KyAir600E

Industrial Wireless AP WEB Operation Manual

Publication **date : January 2024**

Version : V1.0

Disclaimer

Beijing Dongtu Technology Co., Ltd. strives to make the information in this manual as accurate and up-to-date as possible. However, the company cannot We guarantee that this manual is completely free of any technical errors or clerical mistakes, and reserve the right to modify it without notifying the user.

Publisher: Beijing Dongtu Technology Co., Ltd.

Website: http://www.kyland.com.cn

Customer service hotline: 010-88796676

Fax: 010-88796678

Email: services@kyland.com.cn

Table of contents

Conventions in this Manual

1. Text format conventions

Format description	
< >	The content in **"< >" indicates the button name, such as "Click the <Apply> button".**
[ ]	The content in **"[ ]" indicates the window name or menu name, such as clicking the "[File]" menu item.**
{ }	The content in **"{ }" indicates a combination, such as "{IP address, MAC address }" means that the IP address and MAC address are a combination.** **To configure and display together.**
ÿ	**Multi-level menus are separated by "ÿ", such as "StartÿProgramsÿAccessories" means the [Accessories] menu under the [Programs] submenu under the [Start] menu.** **item.**
/	**Choose one from two or more and separate them with "/", such as "plus/minus" means addition or subtraction.**
~	**Indicates a range, such as "1~255" means the range from 1 to 255 .**

2. Command line format convention

Format	illustrate
Bold	**Command line keywords are the parts that are typed in the CLI** configuration, such as "show **version" to display the software version of the switch.**
Italic	**Command line parameters must be replaced by actual values, such as "show vlan vlan id" displays** the **VLAN number as vlan** **VLAN** information **of the id .**

3. Logo Convention

Logo	illustrate
Notice	**Reminds you of matters that should be noted during operation and configuration, and supplements the description of the operation content.**
illustrate	**Provide necessary explanations for the operation contents.**
warn	**Special attention should be paid to the following points: incorrect operation may result in data loss or equipment damage.**

Version Notes

Software Applicable Version Release	Time Revision Chapter		author

1.1.15	Created on 2020-12-21		Ma Haiyu
1.1.24	2021-01-12	Added WIFI probe, load balancing function description, and updated some parts Text description and pictures	Yang Yan
1.1.38	2021-03-30	Updated some text descriptions and pictures, and added SNMP function description bright	Yang Yan
1.1.44	2021-05-17Updated some text descriptions and pictures		Yang Yan
1.1.56	2021-12-15Updated some instructions and pictures		Yang Yan

1Product Installation

1.1 Interface Description

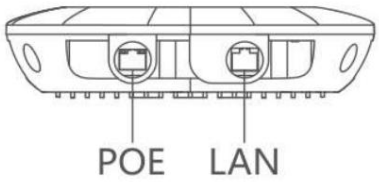


Figure 1 Schematic diagram of device interface

Figure 2 Schematic diagram of the power adapter interface

Table 1 Interface Description

object	Interface Name		illustrate
KyAir600E Device	POE device power supply interface		Connect the network cable to the "POE" port on the power adapter to power the device. Power supply and data transmission.
	The LAN data transmission interface can be connected to network devices such as switches via a network cable.		
Power adapter	The POE device power supply interface is connected to the "POE" port of the device through a network cable.		
	The LAN data transmission interface can be connected to network devices such as switches via a network cable.		

1.2 Line connection

Installation diagram:

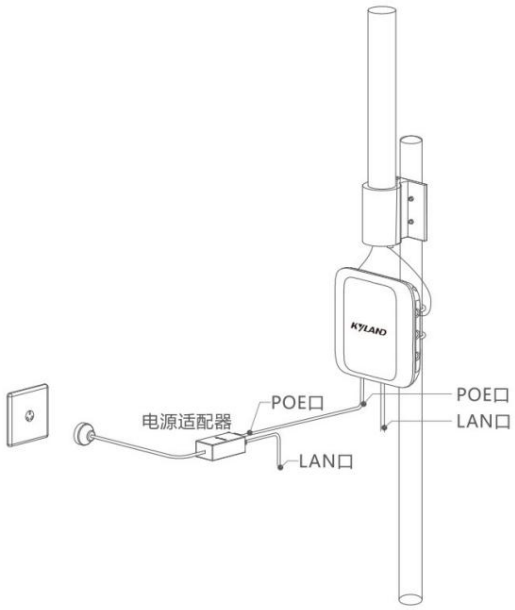


Figure 3 Route connection

1.3 Default

Table 2 Main parameters of factory default settings

project	KyAir600E
IP address	IPv4 dynamic (default fallback address: 192.168.10.1)
username	admin
password	123
Wireless Mode	Access Point
Safe Mode	WPA2-PSK
Key	kyland1234

2 Quick Configuration

2.1 Login

Before logging in, you need to perform a simple configuration on the computer connected to the device so that the IP addresses of the computer and the device **are in the same network segment.**

The operation steps are as follows (taking Windows 10 as an example):

1. Right-click the network icon in the taskbar, click Open "Network and Internet Settings", and a window as shown below will pop up.

mouth:

Figure 4 Network status page

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

Figure 5 Local Area Connection Properties

3. Double-click Internet Protocol Version 4 (TCP/IPv4) and a window as shown below will pop up:

Figure 6 IP settings

4. Set the IP address to the same network segment as the device , and the IP cannot be the same as the device. For example, the default IP configuration of the device is IPv4 dynamic, if there is a DHCP server in the link, the host can use the "automatic IP address" method; if there is no DHCP server, the device has a default backup address: 192.168.10.1, in this case, the host IP address can be set to static IP, such as 192.168.10.110.

5. Enter the default backup **IP address 192.168.10.1 of the device in the browser address bar** (if there is a **DHCP server,** Enter the dynamically obtained address), press Enter, and jump to the page shown in the figure below.

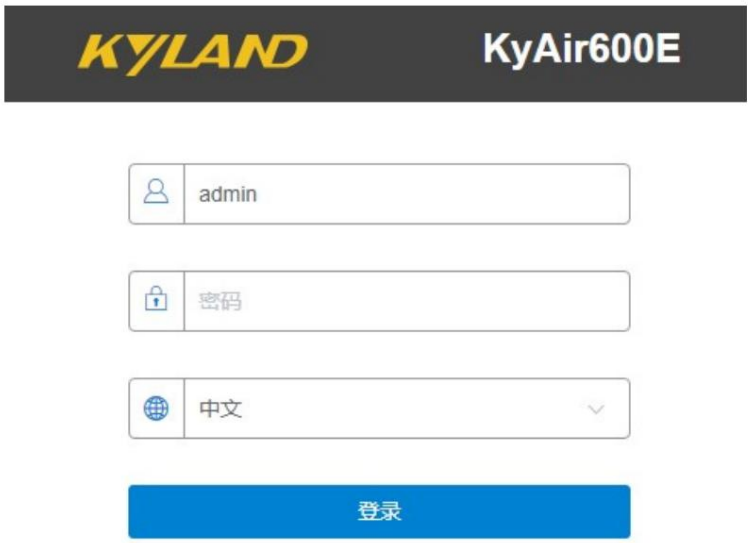


Figure 7 Device login interface

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

2.2 Wizard configuration wireless association

The wizard page can be used to quickly configure the wireless association between two devices (the wireless settings page can also be configured, see Chapter 4 for details).

4.1). The device supports four modes: access point, client, access point (WDS), client (WDS), client

The client and access point are used together, and the access point (WDS) and client (WDS) are used together.

CAUTION

Notice:

After the wizard configuration, the configuration will take effect in the wizard. Except for the configuration items in the wizard, other network and wireless configurations will be restored to default. value.

2.2.1 Configuring access points

(1) After successful login, you will enter the "Status Display" page by default. Click "Wizard" in the upper right corner to enter the "Wizard-Network" page, as shown below. The default IPV4 dynamic address is obtained. When the address is not successfully obtained, the default backup is enabled. The address is 192.168.10.1. The backup address can be switched to static IP type modification. When there is no DHCP server, To prevent backup IP address conflicts between devices, you can switch the IP type to static and change the device address to a planned address.

Figure 8 Wizard-Network

(2) Click "Next" to enter the "Wizard-Wireless" page, which displays the basic wireless

Parameters, as shown in the figure below. Modify the wireless parameters of the wireless frequency band to be used, for example, modify the wireless (5G wifi)

"Network Name" is 5Glink, and other settings remain unchanged (default "Wireless Mode" is Access Point, "Channel Bandwidth" is 80MHz， Frequency (Channel) is Auto, "Security Mode" is WPA2-PSK， The "Key" is kyland1234).

Figure 9 Wizard-Wireless

(3) Continue to click "Next" to enter the "Wizard-Complete" page, as shown below. Click the "Finish" button You can also click "Previous" to change the previous configuration.

Figure 10 Wizard-Complete

The access point configuration is complete.

2.2.2 Configuring the Client

(1) After successful login, you will enter the "Status Display" page by default. Click "Wizard" in the upper right corner to enter the "Wizard-Network" page, as shown below. The default IPV4 dynamic address acquisition, when the address is not successfully acquired, enable the backup address 192.168.10.1, the backup address can be switched to static IP type modification. When there is no DHCP server, be careful to prevent To prevent backup **IP** address conflicts **between devices , you can switch the IP type to static and change the device address to the planned address.**

Figure 11 Wizard-Network

(2) Click "Next" to enter the "Wizard-Wireless" page, which displays the basic wireless parameters of 2.4G and 5G . As shown in the figure below. Change the wireless mode of the wireless band to be used to client, and configure it to be consistent with the access point you want to associate with.

For example, if you want to **access** a **previously modified 5G band network named 5Glink ,**

Enter the point, change "Wireless (5Gwifi)" to client mode, "Network Name" to 5Glink, and "Security Mode" to

WPA2-PSK, the "key" is kyland1234, which is consistent with the access point, and other parameters can remain default.

Figure 12 Wizard-Wireless

(3) Continue to click "Next" to enter the "Wizard-Complete" page, as shown below. Click the "Finish" button

You can also click "Previous" to change the previous configuration.

Figure 13 Wizard-Complete

The client configuration is complete. The client can now successfully connect to the access point with the network name 5Glink .

2.2.3 Configuring Access Point (WDS)

(1) After successful login, you will enter the "Status Display" page by default. Click "Wizard" in the upper right corner to enter the "Wizard-

Network" page, as shown below. The default IPV4 dynamic address acquisition, when the address is not successfully acquired, enable the backup address

192.168.10.199, the backup address can be switched to static IP type modification. When there is no DHCP server, please note

To prevent backup **IP** address conflicts **between devices , you can switch the IP type to static and change the device address to a planned address.**

Figure 14 Wizard-Network

2) Click "Next" to enter the "Wizard-Wireless" page, which displays the basic wireless parameter configuration for 2.4G and 5G.

Modify the wireless parameters of the wireless frequency band you want to use, such as modifying the "Wireless

(5Gwifi)", set “Wireless Mode” to Access Point (WDS) , “Network Name” to 5GWDSlink, and keep other settings unchanged.

Change ("Channel bandwidth" to 80MHz, "Frequency (channel)" to automatic, "Security mode" to WPA2-PSK,

The "key" is kyland1234).

Figure 15 Wizard-Wireless

(3) Continue to click "Next" to enter the "Wizard-Complete" page, as shown below. Click "Finish"

You can also click "Previous" to change the previous configuration.

Figure 16 Wizard-Complete

The access point (WDS) configuration is complete.

2.2.4 Configuring the Client (WDS)

(1) After successful login, you will enter the "Status Display" page by default. Click "Wizard" in the upper right corner to enter the "Wizard-Network" page, as shown below. The default IPV4 dynamic address acquisition, when the address is not successfully acquired, enable the backup address 192.168.10.199, the backup address can be switched to static IP type modification. When there is no DHCP server, please note

To prevent backup **IP** address conflicts **between devices , you can switch the IP type to static and change the device address to a planned address.**

Figure 17 Wizard-Network

(2) Click "Next" to enter the "Wizard-Wireless" page, which displays the basic wireless parameters of 2.4G and 5G.

Configuration and wireless encryption options, as shown below. Change the wireless mode of the wireless band to be used to client (WDS),

Configure the network name, security mode, and key that are consistent with the access point (WDS) you want to associate with.

The 5G band network name is 5Glink access point (WDS), change "Wireless (5Gwifi)" to client (WDS) mode

Type, Network Name is 5GWDSlink, Security Mode is WPA2-PSK, Key is kyland1234,

Keep it consistent with the access point (WDS) and keep other parameters as default.

Figure 18 Wizard-Wireless

(3) Continue to click "Next" to enter the "Wizard-Complete" page, as shown below. Click the "Finish" button

You can also click "Previous" to change the previous configuration.

Figure 19 Wizard-Complete

The client (WDS) configuration is complete. At this time, the client (WDS) can communicate with the access point with the network name **5GWDSlink.**

(WDS) Connection successful.

Notice:

The client and access point are used together, the client (WDS) and access point (WDS) are used together, do not mix them.

3 Status

After successful login, the default display page is the status page, which displays some of the current parameter configurations of the device and real-time Monitor the current working status, which includes information, statistics, network, and log sub-pages.

3.1 Status-Information Page

The Status-Information page displays some of the current configuration information of the device:

Device information: The system information of the device, including the device name, device model, firmware version, running time, device time, between.

Figure 20 Device information

Network information: device network related information, including network mode, IP address, etc., which can be found in Settings-Network Settings in configuration.

Figure 21 Network information

Wireless information: Displays the device's 2.4G and 5G wireless information, including network name, wireless mode, frequency, security Mode, etc. can be configured in Settings-Wireless Settings.

Figure 22 Wireless information

Connected wireless device information: information about the other device when the device is associated, including network name, RSSI (signal strength), speed), peer device IPv4 address, peer device MAC address, TX/RX speed (i.e., sending/receiving speed), connection speed Connection time, etc.

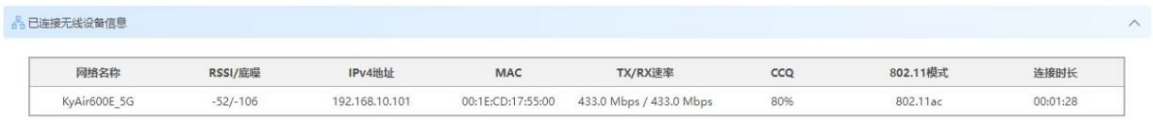


Figure 23 Connected wireless device information

3.2 Status-Statistics Page

This page displays the network interface statistics and traffic statistics of the device, which refers to the amount of data transmitted on the network per unit time. It is the main indicator for measuring network performance. The specific information is as follows:

Network interface statistics: includes the number of bytes and data packets received and sent by the device's wired and wireless ports.

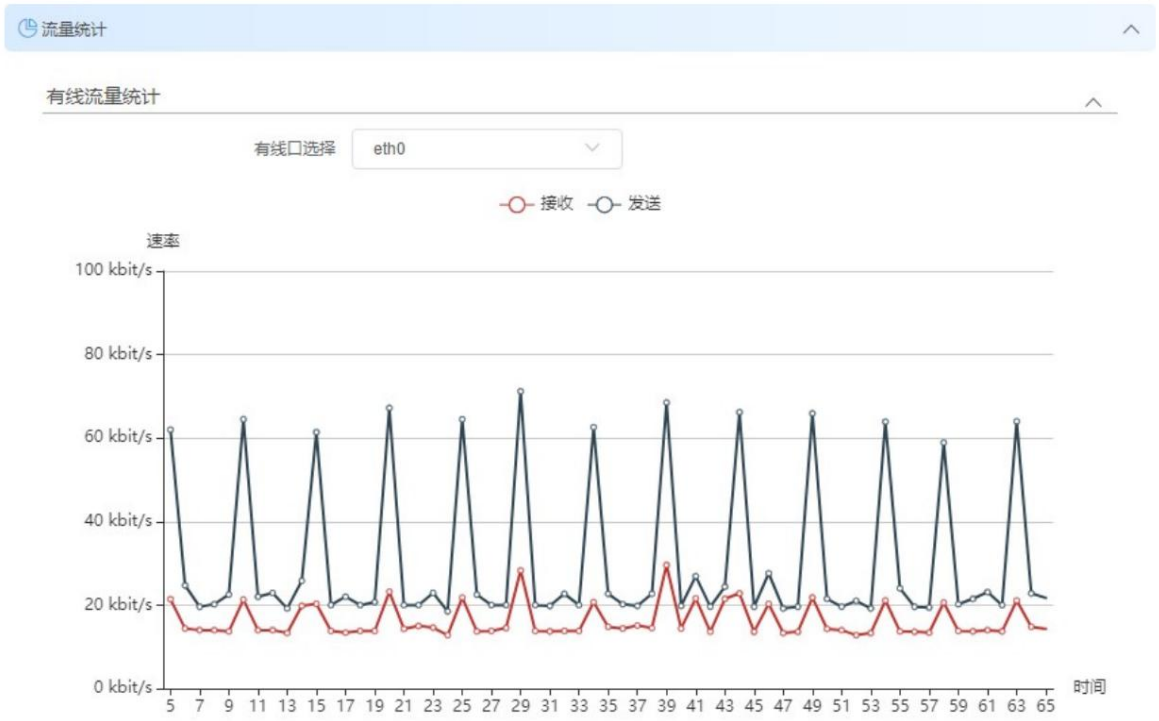
网络接口统计

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	00:1E:CD:17:54:FA	985733 Byte	1870547 Byte	5742	10715	0	0
eth1	00:1E:CD:17:54:FB	0 Byte	0 Byte	0	0	0	0
无线口							
ath0	00:1E:CD:17:54:FC	0 Byte	0 Byte	0	0	0	0
ath01	06:1E:CD:17:54:FC	0 Byte	0 Byte	0	0	0	0
ath1	00:1E:CD:17:54:FD	860318 Byte	972396 Byte	5424	4232	0	0

Figure 24 Network interface statistics

Traffic statistics: including wired traffic statistics and wireless traffic statistics, showing the sending and receiving of real-time traffic in the form of charts

More intuitive and clear.



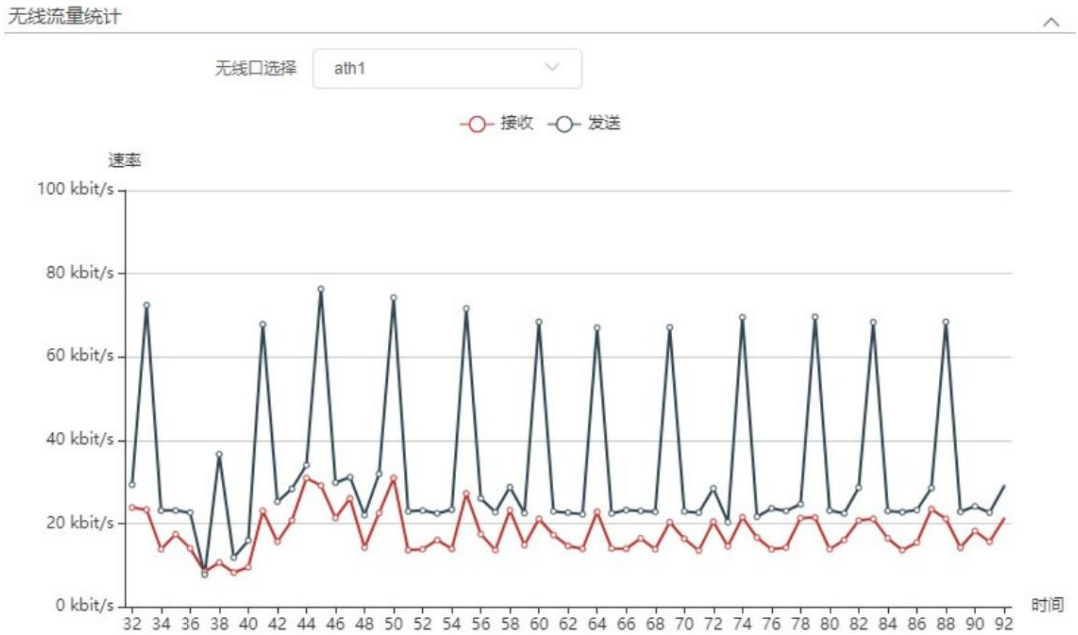


Figure 25 Traffic statistics

3.3 Status-Network Page

This page displays the device's routing table, ARP table, and bridge device list. The specific information is as follows:

Routing table: The routing table stores the paths to the network where the device is located.

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	192.168.10.254	br-lan	0
192.168.10.0	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 26 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	::	ath01	256
fe80::	64	::	ath1	256
::1	128	::	lo	0
fe80::	128	::	lo	0
fe80::	128	::	lo	0
fe80::	128	::	lo	0
fe80::	128	::	lo	0
fe80::9eb7:93ff:fee6:e6c8	128	::	lo	0
fe80::9eb7:93ff:fee8:e6c7	128	::	lo	0
fe80::9eb7:93ff:fee8:e6c8	128	::	lo	0
fe80::a0b7:93ff:fee8:e6c8	128	::	lo	0
ff00::	8	::	br-lan	256
ff00::	8	::	ath0	256
ff00::	8	::	ath01	256
ff00::	8	::	ath1	256

Figure 27 IPv6 routing table

ARP table: The device obtains **the correspondence between the used IP addresses and MAC** addresses within **30** seconds.

ARP 表

IP地址	MAC地址	接口
192.168.10.11	60:67:20:A9:B5:0C	br-lan
192.168.10.125	AC:BC:32:7E:6E:27	br-lan
192.168.10.233	9C:E8:95:6A:86:2F	br-lan

Figure 28 ARP table

Bridge device list: The device obtains the **MAC addresses and aging time** of other devices that communicate through it within **300** seconds

The corresponding relationship.

Figure 29 Bridge device list

3.4 Status-Log

This page displays the log information of the device.

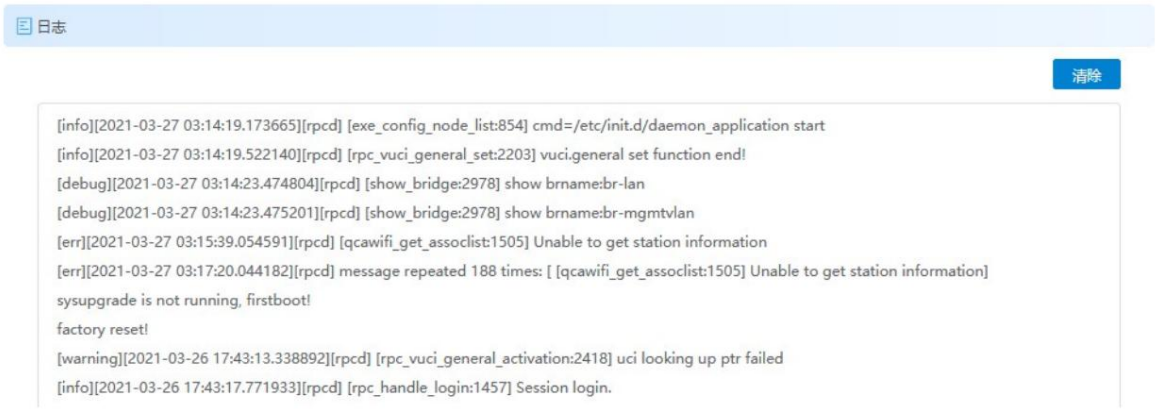


Figure 30 Log information

4 Settings

The settings page allows detailed configuration of the device, including wireless settings, network settings, traffic management, service settings, System settings.

4.1 Wireless Settings

The wireless settings page is shown below:

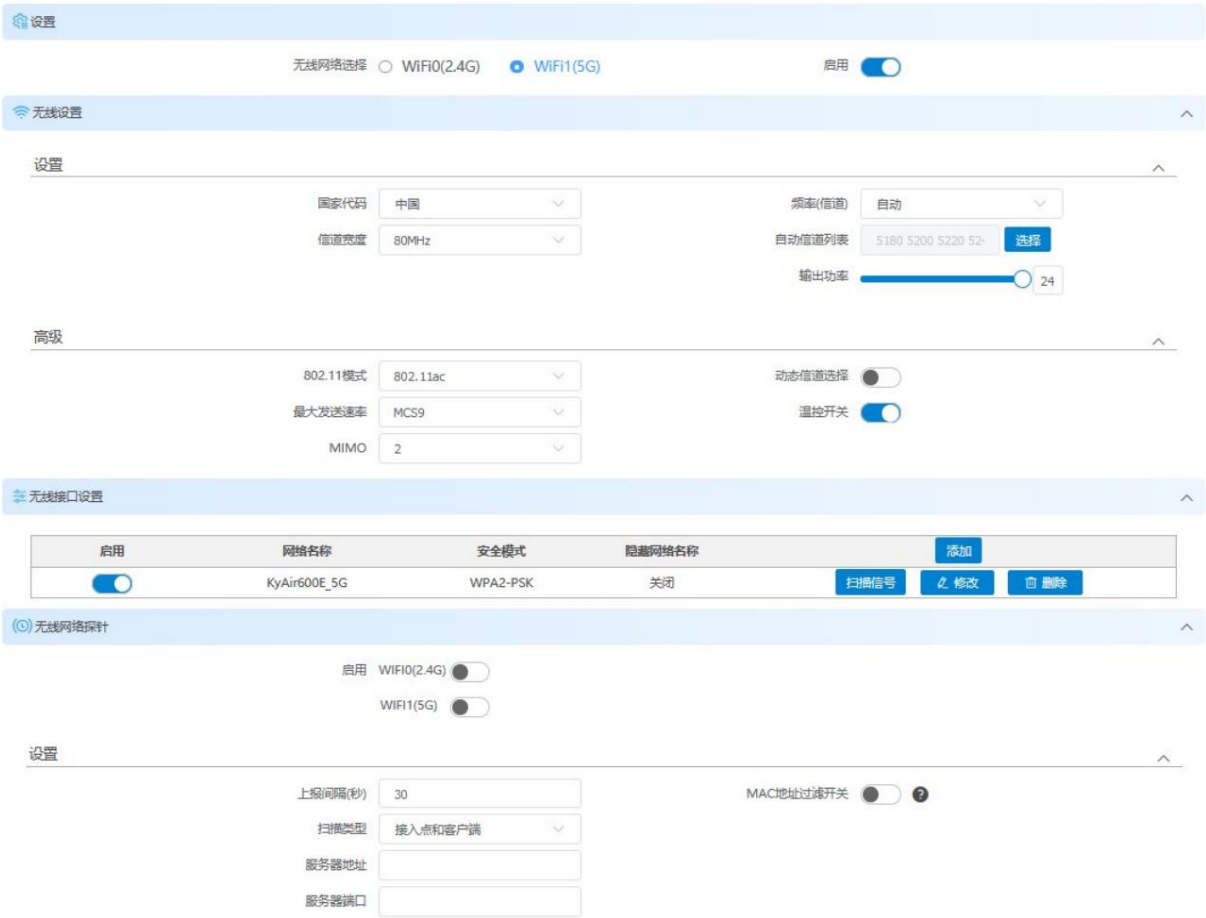


Figure 31 Wireless Settings - 5G Access Point Mode

The parameters are described as follows:

Settings : Select the wireless network. The device supports 2.4G and 5G bands . 5G wireless is configured. If it is turned off, the corresponding wireless frequency band is turned off.

Wireless Settings: The Wireless Settings page contains basic settings and advanced settings, which can configure the following parameters:

Country code: Different countries or regions have different standard channels. Select the corresponding country code according to your needs.

Channel Width: Limits the upper and lower limits of the frequency of the signal that is allowed to pass through the channel. (The default setting is automatic in client mode.

That is, automatically follow the configuration of the matching access point)

Frequency (channel): The center frequency of the carrier. When the access point and the client are associated, the frequency must be consistent.

Output power: The power of the wireless signal transmitted by the device. Users can adjust it according to the distance between devices. When the output power is increased

When the signal strength is increased, the transmission distance of the device will be increased.

802.11 Mode: 2.4G wireless only supports 802.11b/g/n, 5G supports 802.11ac and 802.11a/n, default

Think 802.11ac.

Maximum transmission rate: The maximum transmission rate of the device. By setting it, you can limit the maximum transmission rate of the device to ensure that the device

The stability of equipment performance.

MIMO: Users can select 1 or 2 to adjust whether the device works with 1 transmit and 1 receive or 2 transmit and 2 receive when wirelessly operating.

Dynamic channel selection: Dynamic channel selection is a function that detects and avoids interference.

When the interference reaches a certain level, the device will dynamically switch to a channel with less interference. This function takes effect when the frequency is set to "Auto".

After the channel is fixed, this function cannot be configured.

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

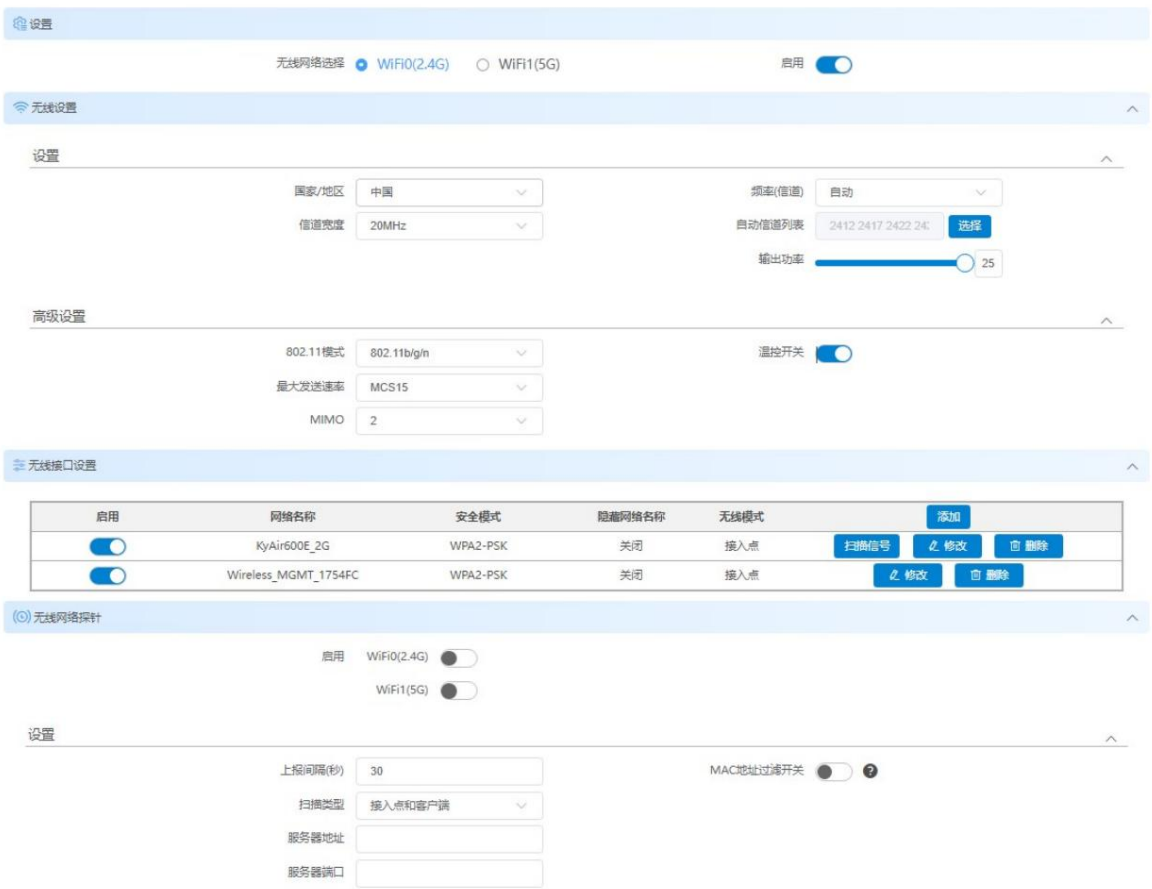


Figure 32 Wireless Settings - 2.4G Access Point

Wireless interface settings: You can add, modify, and delete wireless interfaces. You can add up to 8 wireless networks in one frequency band.

Interface. In the **2.4G wireless interface settings, two wireless interfaces are enabled by default.**

When the network interface has "MGMT" in the network name, the device can be accessed and managed, but the terminal cannot access the Internet.

This interface is the management wireless interface; the network interface without "MGMT" in the associated network name can be accessed by the terminal.

It also supports Internet access. If you configure the wireless network, click Modify and the following page will pop up.

CAUTION

Notice:

A network with "MGMT" cannot be restored by "Add" after being deleted, but can be restored by the Reconfiguration Wizard.

Figure 33 Wireless interface settings - normal wireless network

Figure 34 Wireless interface settings - MGMT manages wireless network

The parameters are described as follows:

ÿ Network name (SSID): A value used to control access to a wireless network. When other devices try to connect to this device,

Only when the SSID is set **to the same can they communicate with each other and establish a wireless connection. The network name only supports 1~32 characters (1**

Chinese characters occupy 3 digits), English, numbers, special symbols!@#$%^&*()_+-=<>?/:|[]{}`. and non-first and last spaces.

ÿWireless Mode: There are 4 wireless modes for the device, including access point, client, client (WDS), access point

(WDS).

Notice:

Client mode and access point mode are used together. Client (WDS) and access point (WDS) are used together. Do not mix them.

ÿSecurity mode: Encrypt the wireless connection. Users can choose the corresponding encryption mode according to their security requirements.

The wireless encryption of the devices to be associated with each other must be set to the same, otherwise, the association will fail.

ÿHide network name: Hide the wireless network name (SSID). After checking this function, other mobile phones, computers and other terminals

And the client device will not be able to search the network name (SSID) of the access point device, avoiding being connected by others without affecting

For your own use. (Only displayed on the access point page).

ÿClient Isolation: Enabling this function prevents devices connected to the same access point from communicating with each other.

Even if the IP addresses of different clients are repeated, it will not affect the communication (only the access point page is displayed).

ÿ MAC address lock: In a networking environment where there are multiple identical SSIDs , the client device can lock the MAC address by setting

Set the wireless MAC address of the corresponding access point to specify the access point to be associated (displayed only on the client page).

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

WDS access points do not support user speed limit function).

ÿMaximum number of users: The access point limits the number of connected users by setting this (displayed only on the access point page).

ÿMinimum access signal limit: The access point sets the minimum signal strength of the associated device.

Devices with a signal strength lower than the set value cannot be successfully associated; even if the association is successful, once the associated signal strength is lower than the set value, the client

The client will be kicked off the access point device. The value range is -95 ~ -1, the larger the value, the higher the signal strength

(Only displayed for the Access Points page).

ÿ MAC filtering: Allow devices in or outside the list to communicate (displayed only on the access point page).

ÿ 802.11r: Enables roaming of wireless terminal devices through the fast switching mechanism (Fast BSS Transition).

(Only supports WPA2-PSK security mode). When using the roaming function: Keep the network name, encryption method, and other security features between access point devices.

The mode and mobility domain are consistent, and the access points can communicate with each other. Other configurations can remain the default and can be customized as needed.

Please make changes on your own.

Figure 35 Wireless Settings - Wireless Network Probe

ÿ Wireless network probe: Enable this function to locate the terminal. When the terminal (such as mobile phone, computer, etc.) is in the device

When within the signal coverage range, the device can detect all messages sent by the terminal and report them to the server for analysis and calculation.

The following parameters can be configured.

ÿReporting interval: the time interval for reporting data to the server.

ÿServer address: The IP address of the server that receives the data.

ÿServer Port: Server port for receiving data.

ÿ MAC address filtering switch: The switch is off by default. When turned on , MAC address filtering will be performed.

Only the device data that meets the address filtering rules will be reported, otherwise it will be discarded. Supports adding up to 5 filtering rules, supports fuzzy filtering, match.

The following section will describe how to configure the wireless association between two devices (the wizard page can also be quickly configured, see section 2 for details). Chapter 2.2), the device supports four modes: access point mode, client mode, access point (WDS) mode, client Client (WDS) mode, it is recommended to use client mode and access point mode together, access point (WDS) mode and client (WDS) mode.

Notice:

When wirelessly associating, the network name, frequency (channel), security mode, and key of the access point and client device must be consistent.

4.1.1 Configuring access points

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

Figure 36 Wireless network selection

Click the "Modify" button in "Wireless Interface Settings" and configure the corresponding parameters as needed, such as modifying the "Network Name" For Wireless_link, click “Finish” to exit the current configuration pop-up window.

Figure 37 Wireless Interface Settings - Modify SSID

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

Figure 38 Save

4.1.2 Configuring the Client

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

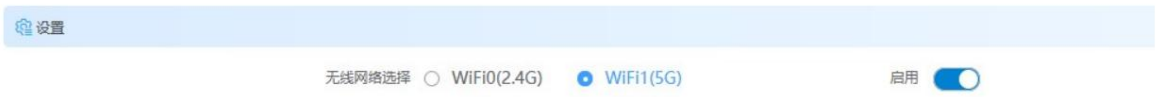


Figure 39 Wireless network selection

Click the "Modify" button in "Wireless Interface Settings" and change the "Wireless Mode" to Client and the "Network Name" to

Wireless_link, click Done.

Figure 40 Wireless interface settings - Modify wireless mode and SSID

Click "Save" in the upper right corner to complete the client configuration.

Figure 41 Save

At this point, the client can successfully connect to the access point with the network name Wireless_link .

4.1.3 Configuring Access Point (WDS)

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

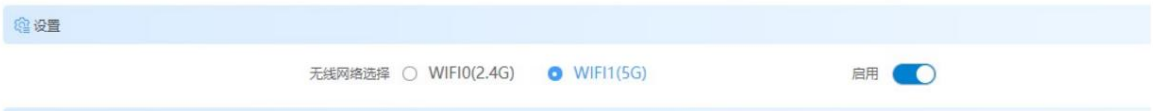


Figure 42 Wireless network selection

Click the "Modify" button in "Wireless Interface Settings", and then change the "Wireless Mode" to Access Point (WDS).

Set the Network Name to Wireless_WDS and click Finish.

Figure 43 Wireless interface settings - modify network name and wireless mode

Click "Save" in the upper right corner to complete the access point configuration.

Figure 44 Save

4.1.4 Configuring the Client (WDS)

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

Figure 45 Wireless network selection

Click the "Modify" button in "Wireless Interface Settings" and change the "Wireless Mode" to Client (WDS).

Set the Name to Wireless_WDS and click Finish.

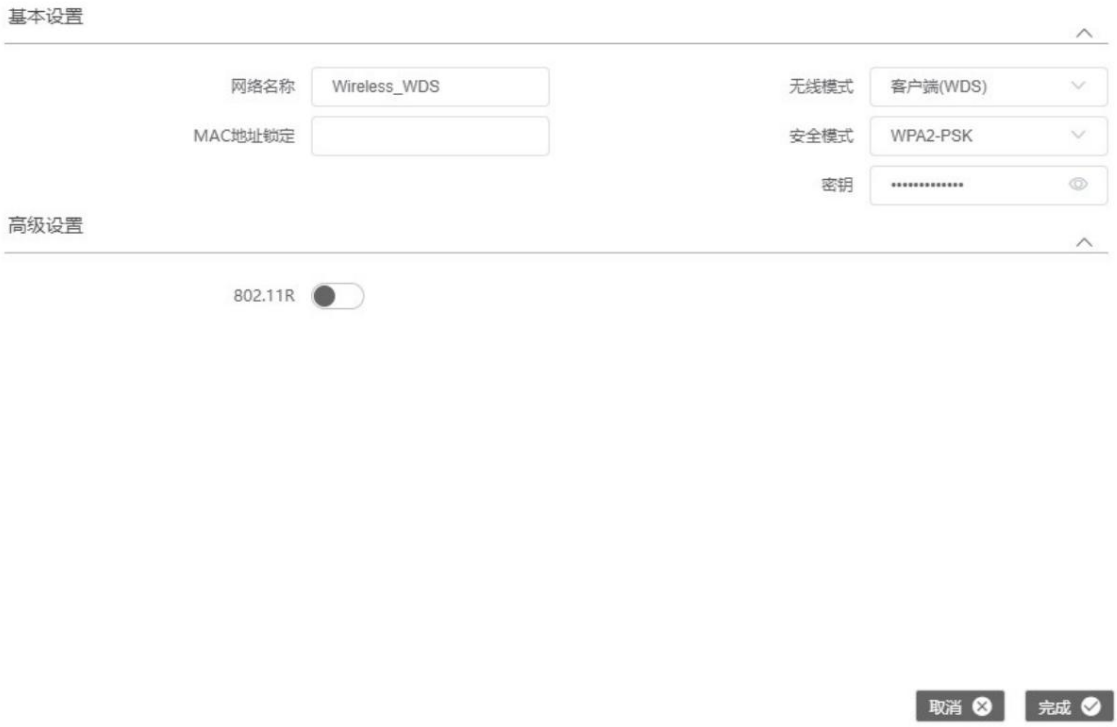


Figure 46 Wireless interface settings - modify network name and wireless mode

Click "Save" in the upper right corner to complete the client (WDS) configuration.

Figure 47 Save

At this point, the client (WDS) can successfully connect to the access point (WDS) with the network name Wireless_WDS .

4.1.5 Scan signal association

Sections **4.1.1-4.1.4 use the manual configuration method to configure association. In addition to the above methods, devices can also be connected through scanning Signal association.**

Here are the steps:

Device: Click the "Scan Signal" button at "Wireless Interface Settings".

Figure 48 Scan association-scan signal

2. Find the network name you want to associate on the scan result page, click the circle at the serial number to select it, and click the Click the "Check" button. Click "Lock" and the client will lock the MAC address of the network name.

Figure 49 Scan association-select network name

3. If the network name of the access point device is encrypted, a password input box will pop up. Enter the correct password. Key, click "OK". If you don't want to encrypt, just select Finish.

Figure 50 Scan association-enter key

Enter the key and click OK to jump to the wireless settings page, then click "Save".

When you log in, the wireless mode of the device will automatically switch to client mode, and the encryption method will automatically follow. This method is relatively simple.

Figure 51 Scan association-Save

4.2 Network Settings

4.2.1 Network Settings

You can select the network mode: bridge mode and routing mode, and configure the management VLAN related parameters. Management VLAN

Closed by default, see section 4.2.3 Advanced Settings for detailed instructions.

Figure 52 Network settings

4.2.2 Interface Settings

The interface settings are used in conjunction with the network mode in the network settings. When the network mode is selected as bridge mode, the interface settings are as follows:

As shown in the figure below:

Figure 53 Interface Settings - Bridge Mode - IPv4 Dynamic

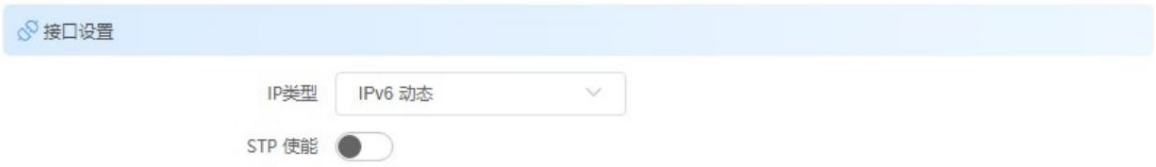


Figure 54 Interface Settings - Bridge Mode - IPv6 Dynamic

ÿ IP types include static, IPv4 dynamic, and IPv6 dynamic. The device enables IPV4 dynamic by default .

When the device is connected to the **DHCP server, it can obtain a dynamically assigned address .**

If **the IP** address fails **to be obtained ,** you can **enter the device page for management through the backup IP .**

Notice:

IPV6 dynamic has no backup address. When the dynamic address cannot be obtained correctly, the device will not be able to enter the page. Please use this function with caution.

able.

ÿ When the IP type is static, users can set **the IP address, subnet mask, default gateway and** DNS **according to their needs ;**

Make sure the IP address is different from **that of other devices in the same network to avoid IP address conflicts .**

The addresses must be in the same network segment.

ÿ If you want to enable the device to access the external network, you need to connect the device to the external network and modify the device IP and the Internet router in the LAN.

The IP is in the same network segment, the gateway is the **IP** address **of the upper-layer routing port to which it is connected , and the device is connected to the router via a network cable.**

Figure 55 Interface Settings - Bridge Mode - Static

IPv4 DHCP server: disabled by default, you can set the start address, end address, lease time, gateway after enabling

When mobile phones, computers and other terminals and client devices are wirelessly associated, **the device-assigned DNS parameters can be obtained .**

IPV4 address.

IPv6 DHCP server: disabled by default, enabled when the server is selected.

After the device is wirelessly associated, the **IPV6** address **assigned to the device can be obtained .**

STP enable: After enabling, network loops can be eliminated. When a loop occurs, the network link is guaranteed to be smooth.

IPv6 address: You can set the static IPv6 address of the device.

When the network mode is selected as routing mode, it is divided into LAN port settings and WAN port settings. When switching to routing mode, this page

The default bound interfaces of the device **LAN and WAN will be automatically displayed in the bridge interface settings .**

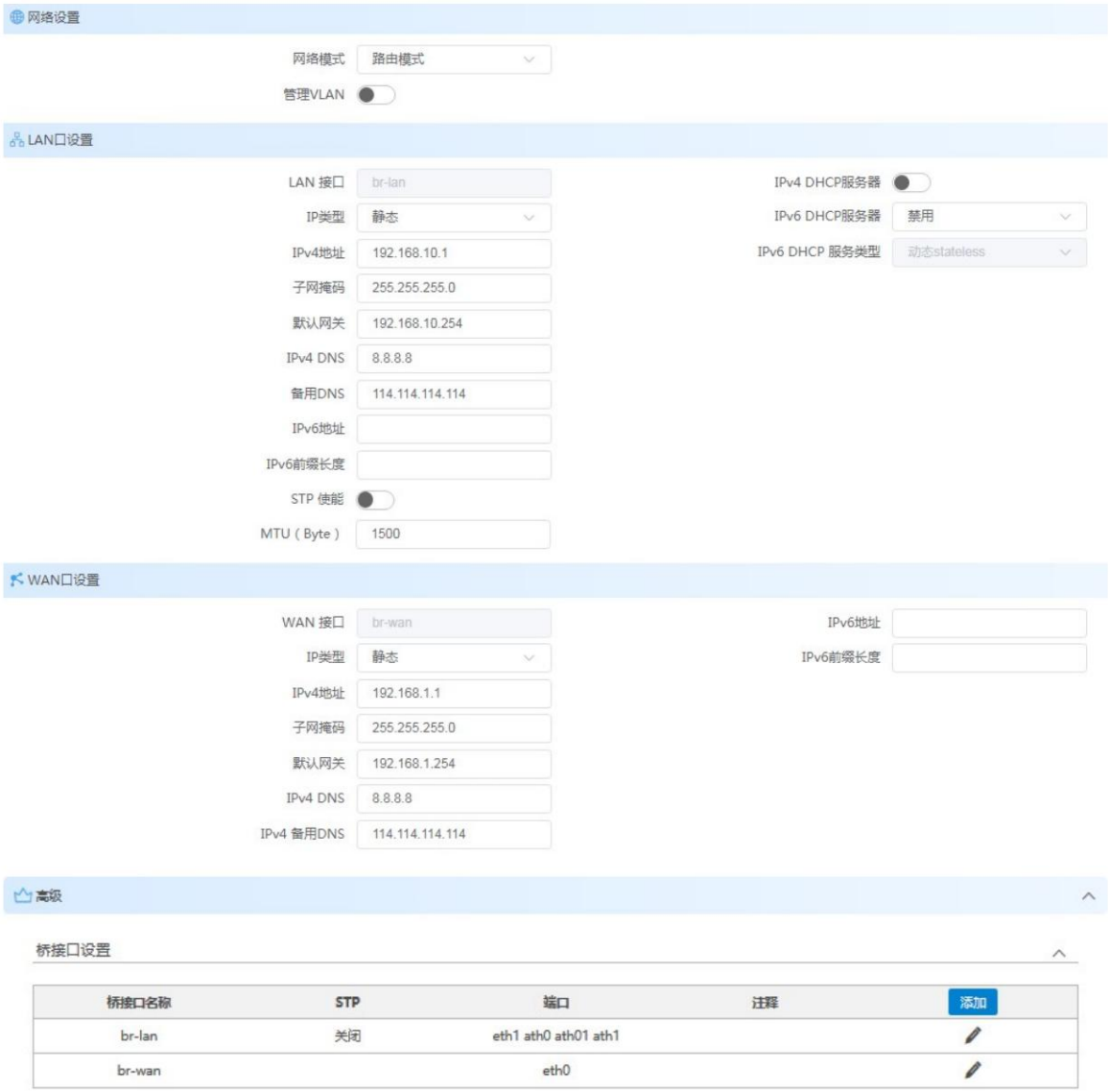


Figure 56 Interface Settings - Routing Mode

ÿ LAN port settings: For configuration, refer to the interface settings in bridge mode. After enabling routing, it is recommended to use static State address.

ÿ WAN port settings: The **IP** type **of the WAN interface is** the way **the WAN port obtains an IP address, which can be divided into static,** There are three types: **IPv4 dynamic and PPPOE . When setting a static IP , the user needs to manually set it to the same network as the network to be connected.**

When set to IPv4 dynamic , the device can automatically obtain the IP address from **the DHCP** server.

Address; when set to PPPOE , the user needs to fill in the **PPPOE Internet account and password, server name,**

The device uses dial-up authentication to obtain an IP address through a **PPPoE** server .

Notice:

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 a static IP , it cannot be set to**

The existing IP on the network can prevent IP conflicts. The device only allows one gateway. In routing mode, it is recommended to set the gateway on the WAN port.

Easy to connect to the Internet.

4.2.3 Advanced Settings

Advanced settings include bridge interface settings, VLAN, Ethernet interface settings, IPv4 static routing, IPV6 static routing , Isolate by,interface.

Bridge interface settings: You can add a bridge interface by yourself and configure the bridge interface parameters when adding it, such as IP address, subnet mask, etc. The above parameters are optional and can be set according to needs. You can also delete the newly created bridge.

Note that the bridge interface created by the system cannot be deleted. The device contains five interfaces by default: eth0, eth1, ath0, ath01, and ath1 . eth0 corresponds to the LAN port on the power adapter , eth1 is the LAN1 port on the device , and ath0 is the 2.4G wireless interface. ath01 is the 2.4G management wireless interface, and ath1 is the 5G wireless interface. The bridge position of the interface can be allocated according to needs.

The following figure shows the default display of a bridge interface in routing mode.

Notice:

When there are multiple bridge interfaces, there can be only one gateway. Please plan the network reasonably and set the gateway effectively.

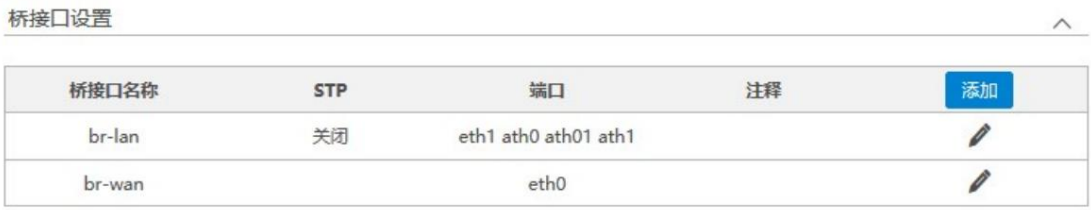


Figure 57 Bridge interface settings

VLAN: The VLAN function allows users to add multiple VLAN interfaces on each network interface . The range is 3 to 4094, and each ID represents a different VLAN. As shown in the figure below, on ath0 (i.e., wireless link), add Add VLAN 10 .

Figure 58 VLAN

The VLAN function needs to be used together with the bridge interface settings. As shown in the figure below, both devices eth0 and ath0 are added.

VLAN, ID 10 , and put them in a newly created bridge interface VLAN10 (can also be the default bridge interface).

The **eth0 interface needs to be connected to a device that supports VLAN 10 (such as** a **VLAN switch, and the switch port needs to support VLAN 10)**

You can access the device for management through the bridge address of **eth0.10 . For wireless services through VLAN , no**

The peer device associated with the line must also support VLAN 10 (for example, add VLAN 10 **to ath0).**

Figure 59 VLAN settings

Common connection methods are shown in the figure below:

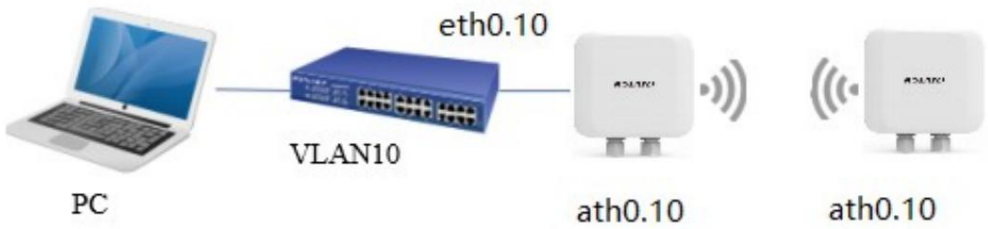


Figure 60 VLAN connection diagram

Management VLAN: **After you** enable the management **VLAN in the network settings** and save **it, the device wired**

and the VLAN of the wireless interface . A new mgmtvlan will be created in the bridge interface settings . Add the created VLAN interface to

In mgmtvlan , after connecting a device that supports **VLAN3 (such as** a **VLAN switch that supports VLAN ID 3), you can**

Use the IP address **set in** the management **VLAN to access the device page for management, but the management VLAN does not support data service forwarding.**

Figure 61 Management VLAN settings

Ethernet interface settings: Users can set the Ethernet interface for eth0 (LAN port **on the power adapter).**

Select the auto-negotiation mode, and the Ethernet port of the device will automatically negotiate the maximum transmission rate according to the connected device; select non

During auto-negotiation, users can set the speed (10M/100M/1000M) and duplex (full duplex) of the device Ethernet port.

duplex/half-duplex).

Figure 62 Ethernet interface settings

IPv4 static routing: This function can set IPv4 static routing. Click Add to pop up the following page:

Figure 63 IPv4 static route-add

ÿOutgoing interface: the bridge interface of the corresponding network segment.

ÿTarget network: that is, the target network segment.

ÿHop number: the number of routers passed during the transmission process.

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

Figure 64 IPv4 static routing

IPv6 static routing: This function can set IPv6 static routing. Click Add to pop up the following page:

Figure 65 IPv6 static route-add

After configuring the corresponding parameters, click Finish, as shown below:

Figure 66 IPv6 static routing

Interface isolation:

Wired interface isolation: closed by default. When enabled, the wired ports of the devices cannot communicate with each other.

Wireless interface isolation: It is disabled by default. When it is enabled, the wireless interfaces of the device cannot communicate with each other.

Figure 67 Interface isolation

4.3 Traffic Management

This page allows you to configure firewall settings, interface speed limits, and QoS priorities.

Firewall: When users want to block certain devices, they can use a firewall to achieve this function. This function is disabled by default.

Figure 68 Firewall

Note: In the filter settings, the "destination" refers to the device of the currently configured firewall, and the "source" refers to the device or phone at the other end.

For example: the device is directly connected to a computer, and firewall rules are configured on the device. The computer is the source and the device is the destination.

If you cannot distinguish the source and destination, you can configure two relative rules:

ÿFilter the report of the device with **IP address 192.168.10.100** on **eth0** port (corresponding to **the LAN** port **on the power adapter) .**

arts.

The firewall is enabled, the default firewall rules are discarded, and two rules are added to the IP filtering settings.

(1) The target is receiving, the interface is eth0, the protocol is IP, the source IP/mask is 192.168.10.100/32, the destination

The IP/mask is 192.168.10.1 (the device's IP address)/32.

(2) The target is receiving, the interface is eth0, the protocol is IP, and the source IP/mask is 192.168.10.1 (the IP address of the device).

The destination IP/mask is 192.168.10.100/32.

Figure 69 IP filtering settings

ÿFilter the report of the device with MAC address 00:00:00:00:00:01 on eth0 (LAN port on the power adapter) .

arts.

ÿ The firewall is enabled, the default firewall rules are discarded, and two rules are added to the MAC filtering settings:

(1) The target is receiving, the interface is eth0, the source MAC is 00:00:00:00:00:01, and the destination MAC is the device bridge MAC address.

(2) The target is receiving, the interface is eth0, the source MAC is the bridge MAC address of the device , and the destination MAC is 00:00:00:00:00:01.

Figure 70 MAC filter settings

Interface speed limit: You can limit the upload and download rates of the device interface, as shown in the figure below.

Figure 71 Interface speed limit

QoS priority: QoS (Quality of Service) refers to the ability of a network to use various basic technologies to

It is a network security mechanism that provides better service capabilities for specified network communications and is used to solve network latency problems.

Delays and blockages.

Figure 72 QoS priority

Target CoS: Target CoS, ranging from 0 to 7, corresponding to the priority;

Target DSCP: Target DSCP, Differentiated Services Code Point,

The priority is distinguished by the code value, ranging from 0 to 63;

The following are the restrictions, and the messages that pass the restrictions are converted:

Source MAC: Source MAC

Destination MAC: Destination MAC

VLAN ID: VLAN.

CoS: priority.

Ethernet Type: Ethernet type.

DSCP: DSCP.

IP Type: IP type.

Source IP: source IP address.

Destination IP: destination IP address.

Source port: refers to the local port.

Destination port: refers to the remote port.

4.4 Service Settings

Time setting: Set the time of the device, and you can choose different time zones; the time synchronization methods are divided into manual time synchronization and NTP time synchronization.

For manual time synchronization, you can set the time yourself, or click to synchronize with the computer time. For NTP time synchronization, you need to fill in the server address,

The default **NTP port and time interval are 15 minutes. At this time, you need to configure the device to access the external network (refer to 4.2.2 Interface Settings).**

If the device is set to the **NTP** server , **it will automatically calibrate the device time from the NTP server and display it on the status display page.**

Figure 73 Service Settings - Time Settings (Manual)

Figure 74 Service Settings - Time Settings (NTP)

Remote management: When SSH is enabled, use terminal connection software that supports the SSH protocol, for example: SecureCRT, Xshell , etc. When using the software, fill in the device's IP address, login account and password to log in to the device.

When **SSH is disabled, you cannot log in to the device backend.**

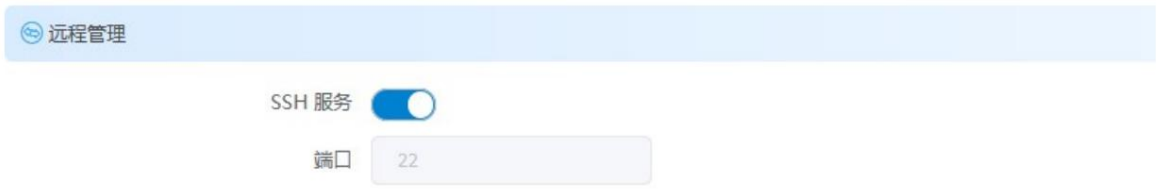


Figure 75 Service Settings - Remote Management

Web service: Users can choose http or https to log in to the device page.

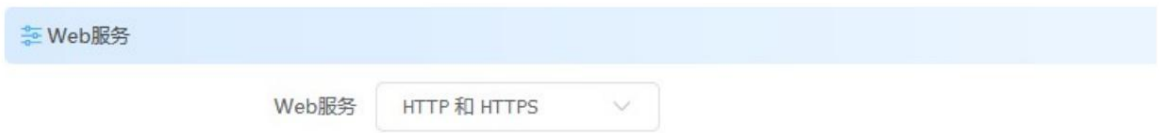


Figure 76 Service Settings-Web Service

Device discovery: When this function is enabled, please use it with a dedicated device discovery tool. The tool window will display the discovered The device's MAC address, IP address, and other related information.

Figure 77 Service Settings - Device Discovery

Scheduled Restart: This function allows you to schedule a restart of the device. This function is disabled by default.

Figure 78 Service Settings - Scheduled Restart

Remote log: Enable the remote log function and set the IP **of the** remote **log** server **and the server port to 514.**

After saving the application, you can view the relevant log information in real time on the remote log server.

Figure 79 Service Settings - Remote Log

AC management: After enabling this function, it must be used in conjunction with the **AC management system. This function is enabled by default.**

Location: The deployment location of the device. You can fill in the device location you want to display on the AC map as needed.

Discovery mode: The way AP discovers AC , which can be divided into manual and automatic.

Timing, you can add the main AC address and backup AC address, the added IP address is the IP of the **AC management system .**

The device IP and AC IP must be in the same network segment. When going online at Layer 3, if you choose automatic discovery, you need to

Enter the **IP** address **of the AC in the Option 43** field . **It is recommended that non-professionals configure the discovery method manually.**

DTLS enabled: After enabling, the device sends messages of the DTLS encrypted type, which is more secure.

Client Retrieval: Enable this feature to facilitate AC to retrieve the client when the client is disconnected from the access point and leaves the AC .

When the client is online, it will enter the recovery mode. Click the client recovery function on **the AC , and the access point can also enter the recovery mode.**

You can then reconnect with it online.

Notice:

The client device can only be connected to the access point device when this function is enabled and the access point device also has the AC function enabled and joined.

The same AC system can be successfully joined to AC.

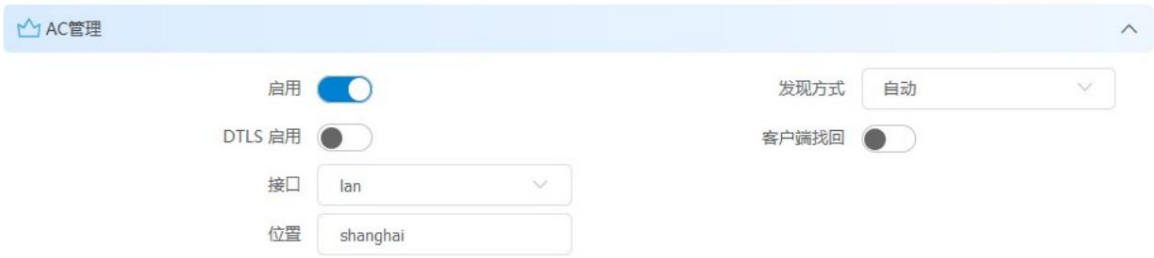


Figure 80 Service Settings-AC Management

ÿ **Ping software dog: used to continuously monitor the operation of the device. The device can ping the target host or device** for a long time

If a **defined** number of **replies are not received by the device, the tool will cause the device to reboot.**

It is recommended that users enable this function on the side with the wireless mode set to "Client". It is not recommended that users enable this function on the side with the wireless mode set to "Access Point".

Enable this function on one side. This function is disabled by default.

ÿ **Ping interval: the time interval between** two **pings ,** in seconds.

ÿ **Ping IP** address: Generally fill in the **IP** address **of the target host or device . "Client" mode enables Ping software**

When the client is connected to a dog, you can fill in the **IP** address **of the access point device to which the client is connected .**

ÿ Startup delay: When the device system starts, the device will start **pinging the target host after the set delay time.**

Machine, unit is seconds.

ÿ **Ping failure times: When the number of consecutive ping failures reaches the set value, the device will restart.**

CAUTION

Notice:

If you want to modify the parameter configuration of the Ping software dog, please disable **the Ping software dog first. After the disabling takes effect, enable the Ping software dog .**

Configure new parameters for the software dog.

Figure 81 Service Settings - Ping Software Dog

Load balancing: Dynamically adjust the number of terminals that can be associated with each access point device based on the number of associated users and traffic thresholds set

The number of APs can be adjusted to achieve load balancing. In the same balancing group, the master AP (whoever is powered on first) is the master AP.

The device is turned off by default.

ÿSwitch group ID: used to identify the balancing group.

ÿSwitch group IP: used to identify the balancing group. It is equivalent to the virtual IP address of the master AP .

The device at this IP address reports its own status to facilitate the master AP scheduling balance. This IP address cannot be the same as the device LAN address

Otherwise, the load balancing function will not take effect.

Notice:

Group ID and group IP are unique identifiers of the balancing group. When there are multiple APs in a LAN, these two values must be the same.

In the same load balancing group.

ÿLoad balancing mode: divided into traffic flow and user number mode, that is, balancing devices according to traffic flow or user number.

ÿHigh -load access window time: the total time of the access window.

ÿ High load minimum authentication interval: limit the client access frequency, the window time divided by the authentication interval should be greater than or equal to the window time.

Number of mouths.

ÿ High-load access window times: The maximum number of times an access point denies terminal access.

When the set value is reached, the client will be allowed to access after another request. If the number of times is not reached, the window time and the number of times will be cleared.

zero.

ÿFlow balancing threshold: The maximum flow rate that triggers the load balancing algorithm when the load balancing mode is flow. It is usually equal to the flow rate.

When the flow rate is less than the threshold, the client can access it at will; when the flow rate is greater than the threshold, the current device will be judged.

Check whether the flow difference between the flow rate and the device with the minimum flow rate reaches the set flow balance difference. If it does not reach the difference,

The device allows the client to access; otherwise, it denies the client access.

ÿFlow balance difference: used in conjunction with flow balance threshold.

ÿ User number balancing threshold: The maximum number of users that trigger the balancing algorithm when the load balancing mode is user number. Usually the same as the user number.

When the number of users is less than the balance threshold, the client can access at will; when the number of users is greater than the threshold,

The difference between the number of clients connected to the current device and the number of clients connected to the device with the least number of clients will be determined. If it is less than the user

If the difference is greater than or equal to the number of users, the device allows the client to access; if the difference is greater than or equal to the number of users, the device denies the client access.

ÿ User number balance difference: used together with user number balance threshold.

Figure 82 Service Settings - Load Balancing (Traffic Mode)

Figure 83 Service Settings - Load Balancing (User Count Mode)

ÿ SNMP: Simple Network Management Protocol, used to manage devices. You can connect to the device through dedicated network management software.

Internally, you can read and write certain information about the device, and modify its configuration. This feature is disabled by default.

ÿ SNMP v2: uses community name authentication, plain text transmission, and has low security. When using network management software, fill in the following settings:

You can connect to the device by typing the two group names you set.

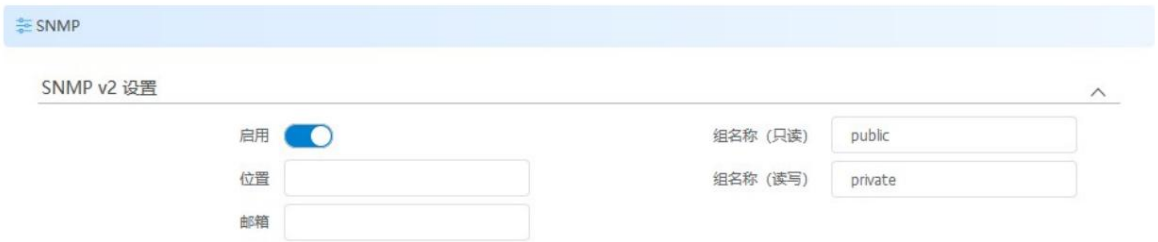


Figure 84 SNMP-SNMP v2

ÿ SNMP v3: Improves the security and management mechanisms based on SNMP v2 .

The corresponding authentication and encryption information can significantly improve security.

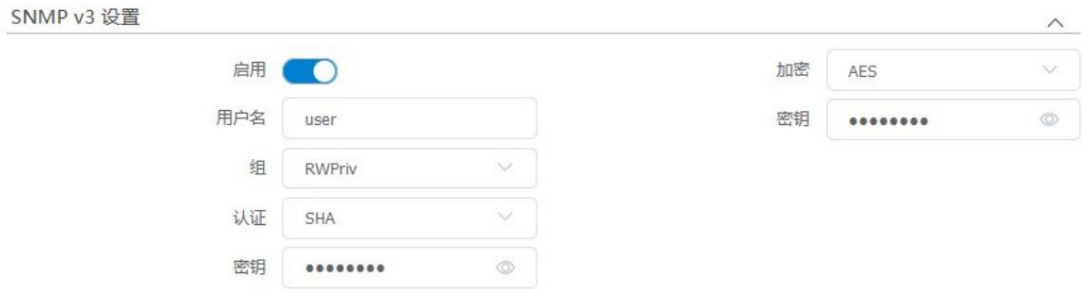


Figure 85 SNMP-SNMP v3

4.5 System Settings

The system settings interface is divided into three items: system settings, firmware configuration, and account management, as shown below:

Figure 86 System settings

ÿDevice name: Users can set the device name to the name they need according to their needs.

ÿLanguage : Users can select the page display language according to their needs.

ÿLogin timeout: When the user does not operate the device for a period of time exceeding the timeout setting, the page will automatically jump to the login interface.

noodle.

ÿConfiguration file export: Click to generate backup, and all current configurations on the web page will be backed up to a local file.

Notice:

The configuration file contents cannot be modified manually.

ÿConfiguration file import: Click Select File, select the previously downloaded configuration file, click Upload Backup, and click OK.

Click Restart Now to restore the device configuration to the state when the configuration file was backed up.

ÿOne -click information export: Click download to export the system log file, which contains the configuration file.

ÿ Factory Reset: Click on the reset button on the web page, and the page will jump to the waiting page.

Switch to the default IP address and the device configuration will be restored to the factory settings.

ÿRestart : Click Restart to restart the device system. After the restart is complete, the configuration remains unchanged.

ÿFirmware upgrade: Click Select File, select the version to be upgraded, click Upload Firmware, and after the firmware is uploaded,

Select whether to keep the configuration file, click OK, and the device will start upgrading.

ÿChange password: When the user password change function is enabled, users can log in to the device web page to change the password according to their needs.

To enhance information security, please change your device password regularly and try not to use a password that is too simple.

Passwords can be numbers, letters, birthdays, etc. Passwords are saved as separate modules. When changing passwords, please do not change other configurations at the same time.

Set.

5 Tools

The tool page is divided into two sub-pages: **Ping IP and Link Test. The details are as follows:**

5.1 Ping IP

Enter the **IP address of a device and click** Ping. The **Ping** result **will be displayed in the collected data , as shown below:**

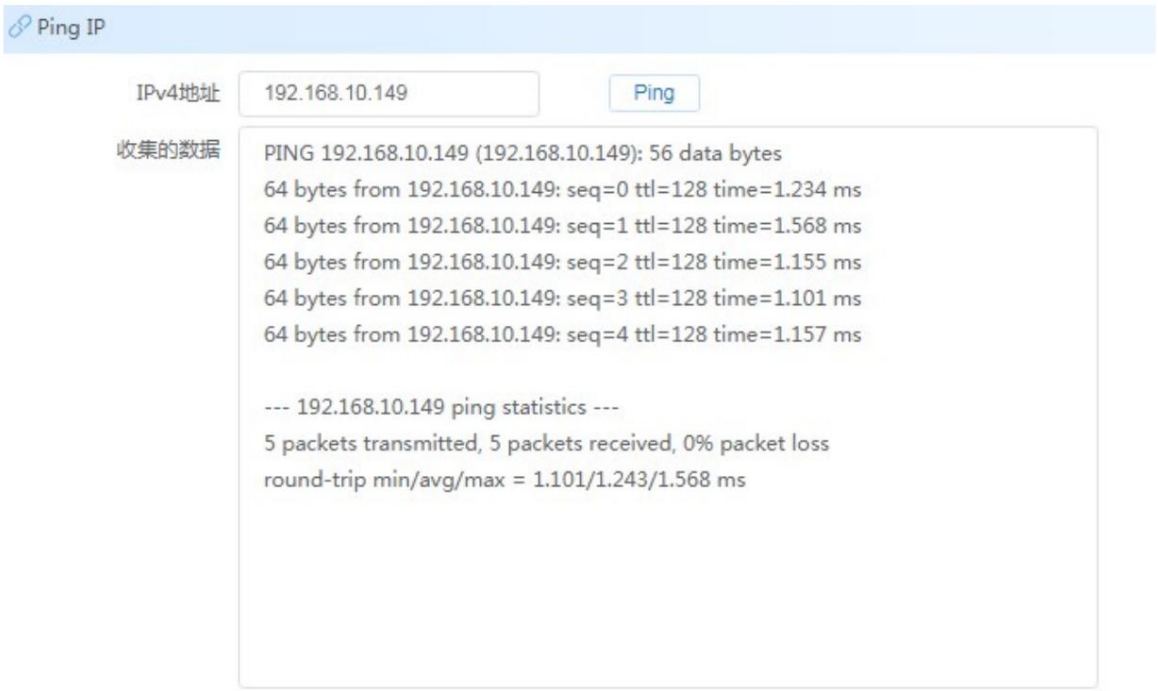


Figure 87 Ping IP

5.2 Link Test

The **Iperf test can test the maximum bandwidth performance and report bandwidth, delay jitter and packet loss. It is divided into customer Client mode and server mode are used to test the throughput of the wireless end between devices. Device 1 selects "Server".**

The **Iperf interval is the interval for displaying throughput on the web page. Select “Client” for** device **2** and fill in the **Iperf server.**

The IP address of device 1. The number of Iperf threads is the number of threads running simultaneously when testing throughput. It is recommended to set it to 10.

The Iperf test time is the number of seconds to run Iperf . The Iperf interval is the interval for displaying the throughput on the web page.

After filling in the data, click the "Start" button to start the test.

Figure 88 Link test - client mode

Figure 89 Link test - server mode

6 Logout

Logout is used to log out of the device page. When the user clicks Logout in the upper right corner, the user will be redirected to the login page.

Figure 90 Logout

7 Troubleshooting

1. Why can't the terminal access the Internet after being associated with the AP ?

ÿConfirm whether the upper-layer router can access the Internet.

ÿConfirm whether the terminal can obtain the correct IP address. Please re-associate and check whether the terminal IP is the upper-level router.

The allocated network segment address.

2. The terminal cannot connect to the AP?

ÿ The signal strength is too poor. Check whether the transmit power is set to the highest. If there are obstacles blocking the AP, adjust the AP deployment position.

Install or add APs.

ÿ Check whether **the AP has enabled the weak signal rejection function, adjust the threshold or disable the function.**

ÿ Check whether **MAC** address filtering **is set and add the terminal's MAC address to the whitelist.**

ÿCheck whether the wireless key is correct.

3. How to retrieve **the AP 's IP address if I forget it?**

ÿ Use the device discovery tool to query.

ÿRestore the factory configuration and **log in using the default backup IP address 192.168.10.1 .**

4. How to perform a factory reset?

ÿ System Settings page, Firmware Management > Factory Restore.

5. The download rate is very low after connecting to the AP ?

ÿ Check whether the network cable is a Gigabit cable above CAT5E .

ÿ Whether the ports of switches and other devices support Gigabit speed.

ÿ Check the interface configuration to see if it is Gigabit full-duplex.

The query path is as follows: Settings > Network Configuration > Advanced > Ethernet Interface Configuration. The recommended configuration is auto-negotiation:

Figure 91 Query path

ÿ Check the wireless configuration 802.11 mode, channel, width, maximum transmission rate and MIMO quantity. It is recommended to refer to

Parameter settings are shown below.

Figure 92 Checking the wireless configuration

ÿ Check the encryption method. When sending the configuration from **the AC ,** please note that the TKIP **authentication type will limit the wireless rate to 54Mbps.**

It is recommended to use CCMP authentication type. The security mode that can be configured on the device page adopts CCMP authentication type by default.

The page authentication type cannot be configured.

Appendix List of Abbreviations

Serial number	definitions and abbreviations	illustrate
1	Access Point (AP)	Access Point
2	Client	Client
3	DCS (Dynamic Channel Selection)	Dynamic channel selection