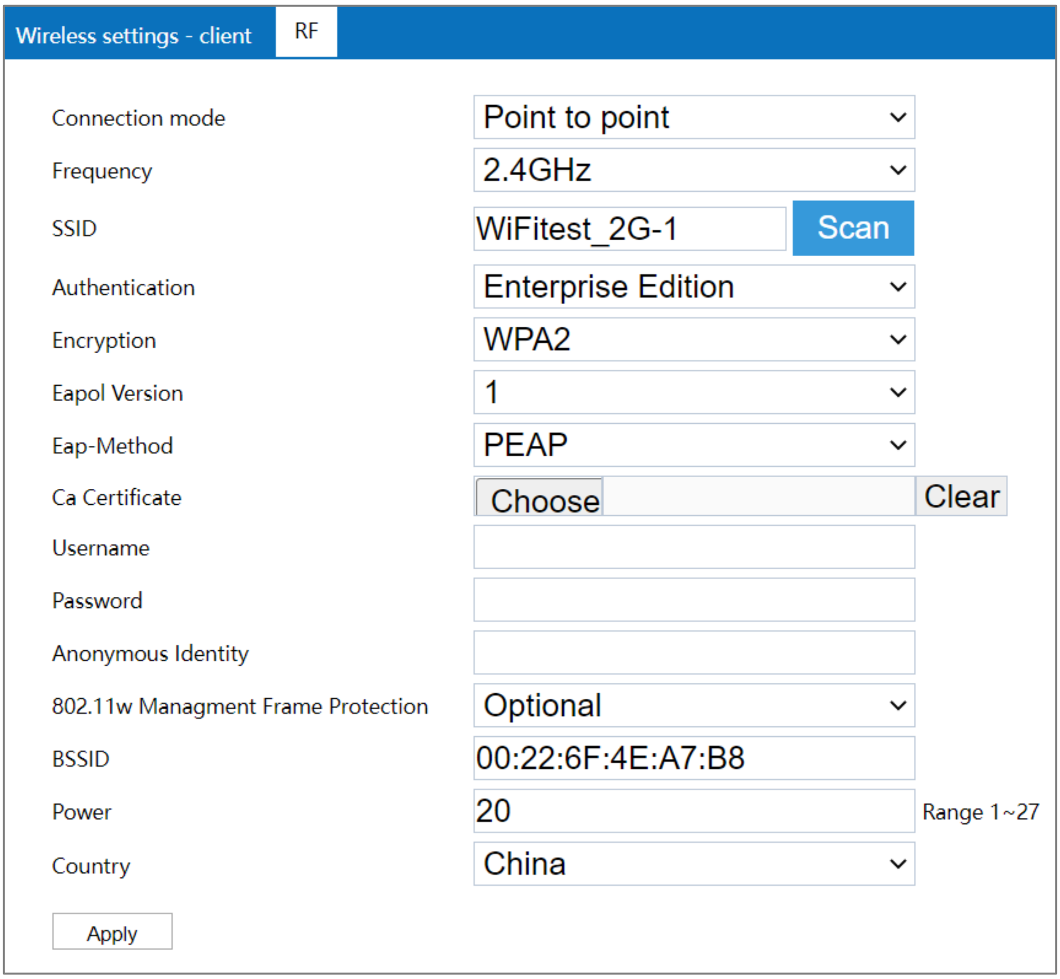
Interface Element	Description
	- 5GHz
SSID	SSID name of the opposite device wireless network. Note: User can add the wireless device for bridge via scan button.
Authentication	Authentication mode of the wireless network at the opposite end: - Personal edition: wireless network WPA/WPA2/WPA3 uses WPA/WPA2-PSK/ WPA3-SAE encryption method and pre-shared key. Personal edition is suitable for personal and home users; - Enterprise edition: wireless network WPA/WPA2/WPA3 uses WPA-802.1X/WPA2-802.1X/WPA3-802.1X encryption method. It is necessary to install Radius server to authenticate, and suitable for enterprise users with high security requirements. Note: When the working mode is WDS bridging, the authentication mode can only be personal version; When the working mode is universal bridging or NAT, the authentication mode can be selected from personal version and enterprise version.
Encryption	Encryption mode of opposite device wireless network, options as follows: - No encryption; - WPA2: WiFi Protected Access II suits for the individual or average family network. It adopts pre-shared key mode and supports TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) encryption modes. - WPA/WPA2: mixed mode of WPA and WPA2, it uses WPA or WPA2 encryption algorithm. - WPA3: the third version of Wi-Fi protected access, with further security improvements over WPA2, longer encryption keys, and SAE authentication. - WPA2/WPA3: mixed mode of WPA2 and WPA3, it uses WPA2 or WPA3 encryption algorithm.
Encryption algorithm	Wireless network encryption algorithm of the opposite device, options as follows: - AES (CCMP): advanced encryption standard; - TKIP/AES: the key integrates 2113 protocol or advanced encryption standard temporarily. Note: When the encryption method is WPA2/WPA3 and WPA3, only AES (CCMP) encryption algorithm is supported.

Interface Element	Description
Password	Password of opposite device wireless network.
BSSID	MAC address of opposite device wireless network. Note: This input box is displayed only when "connection mode" is selected as "point to point".
Power	Transmission power of device wireless signal. Note: • Greater the transmitted power, better the transmittability, longer the transmission range, but stronger the interference; • Different device may has different transmitted power range.
Country	Applied countries and regions of wireless network, options are as follows: • China • USA Note: Different country opens different channels.
Efficient roaming	The switch of efficient roaming function Efficient roaming is a roaming acceleration technology independently developed by our company. Ordinary roaming requires all-channel scanning, while efficient roaming specifies any channels for scanning, and which has optimized the roaming strategy and greatly shortened the roaming time. Note: • Efficient roaming can only be enabled when the"Roaming" is selected as the "Connection Mode". • Only in client mode, efficient roaming is displayed.
Roaming RSSI difference	Roaming RSSI difference of efficient roaming function. The default is the dynamic value calculated automatically, or you can select a fixed value in the drop-down list (range: 5-20). • When the signal strength RSSI difference between the new AP and the current associated AP is higher than this threshold, roaming is triggered; • When the RSSI difference between the signal strength of the new AP and the current associated AP is lower than this threshold, roaming will not be triggered; Note: This drop-down box is displayed only when efficient roaming is enabled.
Scan channel	High-priority scan channels under efficient roaming function. No channel is checked by default, that is, there is no priority channel, and all channels are scanned in sequence. When

Interface Element	Description
	some channels are checked, the designated channel is scanned first, and if no stable signal can be scanned in the designated channel, other channels will be scanned. Note: This item is displayed only when “efficient roaming” is enabled.

Interface Description 2: Authentication Method of Enterprise Edition

The RF1-Enterprise Edition authentication method interface as follows:



Wireless settings - client | RF

Connection mode	Point to point
Frequency	2.4GHz
SSID	WiFitest_2G-1
Authentication	Enterprise Edition
Encryption	WPA2
Eapol Version	1
Eap-Method	PEAP
Ca Certificate	
Username	
Password	
Anonymous Identity	
802.11w Managment Frame Protection	Optional
BSSID	00:22:6F:4E:A7:B8
Power	20 Range 1~27
Country	China

The main element configuration description of RF1-Enterprise Edition authentication method interface:

Interface Element	Description
Connection mode	Connection mode of the device and opposite terminal wireless device, options as follows: ● Point to point: it's used for connecting the appointed wireless device; ● Roam: Switching among wireless devices with the same

Interface Element	Description
	SSID. Note: In the bridge mode, it supports the switching between point-to-point and roaming modes.
Roaming signal threshold	Textbox of roaming signal threshold. ● When the signal strength RSSI falls below this threshold, roaming will be triggered. ● When the signal strength RSSI is higher than this threshold, roaming will not be triggered. Note: This input box is displayed only when connection mode is selected as roaming.
Frequency	Scanning frequency band. Options are as follows: ● 2.4GHz ● 5GHz
SSID	SSID name of the opposite device wireless network. Note: User can add the wireless device for bridge via scan button.
Authentication	Authentication mode of the wireless network at the opposite end: ● Personal version: Wireless network WPA2 is WAP2-PSK pre-shared key mode, and WPA3 provides a more secure handshake protocol and algorithm for WPA3-SAE; Suitable for personal or family users. ● Enterprise: Wireless networks WPA2 and WPA3 are WPA2/WPA3-802.1X access methods, and are authenticated by RADIUS server and extensible authentication protocol EAP. Note: When the working mode is WDS bridging, the authentication mode can only be personal version; When the working mode is universal bridging or NAT, the authentication mode can be selected from personal version and enterprise version.
Encryption	Encryption mode of opposite device wireless network, options as follows: ● WPA 2: the 2nd edition of Wi-Fi protected access ● WPA 3: the 3rd edition of Wi-Fi protected access, which further improves security compared with WPA2.
EAPOL version	The extensible authentication protocol EAPOL on local area network (LAN) is an encapsulation technology defined by 802.1X protocol, which is mainly used to transmit EAP protocol messages between the client and the device in LAN. EAPOL

Interface Element	Description
	protocol version, with the following options: - 1: 802.1X-2001 - 2: 802.1X-2004
EAP method	The 802.1X system uses EAP to realize the interaction of authentication information between the client, the device and the authentication server, and supports a variety of authentication methods. The options are as follows: - PEAP: Protected Extensible Authentication Protocol. EAP-PEAP and EAP-TTLS need to load certificates on the server, but not on the client, so their deployment is relatively flexible and their security is lower than EAP-TLS. - TTLS: Tunneled Transport Layer Security, TTLS is an extension of TLS. The first stage is to establish a TLS tunnel between the user and the authentication server, and the second stage is to use other authentication methods to authenticate in the established tunnel. - TLS: Transport Layer Security. EAP-TLS requires certificates to be loaded on the client and server, which is the most secure.
CA certificate	If the file is in pem format, you can choose no certificate.
User certificate	The file is in p12 format. Note: This item is displayed when EAP type is “TLS”.
User certificate password	User certificate password, which can be letters, numbers and other characters, with a maximum length of 64 bytes. Note: This item is displayed when EAP type is “TLS”.
Stage 2 authentication	EAP-TTLS authentication mode. The authentication mode of Stage 2 is as follows: - PAP: Password authentication protocol, unencrypted authentication. - CHAP: Challenge handshake authentication protocol, encrypted authentication. - MSCHAP: Microsoft version of challenge handshake authentication protocol, Microsoft encrypted authentication.

Interface Element	Description
	- MSCHAP2: Microsoft version of challenge handshake authentication protocol version 2, Microsoft encrypted authentication version 2. Note: This item is displayed when EAP type is "TTLS".
Username	Authentication username, which can be letters, numbers and other characters, with a maximum length of 64 bytes. The configured user name and password are consistent with those configured on the authentication server. Note: This item is displayed when EAP type is "PEAP" or "TTLS".
Password	Authentication password, which can be letters, numbers and other characters, with a maximum length of 64 bytes. Note: This item is displayed when EAP type is "PEAP" or "TTLS".
Anonymous identity	Anonymous authentication username, which can be letters or numbers, with a maximum length of 64 bytes, can be skipped. Note: For some authentication methods, anonymous authentication user names need to be configured. Configuring the anonymous authentication username of 802.1X Client can effectively protect the authentication username from being revealed in the first stage of authentication.
802.11w management frame protection	PMF (Protected Management Frame) is a specification based on IEEE 802.11w standard issued by WFA. Its purpose is to extend the security measures for data frames in WPA2 to unicast and multicast management action frames, so as to improve the credibility of the network. - Disabled - Optional: No matter whether the terminal supports PMF or not, it can access, and only the management frame of the terminal that supports PMF is encrypted and protected. - Mandatory: after this function is turned on, only terminals that support PMF are allowed to access. Note: This function is forced on during WPA3 authentication, and configuration is not supported. If the management frame of WLAN network is not encrypted, it may cause security problems. In order to further protect the security of WLAN network, the Wi-Fi Alliance stipulates that WPA3 must protect the management frame. If the terminal does not support PMF function, it is not allowed to access the terminal.

Interface Element	Description
Password	Password of opposite device wireless network.
BSSID	MAC address of opposite device wireless network. Note: This input box is displayed only when “connection mode” is selected as “point to point”.
Power	Transmission power of device wireless signal. Note: • Greater the transmitted power, better the transmittability, longer the transmission range, but stronger the interference; • Different device may has different transmitted power range.
Country	Applied countries and regions. Options are as follows: • China • USA Note: Different country opens different channels.

5.5 Ring Configuration

Note

Ring configuration is only effective for devices with more than two fiber ports, and a single fiber port cannot be configured with a ring network.

Function Description

On the "Ring Configuration" page, user can enable the private ring network protocol to start link backup, thus improving network reliability.

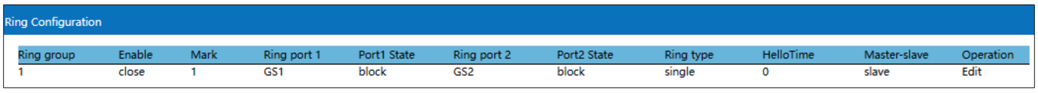
Ring is an Ethernet Ring network algorithm developed and designed for highly reliable industrial control network applications that require link redundancy backup. Ring adopts the design of no master station. The devices running the Ring protocol discover the loop in the network by exchanging information with each other, and block a certain port. Finally, the ring network structure is trimmed into a tree network structure without loop, thus preventing messages from circulating continuously in the ring network, and avoiding the reduction of processing capacity caused by repeated reception of the same message. In a multi-ring network composed of 250 devices, when the network is interrupted or fails, the Ring can ensure that the user network automatically resumes link communication within 20 ms. Ring needs to manually divide the ring network ports in advance, support multiple ring network types such as single ring, coupled ring, chain and Dual Homing. In a single Ring, Ring supports master/slave and no master configuration to meet various network environment requirements.

Operation Path

Please open in order: “Network Settings > Ring Configuration”.

Interface Description

Ring configuration interface as follow:



Ring Configuration

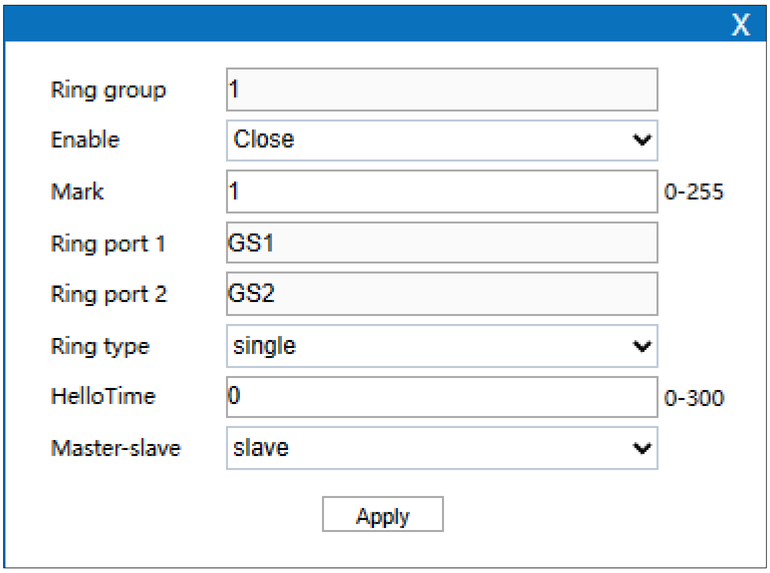
Ring group	Enable	Mark	Ring port 1	Port1 State	Ring port 2	Port2 State	Ring type	HelloTime	Master-slave	Operation
1	close	1	GS1	block	GS2	block	single	0	slave	Edit

The main element configuration description of Ring network interface:

Interface Element	Description
Ring group	Ring group serial number.
Enable	The current enable state of ring group.
Mark	When multiple devices form a ring, its current ring ID would be the network ID. Different ring network has different network ID.
Ring Port 1	Port 1 can be used for the formation of ring network in device.
Port1 State	Forwarding state of Ring Port 1.
Ring Port 2	Port 2 can be used for the formation of ring network in device.
Port2 State	Forwarding state of Ring Port 2.
Ring Type	According to the requirement in the scene, user can choose different ring type. • Single: single ring, using a continuous ring to connect all device together. • Couple: couple ring is a redundant structure used for connecting two independent networks. • Chain: chain can enhance user’s flexibility in constructing all types of redundant network topology via an advanced software technology. • Dual-homing: two adjacent rings share one switch. User could put one switch in two different networks or two different switching equipments in one network.
HelloTime	Hello_time is the sending time interval of Hello packet; via the ring port, CPU sends query packet to adjacent device for confirming the connection is normal or not.
Master-slave	The single ring type supports master and slave device selection, and a single ring can be configured as one-master

Interface Element	Description
	multi-slave mode or no -master mode. When the device is set as master device, one end of it is backup link, it can enable backup link in master station to ensure the normal operation of the network when failure occurs in ring network.
Operation	Click “Edit” button to modify the information of current ring group.

Click “Edit” button to modify the information of current ring.



Ring group: 1
Enable: Close
Mark: 1 0-255
Ring port 1: GS1
Ring port 2: GS2
Ring type: single
HelloTime: 0 0-300
Master-slave: slave

Configuration description of main elements of the Edit interface:

Interface Element	Description
Ring group	Ring group serial number.
Enable	The drop-down list of enabling ring network, options are as follows: ● Disable; ● Enable.
Mark	The ID of ring network, its value range is 0-255.
Ring Port 1	Port 1 can be used for the formation of ring network in device.
Ring Port 2	Port 2 can be used for the formation of ring network in device.
Ring Type	The drop-down list of ring network type, options are as follows: ● Single ● Couple

Interface Element	Description
	• Chain • Dual-homing
HelloTime	The sending cycle of hello-time packet, ranging from 0-300(*100ms), and 0 means not to send.
Master-slave	The drop-down list of master-slave mode selection of single ring, the options are as follows: • Master • Slave

5.6 Optical VLAN

Note

Optical VLAN is only effective for devices with more than two fiber ports, and a single fiber port cannot be configured with fiber port VLAN.

Function Description

On the "Optical VLAN" page, you can configure the fiber port VLAN ID to transmit data frames of multiple different VLANs.

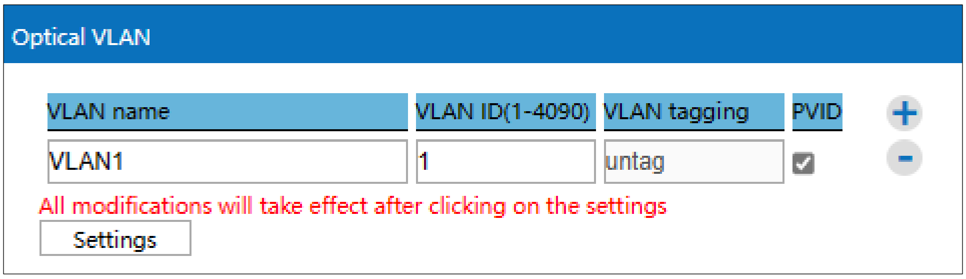
VLAN (Virtual Local Area Network) is a communication technology that logically divides a physical LAN into multiple broadcast domains.

Operation Path

Please open in order: “Network Settings > Optical VLAN”.

Interface Description

Optical VLAN interface is as follows:



Optical VLAN

VLAN name	VLAN ID(1-4090)	VLAN tagging	PVID
VLAN1	1	untag	☑

All modifications will take effect after clicking on the settings

Main elements configuration descriptions of optical VLAN interface:

Interface Element	Description
VLAN name	VLAN interface name, supporting 32 valid characters.
VLAN ID (1-4090)	VLAN ID of the fiber port. Its value range is 1-4090.

Interface Element	Description
	Note: The fiber port VLAN configures the two fiber ports in a unified way and cannot be configured separately.
VLAN tagging	When sending a message, the VLAN ID tag is grayed out and cannot be edited: ● Untag: VLAN ID is PVID, and forwarding without tag; ● Tag: VLAN ID is not PVID, and forwarding with tag.
PVID	When checked, the VLAN ID of the VLAN entry is the default VLAN, that is, PVID (Port Default VLAN ID). Tag the message with corresponding VLAN Tag of port default VLAN ID when receiving the untagged message.
+	Click to add VLAN entry.
-	Click to delete VLAN entries, and PVID cannot be deleted.

5.7 Wireless Probe

Notes

This page is displayed when the device works in AP mode and bridge mode.

Function Description

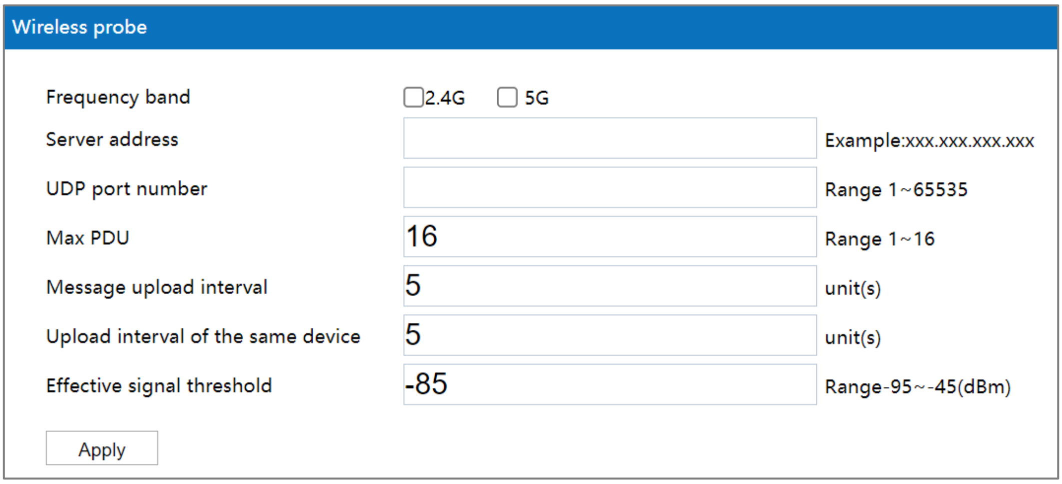
On the "Wireless probe" page of network, user can send detected information of wireless terminal device to appointed server.

Operation Path

Please open in order: "Network > Wireless probe".

Interface Description

Wireless probe interface as follows:



Wireless probe

Frequency band	□2.4G □5G	
Server address		Example:xxx.xxx.xxx.xxx
UDP port number		Range 1~65535
Max PDU	16	Range 1~16
Message upload interval	5	unit(s)
Upload interval of the same device	5	unit(s)
Effective signal threshold	-85	Range-95~-45(dBm)

The main element configuration description of wireless probe interface:

Interface Element	Description
Frequency band	Frequency band used by wireless probe: ● 2.4GHz ● 5GHz
Server Address	The address of the server that receives the wireless device information detected by the wireless probe.
UDP port number	The port number of the server that receives the wireless device information detected by the wireless probe.
Max PDU	Maximum device number that data transmission unit contains, valid value range 1-16.
Message upload interval	The time interval between wireless probes uploading data messages to the server. The unit is in seconds A data message can contain data information of multiple devices.
Upload interval of the same device	Time interval of the same device data upload, unit is second.
Effective signal threshold	Effective wireless signals threshold, unit dBm. Note: If the signal strength of wireless client is less than threshold, it will be regarded as invalid signal.

5.8 AC Management

Function Description

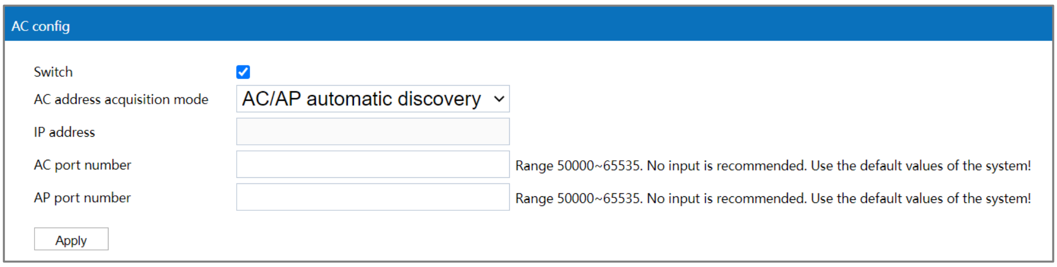
In the "AC Config" page, user can enable AC management, and set AC address, AC port number and AP port number.

Operation Path

Click “Network > AC Config ”.

Interface Description

The AC management interface is as follows:



AC config

Switch ☑

AC address acquisition mode: AC/AP automatic discovery

IP address

AC port number — Range 50000~65535. No input is recommended. Use the default values of the system!

AP port number — Range 50000~65535. No input is recommended. Use the default values of the system!

The main element configuration description of AC management interface:

Interface Element	Description
Switch	Enable AC check box, check it to enable the AC management function.
AC address acquisition mode	AC address acquisition mode, options: ● AC/AP automatic discovery ● DHCP automatic acquisition ● Manual configuration
IP Address	AC IP address information. This parameter needs to be set when the AC address acquisition mode is set manually.
AC port number	AC port number, value range: 50000-65535. Note: ● The AC port number is not modified by default, and is only modified when the port number conflicts. ● If the AC port number is empty, it indicates that the system default is used.
AP port number	AP port number, value range: 50000-65535. Note: ● The AP port number is not modified by default, and is only modified when the port number conflicts. ● If the AP port number is empty, it indicates that the system default is used.

5.9 QoS Config

5.9.1 QoS Strategy

Function Description

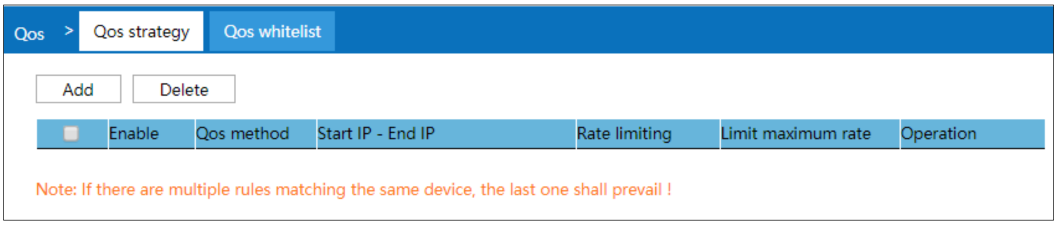
On the “QoS Strategy” page, you can limit the average rate and maximum rate of data transmission for IP or MAC addresses within the policy range.

Operation Path

Click: "Network Settings > QoS Config > QoS Strategy ".

Interface Description

The QoS management interface is as follows:



☐	Enable	Qos method	Start IP - End IP	Rate limiting	Limit maximum rate	Operation

Note: If there are multiple rules matching the same device, the last one shall prevail !

The main element configuration description of QoS strategy interface:

Interface Element	Description
Enable	Enable QoS strategy or not
QoS method	The method of enabling QoS strategy, available values: ● IP-based speed limit ● MAC-based speed limit.
Start MAC-End MAC	The range of the speed limit from the start MAC address to the end MAC address
Start IP-End IP	The range of the speed limit from the start IP address to the end IP address
Speed limit	The average value of limited rate.
Limiting maximum rate	The maximum value of limited rate.
Operation	Click "Edit" button to modify this QoS strategy
Add	Click "Add" button to add QoS strategy Note: If there are multiple repeated rules for the same device, the last rule shall prevail.
Delete	Check the QoS strategy to be deleted, and click the "Delete" button to delete QoS strategy

5.9.2 QoS Whitelist

Function Description

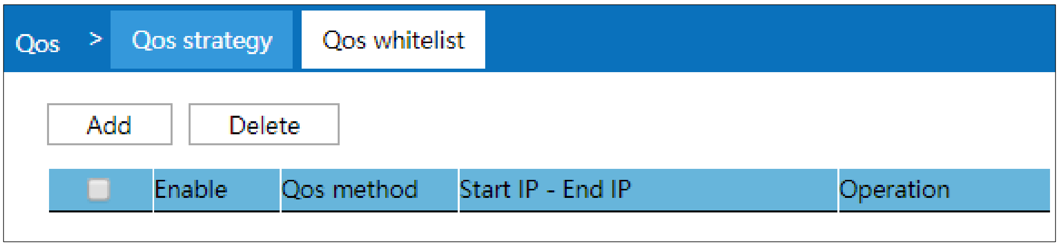
On the "QoS White List" page, you can set the white list of IP or MAC address. The data transmission rate in the list is not limited by the QoS policy.

Operation Path

Click: "Network Settings > QoS Whitelist".

Interface Description

QoS Whitelist interface as follows:



□	Enable	Qos method	Start IP - End IP	Operation

The main element configuration description of QoS white list interface:

Interface Element	Description
Enable	Enable QoS whitelist or not
QoS method	The method of enabling QoS strategy, available values: • IP white list; • MAC whitelist.
Start MAC-End MAC	The range of starting and ending MAC addresses whose rate is not affected by QoS strategy.
Start IP-End IP	The range of starting and ending IP addresses whose rate is not affected by QoS strategy.
Operation	Click "Edit" button to modify this QoS whitelist
Add	Click "Add" button to add QoS whitelist. Note: If there are multiple repeated rules for the same device, the last rule shall prevail.
Delete	Check the QoS whitelist entry to be deleted, and click "Delete" button to delete QoS whitelist

5.10 SNMP Management

Function Description

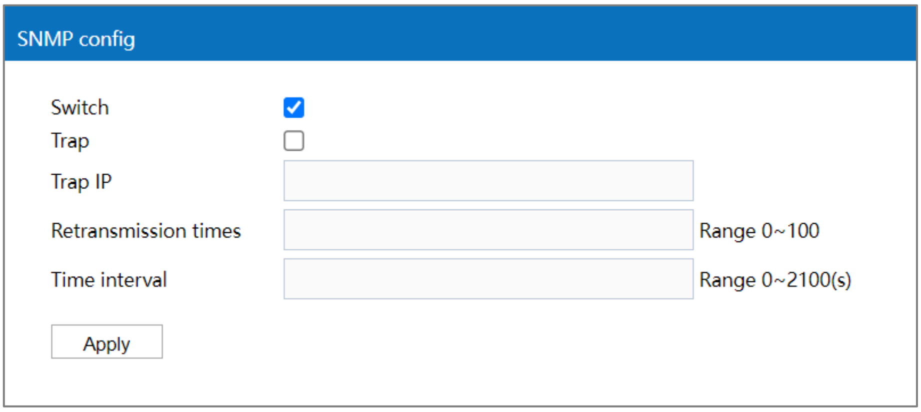
On the "SNMP Management" page, SNMP management can be enabled, and Trap can be enabled.

Operation Path

Click: "Network Settings > SNMP Management".

Interface Description

The SNMP management interface is as follows:



SNMP config

Switch ☑

Trap □

Trap IP

Retransmission times Range 0~100

Time interval Range 0~2100(s)

The main element configuration description of SNMP management interface:

Interface Element	Description
Switch	The check box of the switch, check it to enable SNMP management.
Trap	Trap check box, check it to enable Trap information, and the device actively sends the abnormal situation of the device to the management server. Note: Trap anomaly mainly include wireless client online and offline, hardware and software restarting, etc.
Trap IP	The IP address of the server receiving Trap information.
Retransmission times	Time of resending Trap information.
Time interval	Time interval of device sending Trap information, the unit is second.
Allow multicast transparent transmission	Allow multicast passthrough check box. When checked, multicast data is allowed to passthrough in intranet. After SNMP management is enabled, multicast passthrough is not

Interface Element	Description
	allowed by default.

5.11 QoS Management

Function Description

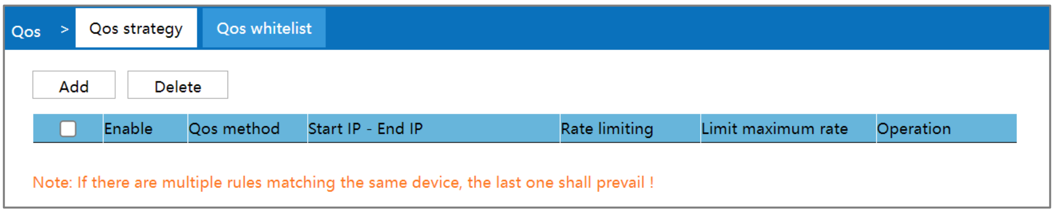
On the “QoS Policy” page, you can limit the average rate and maximum rate of data transmission for IP addresses within the policy range.

Operation Path

Click: "Network Settings > QoS Management".

Interface Description

The QoS management interface is as follows:



Note: If there are multiple rules matching the same device, the last one shall prevail !

The main element configuration description of QoS strategy interface:

Interface Element	Description
Enable	Enable QoS strategy or not
QoS method	The method of enabling QoS strategy, available values: - IP-based speed limit - MAC-based speed limit.
Start IP-End IP	The range of the speed limit from the start IP address to the end IP address
Rate Limiting	The average value of limited rate.
Limit maximum rate	The maximum value of limited rate.
Operation	Click "Edit" button to modify this QoS strategy
Add	Click "Add" button to add QoS strategy Note: - A maximum of 3 policies is supported. - If there are multiple repeated rules for the same device, the last rule shall prevail.
Delete	Check the QoS strategy to be deleted, and click the "Delete"

Interface Element	Description
	button to delete QoS strategy

5.11.1 QoS Whitelist

Function Description

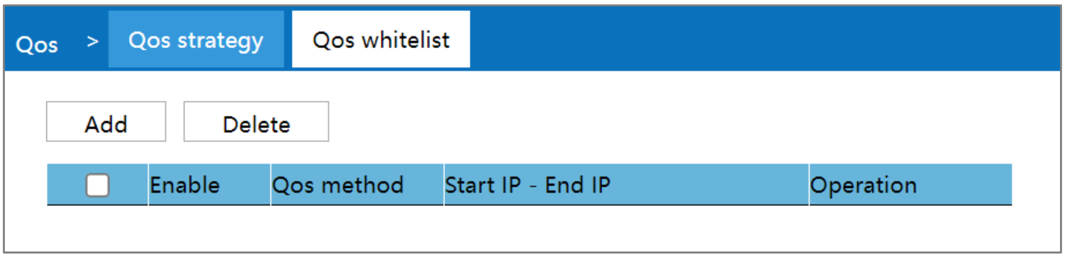
On the "QoS White List" page, you can set the white list of IP or MAC address. The data transmission rate in the list is not limited by the QoS policy.

Operation Path

Click: "Network Settings > QoS Whitelist".

Interface Description

QoS Whitelist interface as follows:



□	Enable	Qos method	Start IP - End IP	Operation

The main element configuration description of QoS white list interface:

Interface Element	Description
Enable	Enable QoS whitelist or not
QoS method	The method of enabling QoS strategy, available values: • IP white list; • MAC whitelist.
Start IP-End IP	The range of starting and ending IP addresses whose rate is not affected by QoS strategy.
Operation	Click "Edit" button to modify this QoS whitelist
Add	Click "Add" button to add QoS whitelist. Note: If there are multiple repeated rules for the same device, the last rule shall prevail.
Delete	Check the QoS whitelist entry to be deleted, and click "Delete" button to delete QoS whitelist

5.12 AP Roaming Control

Notes

When the connection method is “Roaming”, the “Roaming Agent” page is displayed.

Function Description

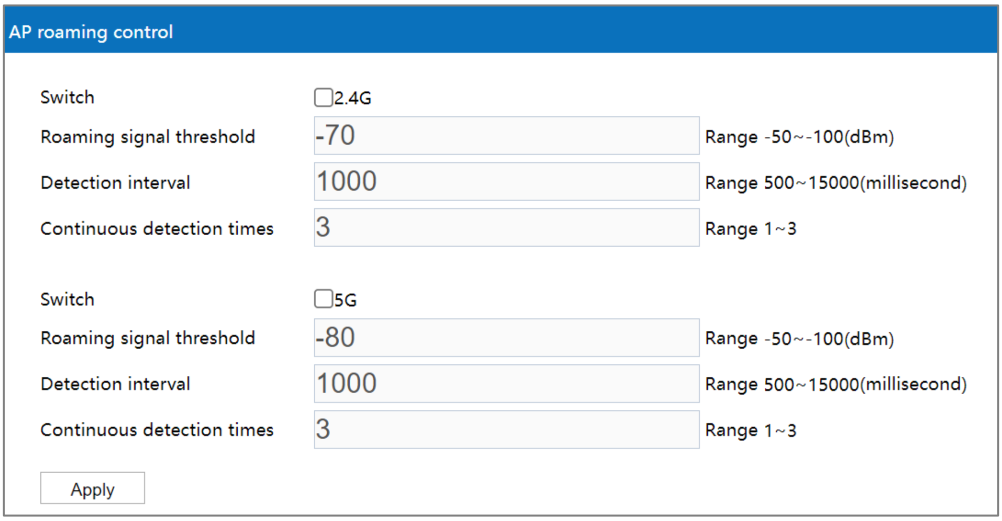
On the “AP Roaming Control” page, you can configure roaming switches and thresholds, which have controlled the connection and disconnection of roaming.

Operation Path

Open in order: "Network Settings > AP Roaming Control".

Interface Description

The AP roaming control interface is as follows:



AP roaming control

Switch	☐2.4G	
Roaming signal threshold	-70	Range -50~-100(dBm)
Detection interval	1000	Range 500~15000(millisecond)
Continuous detection times	3	Range 1~3
Switch	☐5G	
Roaming signal threshold	-80	Range -50~-100(dBm)
Detection interval	1000	Range 500~15000(millisecond)
Continuous detection times	3	Range 1~3

Main elements configuration descriptions of AP roaming control interface:

Interface Element	Description
Switch	2.4G or 5G roaming control switch, Check to enable roaming.
Roaming signal threshold	Input box of roaming signal threshold, you can input -50~100dBm. • When the signal strength RSSI falls below this threshold, roaming will be triggered. • When the signal strength RSSI is higher than this threshold, roaming will not be triggered. Note: This input box is displayed only when connection mode is selected as roaming.
Detection interval	Time interval of roaming signal detection
Continuous	If no roaming signal is detected, the number of times it will be

Interface Element	Description
detection times	continuously detected before disconnecting.

5.13 Roaming Agent

Notes

When the connection method is “Roaming”, the “Roaming Agent” page is displayed.

Function Description

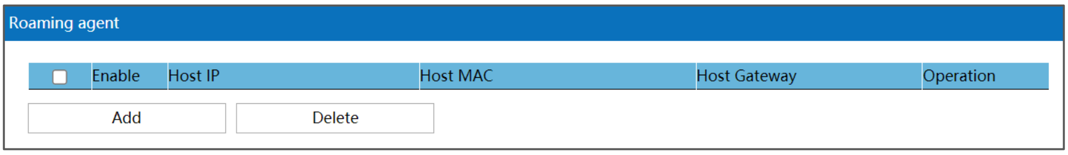
On the roaming agent page, users can configure the network address information of roaming agent host.

Operation Path

Open in order: "Network Settings > Roaming Agency".

Interface Description

Roaming agency interface as follows:



The main element configuration description of roaming agency interface:

Interface Element	Description
Enable	Enable status of roaming agency.
Host IP	IP address of roaming agency device.
Host MAC	MAC address of roaming agency device.
Host gateway	Gateway address of roaming agency device. ● If the gateway address is specified, the device will send free ARP packets by unicast; ● If the gateway address is not filled in, the device will send free ARP packets by broadcast.
Operation	Click the "Edit" button to modify the roaming agency network address information.

6 Wireless Client

Notes

This page is displayed when the device works in routing mode, AP mode and bridge mode.

6.1 Users

Function Description

On the page of "User List", user can:

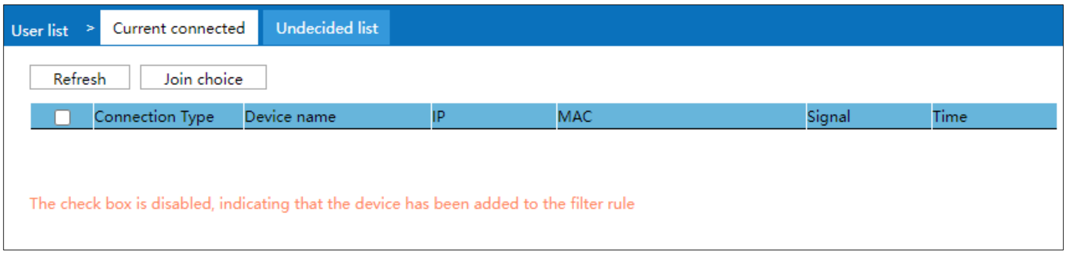
- View the wireless devices currently accessed.
- Set filtering rules for black-and-white list to filter the access of wireless devices.

Operation Path

Please open: "Wireless User > User List”.

Interface Description 1: Current Connected

The interface of the current connected device is as follows:



□	Connection Type	Device name	IP	MAC	Signal	Time

The check box is disabled, indicating that the device has been added to the filter rule

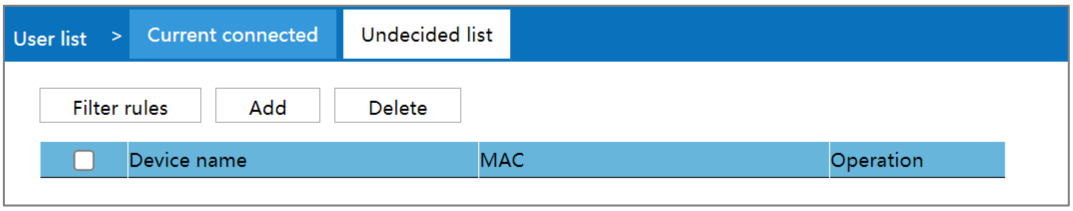
Configuration of the main elements of the current connected device interface:

Interface Element	Description
Connection type	The frequency band accessed by the wireless user and the wireless interface RF1 or RF2.
Device name	The device name of the accessed wireless user.

Interface Element	Description
IP	The IP address of the accessed wireless user.
MAC	The MAC address of the accessed wireless user.
Signal	The signal strength of the accessed wireless user. The unit is dBm, the larger the value, the stronger the signal.
Time	Online time of accessed wireless users.
Refresh	Refresh the current page display.
Add selected	Add the selected wireless users to the current list.

Interface Description 2: Undecided List

Undecided list interface as follows:



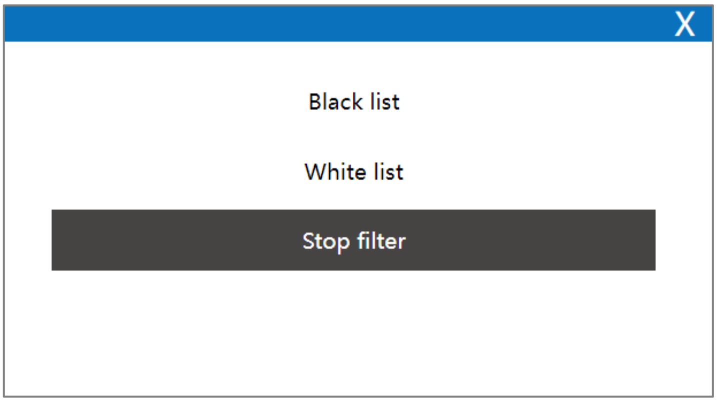
The main element configuration description of Undecided List interface:

Interface Element	Description
Device name	Device name of wireless user.
MAC	The MAC address of the wireless user.
Operation	Edit the selected wireless user information.

Interface Description 3: Filter Rules

Click “Filter Rules” button to switch between pending list, blacklist and whitelist.

The filter rule interface as follows:



The main element configuration description of filter rules:

Interface Element	Description
Black list	Add the wireless users on current page to the blacklist. After adding, the users of this page are prohibited from accessing the device.
White list	Add the wireless users on current page to the whitelist. After adding, only the users of this page are allowed to access the device.
Stop filter	Disable filtering the wireless users of the current page.

Note

When switching lists through filtering rules, it is only effective for the currently selected list.

6.2 User Event

Function Description

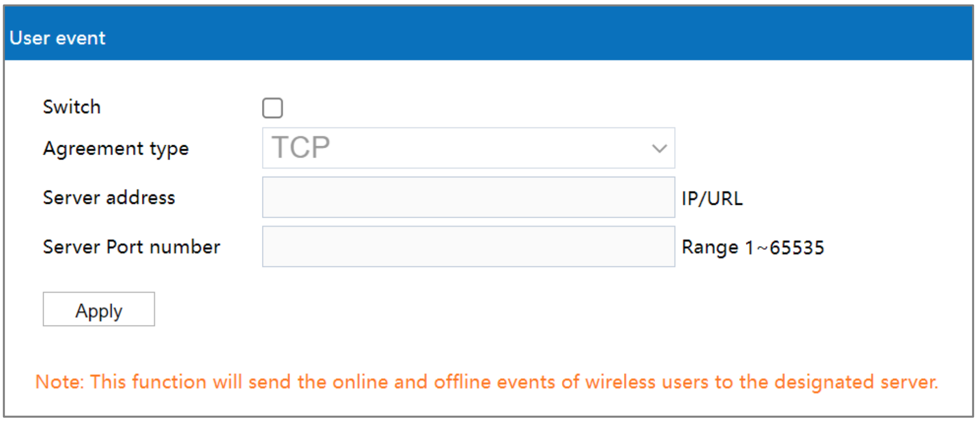
On the “User Event” page, you can transmit online/offline event of wireless users to designated server.

Operation Path

Please open: "Wireless Users > User Event”.

Interface Description

The user event interface as follows:



User event

Switch □

Agreement type: TCP

Server address: IP/URL

Server Port number: Range 1~65535

Note: This function will send the online and offline events of wireless users to the designated server.

The main element configuration description of user event interface:

Interface Element	Description
Switch	Enable “User Events”.
Agreement type	Select the communication protocol that transmits user events.

Interface Element	Description
	● TCP Protocol ● UDP Protocol ● HTTP Protocol
Server Address	The address of the server that receives the wireless user's online and offline events.
Server port number	The port number of the server that receives the wireless user's online and offline events.
Apply	Click “Apply” to save the configuration.

7 Firewall

Notes

Firewall only displays and takes effect when the device is in routing mode or wireless NAT mode. This function is not available in other modes.

7.1 IP Filter

Function Description

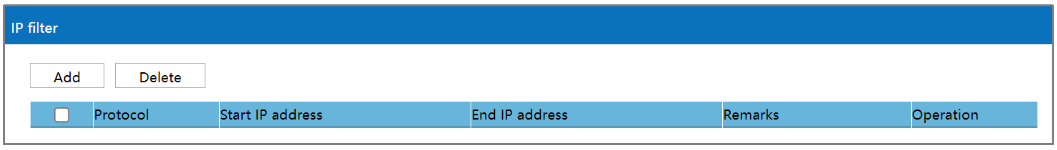
On the "IP filter" page of firewall, user can check or add IP filter to forbid the communication between the clients in LAN and WAN.

Operation Path

Please open in order: "Firewall > IP filter".

Interface Description

IP filter interface as follows:



IP filter

Add Delete

□	Protocol	Start IP address	End IP address	Remarks	Operation

The main element configuration description of IP filter interface:

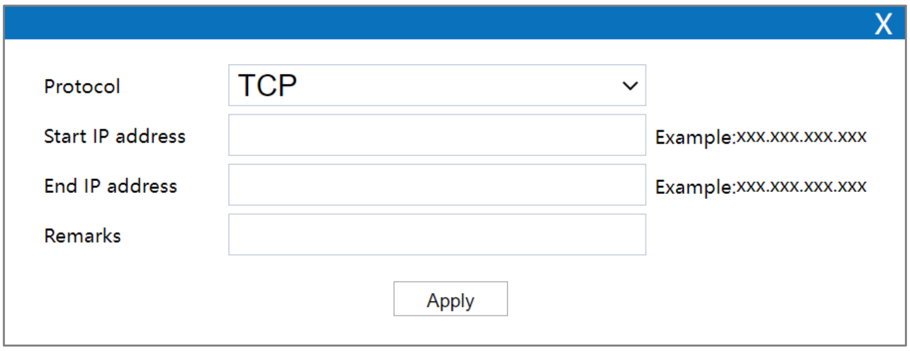
Interface Element	Description
□	Check box of IP address filtering entries, click to check all IP filter entries.
Protocol	Protocols used by data packets.
Start IP address	Start IP address of LAN IP address range filtered by the device.
End IP address	End IP address of LAN IP address range filtered by the device.

Interface Element	Description
Remarks	Remarks of IP filter entries.
Operation	Edit: Modify the filtering entries information.

Interface Description: Add IP Filter Entry

Click "Add" to increase IP filter entry.

IP filter interface as follows:



The main element configuration description of IP filter interface:

Interface Element	Description
Protocol	Drop-down list of data packet protocol, options as follows: ● TCP/UDP; ● TCP; ● UDP.
Start IP address	Start IP address of LAN IP address range filtered by the device, such as: 192.168.1.123.
End IP address	End IP address of LAN IP address range filtered by the device, such as: 192.168.1.123.
Remarks	Remarks of IP filter list support 10 Chinese characters or 32 valid characters, optional.

7.2 MAC Filter

Function Description

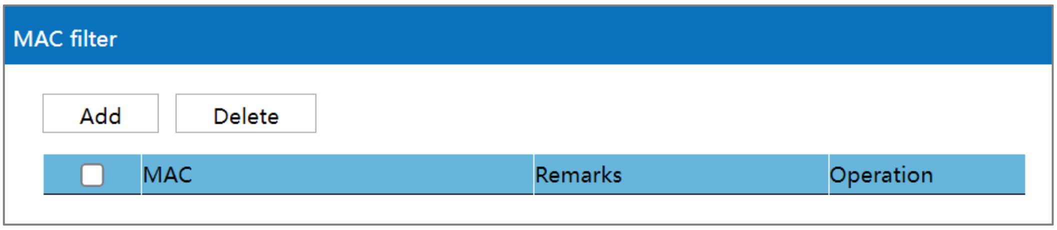
On the "MAC filter" page of firewall, user can check or add MAC filter to forbid the communication between the clients in LAN and WAN; it can effectively control the WAN access rights of user in LAN.

Operation Path

Open in order: "Firewall > MAC filter".

Interface Description

MAC filter interface as follows:



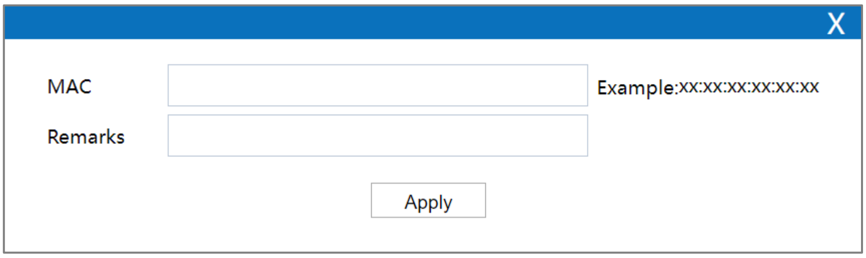
The main element configuration description of MAC filter interface:

Interface Element	Description
□	Check box of MAC address filtering entries, click to check all MAC filter entries.
MAC	MAC address of LAN client filtered by the device.
Remark	Remarks of MAC filter entries.
Operation	Edit: Modify the filtering entries information.

Interface Description: Add MAC Filter Entry

Click "Add" to increase MAC filter entry.

MAC filter interface as follows:



The main element configuration description of MAC filter interface:

Interface Element	Description
MAC	MAC address of LAN client filtered by the device, such as: XX:XX:XX:XX:XX:XX.
Remarks	Remarks of MAC filter entries support 32 valid characters or 10 Chinese characters, optional.

7.3 URL Filter

URL (Uniform Resource Locator) is the brief expression of access method and location of resources gained from Internet; it's the address of standard Internet resources. Each Internet file has a unique URL, which refers to the network address.

Function Description

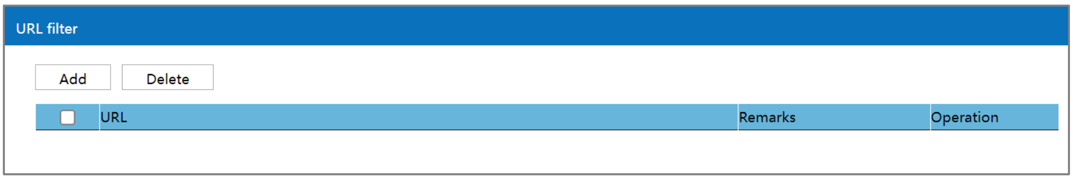
On the "URL filter" page of firewall, user can check or add URL filter to prohibit the client in LAN from accessing URL address in WAN and prevent user from accessing some of the websites.

Operation Path

Please open in order: "Firewall > URL filter".

Interface Description

URL filter interface as follows:



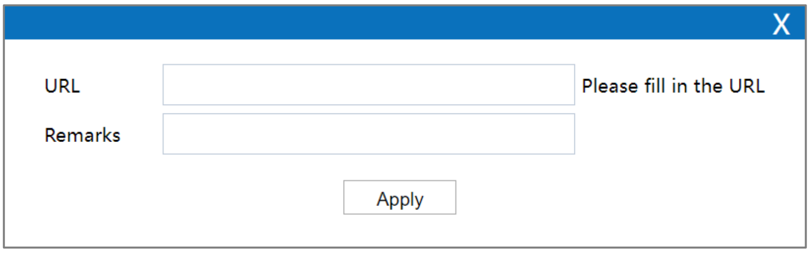
The main element configuration description of URL filter interface:

Interface Element	Description
□	Check box of URL address filtering entries, click to check all URL filter entries.
URL	URL address in LAN filtered by the device.
Remarks	Remarks for URL addresses filtering entries.
Operation	Edit: modify the filter list.

Interface Description: Add URL Filter List

Click "Add" to increase URL filter list.

URL filter interface as follows:



The main element configuration description of URL filter interface:

Interface Element	Description
URL	URL address in WAN filtered by the device, ending with ".com", ".cn" and so on. Such as: http://www.123.cn.
Remarks	Remarks of URL address filtering entry, optional.

7.4 Port Forward

Function Description

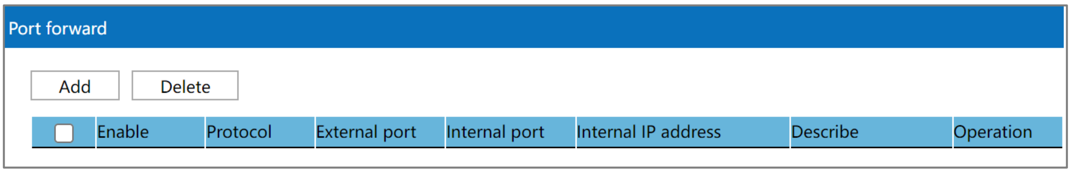
On the "Port forward" page of firewall, user can check or add port forward entry to allow the WAN client to access appointed device in LAN.

Operation Path

Please open in order: "Firewall > Port forward".

Interface Description

The port forward interface as follows:



Port forward

□	Enable	Protocol	External port	Internal port	Internal IP address	Describe	Operation

The main element configuration description of port forward interface:

Interface Element	Description
□	The port forwarding entry checkbox, click to check all the port forwarding entries.
Enable	The enabled state of the current forwarding entry.
Protocol	The protocol type used by port forward data package, like: TCP, UDP.
External port	The port used by the application of internal server.
Internal port	The port used by the external network to access the server application.
Internal IP address	IP address of appointed device in LAN.
Describe	Remarks of port forward entries.
Operation	Edit: modify the port forward entries.

7.5 Port Redirection

Function Description

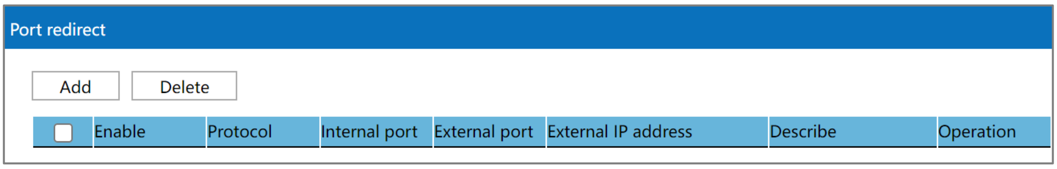
On the “Port Redirection” page, user can check or add port redirection entry, which allows client in LAN to visit the specified port of device with IP address specified by external network via specified port.

Operation Path

Please open in order: "Advanced Network > Port Redirection".

Interface Description

The port redirection interface as follows:



The main element configuration description of port redirection interface:

Interface Element	Description
□	The checkbox of port redirection entry. Click to check all port redirection entries.
Enable	Enable port redirection or not: • ON • OFF
Protocol	The protocol type used by port redirection data package: • TCP • UDP. • TCP/UDP
Internal port	The port used by the application of internal server.
External port	The port used by the external network to access the server application.
External IP address	The device IP address specified by external network
Describe	The remark information of port redirection entry
Operation	Edit: modify port redirection entry information
Add	Click the “add” button to add new port redirection in the pop-up window of “Port Redirection”
Delete	Check the port redirection information that needs to be

Interface Element	Description
	deleted, then click “delete” button to delete the port redirection.

7.6 ARP Binding

ARP (Address Resolution Protocol) is a TCP/IP protocol that gains the physical address according to IP address.

Function Description

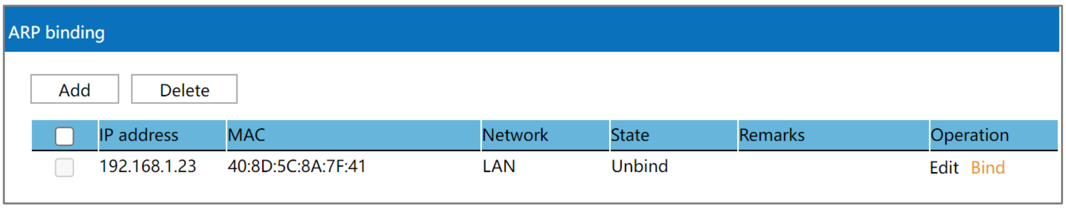
On the "ARP binding" page of firewall, user can check or add ARP binding entry. Binding the client IP address to corresponding MAC address to avoid ARP spoofing. When the client sends ARP request to the device, the device will check ARP binding list according to client IP address; if the MAC address in list is same to the one of client, the device will allow the ARP request; otherwise the request won't be allowed, that is the client can't access the device.

Operation Path

Please open in order: "Firewall > ARP binding".

Interface Description

ARP binding interface as follows:



□	IP address	MAC	Network	State	Remarks	Operation
□	192.168.1.23	40:8D:5C:8A:7F:41	LAN	Unbind		Edit Bind

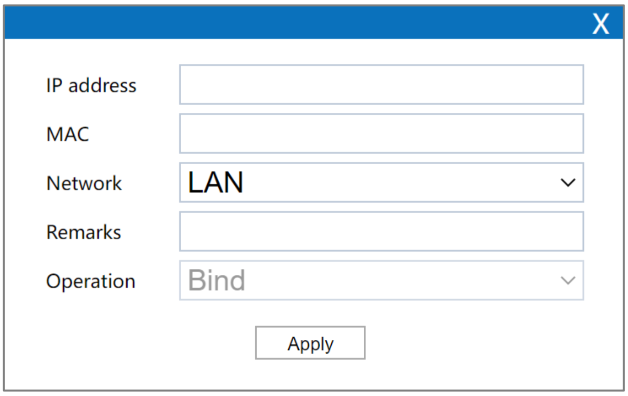
The main element configuration description of ARP binding interface:

Interface Element	Description
□	ARP binding entry check box, click to check all ARP binding entries.
IP Address	IP address of client.
MAC	MAC address of client.
Network	Network properties of client connection.
State	ARP binding status.
Remarks	Remarks of ARP binding entry.
Operation	Edit: modify ARP binding entry. Binding: bind the IP and MAC address of this entry.

Interface Description: Add ARP Binding Entry

Click "Add" to increase ARP binding entry.

ARP binding settings interface as follows:



IP address

MAC

Network: LAN

Remarks

Operation: Bind

The main element configuration description of ARP binding settings interface:

Interface Element	Description
IP Address	IP address of client, such as: 192.168.1.123.
MAC	MAC address of client, such as: 00:22:6F:00:00:01.
Network	Network properties of client connection, options as follows: ● LAN; ● WAN.
Remarks	Remarks of ARP binding entry, support 32 valid characters or 10 Chinese characters, optional.
Operation	ARP binding.

7.7 DMZ Settings

DMZ (Demilitarized Zone) is a buffer zone built between non-safety system and safety system for solving the problem that visitor from external network cannot visit internal network server after the firewall is installed.

Function Description

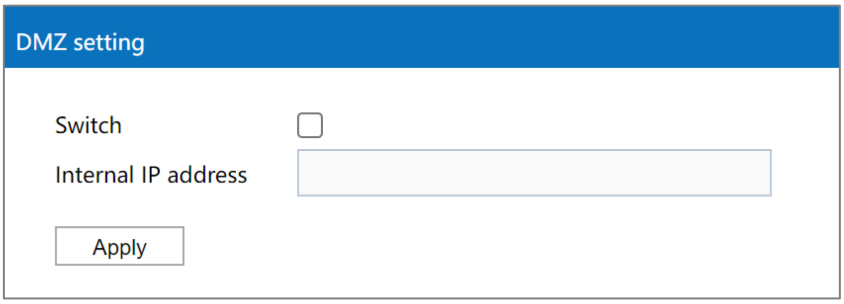
On the page of firewall “DMZ Settings”, user can enable or disable DMZ function. The client can visit the specified LAN client via WAN.

Operation Path

Please open in order: "Firewall > DMZ filter".

Interface Description

The DMZ setting interface as follows:



DMZ setting

Switch □

Internal IP address

The main element configuration description of DMZ setting interface:

Interface Element	Description
Switch	Enable DMZ.
Internal IP address	The IP address of LAN client, for example: 192.168.1.123.

8 System Tools

8.1 Network Detection

Function Description

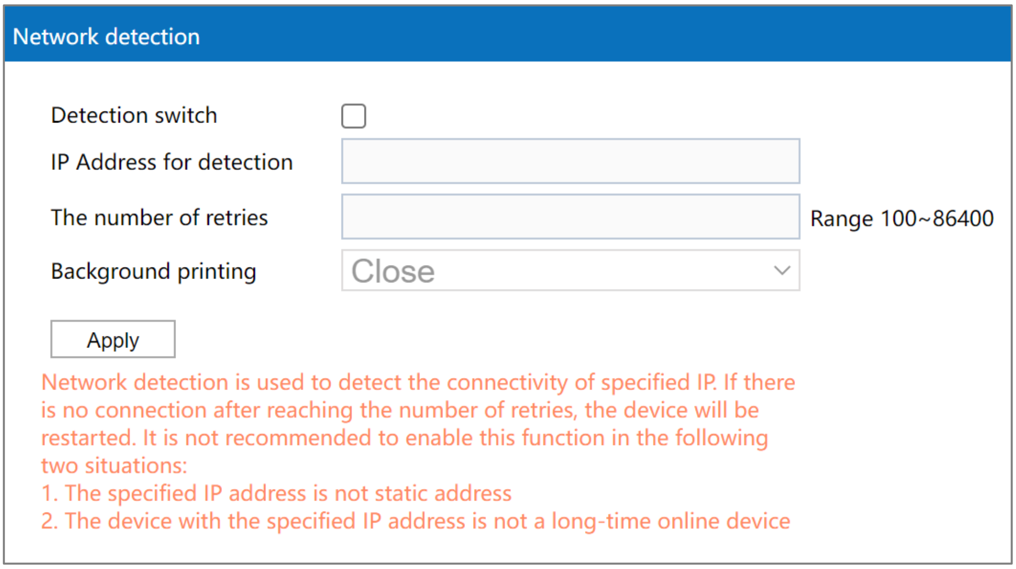
On the “Network Detection” page, users can detect the connection status of the specified IP address to estimate the connection status of network. Enable the network detection function, and the device will continuously detect the connectivity of the specified IP address in the network according to a specified interval time. When abnormal network communication is found and the number of detection retries is reached, the device will restart automatically.

Operation Path

Open in order: "System Manage > Network Detection".

Interface Description

The network detection interface as follows:



Network detection

Detection switch	□	
IP Address for detection		
The number of retries		Range 100~86400
Background printing	Close	

Network detection is used to detect the connectivity of specified IP. If there is no connection after reaching the number of retries, the device will be restarted. It is not recommended to enable this function in the following two situations:

1. The specified IP address is not static address
2. The device with the specified IP address is not a long-time online device

The main element configuration description of network detection interface:

Interface Element	Description
Detection switch	Checkbox, check it to enable the network diagnosis function.
IP Address for detection	The destination IP address of the wireless network detection packet sent by the device. Notice: Please do not use the automatically acquired network address or IP address of the device that is not online for a long time as the detection IP address.
The number of retries	The device will send network detection package for 100 times at least when the detected IP address makes no response.
Background printing	Background printing drop-down list, options as follows: • Disable; • Enable: Enabling the background printing function, the result of network detection will be displayed in system log.

8.2 User Settings

Function Description

On the "User settings" page of system tools, user can modify the access password of the device.

Note

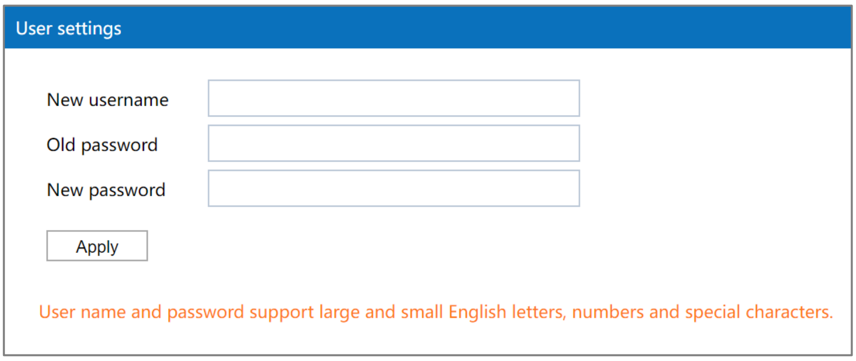
Please log in again after modifying the user name and password.

Operation Path

Please open in order: "System Tools > User settings".

Interface Description

User settings interface as follows:



User settings

User name and password support large and small English letters, numbers and special characters.

The main element configuration description of user settings interface:

Interface Element	Description
New username	New username settings of the device. Note: Both the username and password consist of uppercase and lowercase letters, as well as numbers and underline;
Old password	Login password used by current device.
New password	New password settings of the device. Note: Both the username and password consist of uppercase and lowercase letters, as well as numbers and underline;

8.3 Device Alias

Function Description

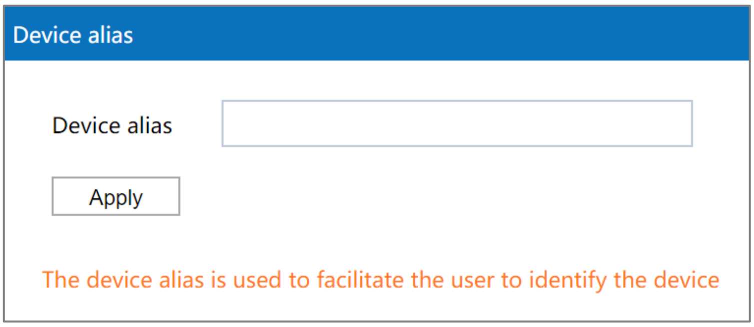
On the “Device Alias” page of system tool, user can set the device alias.

Operation Path

Please open in order: "System Tools > Device Alias".

Interface Description

The Device Alias interface is as follows:



Device alias

The device alias is used to facilitate the user to identify the device

Configuration of the main elements of the device alias interface:

Interface Element	Description
Device Alias	Set the name of the device. The device alias is used to facilitate user identification of the device.
Apply	Click “Apply” button to save device alias.

8.4 Time Settings

Function Description

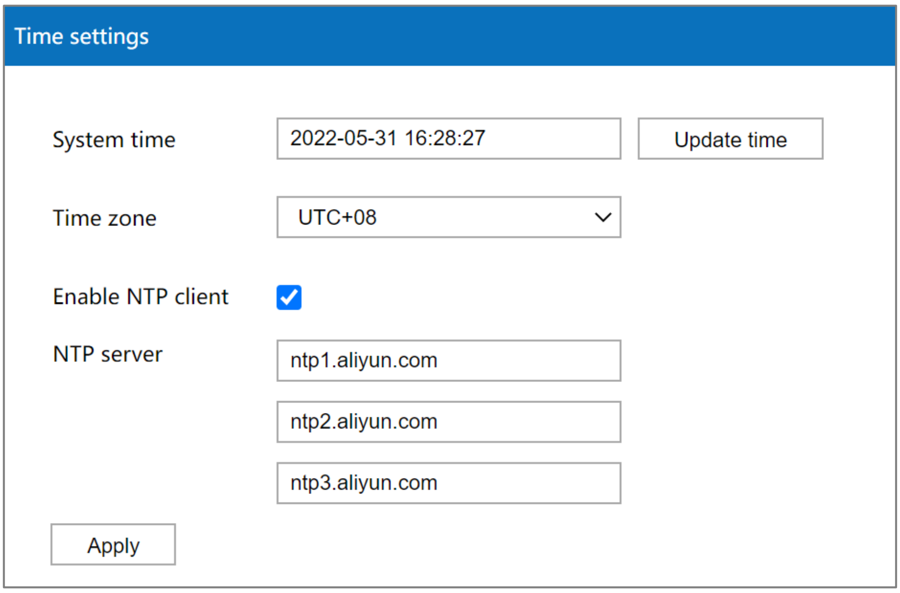
On the "Time Setting" page of the system tool, you can obtain the local time or NTP server time.

Operation Path

Open in order: "System Tools > Time Settings".

Interface Description

Time setting interface as follows:



Time settings

System time: 2022-05-31 16:28:27

Time zone: UTC+08

Enable NTP client: ☑

NTP server: ntp1.aliyun.com

ntp2.aliyun.com

ntp3.aliyun.com

The main elements configuration description of time settings interface:

Interface Element	Description
System Time	Program version used by current device.
Time Zone	Select the current time zone.
Enable NTP Client	When the NTP client is enabled, you can synchronize the time of the NTP server.
NTP Server	NTP server address, 3 addresses can be provided.

8.5 Timed Restart

Function Description

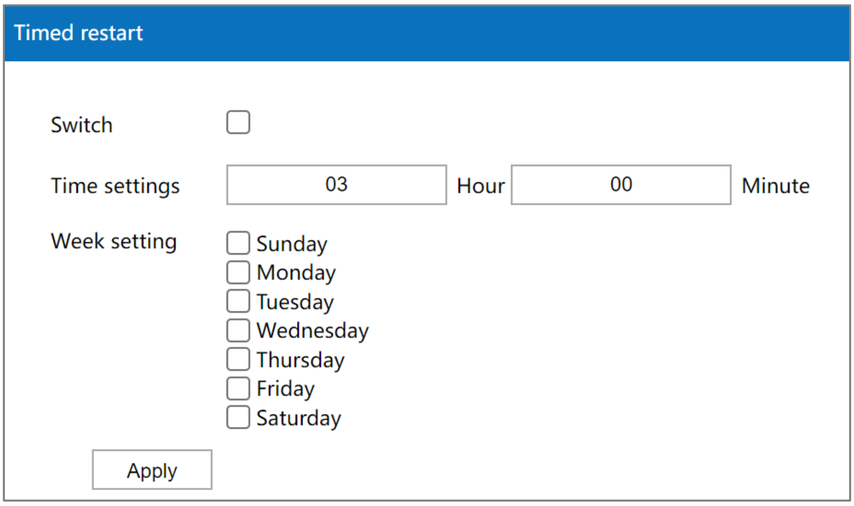
On the "Timed Restart" page of the system tool, you can set the periodic and timed restart of the device in weeks.

Operation Path

Open in order: "System Tools > Timed Restart".

Interface Description

The timed restart interface as follows:



Timed restart

Switch □

Time settings 03 Hour 00 Minute

Week setting

□ Sunday
□ Monday
□ Tuesday
□ Wednesday
□ Thursday
□ Friday
□ Saturday

The main elements configuration description of timed restart interface:

Interface Element	Description
Switch	Program version used by current device.
Time Settings	Set the time of timed restart.
Week Setting	Check the restart date to set periodic timed restart in weeks.

8.6 Access Settings

Notes

It displays and takes effect when the device is in routing mode or wireless NAT mode.

Function Description

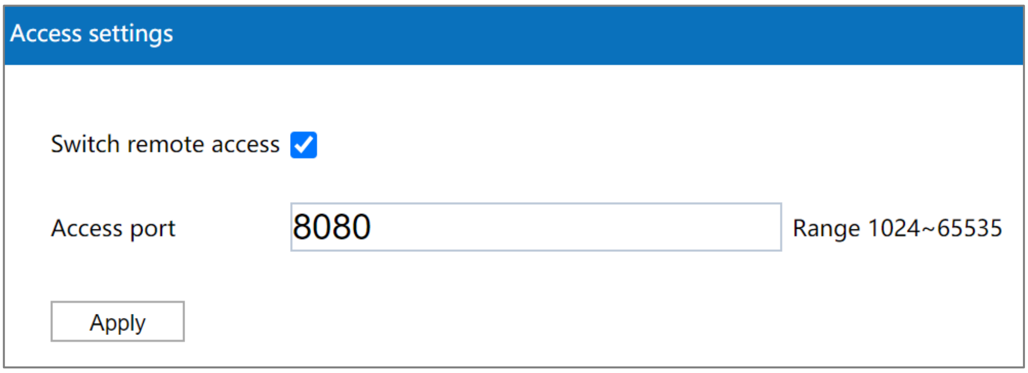
On the “Access Settings” page of the system tool, you can set the switch and port for remote access. The remote access function of Port 8080 (WWW service) is enabled by default. The WEB page of the device can be accessed through the extranet.

Operation Path

Open in order: "System Tools > Access Settings".

Interface Description

Access settings interface as follows:



Access settings

Switch remote access ☑

Access port 8080 Range 1024~65535

The main elements configuration description of access settings interface:

Interface Element	Description
Switch remote access	Enable or disable remote access.
Access port	Remote access port.
Apply	Save the settings.

8.7 System Upgrading

Function Description

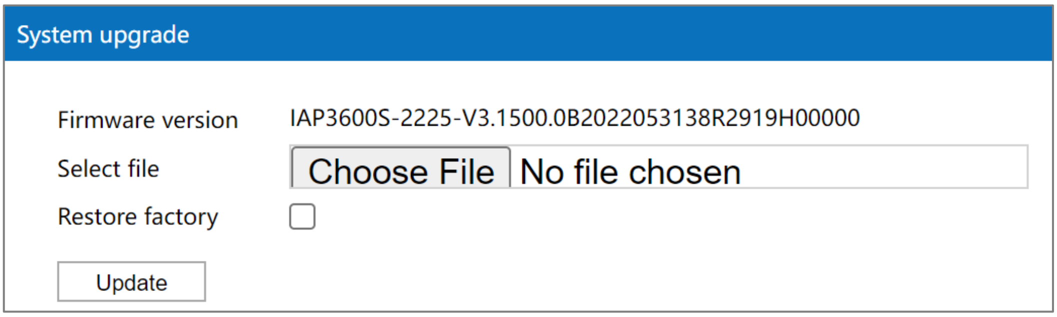
On the "System upgrade" page of system tools, user can update the device system program via firmware upgrade.

Operation Path

Please open in order: "System Tools > System upgrade".

Interface Description

System upgrade interface as follows:



System upgrade

Firmware version IAP3600S-2225-V3.1500.0B2022053138R2919H00000

Select file Choose File No file chosen

Restore factory □

Update

The main element configuration description of system upgrade interface:

Interface Element	Description
Firmware version	Program version used by current device.
Select file	Click "Select file" to select local upgrade file of the host. Note: Please select the program version that is compatible with the current hardware during upgrading.
Update	The button of "Update" to upgrade the device program. Notice: It takes a while during the upgrade process. Do not power off the device.
Restore Factory	Restore factory settings check box, if checked, the system will be restored to factory configuration after successful upgrade; If unchecked, the configuration of the device will remain unchanged and the firmware version information will change after the system upgrade succeeds.

8.8 Config Update

Function Description

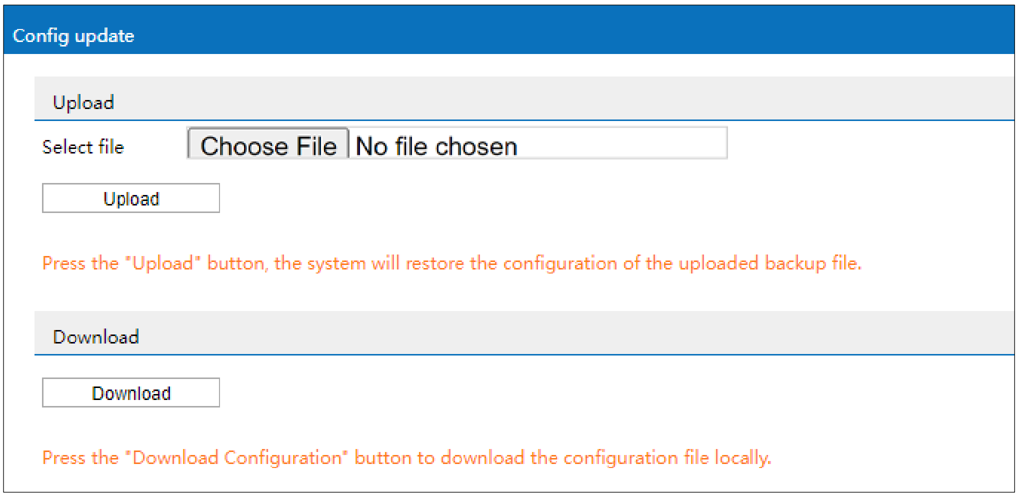
On the "Config update" page of system tools, user can conduct download, upload configuration for the device.

Operation Path

Please open in order: "System Tools > Config Update".

Interface Description

Configuration update interface is as follows:



Press the "Upload" button, the system will restore the configuration of the uploaded backup file.

Press the "Download Configuration" button to download the configuration file locally.

The main element configuration description of config update interface:

Interface Element	Description
Select file	The "Select file" button allows user to select the backup configuration file for the host.
Upload	The "Upload" button to upload the backup configuration file to the current device, so that the device can restore the configuration in the backup file.
Download	Click the "Download" button to download the configuration file of the current device locally and save it in the format of ".file".

8.9 System Management

Function Description

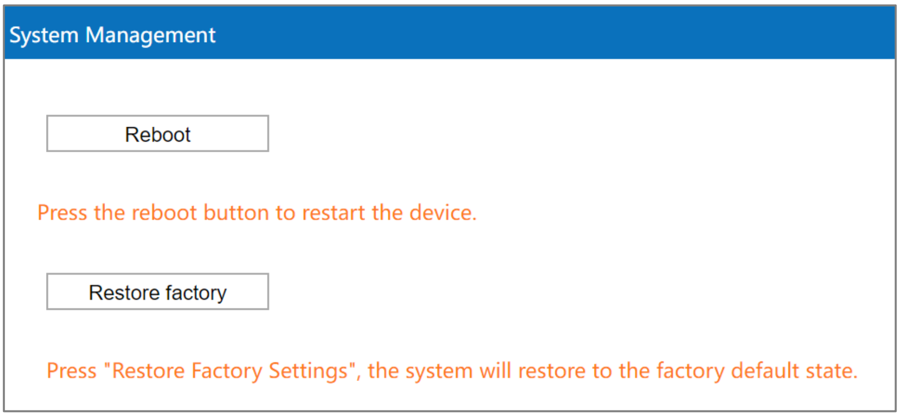
On the system tool "System Management" page, you can restart the device online and restore the factory settings.

Operation Path

Open in order: "System Tools > System Management".

Interface Description

The system management interface is as follows:



System Management

Press the reboot button to restart the device.

Press "Restore Factory Settings", the system will restore to the factory default state.

The main element configuration description of system management interface:

Interface Element	Description
Reboot	Click "Reboot" to restart the device.
Restore Factory	Click the "Restore factory" button, the device will be restored to the default state of factory defaults.

8.10 System Log

Function Description

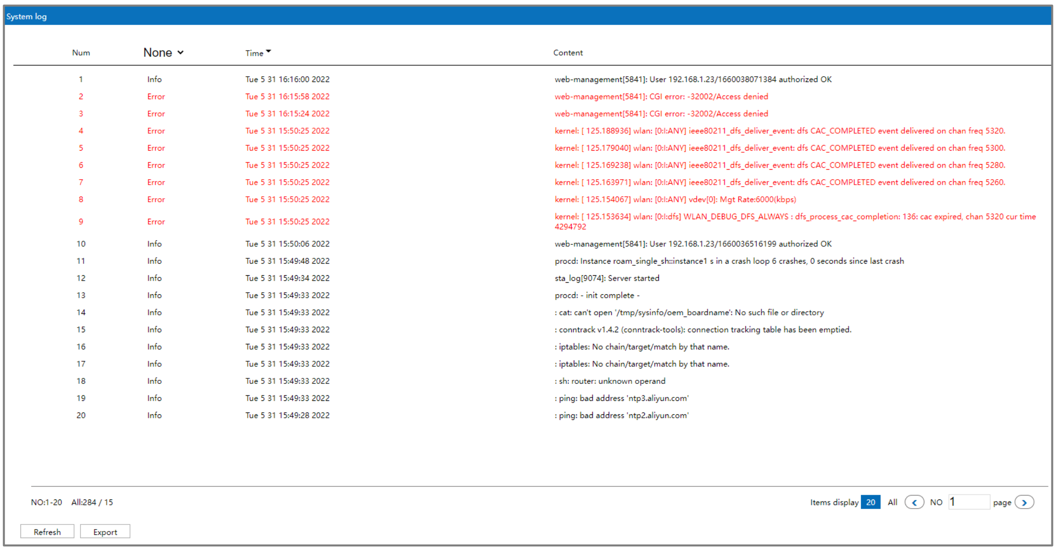
On the "System Log" page of system tools, user can check the device system log message.

Operation Path

Please open in order: "System Tools > System Log".

Interface Description

The system log interface is as follows:



Num	None	Time	Content
1	Info	Tue 5 31 16:16:00 2022	web-management[5841]: User 192.168.1.23/1660038071384 authorized OK
2	Error	Tue 5 31 16:15:58 2022	web-management[5841]: CGI error: -32002/Access denied
3	Error	Tue 5 31 16:15:24 2022	web-management[5841]: CGI error: -32002/Access denied
4	Error	Tue 5 31 15:50:25 2022	kernel: [125.188936] wlan: [0:I:ANY] ieee80211_dfs_deliver_event: dfs CAC_COMPLETED event delivered on chan freq 5320.
5	Error	Tue 5 31 15:50:25 2022	kernel: [125.179040] wlan: [0:I:ANY] ieee80211_dfs_deliver_event: dfs CAC_COMPLETED event delivered on chan freq 5300.
6	Error	Tue 5 31 15:50:25 2022	kernel: [125.169238] wlan: [0:I:ANY] ieee80211_dfs_deliver_event: dfs CAC_COMPLETED event delivered on chan freq 5280.
7	Error	Tue 5 31 15:50:25 2022	kernel: [125.163971] wlan: [0:I:ANY] ieee80211_dfs_deliver_event: dfs CAC_COMPLETED event delivered on chan freq 5260.
8	Error	Tue 5 31 15:50:25 2022	kernel: [125.154067] wlan: [0:I:ANY] vdev[0]: Mgt Rate:6000(kbps)
9	Error	Tue 5 31 15:50:25 2022	kernel: [125.153634] wlan: [0:I:dfs] WLAN_DEBUG_DFS_ALWAYS : dfs_process_cac_completion: 136: cac expired, chan 5320 cur time 4294792
10	Info	Tue 5 31 15:50:06 2022	web-management[5841]: User 192.168.1.23/1660036516199 authorized OK
11	Info	Tue 5 31 15:49:48 2022	procd: Instance roam_single_sh::instance1 s in a crash loop 6 crashes, 0 seconds since last crash
12	Info	Tue 5 31 15:49:34 2022	sta_log[9074]: Server started
13	Info	Tue 5 31 15:49:33 2022	procd: - init complete -
14	Info	Tue 5 31 15:49:33 2022	: cat: can't open '/tmp/sysinfo/oem_boardname': No such file or directory
15	Info	Tue 5 31 15:49:33 2022	: conntrack v1.4.2 (conntrack-tools): connection tracking table has been emptied.
16	Info	Tue 5 31 15:49:33 2022	: iptables: No chain/target/match by that name.
17	Info	Tue 5 31 15:49:33 2022	: iptables: No chain/target/match by that name.
18	Info	Tue 5 31 15:49:33 2022	: sh: router: unknown operand
19	Info	Tue 5 31 15:49:33 2022	: ping: bad address 'ntp3.aliyun.com'
20	Info	Tue 5 31 15:49:28 2022	: ping: bad address 'ntp2.aliyun.com'

The main element configuration description of system log interface:

Interface Element	Description
Num	Log messages display sequence.
None	Log message type, options as follows: ● NONE: display all information; ● Warning: alarm information; ● Error: error information.
Time	The date and time filter button for log information. Note: Click the "Time" button to filter the start date and end date.
Content	A detailed description of the log contents.
Refresh	Click "Refresh" to regain the newest log messages of the device. Note: System log can store maximum 256KB log messages of the device in the most recent period.
Export	Click "Export" to save the log messages to the local host in the form of ".txt".
Items display	"Items display" button, log information display mode, options as follows: ● 20: Display 20 log messages per page; ● All: Single page displays all log information.

8.11 Log Manage

Function Description

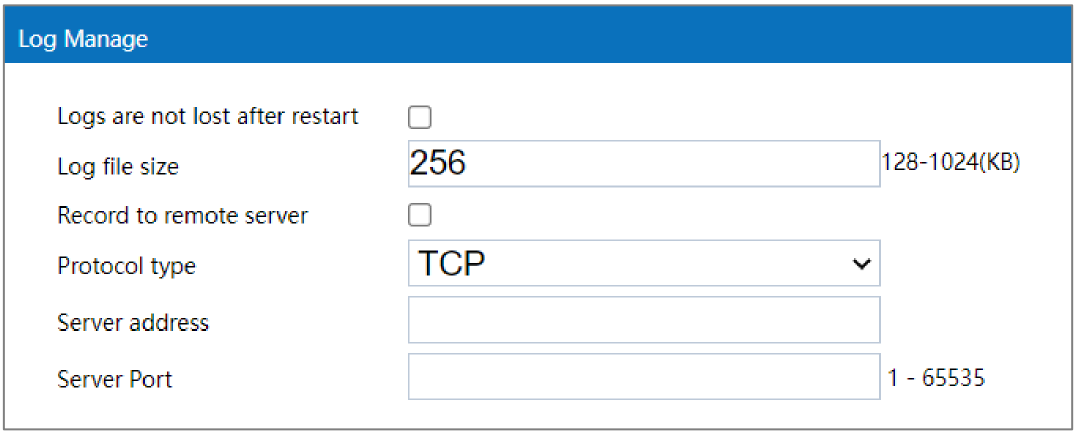
On the “Log Management” page of the system tool, you can synchronize the device system log information to the remote log server.

Operation Path

Open in order: "System manage > Log manage".

Interface Description

The log management interface as follows:



Log Manage

Logs are not lost after restart □

Log file size 256 128-1024(KB)

Record to remote server □

Protocol type TCP

Server address

Server Port 1 - 65535

The main elements configuration description of log management interface:

Interface Element	Description
Log are not lost after restart	When checked, the log will not be lost after the device is restarted.
Log file size	The storage size of system log files is limited, and the value range is 128-1024KB.
Record to remote server	When checked, the system log information can be synchronized to the specified log server.
Protocol type	The protocol type used to record log information to the remote server is as follows: ● TCP ● UDP.
Server Address	IP address of the syslog server.
Server Port	The port number of the syslog server, value range is 0-65535.

9 Diagnostic Tools

9.1 Ping Test

Ping belongs to a communication protocol and is part of the TCP/IP protocol. User can adopt the ping command to check whether the network is connected, which can help us analyze and determine network faults.

Function Description

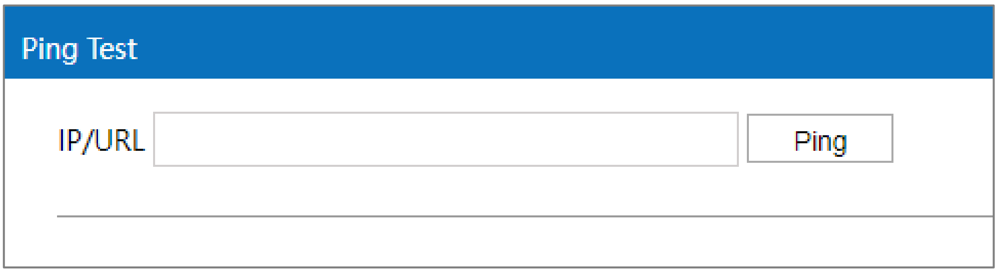
On the page of "Ping test", user can detect whether the target host can be connected.

Operation Path

Open in order: "Diagnostic tools > Ping test".

Interface Description

The Ping test interface as follows:



The main elements configuration description of Ping test interface:

Interface Element	Description
IP/URL	Target IP/URL address information to be detected.
Ping	Click the “Ping” button to start the test, and the test result is displayed below.

9.2 Route Tracking

Route Tracking is a route-tracking utility that determines the path taken by an IP datagram to access a destination. The Route Tracking command uses the IP Time to Live (TTL) field and ICMP error messages to determine the route from one host to other hosts on the network.

Function Description

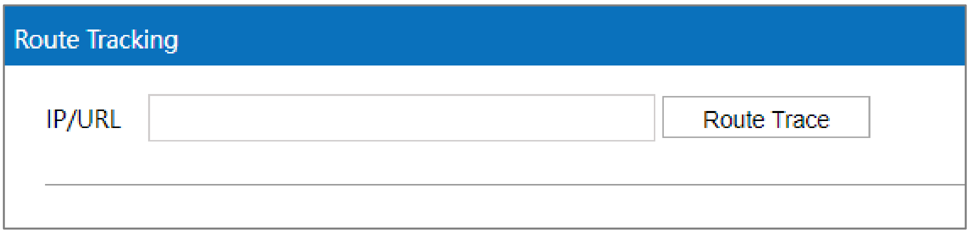
On the page of "Route Tracking", user can perform route tracking for the target host.

Operation Path

Open in order: "Diagnostic tools > Route tracking".

Interface Description

The route tracking interface is as follows:



The main elements configuration description of route tracking interface:

Interface Element	Description
IP/URL	Destination IP/URL address that requires route tracking.
Route Trace	Click the "Route Trace" button to start tracking, and the test results are displayed below.

10 FAQ

1. **Why is the signal strength very good, but the throughput is very low?**

   Sometimes, during the throughput test, it is found that the signal strength of connection is very strong (> 30dbm), but the tested throughput is very low, and even disconnection occurs. A common misconception is that the stronger the signal, the better the quality. This is not true. Signal quality and signal strength are not positively correlated. The signal strength has a saturation RSSI. When the signal strength is above this threshold, the received signal is excessively saturated and the receiver is unable to demodulate, leading to a significant decrease of throughput and even disconnection. This problem can be solved by reducing the AP power or increasing the attenuation between the AP and the client.

2. **Why do some 5G client devices fail to scan the 5G SSID of AP?**

   5G has three frequency bands: high, medium and low. Different countries support different frequency bands. Some support two of them and some only support one of them. Therefore, when AP works in the frequency band that the client does not support, the client cannot scan the SSID of AP, and another client that supports this frequency band can scan it. Another possible reason is the problem mentioned in FAQ 1, that is, the signal is too strong, which will also lead to the failure to scan the SSID. This situation usually occurs when the feeder directly connects the AP to the client without adding an appropriate attenuator.

3. **Why is the near throughput of an outdoor AP worse than an indoor AP?**

   This is determined by the nature of the outdoor AP antenna. The antenna of outdoor AP is different from that of indoor AP. Its advantage lies in long-distance transmission. It is a normal phenomenon that the throughput of an outdoor AP is slightly worse than an indoor AP in the short distance transmission (within 50 meters).

4. **What is a universal bridging?**

   Universal bridging is a way to bridge an AP and a client by creating a proxy forwarding mechanism. Instead of putting the wired network port and the wireless network port in the same bridge, it modifies the policy routing table to make all the host devices connected establish forwarding relationship with the wireless network port, and let the wireless port agent forward data packets, ARP and DHCP packets. In other words, it realizes the soft bridging between wireless port and wired port.

5. **When should universal bridging and WDS be used?**

   General bridge and client mode use WDS to bridge with AP, but WDS does not have a standard protocol, different wireless chip manufacturers implement WDS in different ways, resulting in the WDS bridge of different manufacturers have serious compatibility problems, the phenomenon is unable to bridge or bridge can not communicate. Universal bridging has no compatibility issues, but due to its nature, is not suitable for networks involving routing learning (such as OSPF networks) and is only suitable for simple application scenarios. Therefore, WDS is preferred if WDS is compatible and universal bridging is preferred if WDS is not compatible. At present, the company's self-developed wireless products are all Qualcomm solutions. They have no compatibility problems. Therefore, if both the AP end and the client are our self-developed products, WDS can be used.

6. **Why does throughput not improve after 2.4G is changed from 20M to 40M?**

   In an environment with severe interference, if 2.4G is changed from 20M to 40M, the throughput may not improve, or even get worse. Because there are only 13 channels in 2.4G, each channel is 5M, and all the channels add up to 65M, while a signal of 40M occupies 40M. Therefore, if there are 2.4G signals of similar channels nearby, serious interference problems will inevitably occur due to channel overlap, leading to the throughput failure. Therefore, in the environment with severe interference, 20M is recommended for 2.4G.

7. **How do I access a device when an Intranet IP is acquired dynamically but not connected to a DHCP server?**

   When the self-developed product fails to obtain the address allocated by the DHCP server within 1 minute, a default IP address will be set automatically. The IP address is 192.168.1.254, and you can use this address to access the device. When the device obtains the address allocated by the DHCP server, the default

IP would be automatically overwritten.

11 Maintenance and Service

Since the date of product delivery, our company provides five-year product warranty. According to our company's product specification, during the warranty period, if the product exists any failure or functional operation fails, our company will repair or replace the product for users free of charge. However, the commitments above do not cover damage caused by improper usage, accident, natural disaster, incorrect operation or improper installation.

In order to ensure that consumers benefit from our company's wireless AP, consumers can get help and solutions in the following ways:

- Internet Service;
- Service Hotline;
- Product repair or replacement;

11.1 Internet Service

More useful information and tips are available via our company website.
Website: http://www.3onedata.com

11.2 Service Hotline

Users of our company's products could call technical support office for help. Our company has professional technical engineers to answer your questions and help you solve the product or usage problems ASAP. Free service hotline: +86-4008804496

11.3 Product Repair or Replacement

As for the product repair, replacement or return, customers should firstly confirm with the company's technical staff, and then contact the salesmen to solve the problem. According to the company's handling procedure, customers should negotiate with our company's technical staff and salesmen to complete the product maintenance, replacement or return.

3onedata Co., Ltd.
Headquarter Address: 3/B, Zone 1, Baiwangxin High Technology Industrial Park, Song Bai Road, Nanshan District, Shenzhen, 518108, China
Technology Support: tech-support@3onedata.com
Service Hotline: 4008804496
Official Website: http://www.3onedata.com