
Networking Router

User manual

Document version: V1.0

Published: 2025-11-10

Without the written permission of the Company, no unit or individual shall excerpt or copy part or all of the content of this document without authorization, and shall not disseminate it in any form.

note

The products, services or features you purchase are subject to commercial contracts and terms, and all or part of the products, services or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, KI makes no representations or warranties, express or implied, with respect to the content of this document. Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Unless otherwise agreed, this document is provided as a guide for use only and all statements, information and advice contained in this document do not constitute any express or implied warranty.

preface

This user manual describes how to manage the network of wireless client products.

Audience:

This manual is primarily intended for the following engineers:

- Network administrators responsible for network configuration and maintenance
- On-site technical support and maintenance personnel
- Network Engineer

Port conventions

The port numbers in this manual are for example only and do not represent the ports with this number on the device.

Text formatting conventions

format	illustrate
""	Text with "" represents interface words. For example: "Port number".
>	Multi-level paths are separated by ">". For example, open the local connection path description: Open Control Panel> Network Connection>Local Connection".
Light blue font	Representative clicks on text that enables hyperlinking. Font color such as: "light blue"
About this chapter	In the "About this chapter" section, provide links to each section of this chapter, as well as links to the corresponding principles/operations chapters of this

format	illustrate
	chapter.

icon convention

format	illustrate
 note	Remind you of the precautions that should be paid attention to in the operation, improper operation may result in data loss or device damage.
 warn	The annotations after this sign should be given special attention, and improper operation may cause personal injury.
 illustrate	Tips and tricks for configuring, operating, or using equipment.
 Trick of the trade	In the "About this chapter" section, provide links to each section of this chapter, as well as links to the corresponding principles/operations chapters of this chapter.
 prompt	Actions or information that require special attention to ensure that the device is configured successfully or

format	illustrate
	functioning properly.

Modify the record

Version number	Revision date	Revision Notes
V1.0.0	2025-11-10	Product launch

Table of Contents

1 Log in to the WEB interface	7
1.1 Set the IP address of your PC	7
1.1.1 Wired access mode	7
1.1.2 Wireless access method	8
1.2 Log in to the WEB configuration page	10
2 Home	11
3 Internet	12
3.1 IPv4	13
3.2 IPv6	17
4 Wi-Fi	21
4.1 2.4G Wi-Fi	22
4.2 5G Wi-Fi	23
5 Advanced	25
5.1 Network	26
5.1.1 LAN	26
5.1.2 IPv6	28
5.1.3 VPN	29
5.1.4 IPsec	30
5.1.5 Smart QoS	33
5.1.6 Guest network	34
5.1.7 DDNS	35
5.1.8 firewall	36
5.1.9 parental controls	37
5.1.10 Remote WEB access	39
5.1.11 MAC address cloning	40
5.1.12 WOL	41
5.2 Security	43
5.2.1 Wireless ACL	43
5.2.2 Passwords	45
5.3 SYSTEM	46
5.3.1 System status	46
5.3.2 Time zone	47
5.3.3 Diagnosis	48
5.3.4 Backup	49
5.3.5 Schedule Restarts	51
5.3.6 System upgrades	52

1 Log in to the WEB interface

1.1 Set the IP address of your PC

1.1.1 Wired access mode

table 1The device has a default management network address

IP settings	Default value
IP address	192.168.88.1
Subnet mask	255.255.255.0

When configuring a device via the web:

- Make sure that the computer has an Ethernet adapter installed and enabled.
- Before you configure the remote configuration, make sure that the route between the computer and the device is reachable.
- Before performing local configuration, make sure that the IP address of the computer is in the same subnet as the device.

Illustrate:

If the device is configured locally, make sure that the current PC's network block is 88.

For example, if the IP address of the current PC is 192.168.5.60, it will be | The CIDR block "5" of the P address is changed to "88".

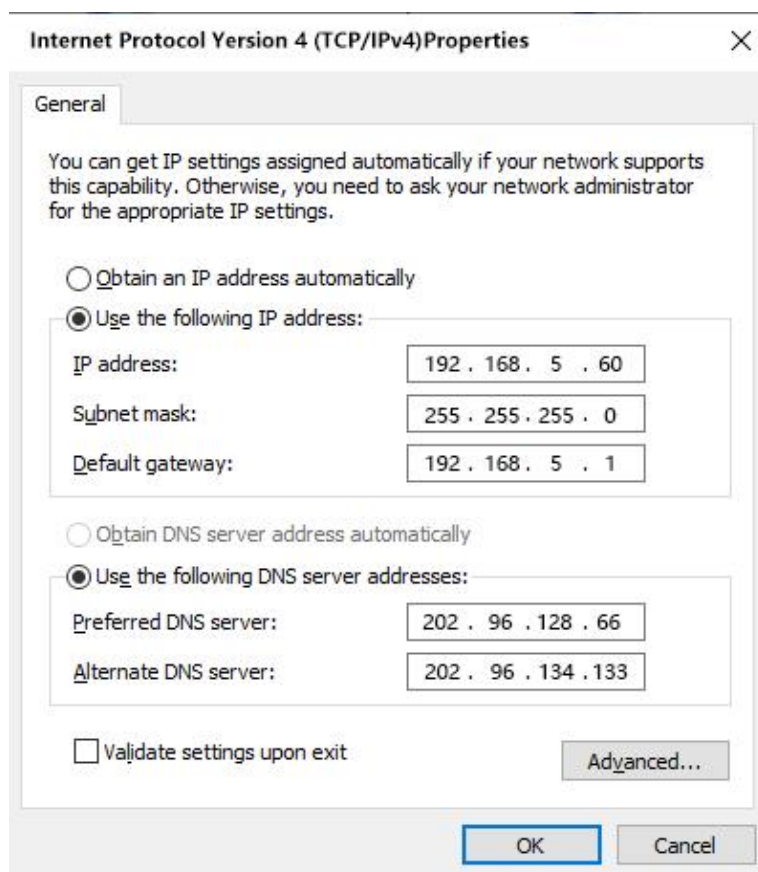
Procedure:

The steps to modify are as follows:

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

2. Change the "5" selected in the red box in the figure to "88".
3. Click OK to successfully modify it.
4. Come to an end.

fig 1 Modify the CIDR segment



1.1.2 Wireless access method

For the default management network address of the device, see "Table 1" shown.

When configuring a device via WEB:

- Make sure that the wireless adapter is installed and enabled on your computer.
- Place your computer within range of your device's wireless network.
- Make sure that the IP address of the computer is in the same subnet as the device.



note

Do not use a proxy server for the device IP address or network segment!

Match the IP address of the computer with the device's | The IP address is set within the same subnet.

Procedure:

The steps for wireless connection are as follows.

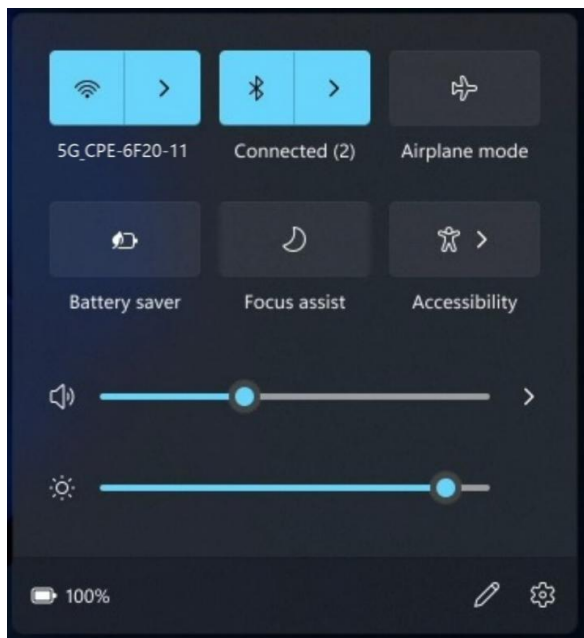
1. Click the wireless icon "" in the lower right corner of the computer  to pop up the wireless list box.
2. Select the wireless network name of the device in the wireless list box, enter the password, and click the "Connect" button.

Illustrate:

The default wireless network names of the device, i.e., the SSID of the WiFi are 5G_CPE-XXXX and 5G_CPE_5-XXXX (the SSID of the wifi contains the 5G_CPE and part of the MAC address information), and the initialization password is 123456789.

3. Come to an end. After a successful connection, the wireless network shows "Connected".

fig 2 The network connection is successful



1.2 Log in to the WEB configuration page

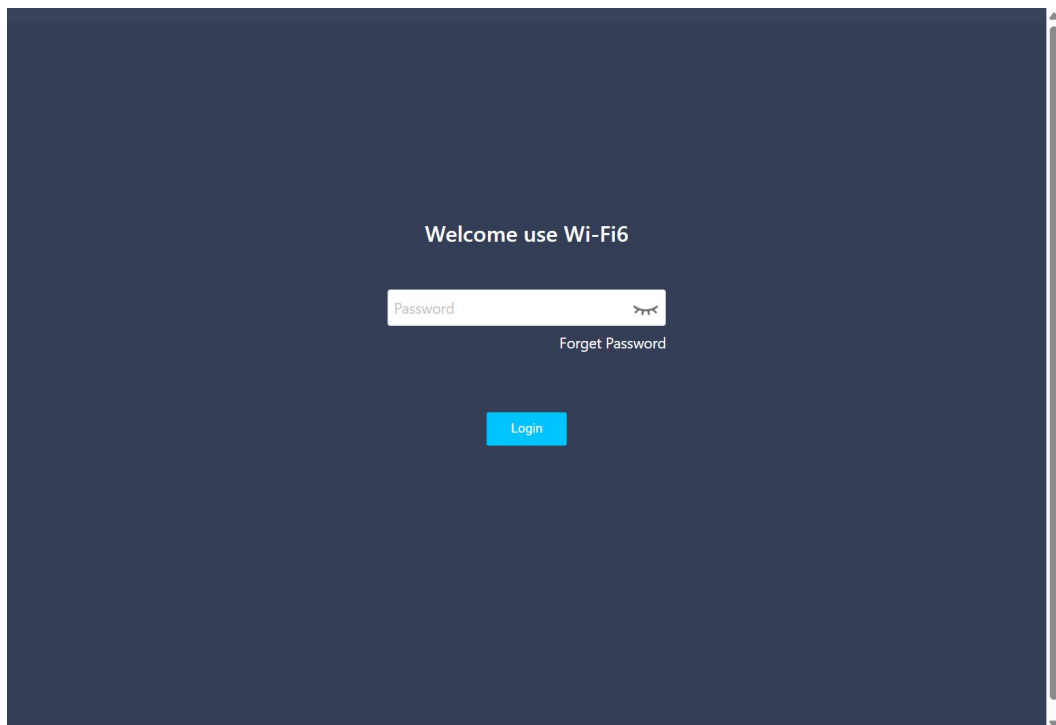
Procedure:

The following are the steps to log in to the WEB configuration interface.

1. Run a computer browser.
2. Enter the address of your device "http://192.168.88.1" in the address bar of your browser.
3. Click Enter.
4. Pop up Figure 3 on the login page shown, enter the administrator password in the login window.
5. Click "Sign in".
6. Come to an end.

After successfully logging in, you can configure the relevant parameters and information of the WEB interface as needed.

fig 3 Login page

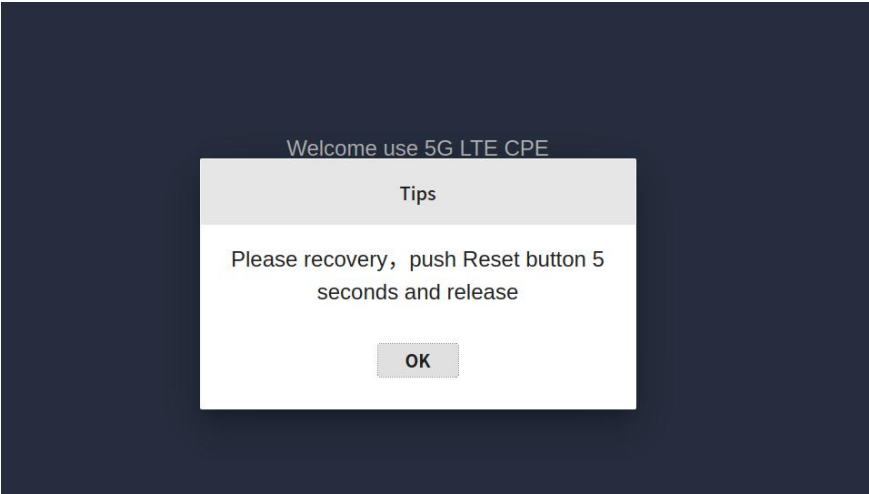


Illustrate:

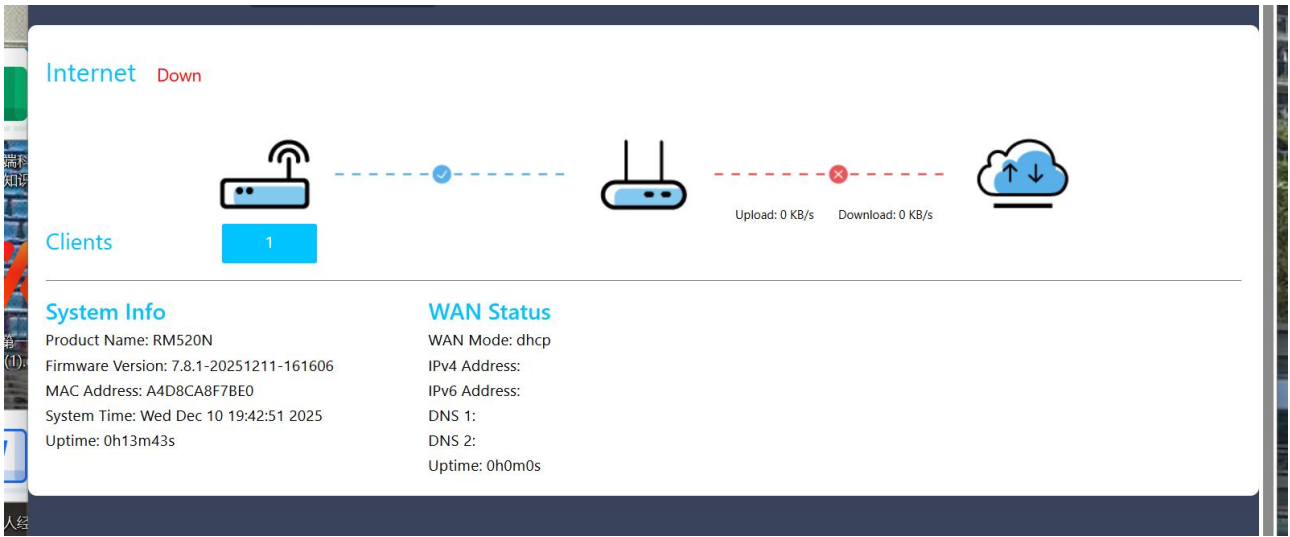
The default initialization administrator password for the device is admin, so be case sensitive when entering.

If you forget your password, click "Forgot Password" to enter the Figure 4 As prompted, press and hold the "Reset" button on the device for 5 seconds and release it to restore the initialized administrator password.

fig 4 Recover your password



2 Home



3 Internet

Function description:

On the Internet settings page, users can select the working mode according to the needs of the site, and then complete the mode setting step by step according to the guidance.

table 3 Internet settings

IP settings	Default value
IP address	192.168.88.1
Subnet mask	255.255.255.0

Action path

Select Internet settings in the navigation bar.

Interface description

fig 6 Internet settings

The screenshot displays the 'Internet Setting' page of a network management interface. At the top, a dark blue navigation bar contains the 'Wi-Fi6' logo and five menu items: 'Home', 'Internet' (selected), 'Wi-Fi', and 'Advanced'. Below the navigation bar, the 'Internet Setting' title is followed by a horizontal line. The main content area is divided into three sections: 'MTU' with a value of 1500 and a 'Save' button; 'IPv4' with a 'Working Mode' dropdown set to 'DHCP' and a 'Manual DNS' toggle switch; and 'IPv6' with a toggle switch set to 'ON', a 'Working Mode' dropdown set to 'DHCPv6', and a 'Manual DNS' toggle switch. Each of the three sections has a 'Save' button at the bottom.

table 4 Description of the main elements of the Internet settings interface

Interface elements	illustrate
mode	The mode includes WAN and LAN. The WAN port of the device can be connected to the external network through PPPoE dialing, static IP, and dynamic acquisition, and the LAN port is only used to change the WAN port on the device to the LAN port.
MTU	The maximum length of a single packet that can pass through PPPoE protocol dialing ranges from 576 to 1500 bytes. Illustrate: MTU (Maximum Transmission Unit) If the maximum length of a single packet exceeds the set MTU value, it will be subpackaged, so reasonable settings can optimize the network speed: It is recommended that the MTU value be set to the same as the MTU value of the higher-level router.

3.1 IPv4

Function description:

The WAN port can connect to the public network in three ways over the IPv4 protocol:

- Broadband Dial-up (PPPoE)
- Automatic Internet Access (DHCP)
- Static IP

Interface Description 1: Broadband Dial-up (PPPoE)

Broadband Dial-up (PPPoE) interfaces include:Figure 7 shown.

fig 7 Broadband Dial-up (PPPoE)

IPv4

Working Mode

PPPoE

Username ISP username

Password ISP password

Manual DNS

DNS 1 DNS Address

DNS 2 DNS Address

Advanced

Special Dial ☐ ON ☒ OFF

MTU 1480

Service Name Server Name

Save

table 5 Descriptions of the main elements of the Broadband Dial-up (PPPoE) interface

Interface elements	illustrate
PPPoE dialing	Broadband dial-up PPPOE dialing tab, peer-to-peer protocol dialing on Ethernet to achieve Internet access.
Account	Broadband dial-up PPPoE dial-up Internet account. Illustrate: Account numbers, passwords, and service names are provided by the network provider.
password	Broadband dial-up PPPOE dial-up Internet password. Illustrate: Account numbers, passwords, and service names are provided by the network provider.
Configure manually	DNS The system default value is gray.
DNS1	DNS server addresses provided by network providers or public networks can also be selected by clicking on recommendations to get the default value.

Interface elements	illustrate
DNS2	DNS server addresses provided by network providers or public networks can also be selected by clicking on recommendations to get the default value.
Advanced settings	The system default value is gray.
Special symbols	The default value for the system is Off
MTU	The maximum length of a single packet that can pass through PPPoE protocol dialing ranges from 576 to 1500 bytes. Illustrate: MTU (Maximum Transmission Unit) If the maximum length of a single packet exceeds the set MTU value, it will be subpackaged, so reasonable settings can optimize the network speed: MTU 值推荐与上级路由器 MTU 值设为一致。
Service Name	Broadband dial-up PPPOE dial-up Internet service name. Illustrate: Account numbers, passwords, and service names are provided by the network provider.

Interface Description 2: Automatic Internet Access (DHCP)

Automatic Internet Access (DHCP) interfaces such as:Figure 8 shown.

fig 8 Automatic Internet Access (DHCP) interface

IPv4

Working Mode

Manual DNS ☒

DNS 1

DNS 2

table 6 Configuration description of the main elements of the Automatic Internet Access (DHCP) interface

Interface elements	illustrate
Automatic Internet Access (DHCP)	Dynamic Acquisition tab, automatically obtain network information of the device's WAN port. Note: The device

Interface elements	illustrate
	automatically obtains the network address information assigned by the network provider or the extranet.
Configure DNS manually	The system default value is gray.
DNS1	DNS server addresses provided by network providers or public networks can also be selected by clicking on recommendations to get the default value.
DNS2	DNS server addresses provided by network providers or public networks can also be selected by clicking on recommendations to get the default value.

Interface description 3: Static IP

Static IP interfaces such as Figure 9 shown.

fig 9 Static IP

IPv4

Working Mode

Static IP

IP IP address!

Netmask netmask

Gateway gateway

DNS 1 DNS Address

DNS 2 DNS Address

Save

table 7 Configuration description of the main elements of the static IP interface

Interface elements	illustrate
Static IP	Static IP tab, the network information configuration of the device's WAN port.
IP address	A fixed IP address provided by your network provider or extranet.
Subnet mask	

Interface elements	illustrate
Gateway address	The default gateway address provided by the network provider or extranet.
DNS1	DNS server addresses provided by network providers or public networks can also be selected by clicking on recommendations to get the default value.
DNS2	DNS server addresses provided by network providers or public networks can also be selected by clicking on recommendations to get the default value.

3.2 IPv6

Function description:

WAN ports can connect to the public network in four ways on the IPv6 protocol:

- DHCPv6
- 6to4
- PPPoEv6
- Static IPv6

Interface description 1: DHCPv6

The DHCPv6 interface is as follows Figure 10 shown.

fig 10 DHCPv6 interface

IPv6 ☒ ON

Working Mode

DHCPv6

Manual DNS ☒

DNS 1

DNS 2

Save

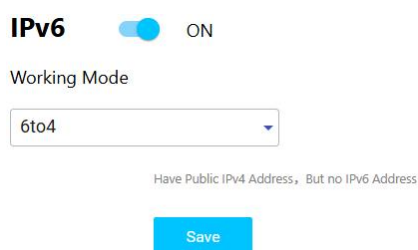
table 8 Configuration description of the main elements of the DHCPv6 interface

Interface elements	illustrate
DHCPv6	IP addresses, IP prefixes, and/or other configured network protocols required for IPv6 hosts operating on IPv6 networks.
DNS1	DNS server address provided by your network provider or extranet.
DNS2	DNS server address provided by your network provider or extranet.

Interface description 2: 6to4

6to4 interface as Figure 11 shown.

fig 11 6to4 interface



IPv6 ☒ ON

Working Mode

6to4

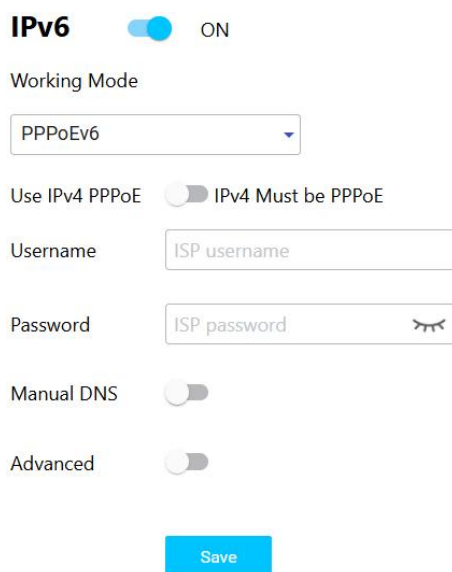
Have Public IPv4 Address, But no IPv6 Address

Save

Interface description 3: PPPoEv6

PPPoEv6 interface is as follows:Figure 12 shown.

fig 12 PPPoEv6 interface



IPv6 ☒ ON

Working Mode

PPPoEv6

Use IPv4 PPPoE ☐ IPv4 Must be PPPoE ☐

Username

Password

Manual DNS ☐

Advanced ☐

Save

table 9 Configuration of the main elements of the PPPoEv6 interface

Interface elements	illustrate
PPPoEv6	A network protocol used to transmit IPv6 packets over an Ethernet connection. It is developed on the basis of PPPoE (Point-to-Point Protocol over Ethernet) and is specifically optimized for IPv6 network environments.
Account	Broadband dial-up PPPoE dial-up Internet account. Illustrate: Account numbers, passwords, and service names are provided by the network provider.
password	Broadband dial-up PPPoE dial-up Internet password. Illustrate: Account numbers, passwords, and service names are provided by the network provider.
Configure manually	DNS The system default value is gray.
DNS1	DNS server address provided by your network provider or extranet.
DNS2	DNS server address provided by your network provider or extranet.
Advanced settings	The system default value is gray.
MTU	The maximum length of a single packet that can pass through PPPoE protocol dialing ranges from 576 to 1500 bytes. Illustrate: MTU (Maximum Transmission Unit) If the maximum length of a single packet exceeds the set MTU value, it will be subpackaged, so reasonable settings can optimize the network speed: It is recommended that the MTU value be set to the same as the MTU value of the higher-level router.
Service Name	Broadband dial-up PPPoE dial-up Internet service name. Illustrate: Account numbers, passwords, and service names are provided by the network provider.

Interface description 4: Static IPv6

Static IPv6 interfaces such as:Figure 13 shown.

fig 13 Static IPv6 interface

IPv6  ON

Working Mode

Static IPv6 ▾

IPv6
Address/Prefix /

LAN IPv6
Address/Prefix /

Gateway

DNS 1

DNS 2

 Save

table 10 Configuration description of the main elements of the static IPv6 interface

Interface elements	illustrate
Static IPv6	Manually configure a fixed IPv6 address on a network device.
IPv6 address/prefix length	
LAN IPv6 address/prefix length	
Gateway address	Gateway addresses automatically assigned by the network provider or extranet.
DNS1	DNS server address provided by your network provider or extranet.
DNS2	DNS server address provided by your network provider or extranet.

4 Wi-Fi

Wi-Fi6

Home

Internet

Wi-Fi

Advanced

Bands Aggregation

OFF

The router automatically selects the best WiFi band for all clients after the feature is enabled

2.4G Wi-Fi

Basic

Switch

ON

OFF

Wi-Fi Name

5G_CPE-7BE0

Security

WPA/WPA2PSK

Password

Hide

OFF

Advanced

Channel

Auto

BandWidth

Auto

Access Limit

128

Tx Power

100

Save

5G Wi-Fi

Basic

Switch

ON

OFF

Wi-Fi Name

5G_CPE_5G-7BE0

Security

WPA/WPA2PSK

Password

Hide

OFF

Advanced

Channel

Auto

BandWidth

Auto

Access Limit

128

Tx Power

100

Save

4.1 2.4G Wi-Fi

Function description:

Select the 2.4G Wi-Fi switch to set the radio frequency 2.4G wireless parameters.

Action path

Select the 2.4G Wi-Fi switch to "On".

Interface description

The 2.4G Wi-Fi interface is as follows Figure 31 shown.

fig 31 2.4G Wi-Fi interface

2.4G Wi-Fi

Basic

Switch

☒ ON ☐ OFF

Wi-Fi Name

5G_CPE-7BE0

Security

WPA/WPA2PSK

Password

.....

Hide

OFF

Advanced

Channel

Auto

BandWidth

Auto

Access Limit

128

Tx Power

100

Save

table 15 2.4G Wi-Fi interface main elements configuration description:

Interface elements	illustrate
switch	2.4G Wi-Fi settings on and off buttons.

Interface elements	illustrate
Wireless name	Wi-Fi wireless name.
Encryption	Encryption method drop-down list
password	Wi-Fi password
No broadcasting	Do not broadcast the drop-down list
Work channel	The working channel drop-down box has a value range of 1-13.
bandwidth	Bandwidth drop-down box.
Maximum number of connections	The maximum number of Wi-Fi devices connected.
Signal strength	Signal strength drop-down box.

4.2 5G Wi-Fi

Function description:

On 5G Wi-Fi, you can set the wireless parameters of RF 5G.

Action path

Select the 5G Wi-Fi switch to "On".

Interface description

The 5G Wi-Fi interface is as follows Figure 32 shown.

fig 32 5G Wi-Fi interface

5G Wi-Fi

Basic

Switch ☒ ON ☐ OFF

Wi-Fi Name

Security

Password

Hide

Advance

Channel

BandWidth

Access Limit

Tx Power

Save

table 16 Description of the main elements of the 5G Wi-Fi interface:

Interface elements	illustrate
switch	5GWi-Fi settings on and off buttons.
Wireless name	Wi-Fi wireless name.
Encryption	Encryption method drop-down list
password	Wi-Fi password
No broadcasting	Do not broadcast the drop-down list
Work channel	The working channel drop-down box has a value range of 1-13.
bandwidth	Bandwidth drop-down box.
Maximum number of connections	The maximum number of Wi-Fi devices connected.
Signal strength	Signal strength drop-down box.

5 Advanced

Wi-Fi6

Home

Internet

Wi-Fi

Advanced

NETWORK

LAN

IPv6

VPN

IPsec

Smart Qos

Guest

DDNS

Firewall

Parental Control

Route

MAC Clone

UPnP

WOL

Security

Wireless ACL

Password

SYSTEM

System Status

Time zone

Diagnosis

Backup

Schedule Restarts

Upgrade firmware

DHCP

ON

DHCP Pool192.168.88.100249

Lease Time720Minutes

DNS 1DNS Address

DNS 2DNS Address

Save

IP & MAC

Name	IP	MAC	Action
Add Rule			

LAN

IP Address192.168.88.1

Subnet Mask255.255.255.0

Save

Function description:

On the advanced settings page, users can select various settings according to their on-site needs, and then follow the guidance to complete the mode settings step by step.

table 17 Advanced settings

Interface elements	illustrate
Network settings	Includes: LAN, IPv6, VPN, IPsec, OpenVpn, Zerotier, TR-069, Smart QoS, Guest Network, DDNS, Remote WEB Access, Firewall, Parental Control, Static Routing, Domain Access Control, MAC Address Cloning, and UPnP.
Safety Center	Includes: "Wireless ACL" and "Manage Passwords".
System management	Includes: System Status, System Diagnostics, System Backup, Scheduled Restart, and System Upgrade.

Action path

Select Advanced settings in the navigation bar.

5.1 Network

5.1.1 LAN

Function description:

On the LAN page, users can implement "DHCP Settings", "IP and MAC Binding" and "LAN Settings" according to the needs of the site, and then follow the guidance step by step.

Action path

Select "Advanced Settings --> Network Settings --> LAN".

Interface description

The settings interface is as follows Figure 33 shown.

fig 33 LAN interface

DHCP

ON

DHCP Pool

192.168.88.100 — 249

Lease Time

720

Minutes

DNS 1

DNS Address

DNS 2

DNS Address

Save

IP & MAC

Name	IP	MAC	Action
------	----	-----	--------

Add Rule

LAN

IP Address

192.168.88.1

Subnet Mask

255.255.255.0

Save

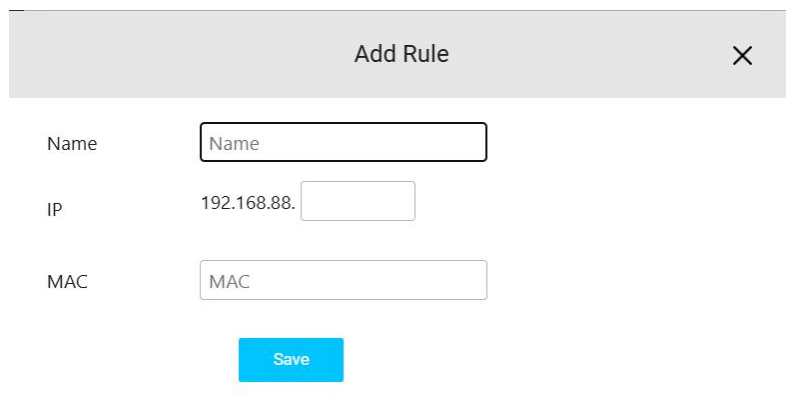
Procedure:

The following are the steps for LAN pages.

1. DHCP Settings.
 - 1) Enter the "Start Address".
 - 2) Enter the Lease Time.
 - 3) Enter "DNS 1".
 - 4) Enter "DNS 2".
 - 5) Click Save.
2. IP is bound to MAC

-
- 1) Click Add Rule in the "IP and MAC Binding" column to enter such as Figure 34 shown.
 - 2) Enter a Rule Name.
 - 3) Enter the IP address.
 - 4) Enter the MAC address.
 - 5) Click Add.

fig 34 IP and MAC binding interface



The screenshot shows a modal dialog box titled "Add Rule" with a close button (X) in the top right corner. The dialog contains three input fields: "Name" with a placeholder "Name", "IP" with a placeholder "192.168.88." and a small adjacent input box, and "MAC" with a placeholder "MAC". Below these fields is a blue "Save" button.

3. Set up a LAN
 - 1) Enter the IP address of the LAN.
 - 2) Enter the LAN Subnet Mask.
4. Finish.

5.1.2 IPv6

Function description:

On the IPv6 page, users can implement "DHCPv6 server", "SLACC server" and "NAT6" according to the needs of the site, and then follow the guidance step by step.

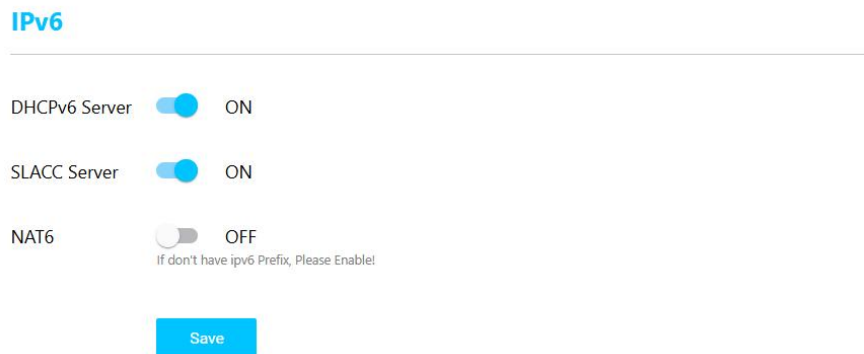
Action path

Select "Advanced settings --> network settings --> IPv6".

Interface description

The settings interface is as follows Figure 35 shown.

fig 35 IPv6 setup interface



5.1.3 VPN

Function description:

On the VPN page, configure the VPN.

Action path

Select "Advanced settings --> network settings -->VPN".

Interface description

The settings interface is as follows Figure 36 shown.

Procedure:

The following are the steps to set up a VPN.

1. Click "VPN Settings" for On.
2. Select Agreements.
3. Enter the VPN server address.
4. Enter the VPN username.
5. Enter the VPN password.
6. Enter MTU.

7. Select "Mode".

8. Determine if manual configuration is required.

- If you need to configure it manually, start the "Manually configure DNS" function to proceed to the steps9.

- If manual configuration is not required, go to the step10.

9. Enter the DNS 1 and DNS 2 addresses.

10. Finish.

fig 36 VPN settings interface

VPN ☒ ON

Protocol

L2TP

Server

server address!

Username

username

Password

password

MTU

MTU

Mode

Local

Manual DNS

☒

DNS 1

DNS1

DNS 2

DNS2

Save

5.1.4 IPsec

Function description:

On the IPsec page, implement the IPsec configuration.

Action path

Select Advanced settings --> network settings -->IPsec”.

Interface description

The settings interface is as follows Figure 37 shown.

Procedure:

The following steps are as follows:

1. Enable the IPsec Settings.
2. Enter Gateway Address, Pre-Shared Key, Local Subnet Range, Local ID, Pair Net Range, and Peer ID.
3. Select Encapsulation Mode, Auto Mode, IKE Version, IKE Lifetime, and Key Lifetime.
4. Enter Phase 1 Encryption Algorithm, Phase 1 Hash Algorithm, Phase 1 DH Group, Phase 2 Encryption Algorithm, Phase 2 Hash Algorithm, and Stage 2 DH Group.
5. Click Save.
6. Finish.

fig 37 IPsec settings

IPsec ON

Gateway	gw
pre shared key	
Local subnet	192.168.88.0/24
Local ID	
Remote subnet	192.168.2.0/24
Remote ID	
Tunnel type	tunnel
Auto mode	Add
IKE version	ikev2
IKE lifetime	10800
Key lifetime	3600
phase 1 encryption alg	AES128
phase 1 hash alg	SHA1
phase 1 dh group	modp768
phase 2 encryption alg	AES128
phase 2 hash alg	SHA1
phase 2 dh group	modp768

Save

5.1.5 Smart QoS

Function description:

On the Intelligent QoS Settings page, complete the configuration of intelligent flow control.

Action path

Select Advanced Settings -> Network Settings -> Smart QoS.

Interface description

The settings interface is as follows Figure 41 shown.

fig 41 Intelligent flow control interface

Smart QoS ☐ OFF

Upload Mbps

Download Mbps

Smart Mode

- ☒ Auto (Auto optimize network)
- ☐ Game (Improve gaming experience)
- ☐ Web (Accelerate internet surfing)
- ☐ Video (Smooth video/audio streaming)

Procedure:

The following steps are set for Smart QoS.

1. Turn on the "Intelligent Flow Control" function.
2. Enter Upload Bandwidth and Download Bandwidth.
3. Select Smart Mode
4. Click Save.

5. Finish.

5.1.6 Guest network

Function description:

On the Guest Network Settings page, complete the guest network configuration.

Action path

Select "Advanced settings -> network settings -> guest network".

Interface description

The settings interface is as follows Figure 42 shown.

fig 42 Guest web interface

Guest WiFi

Switch ☐ ON ☒ OFF

WiFi Name

Security

Hide

Procedure:

The following are the steps to set up a guest network.

1. If you need to turn on the Guest Network feature, select the Turn on key.
2. Enter a "wireless name".
3. Select "Encryption" and "Do Not Broadcast"
4. Click Save.

-
5. Finish.

5.1.7 DDNS

Function description:

On the DDNS Settings page, complete the DDNS configuration.

Action path

Select Advanced Settings --> Network Settings --> DDNS".

Interface description

The settings interface is as follows Figure 43 shown.

fig 43 DDNS Settings Interface

DDNS ☒ ON

Server

Domain Name

Username

Password

Procedure:

The following are the steps to set up DDNS.

1. Enable DDNS.
2. Select Service Type
3. Enter the Host Domain, Username, and Password.
4. Click Save.

-
5. Finish.

5.1.8 firewall

Function description:

On the Firewall Settings page, complete the firewall settings.

Action path

Select Advanced settings --> network settings -> firewalls.

Interface description

The settings interface is as follows Figure 45 shown.

fig 45 Firewall interface

The screenshot displays the Firewall Settings interface. At the top, there is a section titled "Port Forwarding" in blue. Below this, a "Rules List" table is shown with columns: Name, Protocol, Inner IP, Outer port, Inner port, and Action. Below the table is an "Add Rule" button. Further down, there is a section titled "DMZ(Demilitarized Zone)" in blue, followed by a toggle switch currently set to "OFF". Below the toggle is an empty text input field. At the bottom of the form is a blue "Save" button.

Name	Protocol	Inner IP	Outer port	Inner port	Action
------	----------	----------	------------	------------	--------

Add Rule

DMZ(Demilitarized Zone) ☐ OFF

Save

Procedure:

The following steps are performed to set up a firewall.

1. Set up Port Forwarding.

-
2. Click Add rule to enter the following Figure 46 shown.
 3. Enter a Rule Name.
 4. Select Network Protocol.
 5. Enter the Internal Host IP Value.
 6. Click Add.
 7. Choose whether to turn on non-military features.
 - If on, click "On" to enter the steps 8.
 - If it doesn't turn on, go to the step 8.
 8. Click Save.
 9. Finish.

fig 46 Create a new rule

The screenshot shows a dialog box titled "Add Rule" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- A text input field labeled "Name" with a cursor inside.
- A dropdown menu showing "TCP".
- A text input field containing "1-65535".
- A label "Internal IP:" followed by a text input field containing "192.168.88." and another text input field containing "1-65535".
- A blue button labeled "Save" at the bottom.

5.1.9 parental controls

Function description:

On the Parental Control Settings page, complete the parental control settings.

Action path

Select Advanced settings -> network settings -> parental controls.

Interface description

The settings interface is as follows Figure 47 shown.

fig 47 Parental controls - set a period of time when you can't go online

Parental Control - Block the internet time

Rules List

Name	MAC address	Start Time	Internet END time	Repeat	Operating
------	-------------	------------	-------------------	--------	-----------

Add rule

Procedure:

Parental Control - Set the time period to prohibit Internet access The following steps are set.

1. Click Add rule to enter the following Figure 48 shown.
2. Enter the Start Time and End Time.
3. Select Date.
4. Click Add.
5. Click Save.
6. Finish.

fig 48 Added parental control rules

New rules

×

Device name

Fiona

Device address

106838581DE2

Start time (HH:MM:SS)

(HH:MM:SS)

End time (HH:MM:SS)

(HH:MM:SS)

Date

☒ Monday

☐ Tuesday

☐ Wednesday

☐ Thursday

☐ Friday

☐ Saturday

☐ Sunday

Add

5.1.10 Remote WEB access

Function description:

On the Remote WEB Access Settings page, complete the remote WEB access enabled.

Action path

Select Advanced Settings -> Network Settings -> Remote WEB Access.

Interface description

The settings interface is as follows Figure 44 shown.

fig 44 Remote WEB access to the settings interface

Remotw web access

Remote Web Enable ☐

Remote Debug Enable ☐

Save

Procedure:

The following are the steps for setting up remote web access.

1. Enable the "Remote WEB Access" function.
2. Enable the "Remote Debugging On" function.
3. Click Save.
4. Finish.

5.1.11 MAC address cloning

Function description:

On the MAC Address Cloning Settings page, complete the MAC address cloning settings.

Action path

Select "Advanced settings -> network settings ->MAC address cloning".

Interface description

The settings interface is as follows Figure 53 shown.

fig 53 MAC clone interface

MAC Clone

MAC Clone

☒ Router Local MAC (A4D8CA8F6F21)

☐ Online Client MAC (106838581DF7)

☐ Manual

Procedure:

The following are the steps to set up MAC address cloning.

1. Select MAC address clone "Use router's MAC address (A4D8CA8F6F21)" or "Use client's MAC address (106838581DF7)" or enter it manually.
2. If you enter it manually, enter the MAC address in the edit box.
3. Click Save.
4. Finish.

5.1.12 WOL

Function description:

On the Domain Name Access Control Settings page, complete the domain name access control settings.

Action path

Select Advanced settings --> network -> WOL.

Interface description

The settings interface is as follows Figure 51 shown.

fig 51 WOL interface

Wake ON LAN

ON

Broadcast

Name	Mac Address	Password	Action
------	-------------	----------	--------

Add

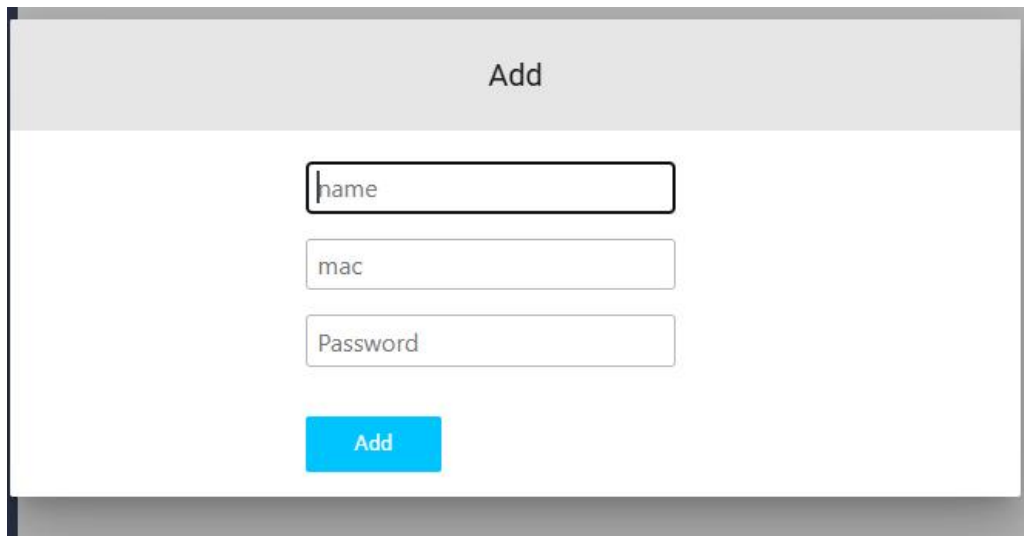
Save

Procedure:

The following are the steps to set up domain name access control.

1. Select Domain Name Access Control as Domain Name Blacklist Mode or Domain Name Whitelist Mode.
2. Click "Add" to enter as shown.
3. Enter the Domain Name and Domain Address.
4. Click Add.
5. Click Save.
6. Finish.

fig 52 WOL interface



The image shows a web interface for adding a new entry to the Wireless ACL. It features a light gray header with the word "Add" in the center. Below the header, there are three text input fields stacked vertically, labeled "name", "mac", and "Password". At the bottom of the form is a blue button with the text "Add" in white.

5.2 Security

5.2.1 Wireless ACL

Function description:

On the Wireless ACL Settings page, complete the wireless access settings for Blacklist of Wireless Devices and Whitelist of Wireless Devices.

Action path

Select Advanced Settings → Security Center → Wireless ACL.

Interface description

The settings interface is as follows Figure 55 shown.

fig 55 Wireless ACL interface

Wireless ACL ☒ ON

☒ **Black mode** (Deny device in device list)
☐ **White mode** (Only allow device in device list)

Name	MAC Addr	Action
No devices		

Add

Save

Procedure:

The procedure for selecting Wireless ACL is as follows.

1. Turn on the "Wireless Device Blacklist" and "Wireless Device Whitelist" functions.
2. Click "Add by Manual" to enter the Figure 56 shown.
3. Enter the Device Name.
4. Enter the MAC address.
5. Click Add.
6. Click Save.
7. Finish.

fig 56 Add by hand

Manual Add ×

Add

5.2.2 Passwords

Function description:

On the Manage Password Settings page, complete the settings for managing passwords.

Action path

Select Advanced Settings --> Security Center -> Manage Passwords.

Interface description

The settings interface is as follows Figure 57 shown.

Procedure:

The following are the steps to manage passwords.

1. Enter your new password.
2. Enter the new password again.
3. Click Save.
4. Finish.

fig 57 Manage password interface

Modify Password

New Password

Confirm Password

Save

5.3 SYSTEM

5.3.1 System status

Function description:

On the System Status Settings page, complete the settings for managing passwords.

Action path

Select Advanced Settings --> System Management -> System Status.

Interface description

The settings interface is as follows Figure 58 shown.

Procedure:

The operation steps of the working mode are as follows.

1. Select the working mode, Routing Mode or Bridge Mode.

Illustrate:

If the device selects bridge mode, you need to press and hold the Reset key on the device for 5 seconds to return to routing mode.

2. Click Save.
3. Finish.

The following are the steps for system language operations.

1. Select the system language.

Illustrate:

Currently, the system only supports Chinese and English languages.

2. Click Save.
3. Finish.

fig 58 System status interface

Working Mode

☒ Router

☐ Bridge

Save

System Language

English ▼

Save

Restore Setting

Restore

Restart System

Restart

5.3.2 Time zone

Function description:

On the System Status Settings page, complete the settings for managing passwords.

Action path

Select Advanced settings --> system management --> system time zone.

Interface description

The settings interface is as follows Figure 59 shown.

fig 59 System time zone interface

Time zone

Current time Mon Nov 4 16:52:34 2024

Time zone

Save

Procedure:

The operation steps of the working mode are as follows.

1. Select Time Zone.
2. Click Save.
3. Finish.

5.3.3 Diagnosis

Function description:

On the System Diagnostics Settings page, complete the system diagnostics detection.

Action path

Select Advanced Settings --> System Management -> System Diagnostics.

Interface description

The settings interface is as follows Figure 60 shown.

fig 60 System diagnostics

System diagnosis

☒ PING communication detection

☐ Traceroute detection

IP/Domain

Please enter the domain name c

PING times

4

PING packet size

64

Start

Procedure:

The following are the steps for system diagnosis.

1. Select the system diagnostic method PING Communication Detection or Route Trace Detection.
2. Enter the Destination IP/Domain Name.
3. Enter the Number of Pings.
4. Enter the PING packet size.
5. Click Start.
6. Finish.

5.3.4 Backup

Function description:

On the System Backup Settings page, complete the system backup and recovery.

Action path

Select Advanced Settings --> System Management -> System Backup.

Interface description

The settings interface is as follows Figure 61 shown.

fig 61 System backup

System Backup

Download backup file

System backup and recovery

Select File

select file

Upload

Procedure:

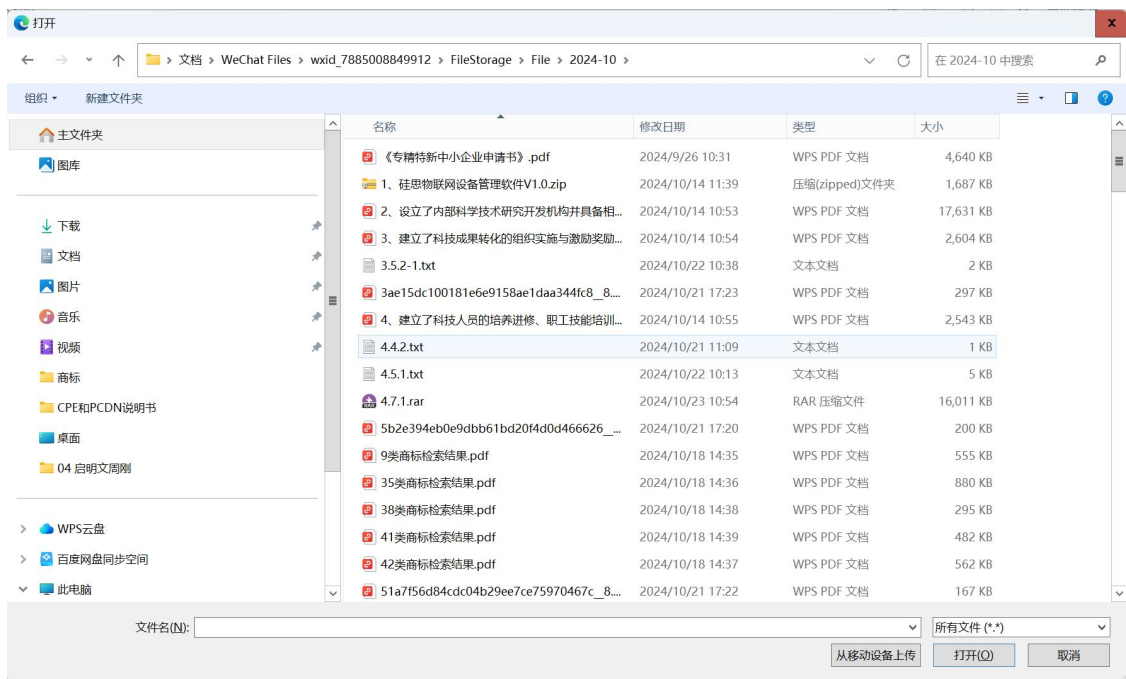
The following are the steps for system backup.

1. Click "Download Backup File".
2. The backed up files are automatically saved to the normal download path of your computer.
3. Finish.

The following steps are as follows:

1. Click Select File to proceed Figure 62 shown.

fig 62 File path



2. Select the file to upload.
3. Click Upload.
4. Finish.

5.3.5 Schedule Restarts

Function description:

On the Scheduled Restart Settings page, complete the scheduled restart settings.

Action path

Select "Advanced Settings --> System Management -> Scheduled Restart".

Interface description

The settings interface is as follows Figure 63 shown.

fig 63 Restart regularly

Scheduled Restart Time

☐ off

Week

- ☐ Monday
- ☐ Tuesday
- ☐ Wednesday
- ☐ Thursday
- ☐ Friday
- ☐ Saturday
- ☐ Sunday

Please select at least one

Restart time

00 : 00

Save

Procedure:

The procedure for scheduled restart is as follows.

1. Turn on the "Scheduled Restart" function.
2. Select a restart date, you can select multiple times.
3. Scheduled restart time.
4. Click Save.
5. Finish.

5.3.6 System upgrades

Function description:

On the System Upgrade Settings page, complete the system upgrade.

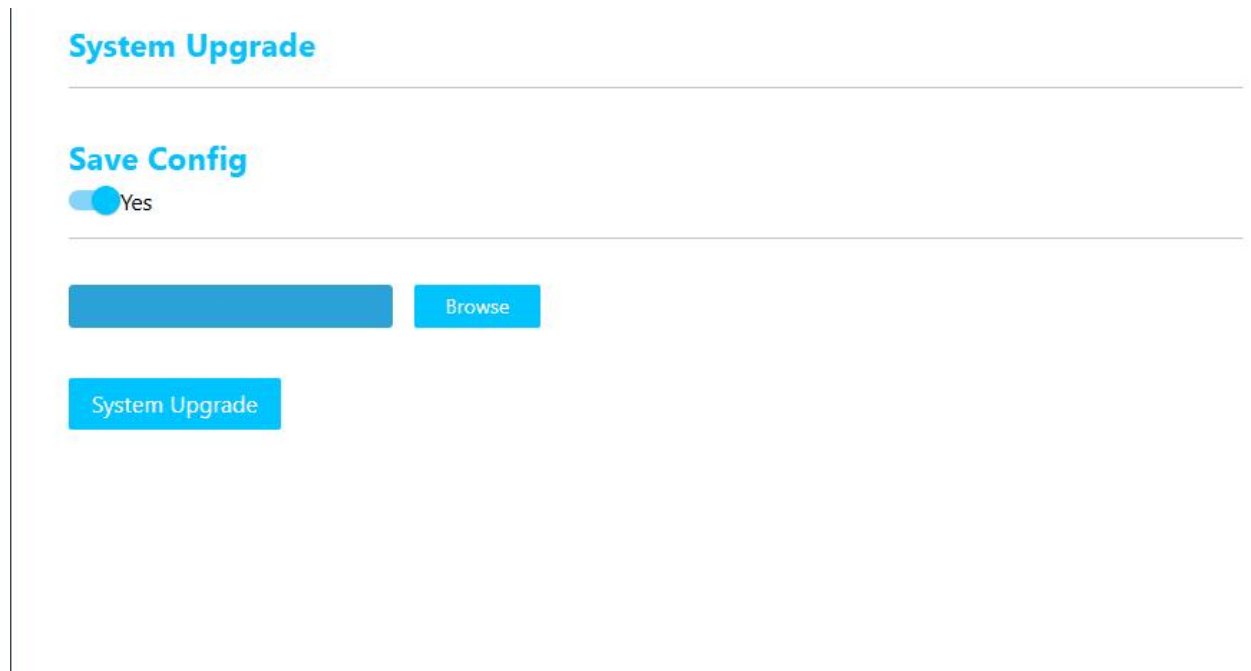
Action path

Select "Advanced Settings --> System Management -> System Upgrades".

Interface description

The settings interface is as follows Figure 64 shown.

fig 64 System upgrades



Procedure:

The following are the steps for system update.

1. Click "Browse" to enter the file browsing page.
2. Choose the latest software that needs to be updated.
3. Click Start Update.
4. Finish.

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.