KyAir800E

Industrial Wireless AP WEB Operation Manual

Publication Date：2024 January 2024

Version：V1.0

KYLAND

Disclaimer

Beijing Kyland Technology Co., Ltd. strives to ensure the information in this manual is as accurate and up-to-date as possible. However, the company cannot guarantee that this manual is entirely free of technical or typographical errors and reserves the right to make changes without notifying users.

Publication: Beijing Kyland Technology Co., Ltd.

Website:

http://www.kyland.com.cn

http://www.kyland.cn

Customer Service Hotline:

010-88796676

Fax: 010-88796678

Email:services@kyland.com.cn

Table of Contents

Manual Conventions

1、Text Format Conventions

Format	Description
< >	Content within < > indicates a button name, e.g., “Click <Apply> button.”
[ ]	Content within [ ] indicates a window or menu name, e.g., “Click [File] menu item.”
{ }	Content within { } indicates a combination, e.g., {IP address, MAC address} means that IP address and MAC address are a pair and can be configured or displayed together.
→	Indicates multilevel menus, e.g., “Start → Programs → Accessories” refers to the [Programs] submenu under the [Start] menu, leading to the [Accessories] menu item.
/	Indicates a choice between two or more options, e.g., “Add/Subtract” means either add or subtract.
~	Indicates a range, e.g., “1~255” means a range from 1 to 255.

2、Command Line Format Conventions

Format	Description
Bold	Command line keywords that should be entered exactly as shown, e.g., **show version** displays the software version of the switch.
Italic	Command line parameters that must be replaced with actual values, e.g., **show vlan** vlan id displays VLAN information for the VLAN ID specified by vlan id.

3、Symbol Conventions

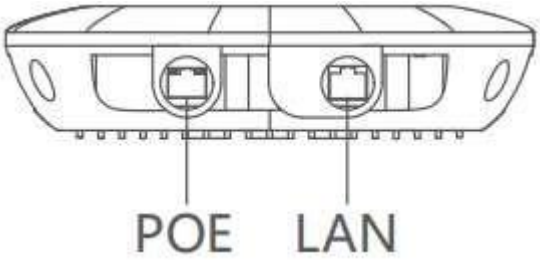
Format	Description
Caution	Highlights considerations or supplementary descriptions for the operation or configuration.
Note	Provides necessary explanations of the operation’s content.
Warning	Indicates critical points that require extra attention. Incorrect operations may lead to data loss or device damage.

Product Version Description

Software Version	Release Date	Date Revised	Author
V1.0.29	2023-4-26	Initial Creation	Guo Liwei

1 Product information

1.1 Interface Description



Schematic diagram of the device interface

Schematic diagram of the power adapter interface

Table 1 Interface Description

Object	Interface	Name	Description
KyAir800E Device	POE	Equipment power supply interface	Connect the network cable to the POE port on the power adapter for power supply and data transmission.
	LAN	Data transmission interface	Connects to network devices such as switches through network cables.
Power adapter	POE	Equipment power supply interface	Connects to the POE port of the device through a network cable.
	LAN	Data transmission interface	Connects to network devices such as switches through network cables.

1.2 Line connection

Installation diagram:

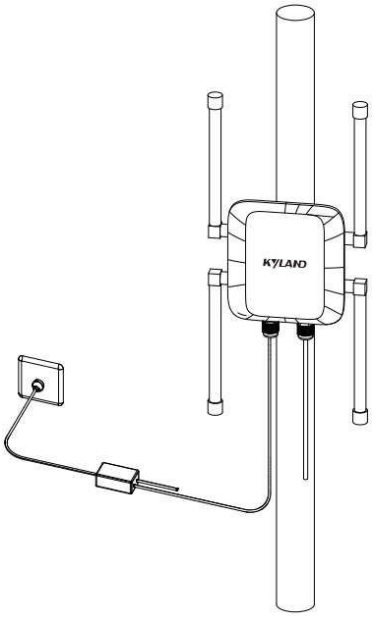


Figure 3 Line connection

1.3 Default Parameters

Table 2 Main parameters of default factory Settings

Item	KyAir800E
IP Address	IPv4 dynamic (Default alternate address: 192.168.10.1)
Username	admin
Password	123
Wireless mode	Access point
Security Mode	WPA2-PSK/WPA3-SAE
Key	kyland1234

2 Quick Configuration

2.1 Log in

Before logging in, you need to configure the PC connected to the device to ensure that the IP addresses of the PC and the device are on the same network segment. Perform the following operations (using Windows10 as an example) :

1. Right-click the network icon in the taskbar, click to open "Network and Internet Settings", and the window as shown in the following picture will pop up:

Figure 4 Network Status Page

2. Click Change Adapter Options -> Ethernet -> Properties to enter the property configuration page, as shown below:

Figure 5 Local connection properties

3. Double-click Internet Protocol version 4 (TCP/IPv4) to bring up the window shown below:

Figure 6 IP Settings

4. Set the IP address to an IP address in the same network segment as the device, and the IP address cannot be the same as that of the device. For example, if the default IP address of the device is IPv4 dynamic, and the DHCP server is deployed on the link, the host can use the Obtain an IP Address automatically mode. If the DHCP server is not available, the device has the default standby IP address 192.168.10.1. In this case, set the host IP address to a static IP address, for example, 192.168.10.110.

5. In the address bar of the browser, enter the default standby IP address 192.168.10.1 (if a DHCP server is deployed, enter the dynamic IP address), and press Enter to switch to the page shown in the following figure.

Fig. 7 Device login screen

6. Enter the default password 123 in the password box. Click the login button to switch to the device page (default user name: admin).

2.2 Wizard to configure wireless association

The wizard page allows you to quickly configure the wireless association between the two devices (this can also be configured on the Wireless Settings page, see Chapter 4, sections 4.1-4.2 for details). The device supports four modes: Access Point, Client, Access Point (WDS), and Client (WDS). Access Point and Client are paired, and Access Point (WDS) and Client (WDS) are paired.

Caution：

After the wizard configuration is complete, all wireless and network parameters except those modified in the wizard configuration are restored to their initial

2.2.1 Configuring the Access Point

（1）After successful login, the Status Display page is displayed by default. Click "Wizard" in the upper right corner to enter the "Wizard - Network" page, as shown below. To prevent IP conflict, change the IPv4 address.

Figure 8 Wizard - Network - Default

(2) Click "Next" to enter the "Wizard - Wireless" page, showing the basic wireless parameters of 2.4G and 5G devices, as shown in the figure below. For example, change the network name of Wireless (2.4Gwifi) and wireless (5Gwifi) to 2Glink and 5Glink respectively, and set the key to 12345678. Others can remain unchanged (default wireless mode is access point, channel width is 160/80/40/20MHz, frequency (channel) is automatic, safe mode is WPA2-PSK/WPA3-SAE). The above parameters can be set as required.

Figure 9 Wizard - Wireless

(3) Continue to click "Next" to enter the "Wizard - Completion" page, as shown below. Click the "Finish" button to save all the Settings, or click "Back" to change the previous configuration.

Figure 10 Wizard-Complete

The access point is configured.

2.2.2 Configuring the client

（1）After successful login, the Status Display page is displayed by default. Click "Wizard" in the upper right corner to enter the "Wizard - Network" page, as shown below. To prevent IP conflict, change the IPv4 address.

Caution：

The client device and the access point device cannot be configured with the same IP address to prevent address conflict.

Figure 11 Wizard - Network

（2）Click "Next" to enter the "Wizard - Wireless" page, showing the basic wireless parameters of 2.4G and 5G, as shown below. Change the wireless mode of the wireless band to be used to the client (you are not advised to change it to the client for both 2.4G and 5G), and set the network name, security mode, and key to the same as that of the access point to be associated. For example, to access the access point of the 5G band network named 5Glink

modified before the planned access, change "Wireless (5Gwifi)" to the client mode, the network name to 5Glink, the security mode to WPA2-PSK/WPA3-SAE, and the key to 12345678, which are consistent with the access point. Retain the default values for other parameters.

Figure 12 Wizard - Wireless

(3) Continue to click "Next" to enter the "Wizard - Completion" page, as shown below. Click the "Finish" button to save all the Settings, or click "Back" to change the previous configuration.

Figure 13 Wizard-Complete

When the configuration of the client is completed, you can see the association information on the “Status - Connected Wireless Device Information” page, and the client and the access point with the network name of 5Glink are connected successfully.

网络名称	RSSI/底噪	IPv4地址	MAC	TX/RX速率	CCQ	802.11模式	连接时长
5Glink	-42/-106	192.168.1.12	9C:B7:93:89:9C:02	2161.8 Mbps / 2882.4 Mbps	85%	802.11ax	00:01:19

Figure 14 Client-connected wireless device information

2.2.3 Configuring Access Points (WDS)

As in 2.2.1, change the access point mode to Access Point (WDS) mode.

2.2.4 Configuring Client (WDS)

As in 2.2.2, change the client mode to Client (WDS) mode.

3 Status

The default display page after successfully logging into the interface is the Status page. This page shows some of the current configuration parameters and provides real-time monitoring of the device's operating status. It includes subpages for Information, Statistics, Network, and Logs.

3.1 Status - Information Page (Mesh Mode)

The Status - Information Page (Mesh Mode) displays the current configuration details of the device, including:Mesh topology diagram, device information, network information, wireless information, and connected wireless device information.:

Mesh Topology Diagram: Displays the current status of the CAP and RE devices and whether they have formed a Mesh network.The connection between the CAP and RE is represented by a green line.The connection between the CAP and RE is represented by a green line.After the network is formed, clicking on a Mesh-connected device (RE) icon in the CAP's topology diagram allows you to directly jump to the login page of the corresponding RE device by clicking its IP address.

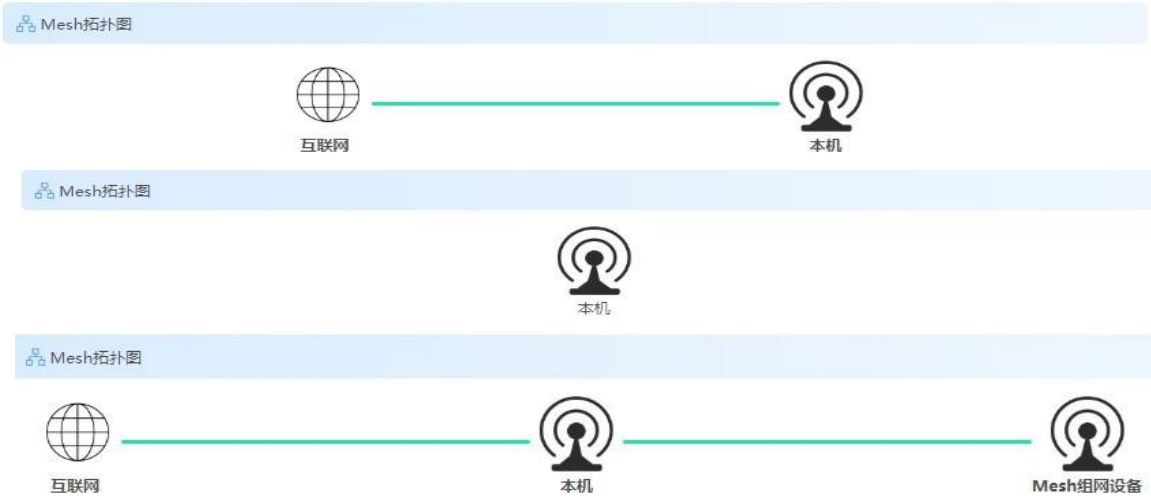


Figure 15 Mesh topology -CAP mode

Figure 16 Mesh topology -RE mode

Figure 17 Mesh topology -CAP- Association status

Figure 18 Mesh topology -RE- Association status

3.2 Status - Information Page (Standard Mode)

The Status - Information Page (Standard Mode) displays the current configuration details of the device, including:

Device Information: The system information of the device, including device name, model, firmware version, uptime, and system time.

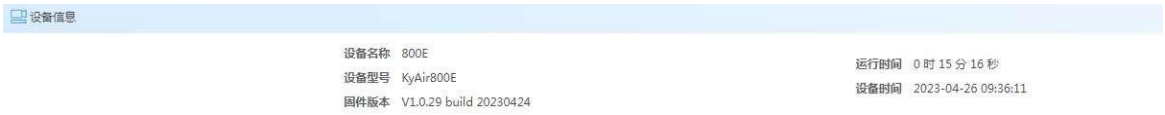


Figure 19 Device information

Network Information:

The network-related information of the device, including network mode, IP address, etc., which can be configured in Settings > Network Settings.

Figure 20 Network information

Wireless Information: Displays the 2.4G and 5G wireless information of the device, including SSID, wireless mode, frequency, security mode, etc., which can be configured in Settings > Wireless Settings.

Figure 21 Wireless information

Connected Wireless Device Information:

Displays information about connected devices, including SSID, RSSI (signal strength), IPv4 address, MAC address, TX/RX rates (transmit/receive speeds), and connection duration.

网络名称	RSSI/底噪	IPv4地址	MAC	TX/RX速率	CCQ	802.11模式	连接时长
whc-899C03	-44/-104	192.168.1.14	9C:B7:93:AA:BB:CC	3458.8 Mbps / 2882.4 Mbps	79%	802.11ax	00:10:44

Figure 22 Connected wireless device information

3.3 Status - Statistics Page

This page shows the network interface and traffic statistics of the device, measuring the amount of data transferred over the network in a given period, which is a key metric for network performance.

Network Interface Statistics:

Shows the number of bytes and packets sent and received through wired and wireless interfaces.

网络接口统计

接口名称	MAC地址	接收字节数	发送字节数	接收数据包个数	发送数据包个数	接收数据包错误	发送数据包错误
有线口							
eth0	9C:B7:93:99:CC:01	14650378 Byte	42703169 Byte	106584	101004	0	0
eth1	9C:B7:93:89:9C:02	0 Byte	0 Byte	0	0	0	0
无线口							
ath0	9C:B7:93:89:9C:03	0 Byte	0 Byte	0	0	0	0
ath1	9C:B7:93:66:99:04	0 Byte	0 Byte	0	0	0	0

Figure 23 Network interface statistics

Traffic Statistics:

Includes wired and wireless traffic statistics, showing real-time TX and RX (transmit and receive) traffic in graph form for better clarity.

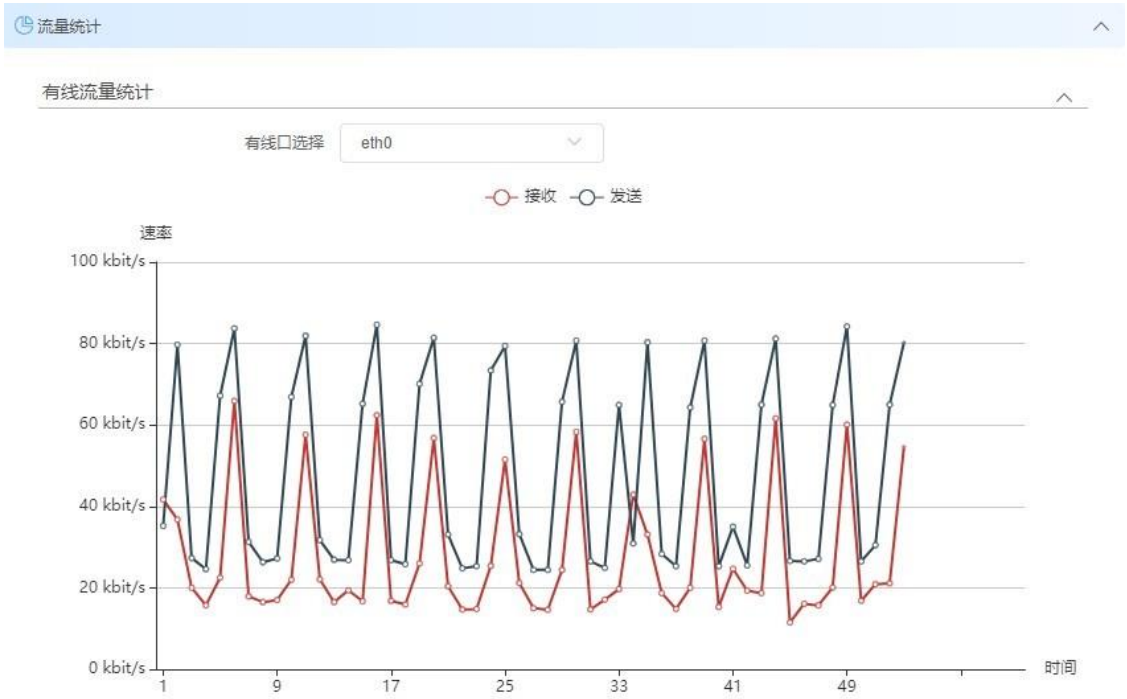


Figure 24 Traffic statistics

3.4 Status - Network Page

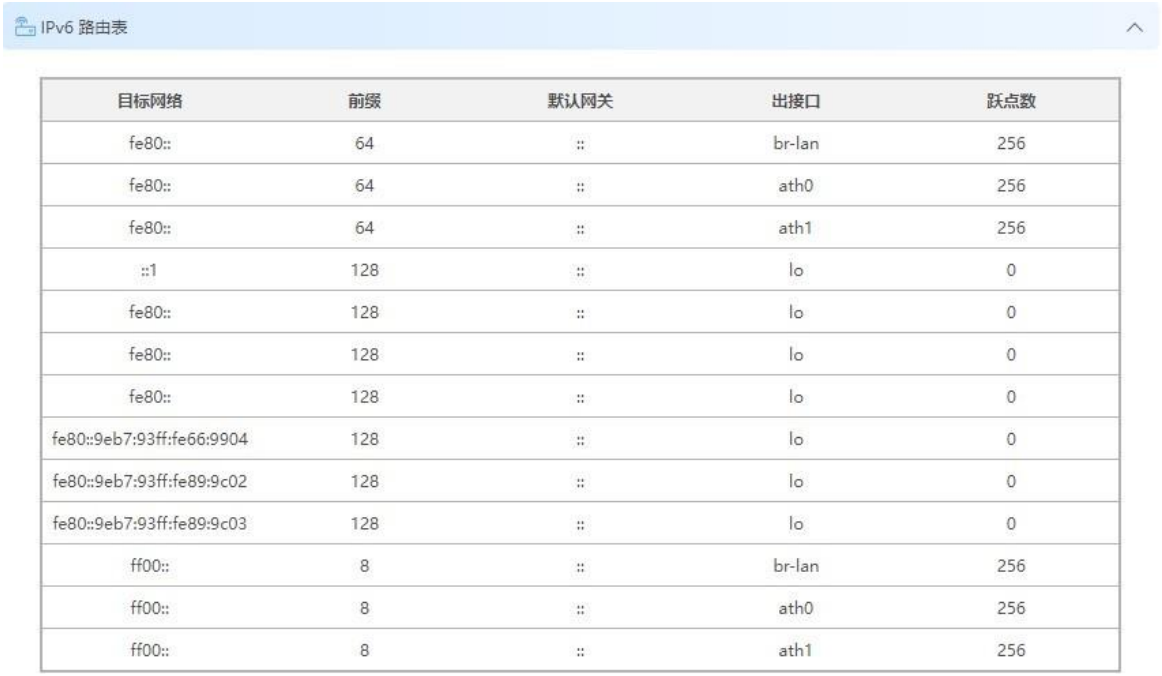
This page displays the device's routing table, ARP table, and bridge device list.

Routing Table: Stores the paths leading to the network to which the device is connected.

IPv4 路由表

目标网络	子网掩码	默认网关	出接口	跃点数
0.0.0.0	0.0.0.0	192.168.1.220	br-lan	0
192.168.1.0	255.255.255.0	0.0.0.0	br-lan	0
224.0.0.0	240.0.0.0	0.0.0.0	br-lan	0

Figure 25 IPv4 routing table


IPv6 路由表

目标网络	前缀	默认网关	出接口	跃点数
fe80::	64	::	br-lan	256
fe80::	64	::	ath0	256
fe80::	64	::	ath1	256
::1	128	::	lo	0
fe80::	128	::	lo	0
fe80::	128	::	lo	0
fe80::	128	::	lo	0
fe80::9eb7:93ff:fe66:9904	128	::	lo	0
fe80::9eb7:93ff:fe89:9c02	128	::	lo	0
fe80::9eb7:93ff:fe89:9c03	128	::	lo	0
ff00::	8	::	br-lan	256
ff00::	8	::	ath0	256
ff00::	8	::	ath1	256

Figure 26 IPv6 routing table

ARP Table: Records the mapping between used IP addresses and MAC addresses.


ARP 表

IP地址	MAC地址	接口
192.168.1.220	00:E0:4C:67:34:C7	br-lan

Figure 27 ARP table

Bridge Device List:

Lists the MAC addresses of other devices communicating through the device within 300 seconds and their aging times.


桥接设备列表

MAC地址	老化时间
9C:B7:93:AA:BB:CC	1秒
9C:B7:93:99:CC:01	0秒
9C:B7:93:89:9C:03	0秒
9C:B7:93:89:9C:02	0秒
9C:B7:93:66:99:04	0秒
3C:97:0E:84:1B:D9	6秒
00:E0:4C:67:34:C7	0秒

Figure 28 List of bridging devices

3.5 Status - Logs

This page displays the log information of the device.

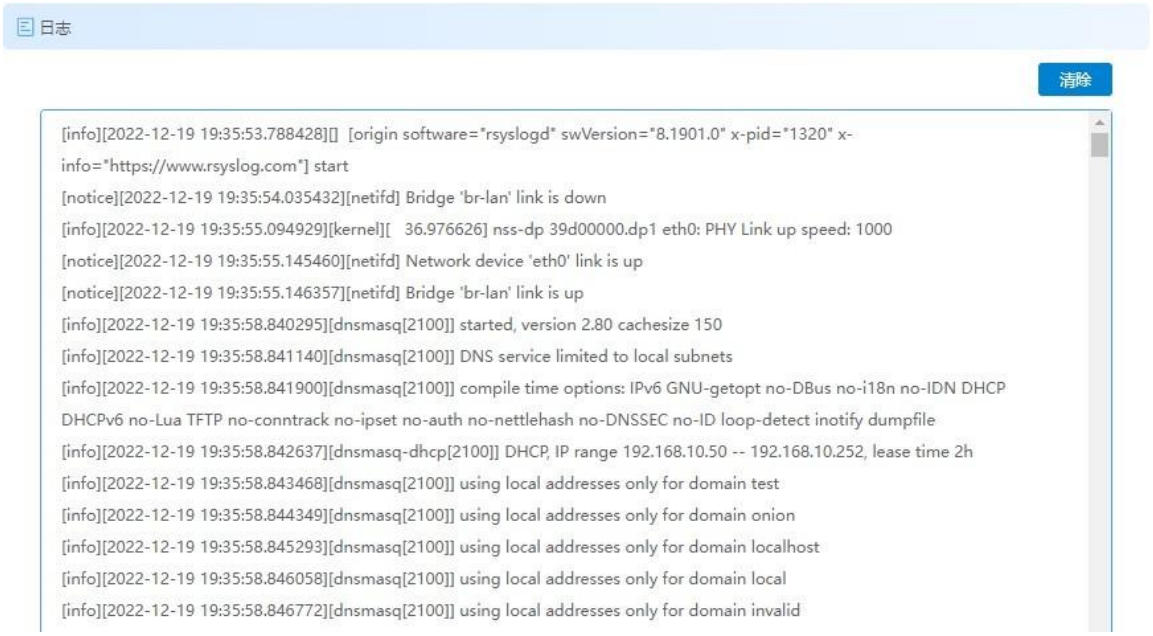


Figure 29 Status - Logs

4 Settings

The Settings page allows detailed configuration of the device, including Wireless Settings, Network Settings, Traffic Management, Service Settings, and System Settings.

4.1 Wireless Settings

4.1.1 Wireless Settings - Standard Mode

In Standard Mode (i.e., Mesh Mode is disabled), the wireless settings page is shown as below (5G as an example):

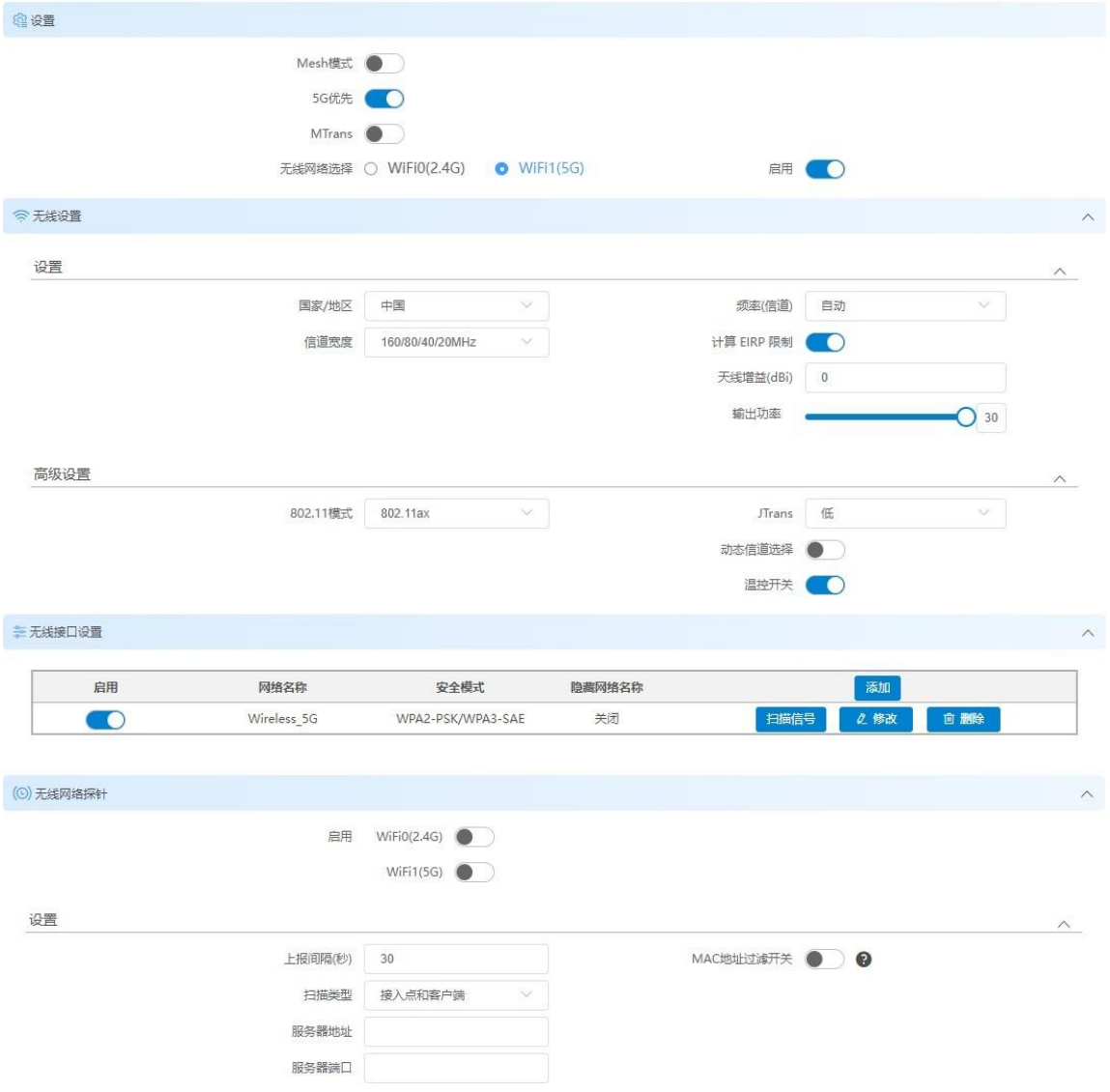


Figure 30 Wireless Setup - 5G Access Point Mode

Settings: For selecting wireless networks, the device supports **2.4G** and **5G bands.**

When enabled, the corresponding band can be configured; when disabled, the band is turned off.

Mesh Mode: When Mesh Mode is enabled, the device enters Mesh Mode, and wireless configurations revert to Mesh defaults. Clicking Add Node in CAP or RE starts Mesh network formation. Disabling Mesh Mode restores the device to Standard Mode with default wireless settings.

5G Priority: Enabled by default, this feature works only when 2.4G and 5G SSIDs are the same. It ensures that wireless terminals prioritize connecting to the 5G band.

MTrans (Seamless Roaming): This feature works only in client mode, ensuring all 2.4G and 5G wireless interfaces are not in access point mode.

Figure 31 Wireless Settings -Mtrans

Minimum Signal Strength for Operation: The threshold value for roaming switching; roaming occurs only if the signal strength drops below this value. The result depends on the signal strength difference.

Signal Strength Difference: Roaming succeeds only when the signal strength of the new frequency band is greater than: minimum signal strength + signal strength difference.

Example: If the current 5G signal strength is -50, roaming occurs when it drops below -55 (minimum signal strength). It succeeds only if the 2.4G signal exceeds -45 (-55 + 10).

Wireless Settings Page: The wireless settings page contains Basic Settings and Advanced Settings, allowing the following configurations:

Country/Region: : Different standards apply to different regions; select the

appropriate country code.

Channel Width: Limits the upper and lower frequency range allowed on the channel. Default is automatic in client mode.

Frequency (Channel): Center frequency of the carrier; must match between access points and clients.

Auto Channel List: Configurable when the frequency is set to automatic, controlling the range of working channels.

Output power: the power of the device transmitting wireless signals, users adjust it according to the distance between the devices, when the output power is increased, the signal strength will be improved, so as to increase the transmission distance of the device.

802.11 mode: 2.4G wireless support 802.11b/g/n, 802.11ax, the default is 802.11ax, 5G support

802.11a/n, 802.11ac, 802.11ax, the default is 802.11ax (Note: some countries and regions do not support it)

802.11AX).

JTrans: After it is enabled, it will interfere with other devices on the same channel indiscriminately, and the wireless service of the interfered device will not be available. The interference capability decreases according to the different levels of high, medium, and low. When it is low, this function has basically no impact. When it is high, the interference ability is the highest

If yes, the interfered device may be disconnected. Enable this function with caution.

Dynamic channel selection (DCS): Dynamic channel selection is a function that detects and avoids interference. When the bottom noise or interference of the channel reaches a certain level, the device will dynamically switch to a channel with less interference. This function selects "Automatic" at the frequency

This function takes effect when there are multiple channels in the automatic channel list, and cannot be configured after a fixed channel or when there is only one channel in the automatic channel list.

Temperature control switch: The temperature control switch is enabled by default to prevent the CPU temperature from being too high and damaging the device due to high load.

Wireless Interface Setting: The wireless interface can be added, modified, deleted, and a maximum of 8 wireless networks can be added in a frequency band Interface. In the 2.4G wireless port Settings, two wireless ports are enabled by default. The network with MGMT in the following figure is the wireless management port. When a mobile phone or laptop is associated with this network port, it can access and manage the device, but cannot access the Internet. When a network port without MGMT in the network name is associated, the terminal can access the device and the Internet.

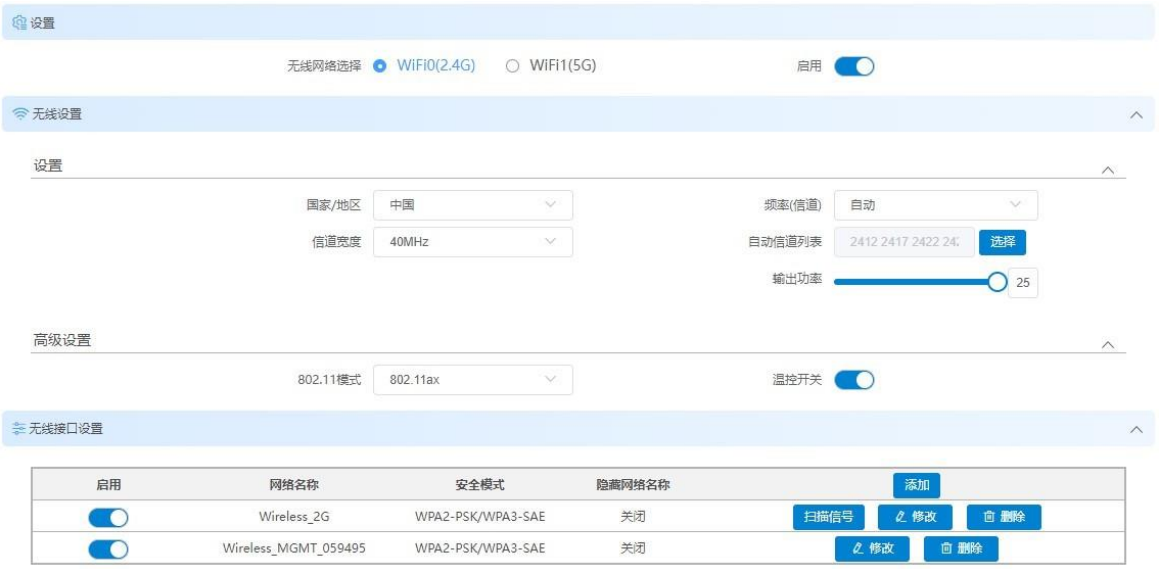


Figure 32 Wireless Settings - 2.4G access point

Caution：

Networks with “MGMT” cannot be restored via ''Add'' after deletion, but can be restored via the reconfiguration wizard.

To configure the wireless network, click "Modify" button, the following page will pop up.

Figure 33 Wireless interface Settings - Common wireless network 2G

Figure 34 Wireless Port Settings -MGMT Manages the wireless network

The following parameters can be set:

Network Name(SSID): The value used to control the access to the wireless network. When other devices connect to this device, only the same SSID can communicate with each other and establish a wireless connection. The network name can contain 1 to 32 characters (1 Chinese character3 digits), English, numbers and special symbols! @ # $% ^ & * () _ + - = < >? /:|[]{} '. And non-starting and ending Spaces.

Wireless mode: The device has four wireless modes, including access point, client, client (WDS), access point (WDS).

Caution :

Client mode and access point mode are used together, and client (WDS) and access point (WDS) are used together, not mixed.

Security Mode: Wireless encryption mode, support: open (no encryption), WPA2-PSK, WPA/WPA2 mixed -PSK, WPA2-PSK/WPA3-SAE four, users can choose the corresponding encryption according to their own security requirements WPA2-PSK/WPA3-SAE has the highest security.

Key: You need to enter the password when associated with the wireless, the key only supports 8~63 bits of upper and lower case English letters, numbers, special symbols! @ # $% ^ & * () _ + - = < >? /:[]{} '. And non-starting and ending Spaces.

Caution :

The network name, security mode, and password of the devices to be associated with each other must be the same. Otherwise, the devices cannot be associated with each

Hide Network name: Hide the wireless network name (SSID). Check this function, other mobile phones, computers and other terminals

The client device cannot search for the SSID of the access point device. This prevents the client device from being connected by others and does not affect its own use. (Only displayed on the access point page).

Client isolation: Enabling this feature prevents devices connected to the same access point device from communicating with each other, i.e

Duplicating the IP of each client will not have any effect on communication (only the access point page is displayed).

MAC address locking: In a network environment where there are multiple identical SSIDs around, the client device can specify the access point to be associated by setting the wireless MAC address locking of the corresponding access point (only displayed on the client page).

User speed Limit: Limits the uplink and downlink speeds of users associated with the device (only displayed on the access point page,

WDS access points do not support user rate-limiting functionality).

Maximum users: the access point limits the number of connected users by setting it (displayed only on the Access Point page).

Minimum access signal limit: The access point limits the minimum signal strength of the associated device by setting it, and devices with signal strength lower than the set value cannot be associated successfully; even if the association is successful, once the associated signal strength is lower than the set value, the client will be kicked off the access point device.

Minimum Access Signal Limit:The access point limits the minimum signal strength of the associated device by setting it, and devices with signal strength lower than the set value cannot be associated successfully; even if the association is successful, once the associated signal strength is lower than the set value, the client will be kicked off the access point device.

MAC Filtering: Allows devices inside or outside the list to communicate (only shown on the Access Point page).

802.11r: Implements roaming of wireless terminal devices through Fast BSS Transition. (Only WPA2-PSK security mode is supported).

Wireless Network Probe: Enable this function to locate the terminal. When the terminal (e.g. cell phone, computer, etc.) is within the signal coverage area of the device, the device can detect all the messages sent by the terminal and report them to the server to analyze and calculate the position of the terminal.

Location. The following parameters can be configured.

Figure 35 Wireless Settings - Wireless network probe

Report interval: indicates the interval at which data is reported to the server.

Scan Type: Indicates the type of terminal devices scanned by the device (access point, client, access point, and client). Server address: IP address of the server that receives data.

Server port: port of the server that receives data.

MAC address filtering switch: This switch is disabled by default. After this function is enabled, MAC address filtering is performed. Only device data matching the MAC address filtering rules is reported. Otherwise, data is discarded. A maximum of five filtering rules can be added and fuzzy matching is supported.

The following section describes how to configure wireless association between two devices (the wizard page can also be quickly configured, see section 2 Chapter 2.2), the device supports four modes: access point mode, client mode,

access point (WDS) mode, and client (WDS) mode. It is recommended that client mode and access point mode be used together, and access point (WDS) mode and client (WDS) mode be used together.

Caution :

During wireless association, the network name, frequency (channel), security mode, and key of the access point and client device must be consistent.

4.1.1.1 Configuring an Access Point

In the "Wireless Network" selection, tap the wireless band you want to use, such as "WIFI1(5G)".

Figure 36 Wireless network selection

Click Modify in Wireless Interface Settings and set the parameters as required, for example, change Network Name to Wireless_link, and click Finish to exit the current configuration window.

Figure 37 Wireless Interface Settings - Modify the SSID

Click "Save" in the upper right corner. The access point is configured.

Figure 38 Save

4.1.1.2 Configuring a Client

In "Wireless Network Selection", tap the wireless band you want to use, such as "WIFI1(5G)".

Figure 39 Wireless network selection

Click the "Modify" button of "Wireless Interface Settings" to change "Wireless Mode" to client and "Network Name" to Wireless_link and click Finish.

Figure 40 Wireless Interface Settings - Modify the wireless mode and SSID

Click Save in the upper right corner. The client configuration is complete.

Figure 41 Save

In this case, the client can successfully connect to the access point named Wireless_link.

4.1.1.3 Configuring an Access Point (WDS)

Follow the same steps as 4.1.1.1 to change the Access Point mode to Access Point (WDS) mode.

4.1.1.4 Configuring a Client (WDS)

The procedure is the same as 4.1.1.2. Change the client mode to WDS mode.

4.1.1.5 Associate devices by scanning signals

Log in to the client device page, enter the wireless setting module, click "Scan Signal", the list of scanned aps will appear, and find the SSID you want to connect in it, such as Wireless_5G. If you do not find the device you want to connect, click below.Rescan. When found, click "Select" or "Lock" below the scan result.

Figure 42 Scanning signal

Enter the key of the access point: for example, "1234567890abc" click OK, click the "Save" button in the upper right corner of the device page, and wait for the wireless connection.

Figure 43 Scan signal - Selected

View status - Connected wireless device information page. If relevant information is displayed, the wireless device is successfully associated.

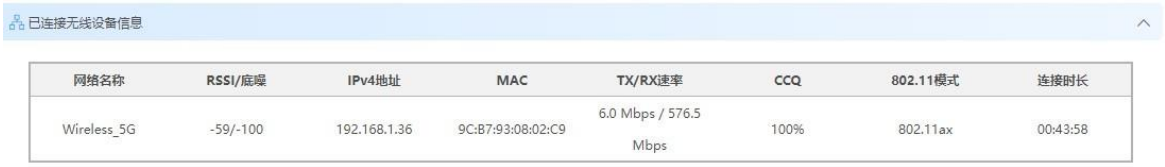


Figure 44 View status

4.1.2 Wireless Settings -Mesh Mode

In Mesh mode (i.e., Mesh mode is turned on), the Wireless Settings page is shown in the following figure (5G for example):

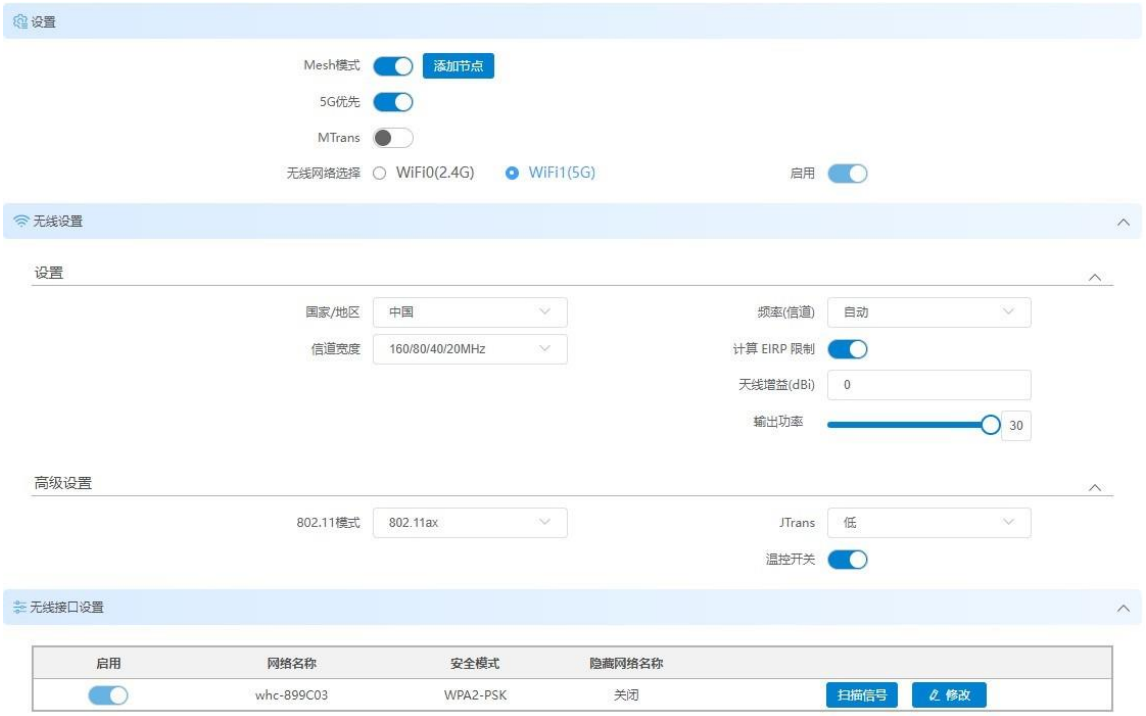


Figure 45 Wireless setting-CAP mode

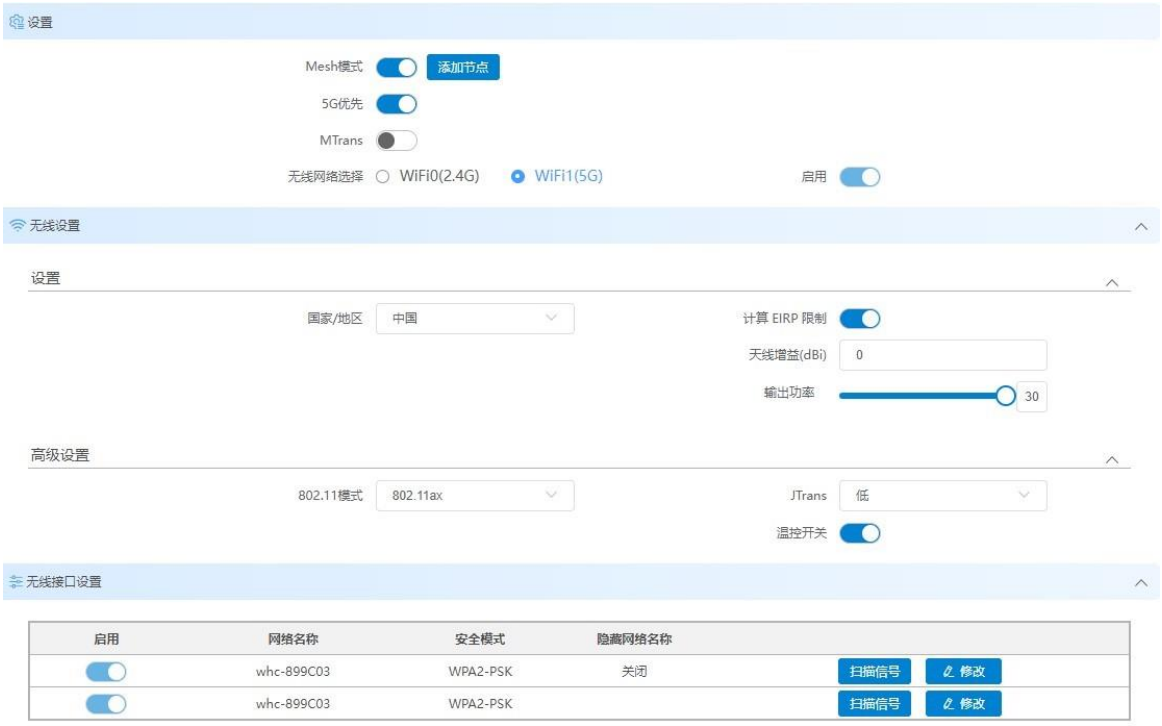


Figure 46 Wireless Settings -RE mode

The parameters in the above page are the same as the normal mode, see chapter 4.1.1 for detailed explanation.

Wireless Network Selection: 2.4G and 5G wireless network cannot be turned off in Mesh mode, and the switch is locked on.

Wireless Interface Setting: In Mesh mode, add/delete wireless network interface is not supported.

Wireless Mode: The wireless mode is WDS mode in Mesh mode, and the wireless mode cannot be changed. Automatic Channel Selection: Mesh mode does not support this function.

Dynamic Channel Selection: This function is not supported in Mesh mode.

Wireless Network Probe: Wireless Network Probe cannot be enabled in Mesh mode, and is disabled by default. To use wireless network probe, you need to switch the device to normal mode.

4.1.2.1 Configuring CAP and RE

Users can switch the device to the CAP or RE mode according to the method described in this section. You can use the following methods:

Change the IP address of the directly connected PC

CAP: Modify the IP address of the directly connected device PC so that it is the same as the gateway of the device, enabling the device to ping its own gateway address via wired ping.

For example, change the IP address of the PC to For example, change the IP address of the PC to 192.168.10.254 (the gateway of KyAir800E is 192.168.10.254).
192.168.10.254).

RE: Change the IP address of the PC directly connected to the device to be different from the gateway of the device, so that the device cannot Ping the gateway through the cable. (If the gateway is empty or the network cable is disconnected, the device works in RE mode.) For example, change the IP address of the PC to 192.168.10.10 (The KyAir800E gateway is 192.168.10.254).

Change the default gateway of the device

CAP: Log in to the device page through the wizard (see section 2.2 for details on the wizard configuration) or network Settings (detailed steps)

See Section 4.2), change the IP address of the default gateway of the device to be the same as that of the PC directly connected, so that the device can Ping through its own gateway address. For example, change the gateway address of the device to 192.168.1.10 (the IP address of the PC is 192.168.1.10).

RE: Log in to the device page through the wizard (see section 2.2 for details on the wizard configuration) or network Settings (see section 2.2 for details)

Section 4.2), change the IP address of the default gateway of the device to be different from that of the PC directly connected, so that the device cannot Ping through its own gateway. For example, change the gateway address of the device to 192.168.1.11 (IP address of the PC to 192.168.1.10).

Change the network mode of the device to routing mode

Log in to the device page and click Settings to enter the network Settings page. Change the network mode to routing mode. After the configuration is saved, the device switches to CAP mode. In routing mode, CAP is fixed. As shown in the picture below:

4.1.2.2 Determining CAP and RE

Users can follow the steps in this section to quickly differentiate between a device in CAP or RE mode.

CAP mode

CAP, that is, the central access point, the unit that manages the network, generally deployed on the home network outlet, also known as the main router. In a group of Mesh networking, there is and can only be one CAP. If the device can Ping its own gateway through a cable (for details about how to configure CAP, see Section 4.1.2.1), the device automatically switches to the CAP mode. (If the network mode is route mode, the CAP mode is fixed by default.) In the topology diagram of the CAP device, the upper-level connection of the local device is the Internet. Both 2.4G and 5G wireless have and only one wireless network interface, and the wireless mode is the access point WDS. As shown in the picture below:

Figure 47 Mesh topology of CAP

Figure 48 Wireless information of CAP

RE Mode

RE: Routers other than the main router in a Mesh network. In RE mode, the device cannot ping its own gateway through a cable (for details about how to configure RE, see Section 4.1.2.1). Only the local device is displayed in the RE device topology. The 2.4G of RE device has only one wireless interface, which is the access point WDS mode. 5G wireless has two wireless network interfaces, and the wireless mode is the access point WDS and the client WDS. As shown in the picture below:

Figure 49 Mesh topology of RE

Figure 50 Wireless information of RE

4.1.2.3 How to Form a Mesh Network

4.1.2.3.1 1V1Mesh Networking

Users can follow the steps in this section to form a 1-to-1 Mesh network with CAP and RE.

Log in to the pages of CAP and RE respectively. On the wireless setting page, click the "Add Node" button of the two device pages respectively (it is recommended to click CAP first and then click RE, with an interval of no more than 1 minute and 30 seconds), as shown in the figure below:

Figure 51 Adding Nodes

After clicking the "Add Node" button on the device page, a message will appear on the page:"Please ensure that the newly added node is in the factory-restored state, otherwise configuration synchronization will fail, whether to continue to add the node" is displayed, as shown in the following figure:

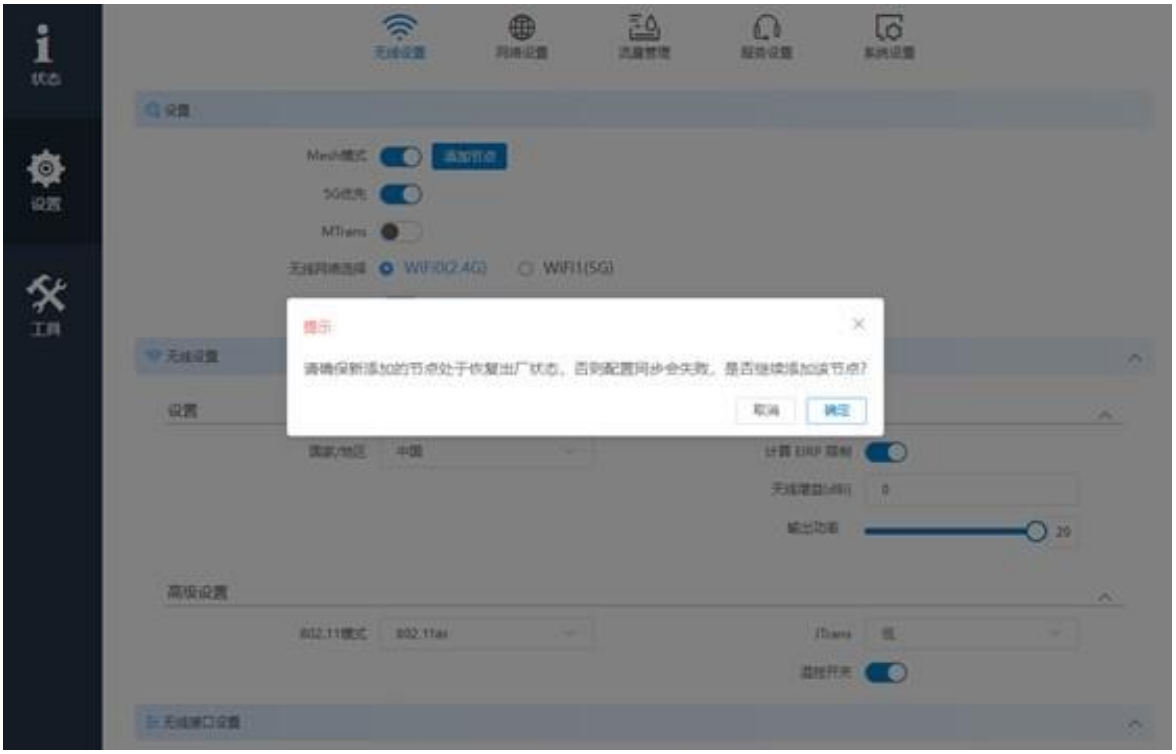


Figure 52 Prompt message

Click the "OK" button to enable Mesh synchronization, and the page will display the message: "Searching for available Mesh. Node, and synchronize the configuration information, wait about 2 minutes ", as shown in the following figure:

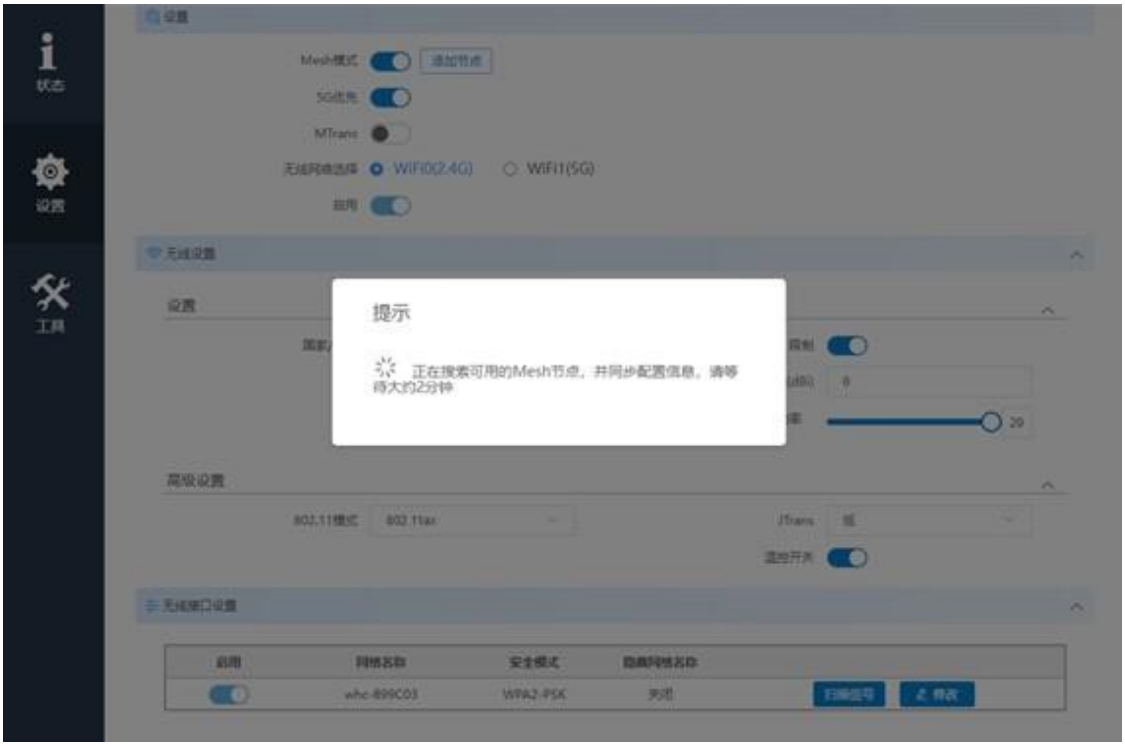


Figure 53: Waiting for prompt message.

After 2 minutes, the prompt information disappears and the page returns to the normal interface. After Mesh synchronization succeeds, the RE synchronizes the wireless information of the CAP and associates it with the CAP. After the Mesh network is formed, the Mesh topology of CAP and RE is shown in the following figure:

Figure 53 Waiting for a prompt message

Figure 55 Mesh Topology Diagram-RE-Association Status

Click the Mesh networking device (that is, the RE device) in the Mesh topology on the CAP page. The IP address and MAC address of the RE are displayed. Click the corresponding IP address to go to the login page of the RE.

Figure 56 CAP topology -Mesh network device information

Note:
The reset key on the device can also be used as a key for Mesh networking synchronization: The CAP device and the RE device hold down the reset button for about 3 seconds respectively. (You are advised to press the CAP button first, and then press the RE button again at an interval of no more than 1 minute and 30 seconds.) The Mesh network starts to form.
It is recommended to preferentially click "Add node" on the page for Mesh synchronization.

4.1.2.3.2 1V Multi-Mesh Networking

Users can form a one-to-many Mesh network between the CAP and multiple RE

according to the following methods.

1, wired synchronization: CAP and multiple RE cable ports are connected to the same switch, wait a few minutes, CAP and RE can complete synchronization. Check the status and number of RE synchronization on the CAP page. After all RE synchronization is complete, pull out the cable port of the RE. Otherwise, a loop may occur.

2、**Wireless synchronization:** After the CAP is synchronized with one RE (2-3 minutes), it can be synchronized with other RE successively. You can click "Add Node" or press the reset button on the page to synchronize the CAP. The specific operations are consistent with those described in section 4.1.2.3.1. Synchronize one device every 2-3 minutes. CAP cannot be synchronized wirelessly with multiple RE devices at the same time. It is recommended that when RE and CAP are synchronized, the distance should be controlled within 2 meters, as shown in the following figure:

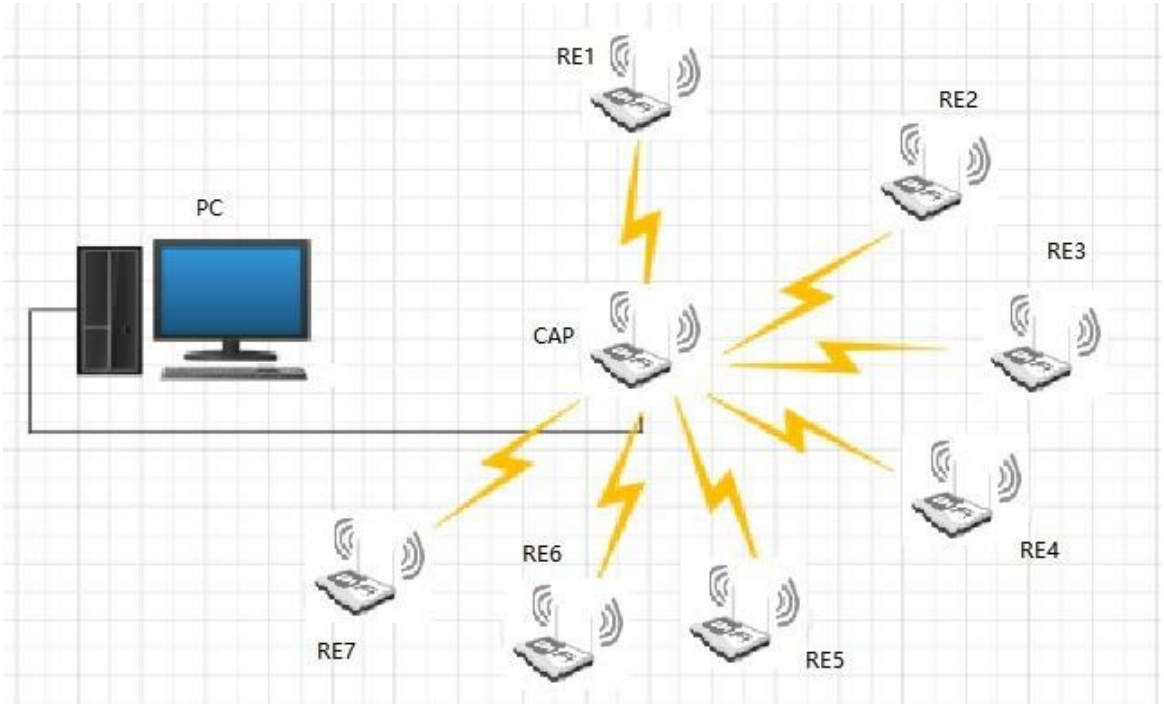


Figure 57 1V multi-mesh networking

According to the above method, after the CAP is synchronized with multiple RE, adjust the position and distance of RE to build the MESH networking architecture. The RE automatically associates with devices with good signals (when there are more than 1V, it is recommended that the number of devices in the network should not exceed 5).

4.2 Network Settings

You can select the network mode, including bridge mode and routing mode, and set parameters related to the management VLAN. The management VLAN is disabled by default.see Section 4.2.2 Advanced Settings for details.

Figure 58 Network Settings

4.2.1 Interface Settings

The interface Settings are used according to the network mode in the network Settings. When the network mode is selected Bridge mode, the interface Settings are shown as follows:

Figure 59 Interface Settings - Bridge mode - Static

Figure 60 Interface Settings - Bridge mode -IPv4 dynamic

Figure 61 Interface Settings - Bridge mode -IPv6 Dynamic

If the IP address type is static, you can set the IP address, subnet mask, default gateway, and DNS as required. Ensure that the IP address is not the same as that of other devices on the same network to avoid IP address conflict. The gateway address and IP address must be on the same network segment.

To enable the device to access the Internet, connect the device to the Internet and change the IP address of the device and the IP address of the router on the LAN

On the same network segment, the gateway is the IP address of the connected upper-layer routing port, and the device is connected to the router through a network cable.

If the IP address type is dynamic, the device can obtain the dynamically assigned IP address after connecting to the DHCP server. If the device does not obtain an IP address or fails to obtain an IP address, you can use the standby IP address to access the device page for management. **Note:** There is no standby **IPV6** dynamic address. If the dynamic address cannot be obtained correctly, the device cannot be accessed through the page. Therefore, use this function with caution.

IPv4 The **DHCP** server is disabled by default. After it is enabled, you can set the start IP address, end IP address, lease time, gateway, and DNS parameters. (The gateway is recommended to be an available IP address; otherwise, service transmission may be affected.) After a terminal such as a mobile phone or computer is wirelessly associated with a client device, the device can obtain an **IPV4** address.

Figure 62 Interface Settings - IPV4 DHCP

The **IPv6 DHCP** server is disabled by default. If Server is selected, the IPV6 address assigned by the device can be obtained after terminals such as mobile phones, computers, and clients are wirelessly associated with each other. (An IPv6 address must be configured on the device before using the DHCP server.)

STP Enable: After STP is enabled, network loops can be eliminated. Ensure that

network links are smooth when loops occur.

IPv6 address: specifies the IPv6 address of the device.

Network Mode When you select the routing mode, you can select LAN port Settings and WAN port Settings. When you change the routing mode, the interface bound to the LAN and WAN by default is displayed on the Bridge interface Settings page.

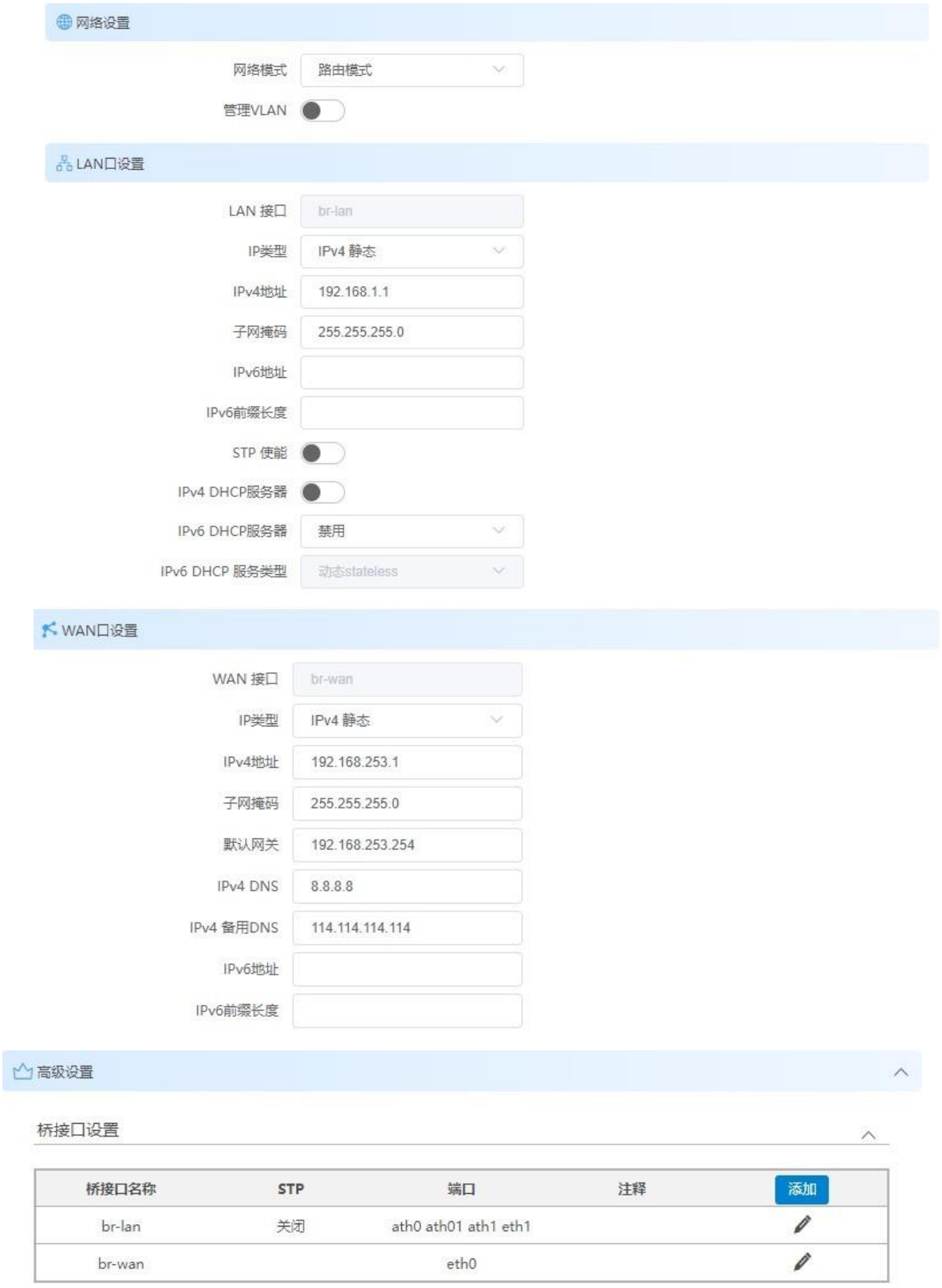


Figure 63 Routing mode

LAN port Settings: For details, see Interface Settings in Bridge mode. After routing is enabled, it is recommended to use the static mode for **LAN** interfaces Address.

WAN Interface Settings: The IP type of the WAN interface is the method used by the WAN interface to obtain an IP address, which can be static or **IPv4** Dynamic and PPPOE. If static IP address is set, you need to manually set the IP address and subnet mask to the same network segment as the network to be connected. If IPv4 dynamic is set, the device automatically dynamically obtains an IP address from the DHCP server. When PPPOE is configured, users need to enter the Internet access account, Internet access password, and server name. The device uses dial Id Authentication You can obtain an IP address from a PPPOE server, as shown in the following figure.

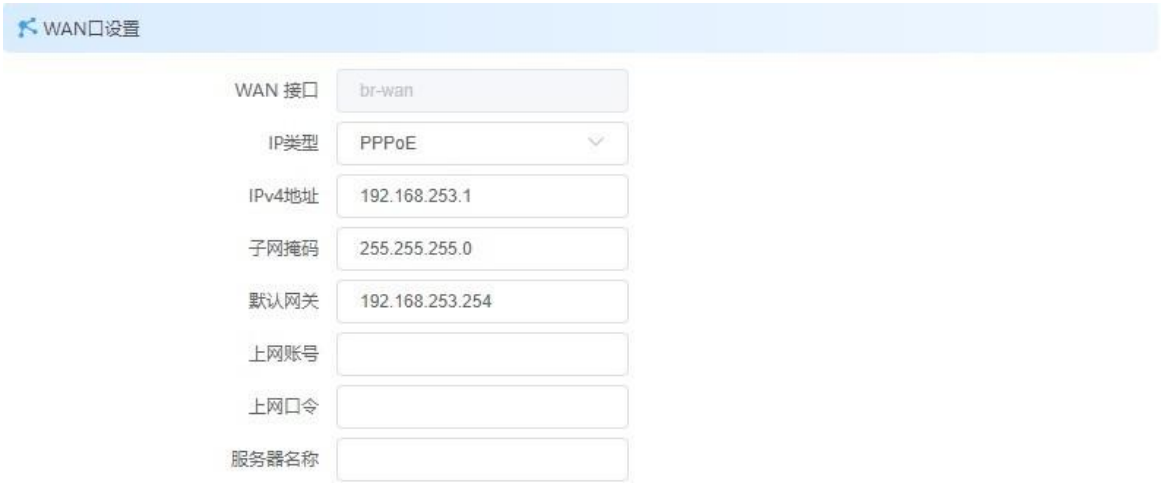


Figure 64 WAN Interface Settings - PPPOE

Caution :

The LAN port IP address cannot be set to the same network segment as the WAN port IP address, when the WAN port is set to static IP, it cannot be set to an existing IP

4.2.2 Advanced settings

Advanced Settings include bridge interface Settings, VLAN Settings, Ethernet interface Settings, IPv4 static routes, IPV6 static routes, and interface isolation.

Bridge Interface Settings: When Mesh mode is off, you can change the bridge location of the interface, add or delete the bridge interface, and modify it

The configuration of the new bridge. For example, the IP address, subnet mask, and gateway of the new bridge are not required. You can set these parameters based on requirements. You can also delete a newly created bridge. A bridge interface created by the system cannot be deleted. The device contains five

interfaces: eth0, eth1, ath0, ath01, and ath1. eth0 corresponds to the LAN port on the POE power adapter, eth1 is the LAN1 port on the device, ath0 is the 2.4G wireless interface, and ath01 is the 2.4G management wireless interface. ath1 is a 5G wireless interface. The following is the default display of the bridge interface in routing mode.

Figure 65 Bridge interface Settings - Routing mode

Caution：

When multiple bridge interfaces are created, only one gateway can be configured. The gateway configuration can be left blank.

VLAN： The VLAN function allows users to connect to each network interface. Add multiple VLAN interfaces. ID of a VLAN

The VLAN ID ranges from 3 to 4094. Each VLAN ID indicates a different VLAN value. Add VLAN whose VLAN ID is 10 to port eth1, as shown in the following figure.

Figure 66 VLAN

The **VLAN** function needs to be used together with the bridge interface settings, as shown in the following figure, add VLANs to both devices eth0 and ath0, with ID 10, and put them in a newly created bridge interface vlan10 (also available as the default bridge interface). The wired eth0 interface needs to be connected to a device that supports VLAN10 (e.g., a VLAN switch whose ports support VLAN 10) to access the device for management via the bridge address where eth0.10 is located. For wireless services via VLAN, the wireless associated peer device should also support VLAN10 (e.g., ath0 adds VLAN 10).

Figure 67 VLAN settings

Common connection methods are shown in the following figure:

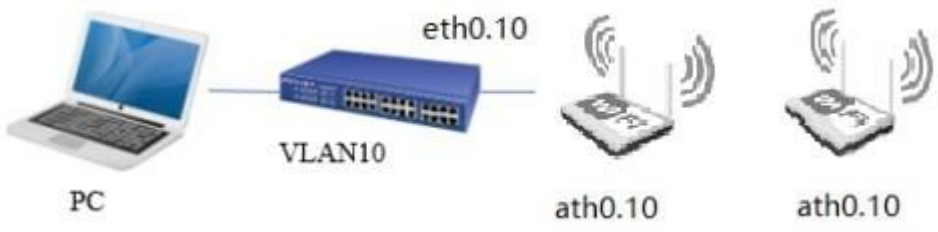


Figure 68 VLAN connection diagram

Management VLAN: After the management VLAN is enabled in network Settings, the VLAN for the device's wired and wireless ports is automatically added to the VLAN Settings. The mgmtvlan is created in bridge port Settings and the created VLAN ports are added to the VLAN Settings

In mgmtvlan, after a device (such as a VLAN switch whose VLAN ID is 3) is connected to VLAN3, you can use the IP address set by the management VLAN to access the device page for management. However, the management VLAN does not support data service forwarding.

Figure 69 Management VLAN Settings

Ethernet interface Settings: You can configure Ethernet interfaces for eth0 and eth1. Select the auto negotiation mode. Set

The standby Ethernet port automatically sets the maximum transfer rate based on the connected device. If auto negotiation is not selected, the user can set the Ethernet port rate (10M/100M/1000M/2500M) and single duplex (full duplex/half duplex).

Figure 70 Ethernet interface Settings

IPv4 Static route: This function allows you to set IPv4 static routes. Click Add and the following page will pop up:

Figure 71 IPv4 static route - Add

Outgoing Interface：Indicates the bridge interface of the corresponding network segment.

Target network: target network segment.

Subnet Mask:the IPv4 address of the gateway and the outgoing interface must be in the same network segment

Leap Points: the number of routers passed during transmission.

Configure the corresponding parameters and click Finish, as shown below:

Figure 72 IPv4 static route

IPv6 Static route: This function allows you to set IPv6 static routes. Click Add and the following page will pop up:

Figure 73 IPv6 static route - Add

Set the corresponding parameters and click Finish, as shown below:

Figure 74 IPv6 static route

Interface isolation:

Wired port isolation: This function is disabled by default. After this function is enabled, wired ports on the device cannot communicate with each other.

Wireless interface isolation: This function is disabled by default. After this function is enabled, wireless interfaces on the device cannot communicate with each other.

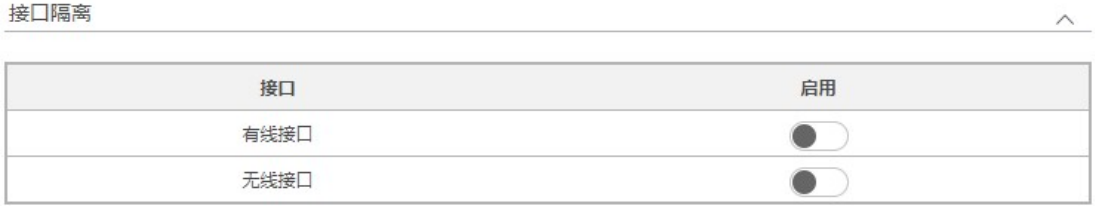


Figure 75 Interface isolation

4.3 Traffic Management

When a user wants to block certain devices, the firewall can be used. Firewall rules do not affect outgoing packets from the device. The default setting is off. When enabled, the default rule is set to “Discard.” Rules in the filter settings default to “Accept,” meaning only packets satisfying these rules are received, and all others are discarded. If the default rule is “Accept,” the filter settings default to “Discard,” meaning packets satisfying these rules are discarded, and all others are received.

Note:
Firewall rules do not affect outgoing packets. Do not set “Source IP” to the device’s IP.
If the default rule is “Discard,” ensure filter rules are correctly configured to avoid service disruptions. Non-professionals should use this feature cautiously.

Figure 76 Firewall Configuration

Example 1: A device is directly connected to a computer. Configure firewall rules on the device to block packets with source IP address 192.168.197.100 on interface eth0. Add two reciprocal rules in the IP filter settings:

① Target: Discard, Interface: eth0, Protocol: IP, Source IP/Mask: 192.168.1.100/32, Destination IP/Mask: 192.168.1./32.

② Target: Discard, Interface: eth0, Protocol: IP, Source IP/Mask: 192.168.1.1/32, Destination IP/Mask: 192.168.1.100/32.

Figure 77 IP Filter Settings

Example 2: A device is directly connected to a computer. Configure firewall rules to block packets with MAC address 00:00:00:00:00:01 on interface eth0.

Enable the firewall, set the default rule to "Accept," and add two rules in the MAC filter settings:

① Target: Discard, Interface: eth0, Source MAC: 00:00:00:00:00:01, Destination MAC: (Device's bridge MAC address).

Note：

The bridge MAC is usually the smallest MAC value among wired ports.

② Target: Discard, Interface: eth0, Source MAC: (Device's bridge MAC address), Destination MAC: 00:00:00:00:00:01.

Figure 78 MAC Filter Settings

Interface Rate Limiting:

You can limit the upload and download rates for device interfaces. This is off by default.Example: Limit the eth1 interface upload and download rates to 1024 kbit/s.

Figure 79 Interface Rate Limiting

QoS Priority:

QoS (Quality of Service) refers to a network's ability to provide better service for specific communications. This is a network security mechanism to address latency and congestion issues.

Figure 80 QoS Priority

Target CoS: Target Class of Service, range 0-7, corresponding to priority levels.

Target DSCP: Differentiated Services Code Point, range 0-63. Used to classify and prioritize traffic.

Conditions:

Source MAC: Source MAC address.

Destination MAC: Destination MAC address.

VLAN ID: VLAN ID.

CoS: Priority level.

Ethernet Type: Ethernet type.

DSCP: DSCP value.

IP Type: IP type.

Source IP: Source IP address.

Destination IP: Destination IP address.

Source Port: Local port.

Destination Port: Remote port.

4.4 Service Settings

Time Settings: Set the device's time by selecting different time zones. Time synchronization methods include:

Manual Time Sync: You can manually set the time or click "Sync with Computer Time."

NTP Time Sync: Enter the server address, NTP port, and synchronization interval (default: 15 minutes). Ensure the device can access the internet (refer to section 4.2.1 for interface settings). The time will be calibrated automatically via the NTP server and displayed on the status page.

Figure 81 Service Settings-Time Settings (Manual)

Figure 82 Service Settings - Time Settings (NTP)

Remote Management ： When SSH is enabled, use terminal software that supports SSH (e.g., SecureCRT, Xshell) to connect. Enter the device IP, login credentials, and manage the device backend.If SSH is disabled, remote backend login is not possible.

Figure 83 Service Settings - Remote Management

web Service： Users can choose to log into the device interface using HTTP or HTTPS.

Figure 84 Service Settings -web Services

Device Discovery： When enabled, this feature works with specific device discovery tools to display discovered devices' MAC address, IP address, and other relevant information.

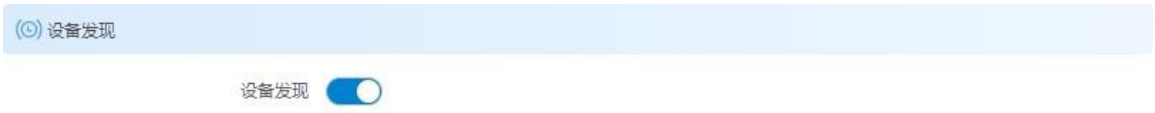


Figure 85 Service Settings - Device Discovery

Scheduled Reboot: Enable this feature to reboot the device at scheduled intervals. By default, this function is disabled.

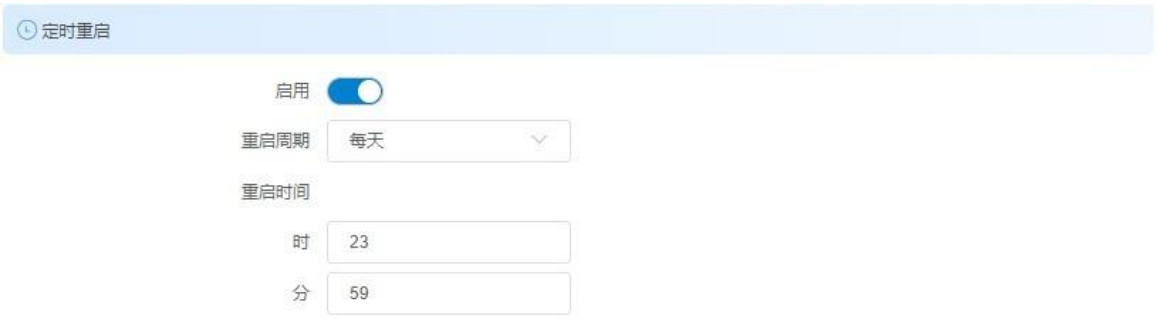


Figure 86 Service Settings - Scheduled reboot

Remote Logs : Enable the remote logging function and set the IP address of the remote log server. The server port is set to 514 by default. After saving and applying, relevant log information will appear in real-time on the remote log server.

Figure 87 Service Settings - Remote Logging

AC Management: This feature is enabled by default and works with the AC management system.

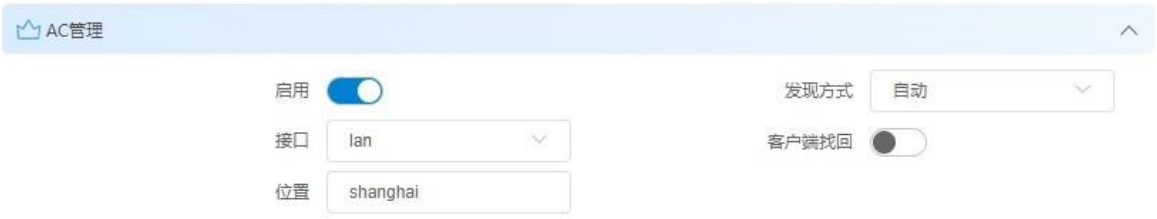


Figure 88 Service Settings -AC management

Position: Input the desired location of the device to display it on the AC map.

Discovery Mode: There are two modes for an AP to discover an AC: manual and automatic Manual Specification: Add primary and backup AC addresses, which correspond to the AC management system's IP.

Automatic Discovery: For Layer 3 connections, configure the DHCP server's

Option43 field with the AC’s IP address. For ease, non-professionals are recommended to use the Manual Specification mode.

Fill in the Option43 field with the IP address of the AC, and you need to configure the IP address of the access point to be obtained automatically, that is, the IP type is IPV4 Dynamic, and it is recommended that non-professionals configure the discovery method manually here.

Option43 Field Format: 8007000001AC122847

- 80: Fixed value, no changes needed.
- 07: Length field, indicating the byte length of the data that follows.
- 0000: Fixed value, no changes needed.
- 01: Indicates the number of IP addresses that follow; in this case, it is one IP address.
- AC122847: Represents the AC IP address (172.18.40.71) in hexadecimal. To use a different AC IP address, modify the last 8 characters to correspond to its hexadecimal value. Other parameters can remain unchanged.

Client Recovery : When enabled, the AC can recover clients that have disconnected from the access point (AP). The AP and AC must have the same system and configuration for this function to work.

Caution :

Client devices can successfully join the AC only when this feature is enabled, the devices are connected to an access point, and that access point has the AC function enabled and is part of the same AC system.

Ping Watchdog : This feature continuously monitors the device's status by pinging a target host or device IP. If a defined number of ping replies are not received, the device will reboot.Recommended for Client Mode, not for Access Point Mode. Disabled by default.

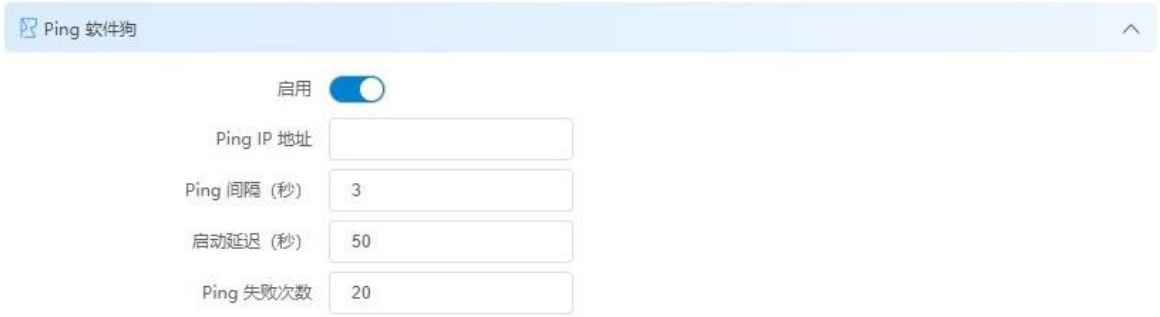


Figure 89 Service Settings -Ping Watchdog

Ping Interval: Time between each ping (seconds).

Ping IP Address: Generally, enter the IP address of the target host or device. Client Mode When the Ping watchdog is enabled, enter the IP address of the access point connected to the client.

Startup Delay: After the system of the device is started, the device will start pinging the target host only after the set delay time has elapsed, in seconds.

Ping Failure Count: Number of failed pings before the device reboots.

Caution:

If you want to modify the Ping watchdog parameter Settings, disable the Ping watchdog first. After the Ping watchdog takes effect, enable the ping watchdog to configure new parameters.

Load Balancing: Dynamically adjusts the number of terminals that can be associated with each AP device according to the set number of associated users and traffic thresholds to achieve load balancing. Within the same equalization group, the configuration of the master AP (whoever powers on first is the master AP) prevails. The configuration of the master AP (whoever powers on first is the master AP) prevails. The device is turned off by default.

Caution :

The load balancing function is available only in common mode. It is unavailable in Mesh mode and route mode.

Figure 90 Service Settings - Load Balancing

Switching Group ID: Identifies a balancing group.

Switchover group IP address: identifies the balancing group. This is the virtual IP address of the master AP. Devices in the balancing group are assigned to this IP address

Devices with IP addresses report their own status, facilitating AP scheduling balance. The IP address cannot be the same as the LAN address of the device; otherwise, the load balancing function does not take effect.

Caution：

- The group IP must be on the same network segment as the LAN IP address.
- Group ID and Group IP are the unique identifiers of a balanced group. When there are multiple APs in a LAN, these 2 values must be unified to be in the same load balanced group.

Load balancing mode: Load balancing modes include traffic and number of users, that is, balancing devices based on traffic or number of users. High-load access window duration: Total access window duration.

Minimum authentication interval with high load: Limits the client access frequency. The window time divided by the authentication interval must be greater than or equal to the number of Windows.

High Load Access Window Count: This is the maximum number of times an access point will reject a terminal device's connection within an access window time. When the count reaches the set value, the client will be allowed to access again after making another request. If the count has not been reached, both the window time and count statistics will be reset.

Traffic Balancing Threshold: This is the maximum traffic value that triggers the load balancing algorithm in traffic-based load balancing mode, usually used in conjunction with traffic difference values. When the traffic is below the threshold, clients can connect freely. When the traffic exceeds the threshold, the system checks if the traffic difference between the current device and the device with the minimum traffic has reached the set traffic balancing difference. If it has not reached the difference, the device will allow the client to connect; if the difference is reached, it will reject the client's access.

Traffic Balancing Difference: This works in conjunction with the traffic balancing threshold.

User Count Balancing Threshold: This is the maximum number of users that triggers the balancing algorithm in user count-based load balancing mode, usually used in conjunction with the user count balancing difference. When the user count is below the balancing threshold, clients can connect freely. When the user count exceeds the threshold, the system checks the difference in the number of connected clients between the current device and the device with the fewest clients. If the difference is less than the user count balancing difference, the device allows the client to connect; if the difference is greater than or equal to the user count difference, it will reject the client's connection.

User Count Balancing Difference: This works in conjunction with the user count balancing threshold.

SNMP (Simple Network Management Protocol): This is mainly used for simple network management of devices through an MIB Browser. It supports SNMPv2 and SNMPv3 protocols, allowing you to read and write certain device information and modify its configurations. By default, the feature is disabled.

SNMP v2: It uses community name authentication and transmits data in plaintext, making it less secure. To use management software, enter the group names configured below to connect to the device.

- **Group Name (Read-Only):** Default is "public", and it can be modified. When using SNMPv2 with MIB Browser, enter the device's group name (Read-only) in the Read community field.
- **Group Name (Read-Write):** Default is "private", and it can be modified. When using SNMPv2 with MIB Browser, enter the device's group name (Read-write) in the Set community field.
- **Location and Email:** By default, these fields are empty, and SNMPv2 can still connect without filling them.

SNMP v3: This improves upon SNMP v2 by enhancing security and management mechanisms. To use SNMPv3, the relevant authentication and encryption information must be provided, offering significantly better security.

- **Username:** Default is "user", and it can be modified. When using SNMPv3 with MIB Browser, enter the device's username in the User Profile name field.
- **Group:** Default is RWPriv (supports read-write with authentication and encryption). It also supports RO (read-only, no authentication or encryption) and RWAuth (read-write with authentication).
- **Authentication:** Default is SHA, but MD5 authentication is also supported.

Authentication Key: Default password is “12345678”.
Encryption: Default is AES, but DES
encryption mode is also supported.
Key: Default password is “12345678”.

Figure 91: Service Settings - SNMP

4.5 System Settings

The system settings interface consists of system settings, firmware configuration, and account management, as shown below:

Figure 92: System Settings

Device Name: Users can set the device name according to their needs.
Language: Users can choose the language for the page display.
Login Timeout: When the user does not operate the device for a time exceeding the set timeout value, the page will automatically redirect to the login page.
Configuration File Export: Clicking "Generate Backup" will back up all current configurations on the web page to a local file.

Note: Configuration files cannot be manually modified.

Note:
Configuration files cannot be manually modified.

Configuration File Import : Clicking "Choose File" and selecting a previously downloaded configuration file and then clicking "Upload" will restore the device configuration to the state of the backup configuration file.
One-Click Information Export: Clicking "Download" will export the system log file, which contains the configuration file.
Factory Reset: Clicking "Execute Reset" on the webpage will redirect the page to the waiting screen. After the reset is complete, the page will redirect to the default backup IP address, and the device's configuration will revert to factory settings.
Restart: Clicking "Restart" will reboot the device system, and the configuration will remain unchanged after the reboot.
Firmware Upgrade: Click "Choose File," select the version to upgrade, and click "Upload Firmware." Once the firmware upload is completed, choose whether to retain the configuration file and check the box as needed. Finally, click "OK" to begin the upgrade.

Figure 93 Firmware upgrade

Modify Password: When the modify user password function is enabled, users can modify the device's username and password from the device's web interface. To enhance information security, please regularly change the device password and avoid using overly simple passwords such as pure numbers, letters, or birthdays. The password is stored in a separate module, so do not change other configurations when modifying the password.

Figure 94: Modify Password

5 Tools

The tools page is divided into two sub-pages: Ping IP and Link Test, which are described below:

5.1 Ping IP

Enter a device's IP address and click "Ping." The collected data will display the Ping result, as shown in the figure below:

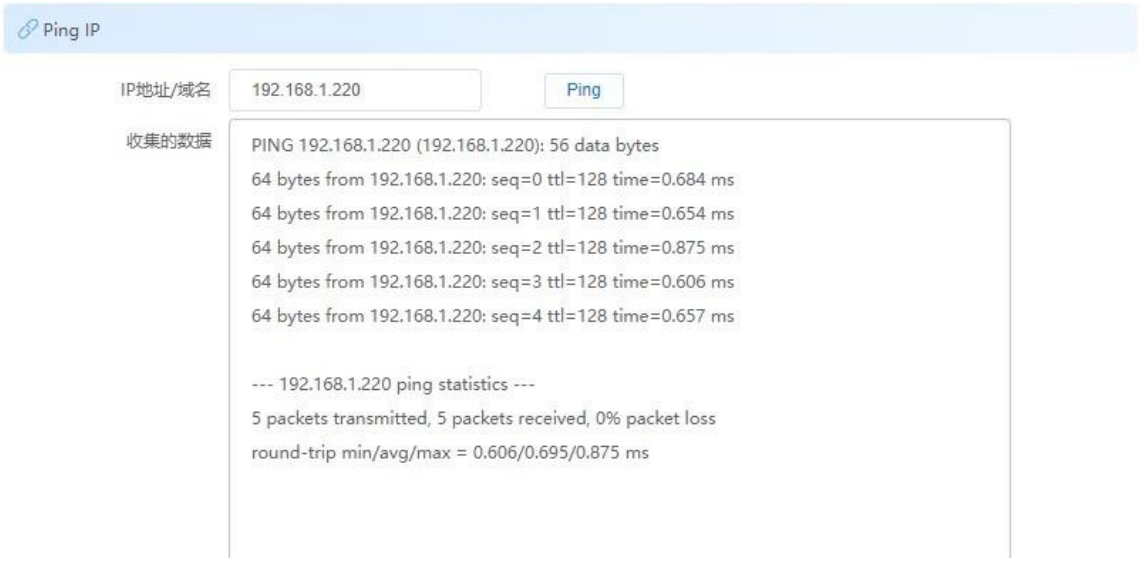


Figure 95: Ping IP

5.2 Link Test

Iperf testing can be used to test maximum bandwidth performance, reporting bandwidth, delay jitter, and packet loss. It has client and server modes for testing the throughput between devices wirelessly. Device 1 selects "Server," and the Iperf interval is the time interval for displaying throughput on the web page. Device 2 selects "Client," and the Iperf server enters Device 1's IP address. The number of Iperf threads corresponds to the number of threads running simultaneously during the throughput test, and it is recommended to set to 10. The Iperf test time corresponds to the number of seconds the Iperf test runs. The Iperf interval is the time between throughput readings shown on the webpage. After filling out these parameters, click "Start" to perform the test.

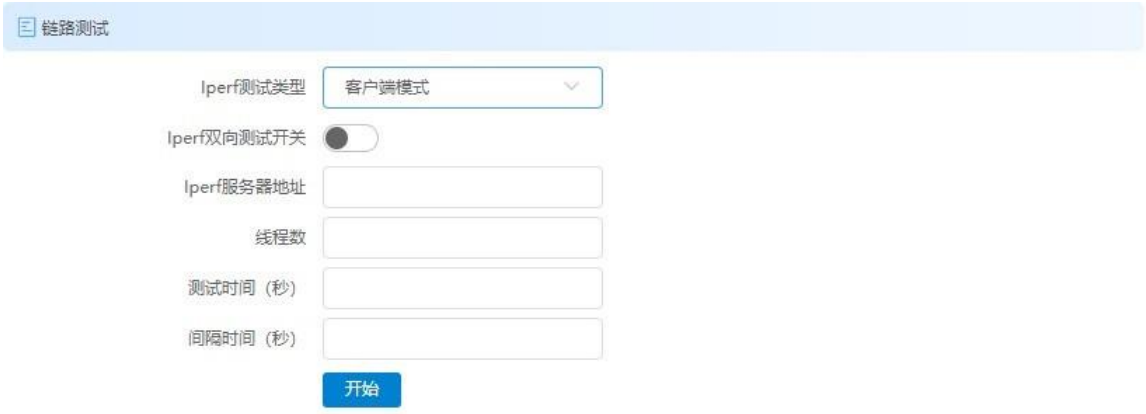


Figure 96: Link Test - Client Mode

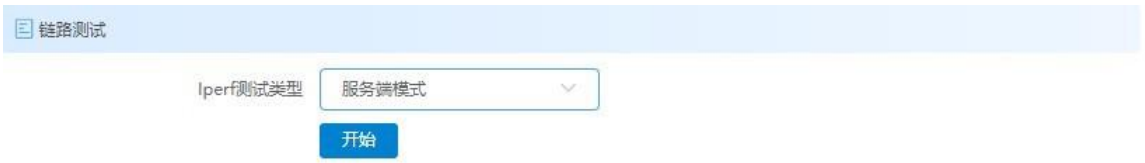


Figure 97: Link Test - Server Mode

6 Logout

“Logout” is used to log out of the device page. When the user clicks “Logout” at the top right, it will redirect to the login page.

Figure 98: Logout

7 Troubleshooting

What should I do if I can’ t log into the device with its IP address?

①Confirm that the device is connected correctly and the network cable is not loose.

②Confirm if the device’ s IP address has been changed.

③Confirm that the computer’ s IP address is 192.168.1.X (X between 2-254, excluding the device’ s IP).

④Restore the device to factory settings and try logging in again.

How to restore factory settings?

①Run cmd on the computer and ping the device’ s IP to confirm if the IP address is correct.

②Make sure that the computer’ s IP address and the bridge’ s IP address are in the same local network.

Why can’ t the terminal device connect to the AP?

①The signal strength is too weak. Check if the transmission power is set to the maximum, and if there are obstructions, adjust the AP deployment position.

②Check if the AP has enabled the weak signal rejection function. Adjust the threshold or disable this function.

③Check if MAC address filtering is enabled. Add the terminal’ s MAC address to the whitelist.

Can’t access the Internet after the terminal is associated with an AP?

①Confirm whether the upstream router can access the internet.

②Check whether the terminal is obtaining the correct IP address.

Reassociate and verify if the terminal’ s IP address falls within the subnet range assigned by the upstream router.

Terminal unable to connect to the AP?

①Signal strength is too weak. Check if the transmission power is set to the maximum. If there are obstructions, adjust the AP’ s deployment location.

②Verify if the AP has enabled the weak signal rejection feature. Adjust the threshold or disable this feature.

③Check whether MAC address filtering is enabled. Add the terminal’s MAC address to the whitelist.

④Verify the wireless key. Ensure it is entered correctly.

Terminal devices (e.g., phones, computers) experience video disconnections or lag:

①Check if the wireless connection is stable. If unassociated, verify whether the access point and the terminal device (phone, computer, etc.) share consistent wireless settings such as network name, channel width, and encryption method.

②Check for obstructions at the installation location. Ensure the AP’s antenna faces the terminal device (phone, computer, etc.) without any obstructions.

③Check if the wired link is functioning correctly.

Check if the wired connection is secure and good. Avoid connection issues due to loose or damaged connectors. Use a computer directly connected to the device and run cmd, using the command to check if the delay is less than 5ms: ping [device IP] -t -l 60000. If the delay is abnormal, replace the network cable or remake the crystal head.

8 Appendix List of abbreviations

Serial Number	Definitions and abbreviations	Description
1	Access Point(AP)	Access point
2	Client	Client
3	DCS(Dynamic Channel Selection)	Dynamic channel selection
4	CAP	Central access point, i.e., main Mesh
5	RE	Sub-Mesh
6	Mesh	Intelligent networking