

IWA5824-624Xi

802.11a/b/g/n/ac/ax dual-band high performance AP

Content

1	Product information	3
1. 1	Default parameters	3
2	Quick configuration	4
2. 1	Login	4
2. 2	Wizard configuration for wireless association	6
2. 2. 1	Configure Access Point	6
2. 2. 2	Configure Client	8
2. 2. 3	Configure Access Point (WDS)	9
2. 2. 4	Configure Client (WDS)	11
3	Status	13
3. 1	Status - Information page (MESH mode)	13
3. 2	Status - information page (MESH Mode)	13
3. 3	Status-statistics page	15
3. 4	Status-network page	16
3. 5	Status-log	18
4	Settings	19
4. 1	Wireless settings in Mesh Mode	19
4. 2	Wireless settings in Normal Mode	22
4. 2. 1	Configure Access Point	26
4. 2. 2	Configure Client	27
4. 2. 3	Configure Access Point (WDS)	28
4. 2. 4	Configure Client(WDS)	29
4. 2. 5	Associating devices by scanning signals	30
4. 3	Network settings	32
4. 3. 1	Interface Settings	32
4. 3. 2	Advanced settings	36
4. 4	Traffic management	41
4. 5	Service settings	44
4. 6	System settings	48
5	Tools	50
5. 1	Ping IP	50
5. 2	Link Test	50
6	Logout	52

1 Product information

1.1 Default parameters

Table 2 Main parameters of the default factory settings

Projects	IWA5821-624Xi
IP address	192.168.1.1
username	root
password	admin
Wireless Mode	Access Point
Encryption	WPA2-PSK/WPA3-SAE
Key	1234567890abc

2 Quick configuration

2. 1 Login

Before logging in, a simple configuration of the computer connected to the device is required so that the IP of the computer and the device are in the same network segment. The steps are as follows (Take Windows 10 as an example).

1. Right-click the network icon in the taskbar and click to open "Network & Internet " to bring up the window shown below.

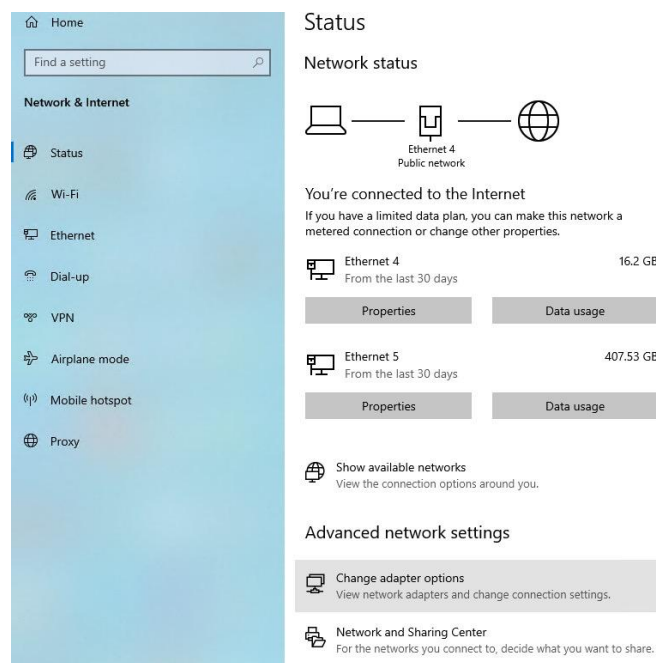


Figure 2- 1 Network status page

2. Click on Change Adapter Options->Ethernet->Properties, go to the property configuration page, as follows.

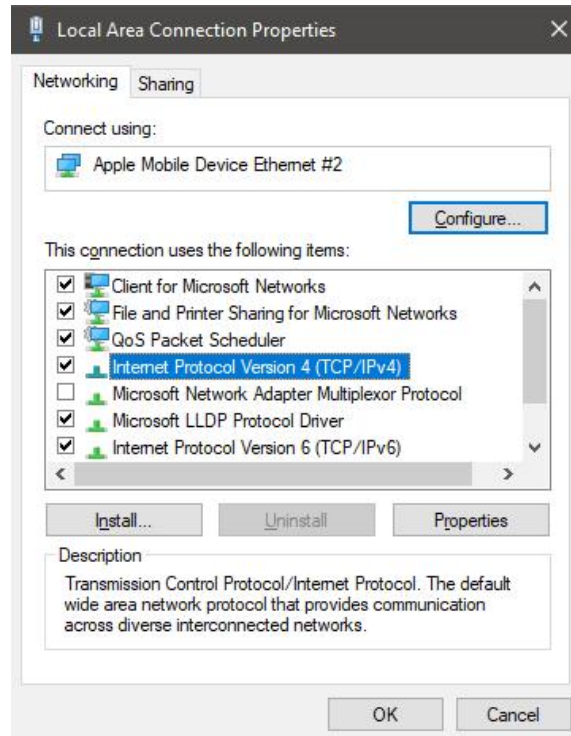


Figure 2-2 Local connection properties

3. Double click on Internet Protocol version 4 (TCP/IPv4), The window shown below pops up.

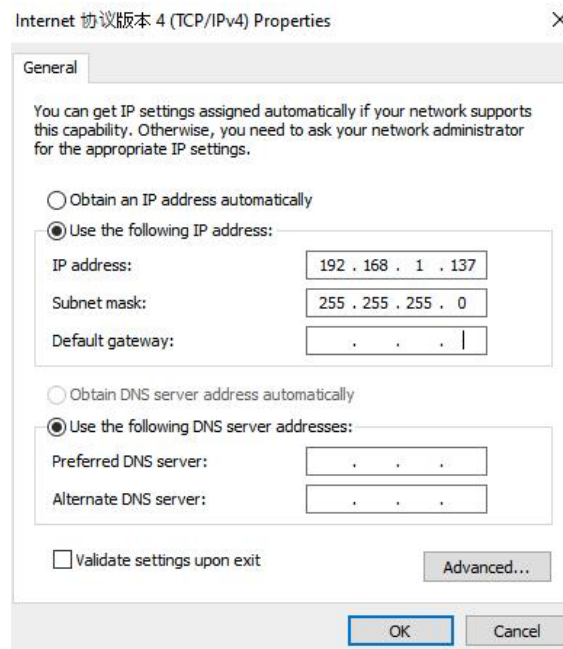


Figure 2-3 IP Settings

4. IP address is set to the same network segment as the device, and the IP cannot be the same as the device. For example: The IP of the device is 192.168.1.1, then the host can be set to 192.168.1.220.

5. Enter the default IP 192.168.1.1 of the device in the address bar of your browser and hit the Enter key to jump to the page shown below.

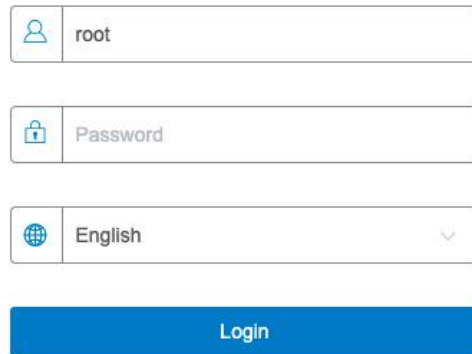
The image shows a login interface with three input fields and a login button. The first field has a user icon and contains the text 'root'. The second field has a lock icon and contains the text 'Password'. The third field has a globe icon and contains the text 'English' with a dropdown arrow. Below these fields is a blue button with the text 'Login'.

Figure 2-4 Device login page

6. Enter the default password in the password entry box :admin. Then click on the login button to jump to the device page(default username: root).

2. 2 Wizard configuration for wireless association

The wizard page allows you to quickly configure the wireless association of two devices (also configurable on the wireless settings page, see chapter 4, subsection 4.1 for details).The device supports four modes: Access Point, Client, Access Point (WDS), Client (WDS), Client and Access Point used together, Access Point (WDS) and Client (WDS) used together.

Note: Once the wizard configuration is complete, all wireless and network parameters will be initially restored to their default values, except for the parameters modified by the wizard configuration.

2. 2. 1 Configure Access Point

(1) Once you have successfully logged in, you will be taken to the "Status Display" page by default. Click on "Wizard" in the top right corner to enter the "Wizard - Network" page as shown below. To prevent IP conflicts, please change the IPv4 address.

① Network ② Wireless ③ Complete

IP Protocol: IPv4 Static IP

IPv4 Address: 192.168.1.223

IPv4 Netmask: 255.255.255.0

Gateway: 192.168.1.254

Next

Figure 2-5 Wizard - Network- Default

(2) Click on "Next" to enter the "Wizard - Wireless" page, which shows the basic wireless parameters of the device for 2.4G and 5G, as shown in the figure below. Modify the wireless parameters of the wireless band to be used, e.g. change the "Network name" of "Wireless (5Gwifi)" to 5Glink, keep the rest unchanged (default "Wireless mode" is Access Point, "Channel Bandwidth" is 160/80/40/20MHz, "Frequency (Channel)" is Auto, "Security Mode" is WPA2-PSK/WPA3-SAE, and "Key" is 1234567890abc).

① Network ② Wireless ③ Complete

Wireless(2.4Gwifi)

Wireless Mode: Access Point

SSID: Wireless_2G

Channel Width: 40 MHz

Frequency(Channel): Auto

Calc the EIRP limit: ☒

Antenna Gain(dBi): 0

Transmit Power: 20

Encryption: WPA2-PSK/WPA3-SAE

Key: *****

Wireless(5Gwifi)

Wireless Mode: Access Point

SSID: Wireless_5G

Channel Width: 160/80/40/20MHz

Frequency(Channel): Auto

Calc the EIRP limit: ☒

Antenna Gain(dBi): 0

Transmit Power: 30

Encryption: WPA2-PSK/WPA3-SAE

Key: *****

Previous Next

Figure 2-6 Wizard - Wireless

(3) Continue by clicking 'Next' to go to the 'Wizard - Finish' page, as shown below. Click on the "Finish" button to save all the settings or click on "Previous" to change the previous configuration.



Figure 2-7 Wizard - Finish

Access point configuration complete.

2. 2. 2 Configure Client

(1) Once you have successfully logged in, you will be taken to the "Status Display" page by default. Click on "Wizard" in the top right corner to enter the "Wizard - Network" page as shown below. To prevent IP conflicts, please change the IPv4 address.

Note: Client devices and access point devices must not be configured with the same IP address to prevent address conflicts



Figure 2-8 Wizard - Network

(2) Click "Next" to enter the "Wizard - Wireless" page, which displays the basic wireless parameters for 2.4G and 5G, as shown in the figure below. Modify the wireless mode of the wireless band to be used as the client, and configure the network name, security mode and key consistent with the access point you want to associate with. For example, if you want to access an access point with the previously modified 5G band network name of 5Glink, modify "Wireless (5Gwifi)" to Client mode, "Network name" to 5Glink, "Security mode" to WPA2-PSK/WPA3-SAE, "Key" to 1234567890abc, which is consistent with the access point, and other parameters can be kept as default.

Figure 2-9 Wizard - Wireless configuration screen. The screen shows two columns of settings for Wireless(2.4Gwifi) and Wireless(5Gwifi). The Wireless(2.4Gwifi) column has settings for Wireless Mode (Access Point), SSID (Wireless_2G), Channel Width (40 MHz), Frequency(Channel) (Auto), Calc the EIRP limit (checked), Antenna Gain(dBi) (0), Transmit Power (20), Encryption (WPA2-PSK/WPA3-SAE), and Key (*****). The Wireless(5Gwifi) column has settings for Wireless Mode (Access Point), SSID (Wireless_5G), Channel Width (160/80/40/20MHz), Frequency(Channel) (Auto), Calc the EIRP limit (checked), Antenna Gain(dBi) (0), Transmit Power (30), Encryption (WPA2-PSK/WPA3-SAE), and Key (*****). At the bottom right are 'Previous' and 'Next' buttons.

Figure 2-9 Wizard - Wireless

(3) Continue by clicking 'Next' to go to the 'Wizard - Finish' page, as shown below. Click on the "Finish" button to save all the settings or click on "Previous" to change the previous configuration.

Figure 2-10 Wizard - Finish screen. The screen shows a progress bar with three steps: Network (checked), Wireless (checked), and Complete (3). Below the progress bar, it says "You have completed the wizard" and "Please click the "Complete" button to save all settings". At the bottom right are "Previous" and "Complete" buttons.

Figure 2-10 Wizard - Finish

Client configuration complete. At this point the client can connect successfully to the access point with the network name 5Glink.

2. 2. 3 Configure Access Point (WDS)

(1) Once you have successfully logged in, you will be taken to the "Status Display" page by default. Click on "Wizard" in the top right corner to enter the "Wizard - Network" page as shown below. To prevent IP conflicts, please change the IPv4 address.

1 Network 2 Wireless 3 Complete

IP Protocol IPv4 Static IP

IPv4 Address 192.168.1.228

IPv4 Netmask 255.255.255.0

Gateway 192.168.1.254

Next

Figure 2- 11 Wizard - Network

(2) Click "Next" to enter the "Wizard - Wireless" page, which displays the basic wireless parameters and wireless encryption options for 2.4G and 5G, as shown in the figure below. Modify the wireless parameters of the wireless band you need to use, for example, change the "Wireless Mode" of "Wireless (5Gwifi)" to Access Point (WDS) and "Network Name" to 5GWDSlink, and keep the other parameters unchanged ("Channel Bandwidth" is 160MHz, "Frequency (Channel)" is Auto, "Security Mode" is WPA2-PSK /WPA3-SAE, "Key" is 1234567890abc).

1 Network 2 Wireless 3 Complete

Wireless(2.4Gwifi)

Wireless Mode Access Point

SSID Wireless_2G

Channel Width 40 MHz

Frequency(Channel) Auto

Calc the EIRP limit ☒

Antenna Gain(dBi) 0

Transmit Power 20

Encryption WPA2-PSK/W

Key

Wireless(5Gwifi)

Wireless Mode Access Point

SSID 5GWDSlink

Channel Width 160/80/40/20M

Frequency(Channel) Auto

Calc the EIRP limit ☒

Antenna Gain(dBi) 0

Transmit Power 30

Encryption WPA2-PSK/W

Key

Previous Next

Figure 2- 12 Wizard - Wireless

(3) Continue by clicking 'Next' to go to the 'Wizard - Finish' page, as shown below. Click on the "Finish" button to save all the settings or click on "Previous" to change the previous configuration.

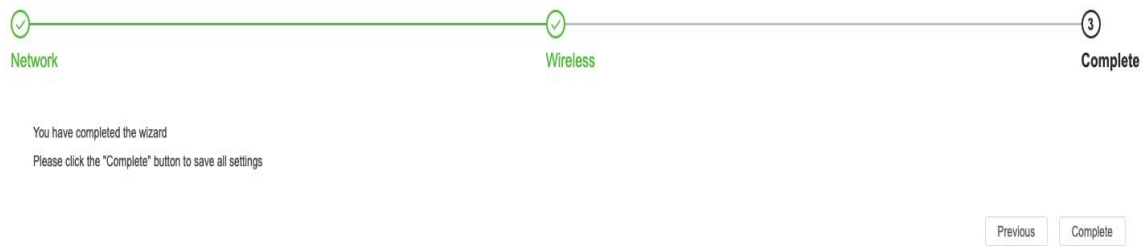


Figure 2- 13 Wizard - Finish

Access Point (WDS) configuration complete.

2. 2. 4 Configure Client (WDS)

(1) Once you have successfully logged in, you will be taken to the "Status Display" page by default. Click on "Wizard" in the top right corner to enter the "Wizard - Network" page as shown below. To prevent IP conflicts, please change the IPv4 address.



Figure 2- 14 Wizard - Network

(2) Click "Next" to enter the "Wizard - Wireless" page, which displays the basic wireless parameters and wireless encryption options for 2.4G and 5G, as shown in the image below. Modify the wireless mode to client (WDS) for the wireless band to be used, and configure the network name, security mode and key to match the access point (WDS) you wish to associate with. For example, if you want to access the access point (WDS) with the previously modified 5G band network name 5GWDSLlink, modify "Wireless (5Gwifi)" to client (WDS) mode, "Network name" to 5GWDSLlink, "Security mode" to WPA2-PSK/WPA3-SAE, "Key" to 1234567890abc, which is consistent with the access point (WDS), and other parameters can be kept as default.

Figure 2-15 shows the 'Wireless' configuration step of a wizard. It features two side-by-side configuration panels for 2.4GHz and 5GHz Wi-Fi. The 2.4GHz panel is titled 'Wireless(2.4Gwifi)' and the 5GHz panel is titled 'Wireless(5Gwifi)'. Both panels include dropdown menus for 'Wireless Mode' (set to 'Access Point'), 'SSID', 'Channel Width', and 'Frequency(Channel)' (set to 'Auto'). They also have a toggle for 'Calc the EIRP limit' (checked), a numeric input for 'Antenna Gain(dBi)' (set to 0), a slider for 'Transmit Power' (set to 20 for 2.4GHz and 30 for 5GHz), a dropdown for 'Encryption' (set to 'WPA2-PSK/W'), and a text input for 'Key'. At the bottom right, there are 'Previous' and 'Next' navigation buttons.

Figure 2- 15 Wizard - Wireless

(3) Continue by clicking 'Next' to go to the 'Wizard - Finish' page, as shown below. Click on the "Finish" button to save all the settings or click on "Previous" to change the previous configuration.

Figure 2-16 shows the 'Complete' step of the wizard. A progress bar at the top indicates that the 'Network' and 'Wireless' steps are completed, and the 'Complete' step is the current step, marked with a '3'. Below the progress bar, a message states: 'You have completed the wizard. Please click the "Complete" button to save all settings'. At the bottom right, there are 'Previous' and 'Complete' navigation buttons.

Figure 2- 16 Wizard - Complete

Client (WDS) configuration complete. At this point the Client (WDS) can be successfully connected to the access point (WDS) with the network name 5GWDSlink.

Note: Use the client and the access point together. Use the client (WDS) and the access point (WDS) together, do not mix them.

3 Status

The default page displayed after a successful login is the status page, which shows the current configuration of some parameters of the device and the current working status of the real-time monitoring, and contains sub-pages such as information, statistics, network and logs.

3.1 Status - Information page (MESH mode)

The Status-Information page (Mesh mode) displays some of the device's current configuration information: Mesh topology diagram, device information, network information, wireless information and connected wireless device information.

Mesh topology diagram: The current status of CAP and RE is displayed, whether they form a MESH network or not; the connection between CAP and RE is indicated by a green line; when RE is disconnected, it is not shown in the mesh topology of CAP; in the topology of CAP, click on the RE icon and a new page window will pop up showing the login page of RE.



Figure 3-1 Equipment information

3.2 Status - information page (MESH Mode)

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

Equipment information: System information about the device, including device name, firmware version, running time and device time.

The screenshot shows the 'System' page with a light blue header. Below the header, the following information is displayed:

Device Name	无线接入点	Uptime	41 d 16 h 48 m 24 s
Firmware Version	V1.0.22B06 build 20220930	Time	2022-11-11 08:21:07

Figure 3-2 Equipment information

Network information: Device network-related information, including network mode, IP address and other information, can be configured in Settings - Network settings.

Network					
Network Mode	Route Mode			IP Protocol (WAN)	IPv4 Static IP
IP Protocol	IPv4 Static IP			MAC (WAN)	9C:B7:93:05:94:7F
IPv4 Address	192.168.10.2			IPv4 Address (WAN)	172.18.10.227
IPv4 Netmask	255.255.255.0			IPv4 Netmask (WAN)	255.255.255.0
Interface	eth1 (LAN1)	eth0 (POE Port)	ath1 (WiFi)	ath0 (WiFi)	IPv4 Gateway (WAN)
					172.18.10.1
					DNS (WAN)
					218.2.135.1
Wired Port MAC Address	9C:B7:93:05:94:7F(eth0)			Secondary DNS (WAN)	172.18.10.5
	9C:B7:93:05:94:80(eth1)			IPv6 Address (WAN)	fe80::9eb7:93ff:fe05:947f164
IPv6 Address	fe80::9eb7:93ff:fe05:9480164				

Figure 3- 3 Network information

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

Wireless

WiFi0

SSID	CC_Office_Caribbean	CCQ / Noise Floor	100% / -89 dBm
Wireless Mode	Access Point (WDS)	Number Of Connections	2
BSSID	9C:B7:93:05:94:7D	Transmit Power	20 dBm
Country/Region	China		
Channel Width	40MHz		
Frequency(Channel)	2417 MHz (2)		
802.11 Mode	802.11ax		
Encryption	WPA2-PSK		

WiFi1

SSID	CC_Office_Caribbean	CCQ / Noise Floor	99% / -104 dBm
Wireless Mode	Access Point (WDS)	Number Of Connections	6
BSSID	9C:B7:93:05:94:7E	Transmit Power	23 dBm
Country/Region	China		
Channel Width	160/80/40/20MHz		
Frequency(Channel)	5745 MHz (149)		
802.11 Mode	802.11ax		
Encryption	WPA2-PSK		

Figure 3- 4 Wireless information

Connected wireless device information: Information about the device at the other end of the device association, including network name, RSSI (i.e. signal strength), IPV4 address of the device at the other end, MAC address of the device at the other end, TX/RX rate (i.e. transmit/receive rate), connection duration, etc.

Station List							
SSID	RSSI/Noise	IPv4 Address	MAC	TX/RX Rate	CCQ	802.11 Mode	Connection Time
CC_Office_Caribbean	-51/-92	0.0.0.0	E2:44:BB:05:A3:AC	1.0 Mbps / 0 Kbps	70%	802.11b/g/n	00:34:03
CC_Office_Caribbean	-50/-92	192.168.10.248	2A:32:7F:AE:CC:F8	1.0 Mbps / 0 Kbps	86%	802.11ax	00:24:54
CC_Office_Caribbean	-52/-92	192.168.10.245	E2:CD:FB:FC:D7:B8	1.0 Mbps / 0 Kbps	99%	802.11ax	00:00:06
CC_Office_Caribbean	-48/-105	192.168.10.3	9C:B7:93:0A:0A:01	6.0 Mbps / 0 Kbps	78%	802.11ax	191:39:52
CC_Office_Caribbean	-49/-105	192.168.10.5	A4:4E:31:19:00:7C	6.0 Mbps / 0 Kbps	78%	802.11a/n	24:33:54
CC_Office_Caribbean	-49/-105	192.168.10.27	28:B2:BD:CE:1B:3E	6.0 Mbps / 0 Kbps	78%	802.11ac	06:30:48
CC_Office_Caribbean	-49/-105	192.168.10.247	82:60:7D:72:F9:C1	6.0 Mbps / 0 Kbps	78%	802.11ac	01:51:35
CC_Office_Caribbean	-49/-105	192.168.10.19	92:41:7A:49:CA:98	6.0 Mbps / 0 Kbps	78%	802.11ac	01:10:32
CC_Office_Caribbean	-49/-105	192.168.10.21	62:73:BE:77:01:3B	6.0 Mbps / 0 Kbps	78%	802.11ax	00:51:59

Figure 3- 5 Connected wireless device information

3. 3 Status-statistics page

This page displays the network interface statistics and traffic statistics for this device, which refers to the amount of data transferred on the network per unit of time and is a key indicator of network performance. Specific information is shown below.

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

Interface Statistics							
Interface	MAC Address	RX Bytes	TX Bytes	RX Packets	TX Packets	RX ERR	TX ERR
Wired Ethernet							
eth0	9C:B7:93:05:94:7F	403479470354 Byte	136743085879 Byte	430195615	260963544	0	0
eth1	9C:B7:93:05:94:80	2066624 Byte	11038890 Byte	7547	30379	0	0
Wireless							
ath0	9C:B7:93:05:94:7D	477269102 Byte	6247173003 Byte	3301494	9092163	896	25810
ath1	9C:B7:93:05:94:7E	138949005256 Byte	383338110374 Byte	271705458	377348704	264	37659

Figure 3- 6 Network interface statistics

Traffic statistics: Includes both wired traffic statistics and wireless traffic statistics, with a graphical representation of TX and RX (i.e. transmitted and received) traffic in real time, which is more intuitive and clear.



Figure 3-7 Traffic statistics

3. 4 Status-network page

This page displays the device's routes table, ARP table and list of bridging devices, as shown below.

Routes table: The routes table stores the path to the network where the device is located.

Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	172.18.10.1	br-wan	0
172.18.10.0	255.255.255.0	0.0.0.0	br-wan	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-wan	0

Figure 3-8 IPv4 Routes table

Destination	Netmask	Gateway	Interface	Metric
fe80::	64	::	br-wan	256
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::	128	::	lo	0
fe80::9eb7:93ff:fe05:947d	128	::	lo	0
fe80::9eb7:93ff:fe05:947e	128	::	lo	0
fe80::9eb7:93ff:fe05:947f	128	::	lo	0
fe80::9eb7:93ff:fe05:9480	128	::	lo	0
ff00::	8	::	br-wan	256
ff00::	8	::	br-lan	256
ff00::	8	::	ath0	256
ff00::	8	::	ath1	256

Figure 3-9 IPv6 Routes table

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

IPv4 Address	MAC Address	Interface
172.18.10.107	00:50:56:32:EE:C3	br-wan
192.168.10.26	E2:44:BB:05:A3:AC	br-lan
169.254.60.11	A0:88:69:FB:33:58	br-lan
169.254.39.159	5C:5F:67:38:61:61	br-lan
192.168.10.25	DA:10:9B:AC:00:CD	br-lan
192.168.10.34	92:41:7A:49:CA:98	br-lan
172.18.10.103	3C:97:0E:79:6D:0B	br-wan
192.168.10.28	E2:CD:FB:FC:D7:B8	br-lan
192.168.10.33	62:73:BE:77:01:3B	br-lan
192.168.10.19	92:41:7A:49:CA:98	br-lan
192.168.10.36	58:91:CF:9E:39:D2	br-lan
192.168.10.205	18:3E:EF:D2:FA:20	br-lan
169.254.127.24	56:58:F2:52:1D:D4	br-lan
192.168.10.22	9E:43:D8:06:10:AD	br-lan

Figure 3-10 ARP table

Bridging Devices List: The device obtains the correspondence between the MAC address and the aging time of other devices whose communication passes through it within 300 seconds.

ARP Table			
IPv4 Address	MAC Address	Interface	
172.18.10.107	00:50:56:32:EE:C3	br-wan	
192.168.10.26	10:82:D7:0B:47:ED	br-lan	
169.254.60.11	A0:88:69:FB:33:58	br-lan	
169.254.39.159	5C:5F:67:38:61:61	br-lan	
192.168.10.25	66:F9:47:7F:D7:35	br-lan	
192.168.10.34	92:41:7A:49:CA:98	br-lan	
172.18.10.103	3C:97:0E:79:6D:0B	br-wan	
192.168.10.28	9E:43:D8:06:10:AD	br-lan	
192.168.10.33	62:73:BE:77:01:3B	br-lan	
192.168.10.19	92:41:7A:49:CA:98	br-lan	
192.168.10.36	58:91:CF:9E:39:D2	br-lan	

Figure 3- 2 Bridging Devices List

3. 5 Status-log

This page displays the log information of the device, as shown below.

System Log		Clear
<pre>[Info][2022-11-11 08:10:01.895590][hostapd] ath0: STA aeb7:93:11:22:11 WPA: received EAPOL-Key frame (2/4 Pairwise) [Info][2022-11-11 08:10:01.965673][hostapd] ath0: STA aeb7:93:11:22:11 WPA: sending 1/4 msg of 4-Way Handshake [Info][2022-11-11 08:10:01.975928][hostapd] ath0: STA aeb7:93:11:22:11 WPA: received EAPOL-Key frame (2/4 Pairwise) [Info][2022-11-11 08:10:02.975915][hostapd] ath0: STA aeb7:93:11:22:11 WPA: sending 1/4 msg of 4-Way Handshake [Info][2022-11-11 08:10:02.992183][hostapd] ath0: STA aeb7:93:11:22:11 WPA: received EAPOL-Key frame (2/4 Pairwise) [Info][2022-11-11 08:10:03.985569][hostapd] ath0: STA aeb7:93:11:22:11 WPA: sending 1/4 msg of 4-Way Handshake [Info][2022-11-11 08:10:04.009405][hostapd] ath0: STA aeb7:93:11:22:11 WPA: received EAPOL-Key frame (2/4 Pairwise) [Info][2022-11-11 08:10:04.996973][hostapd] ath0: STA aeb7:93:11:22:11 IEEE 802.11: disassociated [Info][2022-11-11 08:10:04.998257][hostapd] ath0: STA aeb7:93:11:22:11 IEEE 802.11: disassociated [Info][2022-11-11 08:10:11.930618][hostapd] ath0: STA aeb7:93:11:22:11 IEEE 802.11: authenticated [Info][2022-11-11 08:10:11.984243][hostapd] ath0: STA aeb7:93:11:22:11 IEEE 802.11: associated (aid 1) [Info][2022-11-11 08:10:11.987842][hostapd] ath0: STA aeb7:93:11:22:11 WPA: sending 1/4 msg of 4-Way Handshake [Info][2022-11-11 08:10:12.031376][hostapd] ath0: STA aeb7:93:11:22:11 WPA: received EAPOL-Key frame (2/4 Pairwise) [Info][2022-11-11 08:10:12.095613][hostapd] ath0: STA aeb7:93:11:22:11 WPA: sending 1/4 msg of 4-Way Handshake [Info][2022-11-11 08:10:12.109929][hostapd] ath0: STA aeb7:93:11:22:11 WPA: received EAPOL-Key frame (2/4 Pairwise) [Info][2022-11-11 08:10:13.105670][hostapd] ath0: STA aeb7:93:11:22:11 WPA: sending 1/4 msg of 4-Way Handshake [Info][2022-11-11 08:10:13.134413][hostapd] ath0: STA aeb7:93:11:22:11 WPA: received EAPOL-Key frame (2/4 Pairwise) [Info][2022-11-11 08:10:14.115645][hostapd] ath0: STA aeb7:93:11:22:11 WPA: sending 1/4 msg of 4-Way Handshake [Info][2022-11-11 08:10:14.141670][hostapd] ath0: STA aeb7:93:11:22:11 WPA: received EAPOL-Key frame (2/4 Pairwise) [Info][2022-11-11 08:10:15.127945][hostapd] ath0: STA aeb7:93:11:22:11 IEEE 802.11: disassociated [Info][2022-11-11 08:10:15.138497][hostapd] ath0: STA aeb7:93:11:22:11 IEEE 802.11: disassociated [Info][2022-11-11 08:10:22.554197][hostapd] ath0: STA aeb7:93:11:22:11 IEEE 802.11: authenticated [Info][2022-11-11 08:10:22.599216][hostapd] ath0: STA aeb7:93:11:22:11 IEEE 802.11: associated (aid 1) [Info][2022-11-11 08:10:22.602055][hostapd] ath0: STA aeb7:93:11:22:11 WPA: sending 1/4 msg of 4-Way Handshake [Info][2022-11-11 08:10:22.650647][hostapd] ath0: STA aeb7:93:11:22:11 WPA: received EAPOL-Key frame (2/4 Pairwise)</pre>		

Figure 3- 3 Status-log

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 in Mesh Mode

In Mesh Mode, the wireless settings page is shown below, using 5GHz as an example.

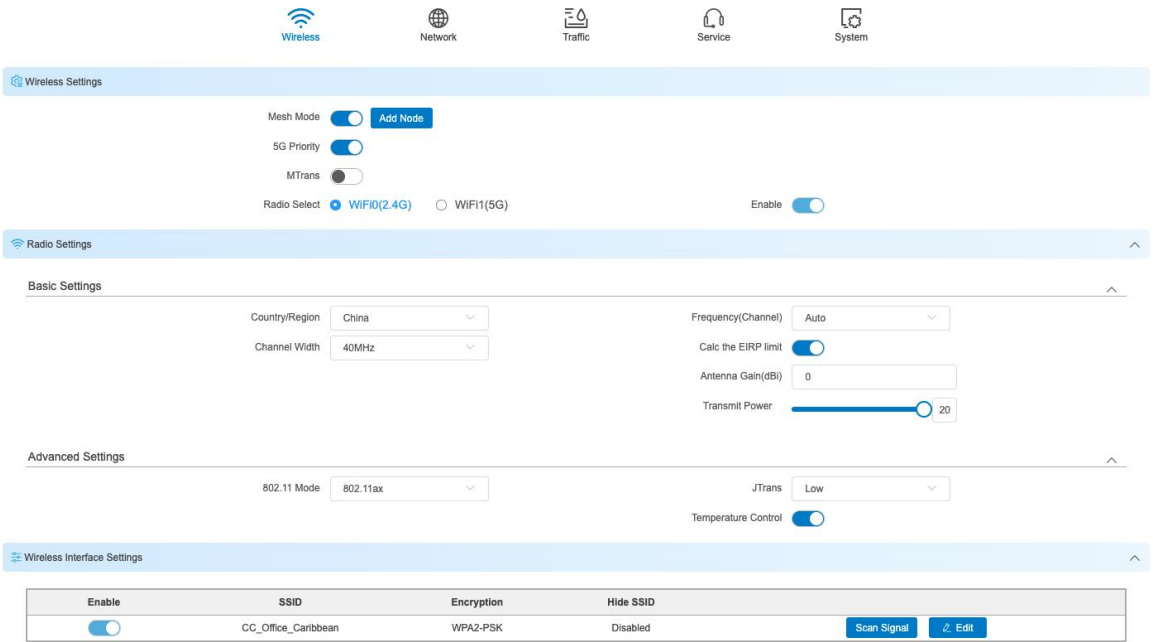


Figure 4-1 CAP Mode

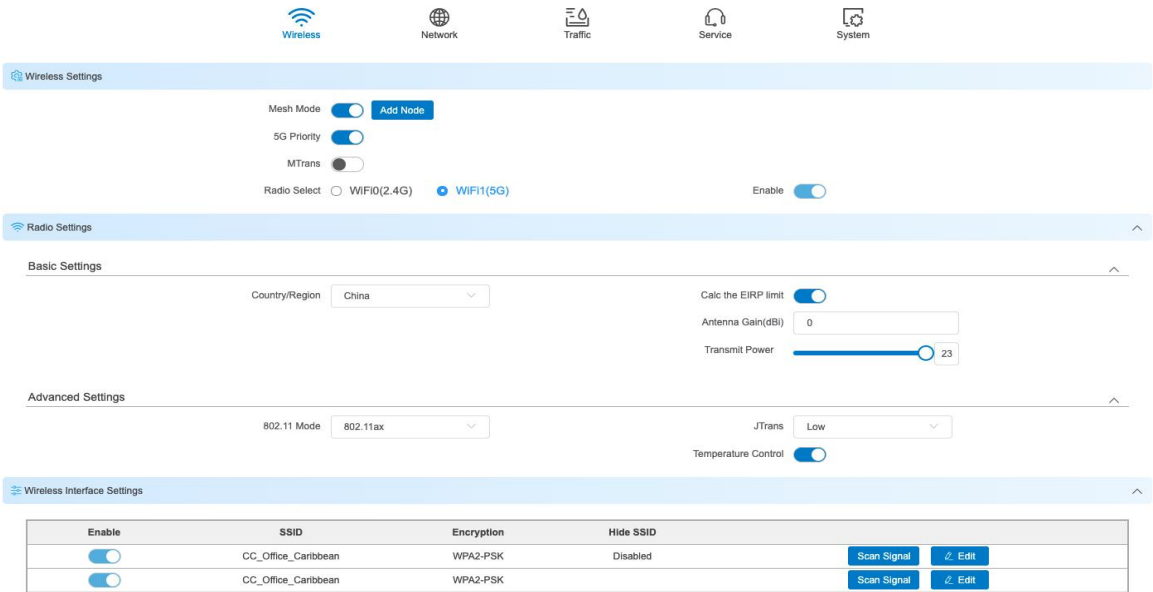


Figure 4-2 RE Mode

Mesh Mode: When Mesh Mode is enabled, the device enters Mesh Mode and the CAP and RE click on the "Add Node" button to start forming a mesh network; when Mesh Mode is disabled, the device enters normal wireless mode and the wireless parameters revert to the default values in normal mode.

5G Priority: Function only works if 2.4G and 5G SSIDs are the same.

Radio Select: Select the wireless network and control whether the wireless is enabled or not, the device supports 2.4G and 5G bands, not configurable in Mesh mode, all 2.4G and 5G bands are enabled by default.

Radio Settings: The Wireless Settings page contains basic and advanced settings, which allow you to configure the following parameters:

- **Country Code:** The standard channel varies from country to country or region to region, so select the corresponding country code as required.
- **Channel width:** Limits the upper and lower frequencies of the signal allowed through the channel.
- **Frequency/(channel):** The center frequency of the carrier, when the CAP and RE form a mesh network, the frequencies will remain the same, with the RE following the CAP.
- **Transmit Power:** The power of the device transmitting the wireless signal is adjusted by the user according to the distance between the devices. When the output power is increased, the signal strength is improved, thus increasing the transmission distance of the device.
- **802.11 Mode:** 2.4G wireless supports 802.11ax and 802.11b/g/n, 5G supports 802.11ax, 802.11ac and 802.11a/n, default is 802.11ax. (Note: some countries and regions do not support 802.11ax)
- **Temperature Control:** The temperature control is off by default, when on it prevents the CPU from getting too hot and damaging the unit due to high load conditions.

Wireless interface settings: In Mesh Mode, no wireless interfaces can be added, deleted or disabled; in CAP mode, there is one and only one wireless interface on a band; in RE mode, there is one and only one wireless interface on the 2.4G band, and in the 5G band two wireless interfaces are enabled by default, one for the access point and one for the client.

- **Network name (SSID):** The value used to control access to the wireless network. The default SSID in mesh mode is 'Saila-xxxxxx' (the last six MAC addresses).
- **Wireless Mode:** In Mesh mode, the default is Access Point WDS and Client WDS mode and cannot be changed.

- **Encryption:** To encrypt the wireless connection, users can choose the appropriate encryption method according to their security requirements. The wireless encryption of the devices to be associated with each other must be set to the same level, otherwise the association will not work.

- **Key:** Wireless access password, the key needs to be consistent When devices are associated wirelessly, otherwise, the association will not work.

- **Hide network name:** Hide the wireless network name (SSID). When this function is checked, other mobile phones, computers and other terminals as well as client devices will not be able to search for the SSID of the access point device to avoid being connected by others and not affecting your own use.

- **MAC address lock:** When there are multiple network environments with the same SSID around, the client device can specify the access point to be associated by setting the wireless MAC address of the corresponding access point (displayed on the Client page only).

- **Client Isolation:** Enable this feature to prevent devices connected to the same access point device from communicating with each other, even if the IPs of the clients are duplicated, there is no impact on communication (This feature is only available in Access Point mode).

- **802.11r:** Through a fast switching mechanism (Fast BSS Transition) to realize roaming of wireless terminal equipment(Only WPA2-PSK security mode is supported).

- **User speed limit:** Restrictions on uplink and downlink speeds for users associated to the device (displayed on the Access Point page only).

- **Max Users:** Limit the number of connected users (displayed on the Access Point page only)

- **Minimum Access Signal Limit:** Requirements for signal strength value of access users, only users with signal strengths greater than the set value are allowed to access. The access point sets it to limit the minimum signal strength of the associated device; devices with a signal strength below the set value cannot be successfully associated; even if the association is successful, once the associated signal strength falls below the set value, the client will be kicked off the access point device. (Only displayed on the Access Point page).

Wireless Network Probe: Wireless Network Probe is not available in Mesh mode and is switched off by default. To use the wireless network probe, switch the device to normal mode.

4. 2 Wireless settings in Normal Mode

In normal mode, the wireless settings page is shown below.

Wireless Settings

Mesh Mode ☐ 5G Priority ☒ MTrans ☐ Radio Select ☐ WIFI(2.4G) ☒ WIFI1(5G) Enable ☒

Radio Settings

Basic Settings

Country/Region: China Frequency(Channel): Auto
Channel Width: 160/80/40/20MHz Calc the EIRP limit: ☒
Antenna Gain(dB): 0
Transmit Power: 30

Advanced Settings

802.11 Mode: 802.11ax JTrans: Low
DCS: ☐ Temperature Control: ☒

Wireless Interface Settings

Enable	SSID	Encryption	Hide SSID	
☒	Wireless_5G	WPA2-PSK/WPA3-SAE	Disabled	Add Scan Signal Edit Delete

Figure 4-3 5G Access Point mode

Wireless Settings: The wireless network is selected and the device supports both 2.4G and 5G bands. The 2.4G and 5G wireless can be configured in the enabled state, and when switched off it means that the corresponding wireless band is switched off.

Radio Settings: The Wireless Settings page contains basic and advanced settings, which allow the following parameters to be configured.

- **Country Code:** Different countries or regions have different standard channels, and the corresponding country code should be selected according to the needs.
- **Channel width:** Limit the upper and lower limits of the signal frequency allowed to pass through the channel.
- **Frequency/(channel):** The centre frequency of the carrier, The frequency needs to be consistent when the access point is associated with the client.
- **Transmit Power:** The power of the device transmitting the wireless signal is adjusted by the user according to the distance between the devices. When the output power is increased, the signal strength is improved, thus increasing the transmission distance of the device.
- **802.11 Mode:** 2.4G wireless supports 802.11ax and 802.11b/g/n, 5G supports 802.11ax, 802.11ac and 802.11a/n, default is 802.11ax. (Note: some countries and regions do not support 802.11ax)
- **Automatic Channel List:** Dynamic channel selection, a function that detects and avoids interference. When the channel bottleneck or interference reaches a certain level, the

device will dynamically switch to a channel with less interference. This function works when the frequency is selected as "Auto" and there are multiple channels in the automatic channel list, but is not available after a fixed channel or when there is only one channel in the automatic channel list.

- **Temperature Control:** The temperature control is off by default, when on it prevents the CPU from getting too hot and damaging the unit due to high load conditions.

Wireless Settings

Mesh Mode ☐ SG Priority ☒ MTrans ☐ Radio Select ☒ WiFi(2.4G) ☐ WiFi(5G) Enable ☒

Radio Settings

Basic Settings

Country/Region: China Channel Width: 40MHz Frequency(Channel): Auto Automatic Channel List: 2412 2417 2422 2427 Select Calc the EIRP limit: ☒ Antenna Gain(dBi): 0 Transmit Power: 20

Advanced Settings

802.11 Mode: 802.11ax JTrans: Low Temperature Control: ☒

Wireless Interface Settings

Enable	SSID	Encryption	Hide SSID	
☒	Wireless_2G	WPA2-PSK/WPA3-SAE	Disabled	Scan Signal Add Edit Delete
☒	Wireless_MGMT_AABBEE	WPA2-PSK/WPA3-SAE	Disabled	Edit Delete

Figure 4- 4 2.4G Access Point mode

Wireless Interface Settings: Wireless interfaces can be added, modified or deleted, and up to 8 wireless network interfaces can be added to a frequency band. Two wireless interfaces are enabled by default in the 2.4G wireless interface settings. When a mobile phone or laptop is associated with a network interface with "MGMT" in the network name, the device can be accessed and managed, but the terminal does not support Internet access, this interface is the management wireless interface. If the network interface without "MGMT" in the associated network name is used, the terminal can access the device as well as support Internet access. To configure the wireless network, click on Modify and the following screen will pop up.

Notes: Networks with "MGMT" cannot be restored via "Add" after deletion, but can be restored via the reconfiguration wizard.

Basic Settings

SSID:

Hide SSID: ☐

Wireless Mode:

Encryption:

Key:

Advanced Settings

Client Isolation: ☐

Speed Limit: ☐

MAC Filtering: ☐

Max Users:

Minimum Access Signal Limit:

Cancel Complete

Figure 4- 5 normal wireless network 5G

Basic Settings

SSID:

Hide SSID: ☐

Wireless Mode:

Encryption:

Key:

Cancel Complete

Figure 4- 6 MGMT Manage wireless networks

The page can be configured for the following parameters.

- **network name (SSID):** The value used to control access to the wireless network. When other devices go to connect to this device, they can only communicate with each other and establish a wireless connection if the SSID set is the same. Network names only support 1 to 32 digits of Chinese (1 Chinese character occupies 3 digits), English, numbers, special [symbols\(!@#\\$%^&*\(\)_+<=>?:|\[\]{}'. \)and](#) non-first and last spaces.
- **Wireless Mode:** The device has 4 wireless modes, with Access Point, Client, Client (WDS) and Access Point (WDS).

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

- **Encryption:** To encrypt the wireless connection, users can choose the appropriate encryption method according to their security requirements. The wireless encryption of the devices to be associated with each other must be set to the same level, otherwise the association will not work.
- **Hide network name:** Hide the wireless network name (SSID). When this function is checked, other mobile phones, computers and other terminals as well as client devices will not be able to search for the SSID of the access point device to avoid being connected by others and not affecting your own use(Only displayed on the Access Point page).
- **Client Isolation:** Enable this feature to prevent devices connected to the same access point device from communicating with each other, even if the IPs of the clients are duplicated, there is no impact on communication(This feature is only available in Access Point mode).
- **MAC address lock:** When there are multiple network environments with the same SSID around, the client device can specify the access point to be associated by setting the wireless MAC address of the corresponding access point (displayed on the Client page only).
- **User speed limit:** Restrictions on uplink and downlink speeds for users associated to the device (displayed on the Access Point page only, WDS access points do not support the user speed limiting function).
- **Max Users:** Limit the number of connected users (displayed on the Access Point page only)
- **Minimum Access Signal Limit:** The access point limits the minimum signal strength of the associated device by setting it, devices with a signal strength below the set value cannot be successfully associated; even if the association is successful, once the associated signal strength falls below the set value, the client will be kicked off the access point device. Settable value range -95 ~ -1, higher values indicate higher signal strength(Only displayed on the Access Point page).
- **MAC Filtering:** Allows devices within or outside the list to communicate (Only displayed on the Access Point page).
- **802.11r:** Through a fast switching mechanism(Fast BSS Transition) to realize roaming of wireless terminal equipment(Only WPA2-PSK security mode is supported).

(C) Wireless Network Probe

Enable WiFi(2.4G) ☐

WiFi(5G) ☐

Settings

Reporting Interval (Seconds) 30

Scan Type Access Point And Client

Server Address

Server Port

MAC Address Filter Switch ☐

Figure 4- 7 Wireless settings - wireless Network Probe

Wireless Network Probe: Enabling this function allows the terminal to be located. When a terminal (e.g. mobile phone, computer, etc.) is within the signal coverage of the device, the device detects all messages sent by the terminal and reports them to the server for analysis and calculation of the terminal's location. The following parameters can be configured.

- Reporting Interval (Seconds): The time interval for data to be reported to the server.
- Scan Type: The type of end device the device scans to (Access Point, Client, Access Point and Client)
- Server Address: IP address of the server receiving the data.
- Server Port: The server port for receiving data.
- MAC Address Filter Switch: The switch is off by default. When enabled, MAC address filtering will be performed and data from devices matching the MAC address filtering rules will only be reported, otherwise it will be discarded. Up to 5 filter rules can be added and fuzzy matching is supported.

The following section describes how to configure the wireless association between two devices (the wizard page can also be quickly configured, see Section 2.2 of Chapter 2 for details). The device supports four modes: access point mode, client mode, access point (WDS) mode, and client (WDS) mode. It is recommended that the client mode and access point mode be used together, and that the access point (WDS) mode and client (WDS) mode be used together.

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

4. 2. 1 Configure Access Point

Click on the wireless band you want to use in the "Wireless network" selection, e.g. "WIFI1 (5G)".



Figure 4- 8 Radio Select

Click on the "Edit" button of "Wireless Interface Settings" and configure the corresponding parameters as required, e.g. change the "Network Name" to Wireless_link, click "Complete" to exit the current configuration pop-up window.

The image displays a 'Wireless Interface Settings' configuration window. It is divided into two sections: 'Basic Settings' and 'Advanced Settings'. In the 'Basic Settings' section, the 'SSID' is set to 'Wireless_link', 'Wireless Mode' is 'Access Point', 'Encryption' is 'WPA2-PSK/WPA3-SAE', and 'Key' is masked with asterisks. The 'Hide SSID' toggle is turned off. In the 'Advanced Settings' section, 'Client Isolation', 'Speed Limit', and 'MAC Filtering' are all turned off. 'Max Users' is set to 127, and 'Minimum Access Signal Limit' is set to -95. At the bottom right, there are 'Cancel' and 'Complete' buttons.

Figure 4- 9 Edit SSID

Click on "Save" in the top right corner. The Access Point configuration is complete.



figure 4- 10 Save

4. 2. 2 Configure Client

Click on the wireless band you want to use in the "Wireless network" selection, e.g. "WIFI1 (5G)".



Figure 4- 11 Radio Select

Click on the "Edit" button of "Wireless Interface Settings", change the "Wireless Mode" to Client and the "Network Name" to Wireless_link, click "Complete".

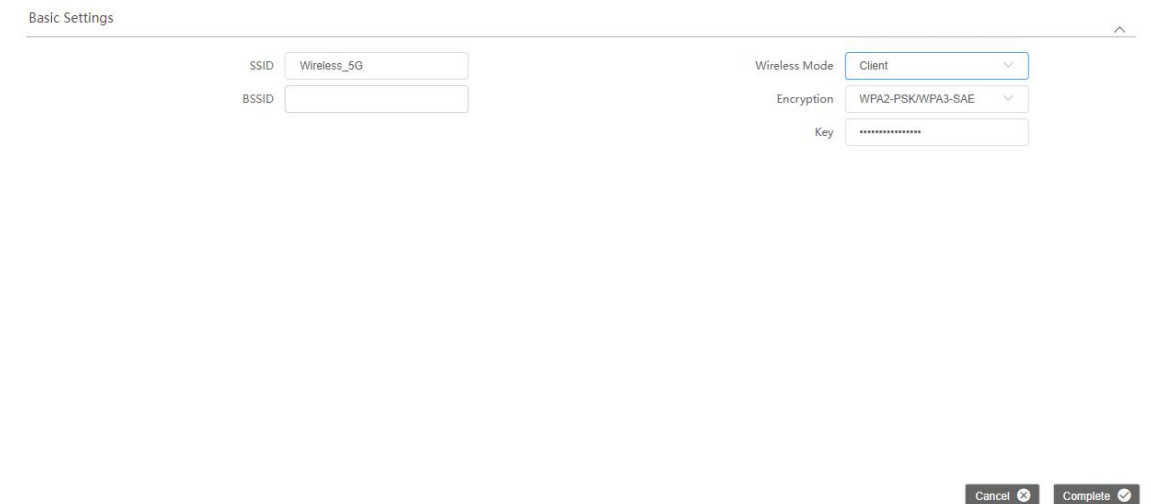


Figure 4- 12 Edit Wireless Mode and SSID

Click on "Save" in the top right corner. The Client configuration is complete.

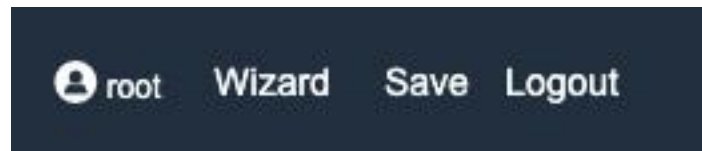


Figure 4- 13 Save

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

4. 2. 3 Configure Access Point (WDS)

Click on the wireless band you want to use in the "Wireless network" selection, e.g. "WIFI1 (5G)".



Figure 4- 14 Radio Select

Click on the "Edit" button of "Wireless Interface Settings", change the "Wireless Mode" to Access Point(WDS) and the "Network Name" to Wireless_WDS, click "Complete".

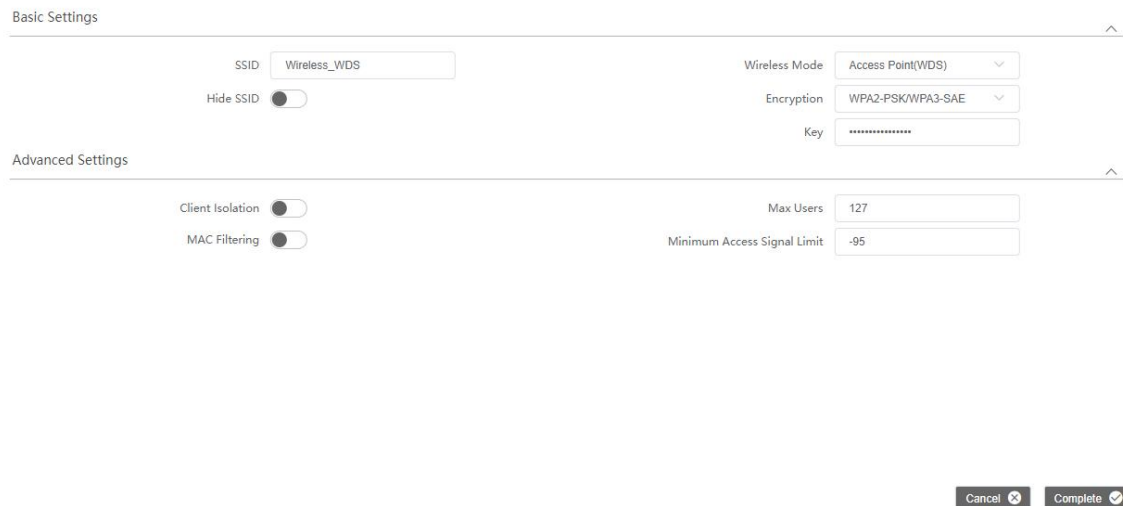


Figure 4- 15 Edit Wireless Mode and SSID

Click on "Save" in the top right corner. The Access Point(WDS) configuration is complete.



Figure 4- 16 Save

4. 2. 4 Configure Client(WDS)

Click on the wireless band you want to use in the "Wireless network" selection, e.g. "WIFI1 (5G)".



Figure 4- 17 Wireless Network Selection

Click on the "Edit" button of "Wireless Interface Settings", change the "Wireless Mode" to Client(WDS) and the "Network Name" to Wireless_WDS, click "Complete".

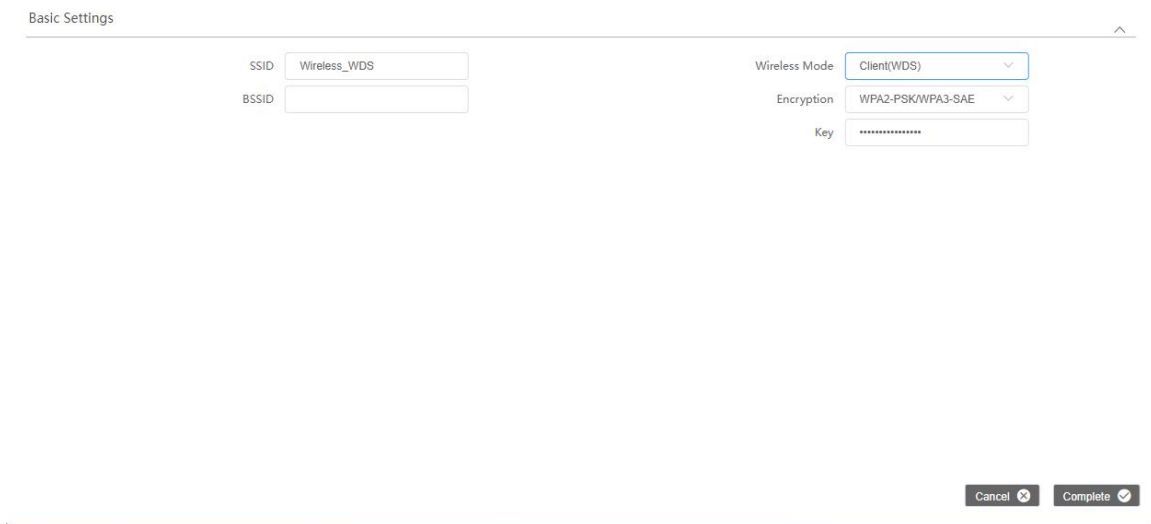


Figure 4- 18 Wireless Interface Settings-Modify SSID

Click on "Save" in the top right corner. The Client(WDS) configuration is complete.



Figure 4- 19 save

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

4. 2. 5 Associating devices by scanning signals

Login to the client device page, enter the wireless settings module, click "Scan for signal", a list of scanned APs will appear, find the SSID you want to connect to in it, e.g. Wireless_5G, if you do not find the device you want to connect to, click "Rescan" below If

you don't find the device you want to connect to, you can click "Rescan" below. Then click "Select" or "Lock" below the scan result.

Scan Results

Serial Number

SSID

MAC

Frequency(Channel)

Signal

1

CC_Office_Caribbean

9C:B7:93:0B:0B:02

5745 MHz (149)

-32

2

KyAir600F_5G

9C:B7:93:EA:0E:5D

5745 MHz (149)

-45

3

OFFICE_RD

9C:B7:93:EA:10:61

5745 MHz (149)

-45

4

Netcore-927C42

0A:10:7A:82:7C:43

5240 MHz (48)

-51

5

Xiaomi_A8C3

64:64:4A:8A:95:9D

5180 MHz (36)

-51

6

06:20:84:5E:0F:0B

5240 MHz (48)

-52

7

CMCC-A7Df-5G

04:20:84:1E:0F:0C

5240 MHz (48)

-52

8

ChinaNet-E69F-5G

A4:1A:3A:C3:E6:A1

5240 MHz (48)

-53

9

BA:1A:3A:C3:E6:A1

5240 MHz (48)

-53

10

CMCC-a3y6-5G

9C:B7:93:AA:BB:08

5745 MHz (149)

-54

Rescan

Select

Lock

Cancel

Total 43

10/page

<

1

2

3

4

5

>

Go to

1

Figure 4- 20 Scan Signal

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

The signal has been encrypted,
please enter the secret key

Key

Cancel

OK

Figure 4- 21 Select

4. 3 Network settings

You can select the network mode: bridge mode and routing mode, as well as configure the parameters related to the management VLAN. The management VLAN is switched off by default, see chapter 4.2.2 Advanced settings for detailed instructions.

Network

Network Mode: Bridge Mode

Management VLAN: ☒

Management VLAN ID: 3

IPv4 Address: 192.168.254.1

IPv4 Netmask: 255.255.255.0

IPv4 Gateway:

Figure 4- 22 Network

4. 3. 1 Interface Settings

The interface settings are paired according to the network mode in the network settings. When the bridge mode is selected for the network mode, the interface settings are shown below.

Network

Network Mode: Bridge Mode

Management VLAN: ☐

Management Interface

IP Protocol: IPv4 Static IP

IPv4 Address: 192.168.10.3

IPv4 Netmask: 255.255.255.0

IPv4 Gateway: 192.168.10.254

IPv4 DNS: 8.8.8.8

IPv4 Secondary DNS: 114.114.114.114

IPv6 Address:

IPv6 Prefix Length:

STP: ☐

IPv4 DHCP Server: ☐

IPv6 DHCP Server: Disabled

IPv6 DHCP Server Protocol: Stateless

Figure 4- 23 Bridge Mode-Static

Management Interface

IP Protocol	DHCPv4 Client
Backup IP Address	192.168.10.3
Backup IPv4 Netmask	255.255.255.0
Backup IPv4 Gateway	192.168.10.254
IPv4 DNS	8.8.8.8
IPv4 Secondary DNS	114.114.114.114
STP	☐

Figure 4- 24Bridge Mode-Dynamic

- When the IP type is static, users can set the IP address, netmask, default gateway and DNS according to their needs; make sure that the IP is not the same as the IP of other devices in the same network to avoid IP address conflicts; the gateway address and IP address should be in the same network segment.

To enable the device to access the external network, you need to connect the device to the external network, modify the device IP to be in the same network segment as the Internet router IP on the LAN, with the gateway being the IP address of the connected upper layer routing port, and connect the device to the router via the network cable.

- When the IP type is dynamic, the device can obtain a dynamically assigned address after connecting to a DHCP server. The device can be managed by accessing the device page through the alternate IP address before the device has obtained an IP address or after the IP address has failed to be obtained. Note: IPV6 dynamic does not have a standby address, so the device will not be able to access the page when the dynamic address is not correctly obtained, please use this function with caution.
- IPv4 DHCP server is turned off by default, after it is enabled, you can set the starting address, number of clients, lease time, gateway and DNS parameters, the configuration is shown in the figure below, Gateways and DNS can be left unconfigured. When mobile phones, computers and other terminals and client devices are wirelessly associated, they can obtain the IPV4 address assigned by the device.

Management Interface

IP Protocol	IPv4 Static IP	IPv4 DHCP Server	☒
IPv4 Address	192.168.10.3	Available Address Range	192.168.10.1 ~ 192.168.10.254
IPv4 Netmask	255.255.255.0	Start Address	192.168.10.4
IPv4 Gateway	192.168.10.254	End Address	192.168.10.20
IPv4 DNS	8.8.8.8	Leasetime	2h
IPv4 Secondary DNS	114.114.114.114	Gateway	192.168.10.3
IPv6 Address		DNS	8.8.8.8
IPv6 Prefix Length		IPv6 DHCP Server	Disabled
STP	☐	IPv6 DHCP Server Protocol	Stateless

Figure 4-25 IPV4 DHCP

- The IPv6 DHCP server is disabled by default and enabled when the server is selected, so that when mobile phones, computers and other terminals and client devices are wirelessly associated, they can obtain the IPV6 address assigned to the device.
- STP: Enabled to eliminate network loops. Ensures a smooth network link in the event of a loop.
- IPv6 address: Allows you to set the IPv6 address of the device.

When the network mode is selected as the route mode, it is divided into LAN Interface and WAN Interface. When the route mode is switched, the interface to which the device LAN and WAN are bound by default will be automatically displayed in the bridge interface setting on this page.

WAN Interface

WAN Interface:eth0	br-wan
IP Protocol	PPPoE
IPv4 Address	172.18.10.227
IPv4 Netmask	255.255.255.0
IPv4 Gateway	172.18.10.1
Username	test
Password	****
Service name	123

Figure 4- 27 PPPOE

Notes:

- The IP address of the LAN port cannot be set to the same network segment as the IP address of the WAN port. when the WAN port is set to a static IP, it cannot be set to an existing IP on the network to prevent IP conflicts.
- Only one default gateway can be configured for a device. When you turn on the routing mode, you should delete any one of the default gateway of LAN port or WAN port gateway before you can save the configuration.

4. 3. 2 Advanced settings

Advanced settings include bridge interface settings, VLAN, Ethernet interface settings, IPv4 static routing, IPV6 static routing, and interface isolation.

Bridge Interface Settings: You can add or delete bridge interfaces and configure ports and other parameters by yourself. Such as IP address, netmask, gateway, etc. The above parameters are not required and can be set according to your needs; you can also delete the newly created bridge, note that bridge interfaces created by the system cannot be deleted. The device contains eth0, eth1, ath0, ath01, ath1 five interfaces, eth0 corresponds to the LAN port on the power adapter, eth1 is the LAN port on the device, ath0 is the 2.4G wireless interface, ath01 is the 2.4G management wireless interface, ath1 is the 5G wireless interface. The figure below shows the default display of the bridge interface in routing mode.

Bridge Interface Settings			
Bridge Name	STP	Port	Comment
br-lan	Disabled	ath0 ath1 eth1	
br-wan		eth0	

Figure 4-28 Bridge Interface Settings

Notes: For multiple bridge interfaces, there is and can only be one gateway, and the gateway configuration can be empty and unconfigured.

VLAN: The VLAN function allows users to add multiple VLAN interfaces on each network interface. The VLANIDs are numbered in the range of 3 to 4094, and each VLAN ID represents a different VLAN value. As shown in the figure below, on ath0 (i.e. the wireless link), add a VL AN with VLANID of 10.

VLAN				
Enable	Interface	VLAN ID	Comment	Add
Enable	eth1	10		 

Figure 4-29 VLAN

The VLAN function needs to be used in conjunction with the bridge interface settings, as shown below, adding VLANs to both eth0 and ath0 with ID 10 and placing them in a newly created bridge interface, vlan10 (which can also be the default bridge interface). The wired eth0 interface needs to be connected to a device that supports VLAN 10 (e.g. a VLAN switch with ports that support VLAN 10) to access the device for management via the bridge address where eth0.10 is located. For wireless services over VLAN, the wireless associated peer device must also support VLAN 10 (e.g. ath0 adds VLAN 10).

Advanced Settings				
Bridge Interface Settings				
Bridge Name	STP	Port	Comment	Add
br-lan	Disabled	ath0 ath01 ath1 eth0 eth1		
VLAN				
Enable	Interface	VLAN ID	Comment	Add
Enable	eth1	3		 
Enable	eth0	3		 

Figure 4-30 VLAN Settings

Common connections are shown in the following diagram.

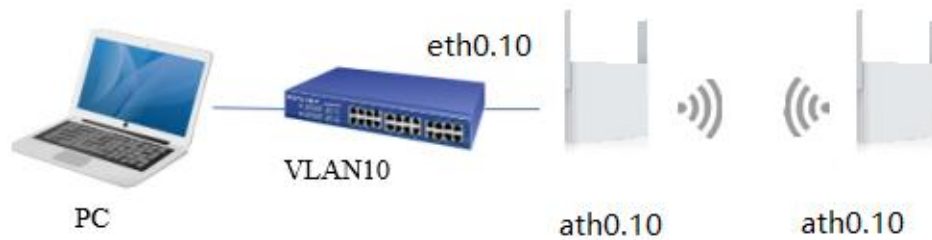


Figure 4-31 VLAN Connection diagram

Manage VLAN: After the management VLAN saving is enabled in the network settings, the VLANs of the device's wired and wireless interfaces will be added automatically in the VLAN settings, and a new mgmtvlan will be created in the bridge interface settings. Add the created VLAN interface to the mgmtvlan, and after connecting a device that supports VLAN3 (such as a VLAN switch with a supported VLAN ID of 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.

Management VLAN ☒

Management VLAN ID

IPv4 Address

IPv4 Netmask

IPv4 Gateway

Advanced Settings

Bridge Interface Settings

Bridge Name	STP	Port	Comment	Add
br-lan	Disabled	eth0 eth1 ath0 ath01 ath1		
mgmtvlan		eth0.3 eth1.3 ath0.3 ath01.3 ath1.3		

VLAN

Enable	Interface	VLAN ID	Comment	Add
Enable	eth0	3		
Enable	eth1	3		
Enable	ath0	3		
Enable	ath01	3		
Enable	ath1	3		

Figure 4-32 VLAN settings

Ethernet interface settings: Users can set the Ethernet interface for eth0 (the LAN port on the power adapter). By selecting auto-negotiation mode, the Ethernet port of the device will be automatically negotiated to the maximum transmission rate according to the connected device; when non-auto-negotiation is selected, the user can set the rate (10M/100M/1000M/2500M) and single-duplex (full-duplex/half-duplex) of the Ethernet port of the device by themselves.

Ethernet Interface Settings ^

Interface	Mode	Speed	Duplex
eth1	Negotiate ▼		
eth0	Negotiate ▼		

Figure 4- 33 Ethernet Interface Settings

IPv4 Static Routes: This function allows you to set up IPv4 static routes. Click Add to bring up the following page.

New IPv4 Static Routes

Interface	lan ▼
Destination	
Netmask	
IPv4 Gateway	
Metric	

Cancel ✕

Complete ✓

Figure 4- 34 IPv4 Static Routes-add

- **Interface:** The bridge interface of the corresponding network segment.
- **Destination:** Target network segment.
- **Netmask:** Gateway and outgoing interface IPv4 addresses must be in the same network segment
- **Metric:** Number of routers passed during transmission.

Configure the appropriate parameters and click Complete, as follows.

IPv4 Static Routes ^

Interface	Destination	Netmask	IPv4 Gateway	Metric	Add
lan	192.168.1.0	255.255.255.0	192.168.10.229	3	 

Figure 4- 35 IPv4 Static Routes

IPv6 Static Routes: This function allows you to set up IPv6 static routes. Click Add to bring up the following page.

New IPv6 Static Routes

Interface

lan 

Destination

Prefix Length

IPv6 Gateway

Metric

Cancel 

Complete 

Figure 4- 36 IPv6 Static Routes-add

Configure the appropriate parameters and click Complete, as follows.

IPv6 Static Routes					
Interface	Destination	Prefix Length	IPv6 Gateway	Metric	
lan	2000::	64	2001::1000	3	 

Figure 4- 37 IPv6 Static Routes

Interface isolation:

Wired interface isolation: off by default, when switched on the wired ports of the device cannot communicate with each other.

Wireless interface isolation: off by default, when switched on the various wireless interfaces of the device cannot communicate with each other.

Interface Isolation	
Interface	Enable
Wired Ethernet	☐
Wireless	☐

Figure 4- 38Interface Isolation

4. 4 Traffic management

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

Firewall: When the user wants to block certain devices, the firewall can be used to implement this function. This function is turned off by default.

Firewall

Enable ☒

Firewall Default Policy

Deny

IP Filter Settings

Enable	Destination	Interface	Protocol	Source IP	Source IP Mask	Dest IP	Dest IP Mask	
								

MAC Filter Settings

Enable	Destination	Interface	Source MAC	Dest MAC	
					

Figure 4- 39 Firewall

Notes: The "Destination" in the filter settings refers to the device on which the firewall is currently configured, while the "source" refers to the device or computer on the opposite end. For example, if the device is directly connected to a computer, and firewall rules are configured on the device, the computer side is the source and the device is the destination. If you cannot distinguish between source and destination, you can configure two relative rules as follows.

- Filter messages from devices with IP address 192.168.10.100 on the eth0 port (corresponding to the LAN port on the power adapter).The firewall is enabled, the firewall default rules are discarded, and two rules are added to the IP filter settings.
 - (1) Destination is receive, interface eth0, protocol is IP, source IP/mask is 192.168.10.100/32, destination IP/mask is 192.168.10.1 (IP address of the device)/32.
 - (2) Destination is receive, interface eth0, protocol is IP, source IP/mask is 192.168.10.1 (IP address of the device)/32, destination IP/mask is 192.168.10.100/32.

Firewall

Enable

Firewall Default Policy

Deny

IP Filter Settings

Enable	Destination	Interface	Protocol	Source IP	Source IP Mask	Dest IP	Dest IP Mask	Add
Enable	Accept	eth0	IP	192.168.10.1	32	192.168.10.100	32	 
Enable	Accept	eth0	IP	192.168.10.100	32	192.168.10.1	32	 

Figure 4-40 IP Filter Settings

- Filter messages from devices with MAC address 00:00:00:00:00:01 on eth0 (LAN port on power adapter)Firewall enabled, firewall default rules discarded, two rules added to MAC filter settings.
 - (1) Destination is receive,Interface eth0 with a source MAC of 00:00:00:00:00:01 and a destination MAC of the device bridge MAC address.
 - (2) Destination is receive,interface eth0, the source MAC is the bridge MAC address of the device and the destination MAC is 00:00:00:00:00:01.

MAC Filter Settings					
Enable	Destination	Interface	Source MAC	Dest MAC	Add
Enable	Accept	eth0	9C:B7:93:E8:0F:D6	00:00:00:00:00:01	 
Enable	Accept	eth0	00:00:00:00:00:01	9C:B7:93:E8:0F:D6	 

Figure 4-41 MAC Filter Settings

Traffic Shaping: Upload rate and download rate limits can be applied to the device interface, as shown below.

Traffic Shaping				
Enable	Interface	Upload Rate(kbit/s)	Download Rate(kbit/s)	Add
Enable	eth1	10240	10240	 

Figure 4-42Traffic Shaping

QoS Priority: QoS (Quality of Service) It refers to a network's ability to use various underlying technologies to provide better service capabilities for specified network communications, a security mechanism for the network, and is used to solve problems such as network latency and blocking.

QoS Priority

Enable	Target CoS	Target DSCP	Source MAC	Dest MAC	VLAN ID	CoS	Eth Type	DSCP	IP Type	Source IP	Dest IP	Source Port	Dest Port	Add
Disabled	0	None				0	All	All	All					 
Disabled	1	None				1	All	All	All					 
Disabled	1	None				2	All	All	All					 
Disabled	0	None				3	All	All	All					 
Disabled	4	None				4	All	All	All					 
Disabled	4	None				5	All	All	All					 
Disabled	6	None				6	All	All	All					 
Disabled	6	None				7	All	All	All					 

Figure 4-43 QoS Priority

- **Target CoS:** Target CoS, The range is 0 to 7, corresponding to the priority level.
- **Target DSCP:** Target DSCP, Differentiated Services Code Point, distinguishing priorities by coded values in the range 0 to 63.

The following restrictions are applied to messages that pass the restrictions.

- **Source MAC:** Source MAC
- **Dest MAC:** Dest MAC
- **VLAN ID:** VLAN。
- **CoS:** Priority
- **ETH Type:** Ethernet type
- **DSCP:** DSCP
- **IP Type:** IP Type
- **Source IP:** Source IP
- **Dest IP:** Dest IP address
- **Source Port:** Source Port
- **Dest Port:** Remote Ports

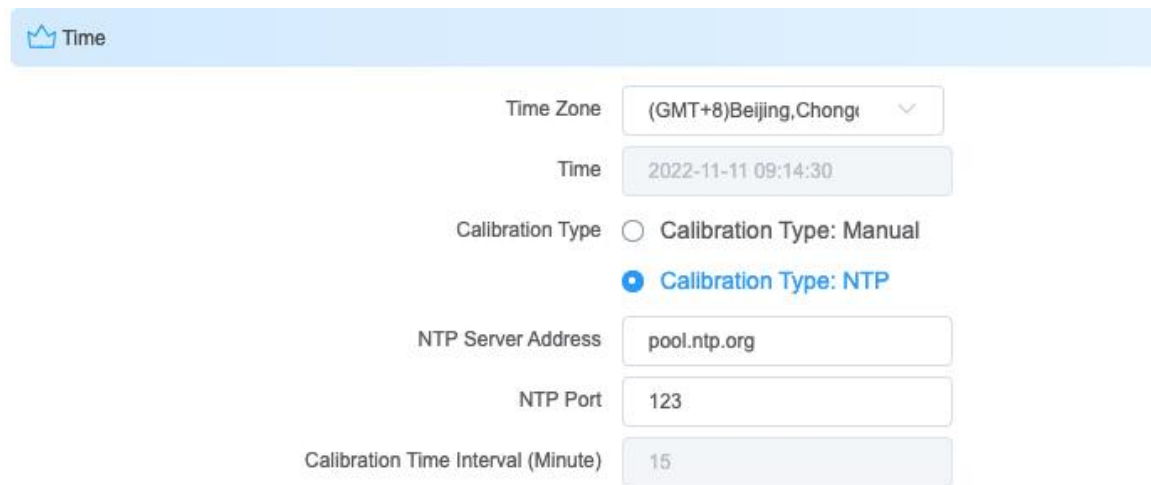
4. 5 Service settings

Time Setting: Set the time of the device, you can choose different time zones; the calibration mode is divided into manual calibration and NTP calibration, manual calibration can set the time by itself or click to synchronize with the computer time, NTP calibration needs to fill in the server address, NTP port, the calibration interval is 15 minutes by default, at this time, you need to configure the device to access the external network (you can refer to 4.2.2 interface settings), it will automatically from the NTP server calibrate the time of the device and show it on the status display page.



The screenshot shows the 'Time' settings page with a light blue header. The 'Time Zone' is set to '(GMT+8)Beijing,Chongqing'. The 'Time' is displayed as '2022-11-11 09:14:07'. Under 'Calibration Type', 'Calibration Type: Manual' is selected with a blue radio button, while 'Calibration Type: NTP' is unselected. Below this, there is a 'Time' input field with a clock icon and a 'Synchronize' checkbox which is unchecked.

Figure 4-44 Service settings-Time settings (Manual)



The screenshot shows the 'Time' settings page with a light blue header. The 'Time Zone' is set to '(GMT+8)Beijing,Chongqing'. The 'Time' is displayed as '2022-11-11 09:14:30'. Under 'Calibration Type', 'Calibration Type: NTP' is selected with a blue radio button, while 'Calibration Type: Manual' is unselected. Below this, the 'NTP Server Address' is set to 'pool.ntp.org', the 'NTP Port' is set to '123', and the 'Calibration Time Interval (Minute)' is set to '15'.

Figure 4-45Service settings-Time settings (NTP)

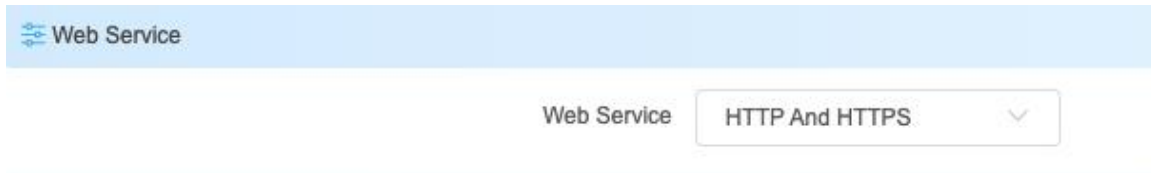
Remote Management: When SSH is enabled, secure CRT, xshell and other serial port printing tools can be used to log in to the device by filling in the IP and port number of the device. When SSH is disabled, the device cannot be logged in.



The interface shows a light blue header bar with a gear icon and the text "Remote Management". Below this, the "SSH Service" is toggled on, indicated by a blue switch. Underneath, the "Port" is set to "22" in a text input field.

Figure 4- 46 Service settings-Remote Management

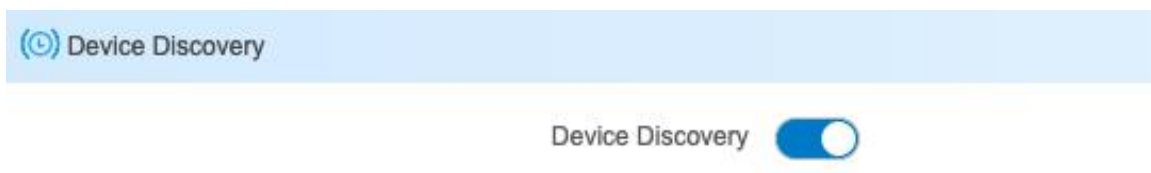
Web service: Users can choose between http or https login to the device page.



The interface features a light blue header bar with a server icon and the text "Web Service". Below the header, the "Web Service" is set to "HTTP And HTTPS" via a dropdown menu.

Figure 4- 47 Service settings-Web service

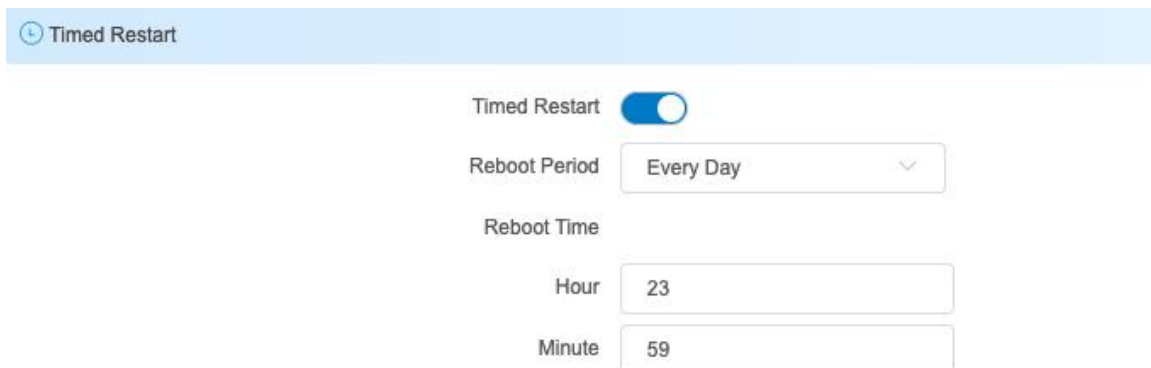
Device Discovery: When this function is enabled, please use it with a special toolset. The toolset window will display the MAC address, IP address, product name, firmware name, etc. of the discovered device. Note: when discovering devices wirelessly, keep multicast support enabled.



The interface has a light blue header bar with a clock icon and the text "Device Discovery". Below the header, the "Device Discovery" is toggled on, indicated by a blue switch.

Figure 4- 48 Service settings-Device Discovery

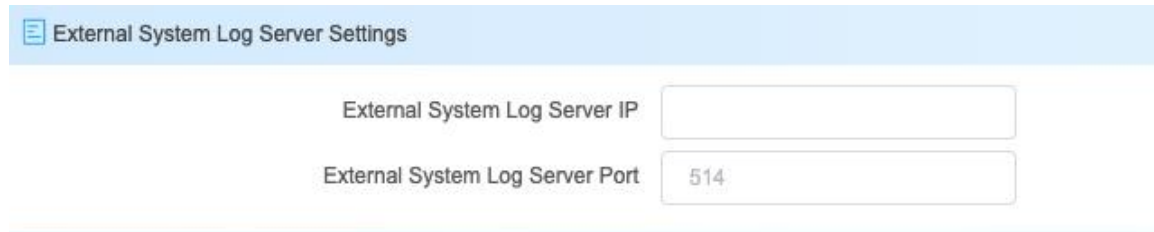
Timed Restart: Through this function, the device can be restarted regularly.



The interface features a light blue header bar with a clock icon and the text "Timed Restart". Below the header, the "Timed Restart" is toggled on, indicated by a blue switch. Underneath, the "Reboot Period" is set to "Every Day" via a dropdown menu. The "Reboot Time" is specified with "Hour" set to "23" and "Minute" set to "59" in separate text input fields.

Figure 4- 49Service settings-Timed Restart

External System Log Server: Remote log: enable the remote log function, fill in the IP address of the PC where the remote log server is located, set the server port to 514, and click Save to record the log information of the device in real time on the log server.



External System Log Server Settings

External System Log Server IP

External System Log Server Port

Figure 4-50 External System Log Server

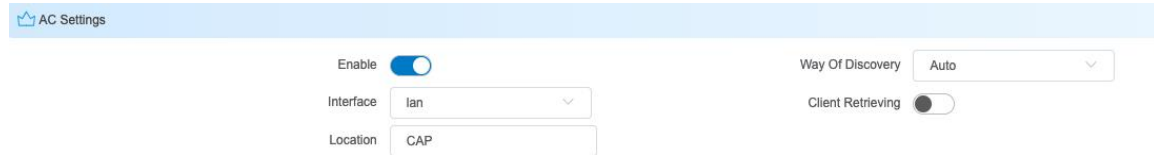
AC Management: When this function is enabled, it needs to be used with AC management system.

- **Location:** The deployment location of the equipment, you can fill in the location of the device that you want to display on the AC map as required.
- **Way Of Discovery:** There are two ways for AP to discover AC, which are manually specified and automatic. When the discovery mode is manually specified, the primary ac address and the standby AC address can be added, and the added IP address is the IP of the AC management system. When layer 2 is online, the device IP and AC ip should be the same network segment. When layer 3 is online, if you select automatic discovery, you need to fill in the IP address of AC in the option43 field of the DHCP server. It is recommended that nonprofessionals configure the manual discovery method here.

Option43 field format: 8007000001AC122847 (80: fixed value, no need to change; 07: length field, the length of the byte of data that follows it; 0000: fixed value, no need to change; 01: indicates the number of IP addresses that follow, in this case an IP address; AC122847: indicates the AC IP address (172.18. 40.71) in hexadecimal, change the last 8 bits of the parameter according to the IP address of the AC, other parameters can remain unchanged).

- **Client Retrieving:** Enabling this function allows the AC to retrieve the client. When the client is disconnected from the access point and goes offline from the AC, it will enter the retrieval mode and the access point can also enter the retrieval mode by clicking on the client retrieval function on the AC.

Note: only when the client device is associated with the access point device, and the access point device has enabled the AC function and joined the same AC system, can it successfully join the AC.



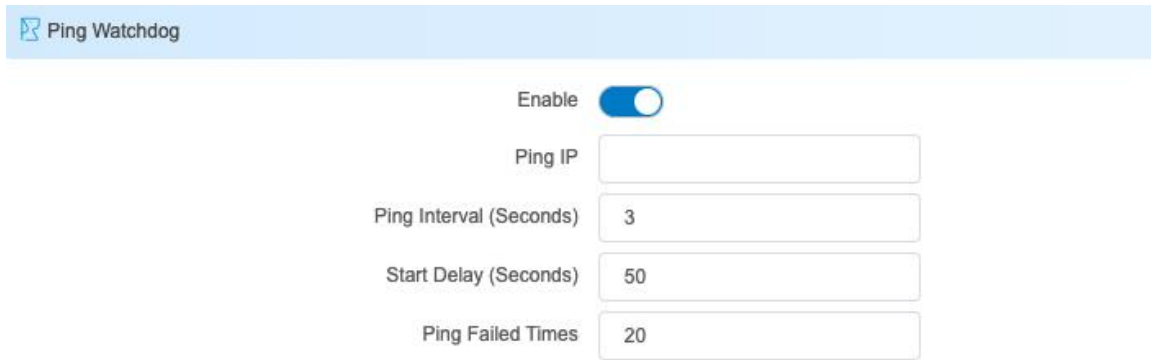
The image shows a web interface titled "AC Settings". It contains several configuration options: an "Enable" toggle switch that is turned on (blue), an "Interface" dropdown menu set to "lan", a "Location" dropdown menu set to "CAP", a "Way Of Discovery" dropdown menu set to "Auto", and a "Client Retrieving" toggle switch that is turned off (grey).

Figure 4-51 AC Management

Ping Watchdog: This function is designed for continuous monitoring of equipment operation. The device can ping the IP address of the target host or device for a long time. If a certain number of replies are not received, the tool will restart the device. It is recommended that the user enable this function on the side where the wireless mode is "Client". It is not recommended that users enable this function on the side where the wireless mode is "Access Point".

- **Ping Interval:** The time interval between two pings, in seconds.
- **Ping IP:** Generally fill in the IP address of the target host or device. When Ping dongle is enabled in "Client" mode, the IP address of the access point device to which the client is connected can be filled in here.
- **Start Delay:** When the system of the device is started, the device will start to Ping the target host after the set delay time, in seconds.
- **Ping Failed Times:** When the number of consecutive Ping failures reaches the set value, the device will restart the device.

Note: if you want to modify the parameter configuration of Ping dongle, please disable Ping dongle first. After the disable takes effect, Ping dongle can be enabled for new parameter configuration.



Ping Watchdog

Enable ☒

Ping IP

Ping Interval (Seconds)

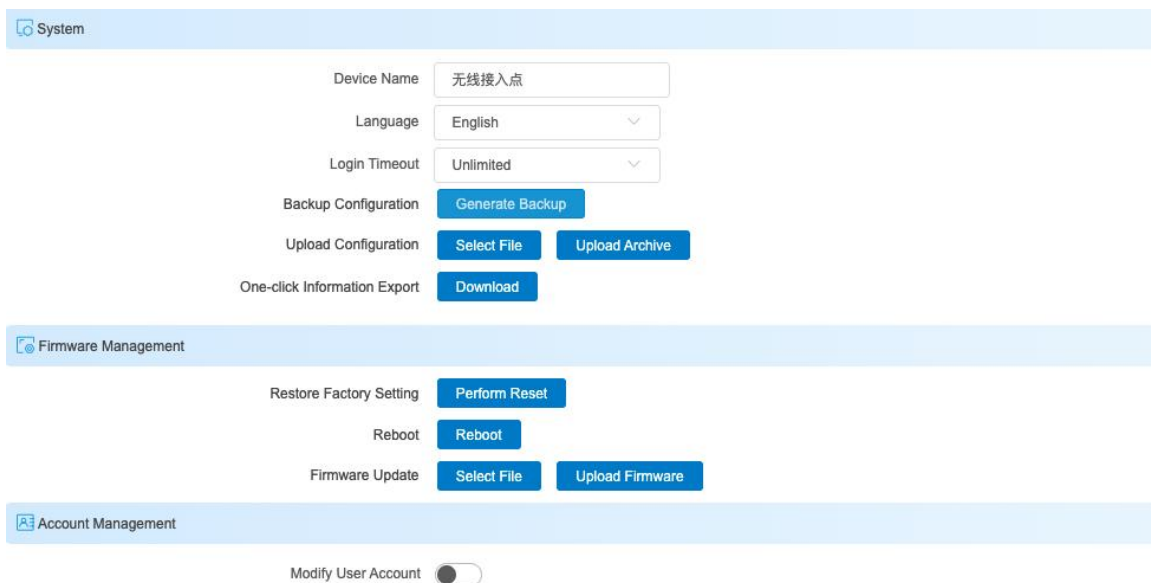
Start Delay (Seconds)

Ping Failed Times

Figure 4-52 Ping Watchdog

4. 6 System settings

The system setting interface is divided into system settings, firmware configuration and account management, as shown in the following figure:



System

Device Name

Language

Login Timeout

Backup Configuration

Upload Configuration

One-click Information Export

Firmware Management

Restore Factory Setting

Reboot

Firmware Update

Account Management

Modify User Account ☐

Figure 4-53 System settings

- **Device Name:** Users can set the setting name to the name they need according to their own needs.
- **Language:** Users can choose the page display language according to their own needs.
- **Login Timeout:** When the user does not operate the device for a time-out, the login timeout value will automatically jump to the login interface when operating the page again.

- **Backup Configuration:** Click generate backup. All the current configurations on the web page will be backed up to the local file. Note that the content of the configuration file cannot be modified manually.
- **Upload Configuration:** Click Select file, select the previously downloaded configuration file, and click upload to restore the device configuration to the device configuration when the configuration file was backed up.
- **One-click Information Export:** Click download to export the system log file, which contains the configuration file.
- **Restore Factory Setting:** Click execute reset on the webpage, and the page will jump to the waiting page. After the reset is completed, the page will jump to the login page, and the device configuration will return to the factory setting state.
- **Reboot:** Click restart to restart the device system. After the restart, the configuration remains unchanged.
- **Firmware Update:** Click browse, select the version to be upgraded, click upgrade, and the device will start to upgrade.

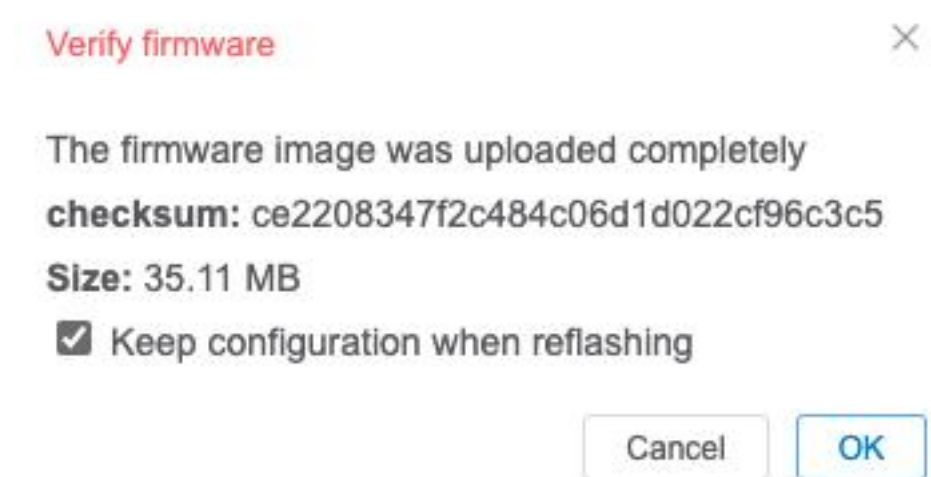


Figure 4-54 Firmware Update

- **Modify User Account:** When user password modification is enabled, users can modify the user name and password of login device management web page according to their own needs. In order to enhance information security, please change the device password regularly, try not to use too simple password, such as pure numbers, letters, birthday, etc.

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

Fill in the IP address of a device and click Ping. Ping results will be displayed in the collected data, as shown in the following figure:

The screenshot shows a web-based tool titled "Ping IP". It has a text input field for "IPAddress/Domain" containing "192.168.10.3" and a "Ping" button. Below the input field, the "Ping Result" section displays the following text:

```
PING 192.168.10.3 (192.168.10.3): 56 data bytes
64 bytes from 192.168.10.3: seq=0 ttl=64 time=3.770 ms
64 bytes from 192.168.10.3: seq=1 ttl=64 time=1.524 ms
64 bytes from 192.168.10.3: seq=2 ttl=64 time=3.031 ms
64 bytes from 192.168.10.3: seq=3 ttl=64 time=7.320 ms
64 bytes from 192.168.10.3: seq=4 ttl=64 time=1.788 ms

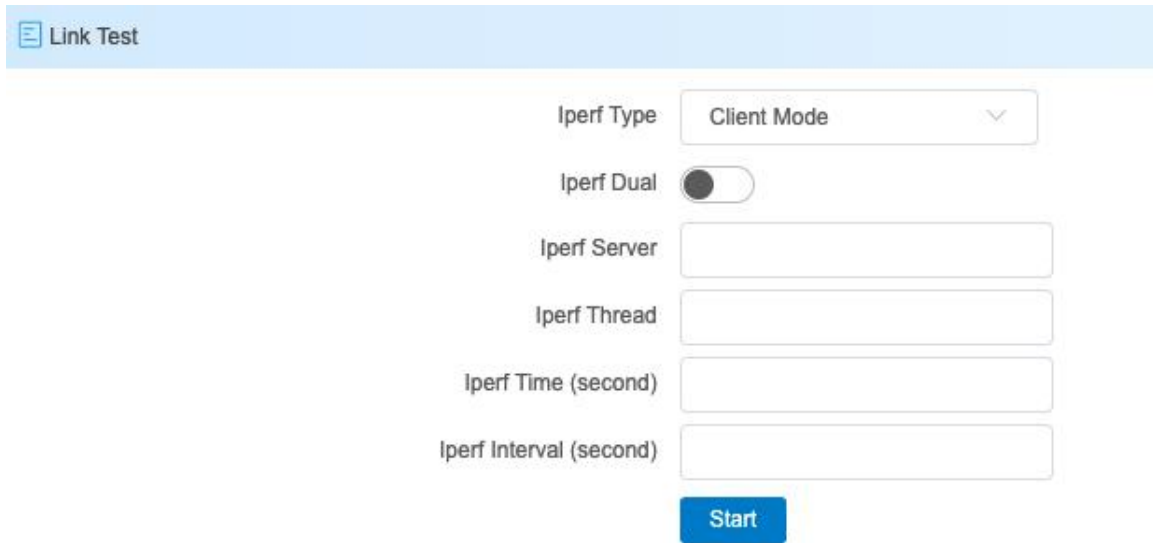
--- 192.168.10.3 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.524/3.486/7.320 ms
```

Figure 5- 1 Ping IP

5. 2 Link Test

Iperf test can test the maximum bandwidth performance, and can report bandwidth, delay jitter and packet loss. It is divided into client mode and server mode, which is used to test the throughput of wireless terminals between devices. For device 1, select "server", and iperf interval is the interval time for displaying throughput on the web page. Select "client" for device 2, and iperf server fills in the IP address of device 1. The number of iperf threads is the number of threads running at the same time when testing throughput. It is recommended to set it to 10. Iperf test time is the number of seconds that iperf was run. Iperf interval is the

interval between displaying throughput on a web page. After these parameters are filled in, click the "Start" button to test.



The interface for the Link Test in Client Mode. It features a light blue header bar with a menu icon and the text "Link Test". Below the header, the "Iperf Type" dropdown is set to "Client Mode". The "Iperf Dual" toggle switch is turned off. There are four empty input fields for "Iperf Server", "Iperf Thread", "Iperf Time (second)", and "Iperf Interval (second)". A blue "Start" button is positioned at the bottom right of the form.

Figure 5- 2 Link Test-Client Mode



The interface for the Link Test in Server Mode. It features a light blue header bar with a menu icon and the text "Link Test". Below the header, the "Iperf Type" dropdown is set to "Server Mode". A blue "Start" button is positioned below the dropdown menu.

Figure 5- 3 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, it will jump to the login page.

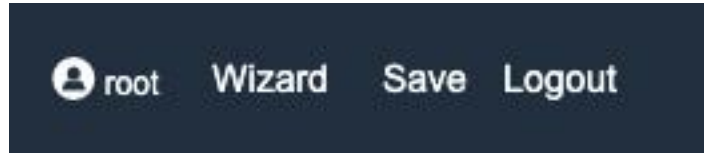


Figure 6- 1 Logout

FCC Warning

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.