Wireless Router

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and loGo to s are the properties of Hikvision in various jurisdictions.
- Other trademarks and loGo to s mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE

OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Applicable Models

This manual is applicable to wireless router.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
ℹ Note	Provides additional information to emphasize or supplement important points of the main text.
⚠ Caution	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
⚠ Danger	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

TABLE OF CONTENTS

Chapter 1 First-Time Use

Activation is required before you use the router (hereafter referred to as device) for the first time. After activation, the router can be configured via Web.

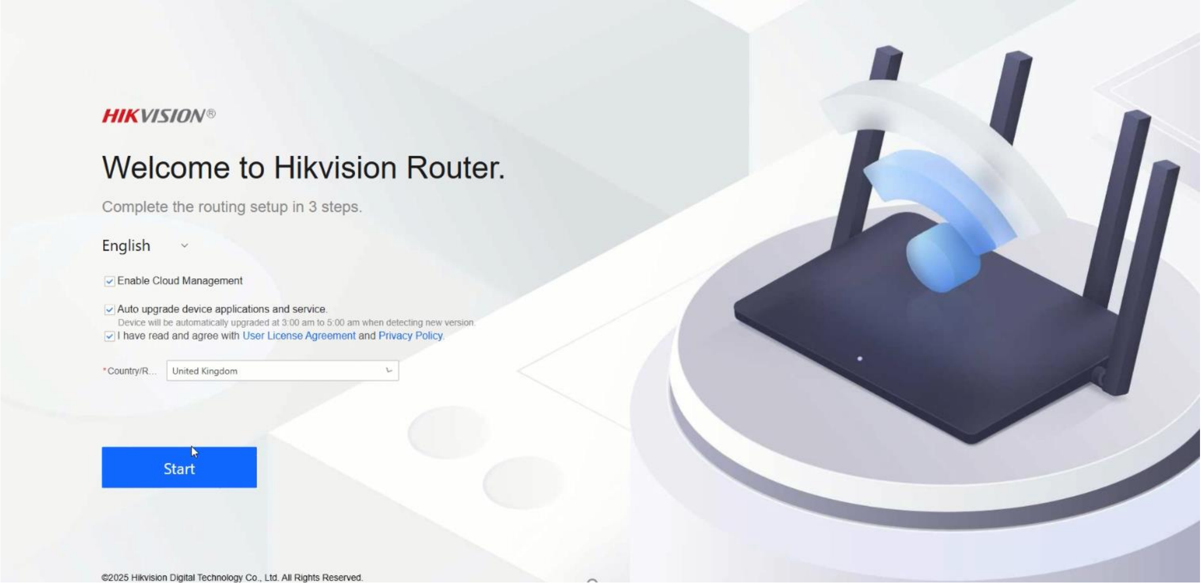
1.1 Activation

The device can be activated via a mobile device or PC. Make sure the device is connected to network and power supply before being activated.

Step 1 Connect your phone or PC to the wireless router.

- Wireless Mode: Connect any LAN port of the device to the network port of the PC directly with an Ethernet cable.
- Wired Mode: Check the label at the router to get Wi-Fi Name (HIKVISION_XXXX) and connect your phone or PC to the Wi-Fi.

Step 2 Enter IP address (https://192.168.9.1) or the login address (https://hikrouter.net) in the browser address bar to go to the activation page.



Welcome to Hikvision Router.

Complete the routing setup in 3 steps.

English

☑ Enable Cloud Management

☑ Auto upgrade device applications and service.
Device will be automatically upgraded at 3:00 am to 5:00 am when detecting new version.

☑ I have read and agree with User License Agreement and Privacy Policy.

*Country/R... United Kingdom

©2025 Hikvision Digital Technology Co., Ltd. All Rights Reserved.

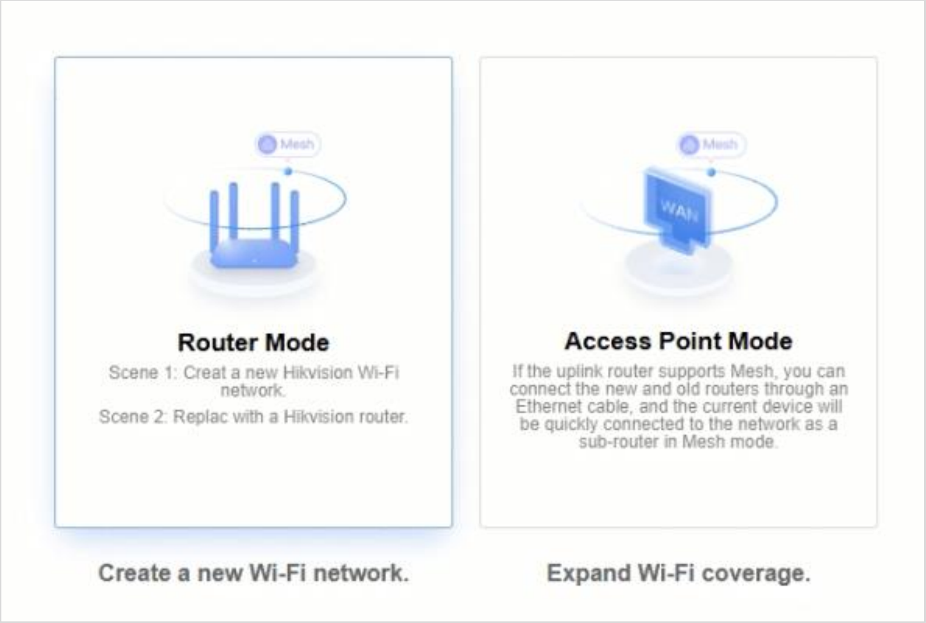
Figure 1-1 Activation Page

Step 3 Select your **Country/Region** and click **Start**.

1.2 Setup Wizard

1.2.1 Create New Wi-Fi

Step 1 Select the **Operation Mode** as **Router Mode**.



Router Mode

Scene 1: Creat a new Hikvision Wi-Fi network.

Scene 2: Replac with a Hikvision router.

Access Point Mode

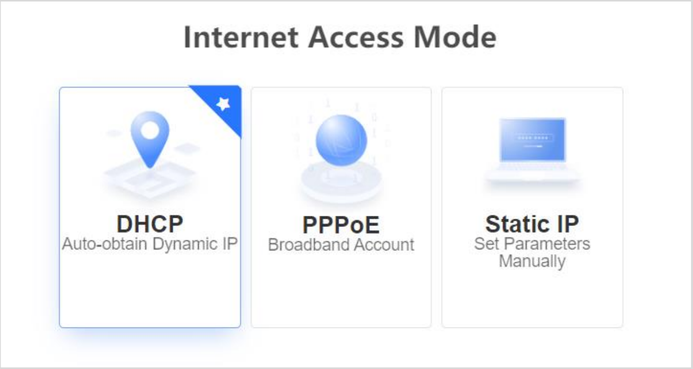
If the uplink router supports Mesh, you can connect the new and old routers through an Ethernet cable, and the current device will be quickly connected to the network as a sub-router in Mesh mode.

Create a new Wi-Fi network.

Expand Wi-Fi coverage.

Figure 1-2 Select Operation Mode

Step 2 The system will detect the **Internet Access Mode** automatically, or you can select it manually.



Internet Access Mode

DHCP
Auto-obtain Dynamic IP

PPPoE
Broadband Account

Static IP
Set Parameters Manually

Figure 1-3 Internet Access Mode

- **DHCP**: It is recommended to select this mode. Dynamic IP address will be allocated automatically. No additional configuration is required.
- **PPPoE**: You can select this mode if your Internet Service Provider (ISP) has provided a broadband account and password, or if you are going to use a new router to replace the old one.
- **Static IP Address**: It is not recommended to select this mode, unless your ISP has provided a static IP address and other information.

Step 3 (Optional) Replace the old router with a new one: If you have an old router that can access the Internet normally, you can migrate data under PPPoE mode by connecting the new and old routers.

1) Select **PPPoE** mode.
2) Click **Auto-Obtain**.

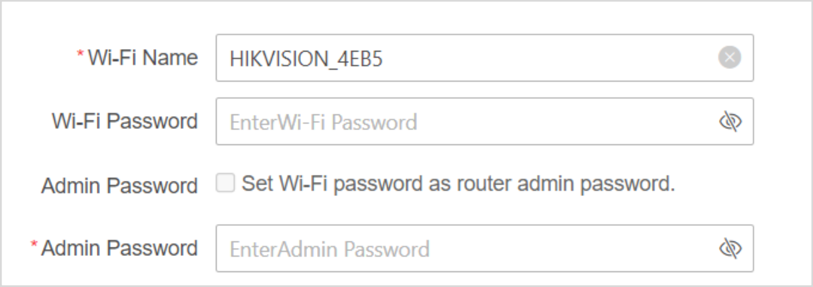
3) Connect the new and old routers to the power cable.
4) Connect the WAN port of the old router to any LAN port of the new router with an Ethernet cable.
5) Click **Obtain** to get the broadband account and password from the old router.

Step 4 (Optional) Support quick **Enable VPN** or **Enable VLAN**. More information refers to ***4.3.8 VPN*** and ***4.3.9 VLAN***.

Note

The function is only available for some models. The actual interface prevails.

Step 5 Click **Next** to configure Route Settings.



*Wi-Fi Name: HIKVISION_4EB5

Wi-Fi Password: EnterWi-Fi Password

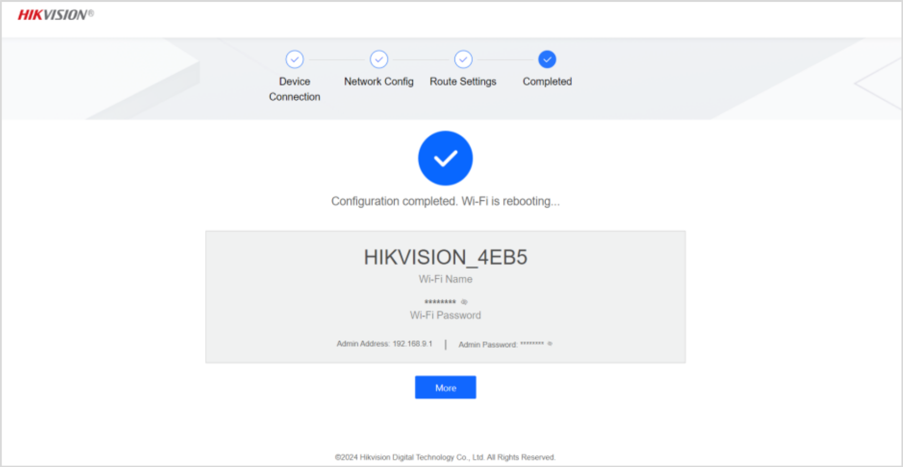
Admin Password: □ Set Wi-Fi password as router admin password.

*Admin Password: EnterAdmin Password

Figure 1-4 Wi-Fi Settings

- **Wi-Fi name**: The name on the label by default. Editing is supported.
- **Wi-Fi password**: The password to be entered when a terminal device connecting to router Wi-Fi. Custom 8 to 16 characters is supported.
- **Admin Password**: The password to be entered when logging in Web management page to configure the router. Custom 8 to 16 characters is supported.
- **Country/Region**: Select your location.

Step 6 Click **Next**. The router will reboot automatically after being activated.



Configuration completed. Wi-Fi is rebooting...

HIKVISION_4EB5
Wi-Fi Name

****
Wi-Fi Password

Admin Address: 192.168.9.1 | Admin Password: ********

©2024 Hikvision Digital Technology Co., Ltd. All Rights Reserved.

Figure 1-5 Figure 1-6 Configured

Note

It is recommended to save the password page.

1.2.2 Extend Wi-Fi Range

Mesh networking can quickly activate a **sub router** and extend the Wi-Fi range of **main router**.

Before You Start

- Ensure that both routers support Mesh and the function is enabled.
- If your device does not support Mesh, you can extend Wi-Fi by **Wireless Extender Mode** or **Access Point Mode** (refer to ***4.2.1 Basic Settings***).
- Ensure that the **main router** can access the Internet normally.
- Ensure that the **sub router** is inactivated (long press the WPS button for 8s to restore if it has been activated).

Steps

Step 1 Power on the **sub router** and place it near the **main router**. The indicator on the **sub router** is solid red.

Step 2 Press the WPS buttons on both the **main router** and the **sub router** for 1-3 seconds. Wait until the indicator on the **sub router** is solid blue.

Step 3 Disconnect the power supply on the **sub router**, and place it in the location where Wi-Fi coverage needs to be expanded.

Step 4 Reconnect the **sub router** to the power supply. Wait until the indicator on the **sub router** is solid blue again.

Note

- The Wi-Fi name and password of the **main router** and the **sub router** are the same.
- If step 2 is failed, try to connect a LAN port of the **main router** and the WAN port of the **sub router** by an Ethernet cable, and repeat the next steps after the indicator on the **sub router** is solid blue.
- WPS buttons vary with different models. Please refer to the Quick Start Guide.

1.3 Login

After the device is activated, the Wi-Fi password is updated and you need to reconnect to log in.

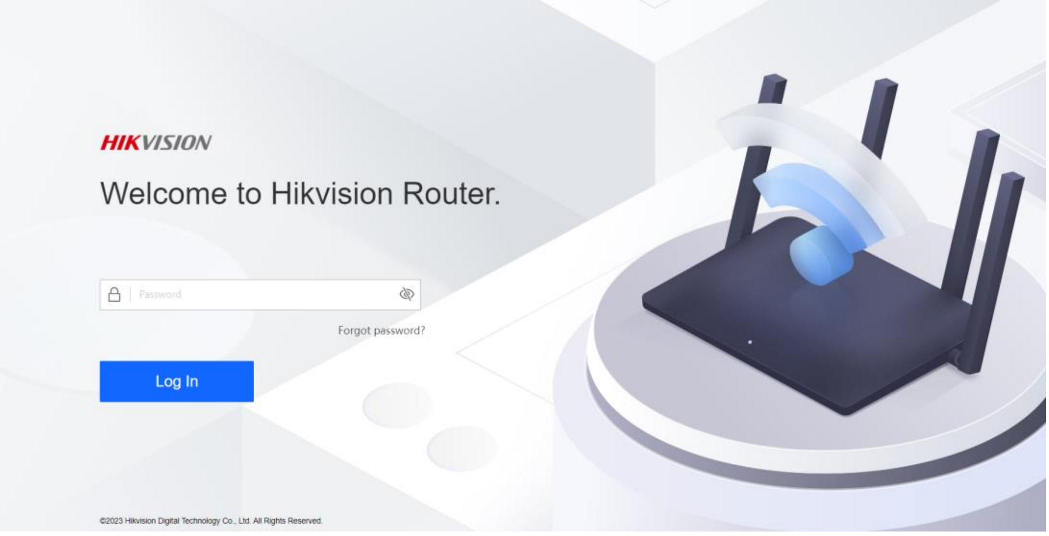
Step 1 Connect to the device again using the Wi-Fi password set during activation.

Note

If Wi-Fi name is changed during activation, please select the Wi-Fi network again.

Step 2 Refresh the activation page or enter management IP address (192.168.9.1) in the address bar, and go to login page.

Step 3 Enter router admin password and click **Log In**.



HIKVISION

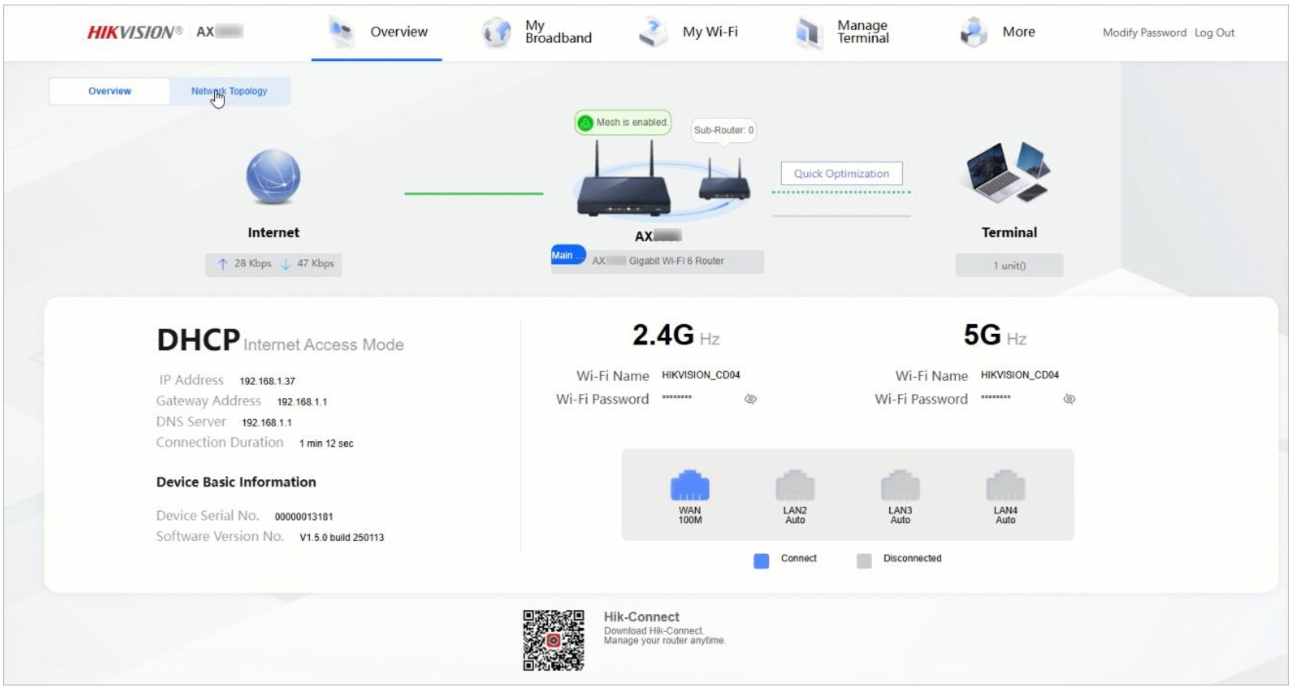
Welcome to Hikvision Router.

Password
Forgot password?
Log In
©2023 Hikvision Digital Technology Co., Ltd. All Rights Reserved.

Figure 1-6 Login

Chapter 2 Overview

After logging in to the device, you can go to the overview page to check network connection status, number of terminals, and Wi-Fi information.



DHCP Internet Access Mode

IP Address 192.168.1.37

Gateway Address 192.168.1.1

DNS Server 192.168.1.1

Connection Duration 1 min 12 sec

Device Basic Information

Device Serial No. 00000013181

Software Version No. V1.5.0 build 250113

2.4G Hz

Wi-Fi Name HIKVISION_CD04

Wi-Fi Password ********

5G Hz

Wi-Fi Name HIKVISION_CD04

Wi-Fi Password ********

Figure 2-1 Overview

2.1.2 Network Topology

Click Network Topology to check networking information.

Support editing name, rebooting, restoring, and managing the routers in the topology quickly.

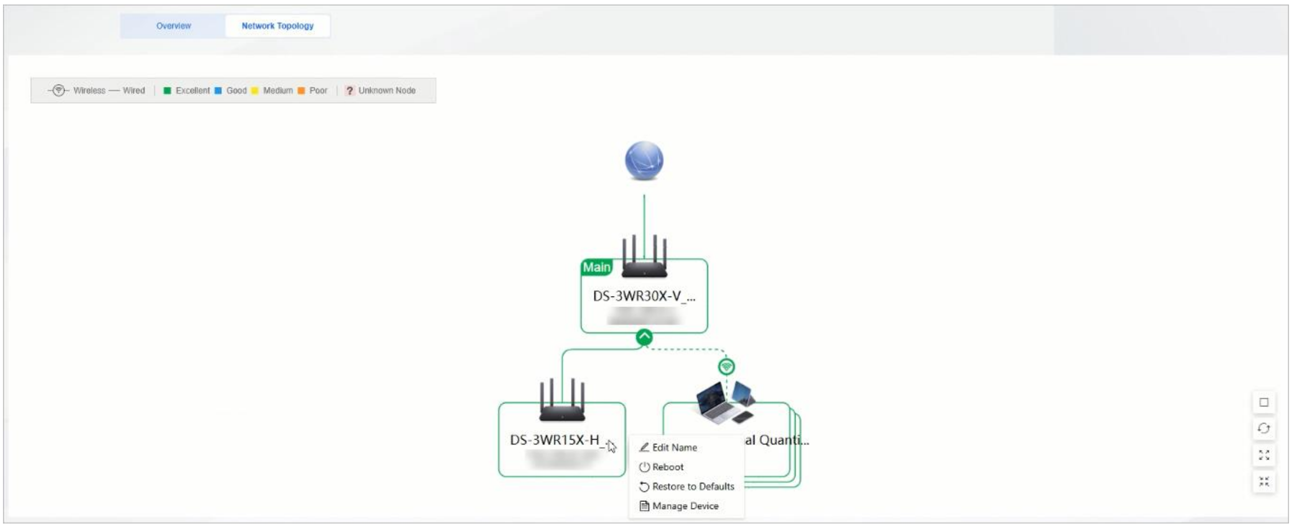


Figure 2-2 Check Network Topology

2.1.3 Quick Diagnosis

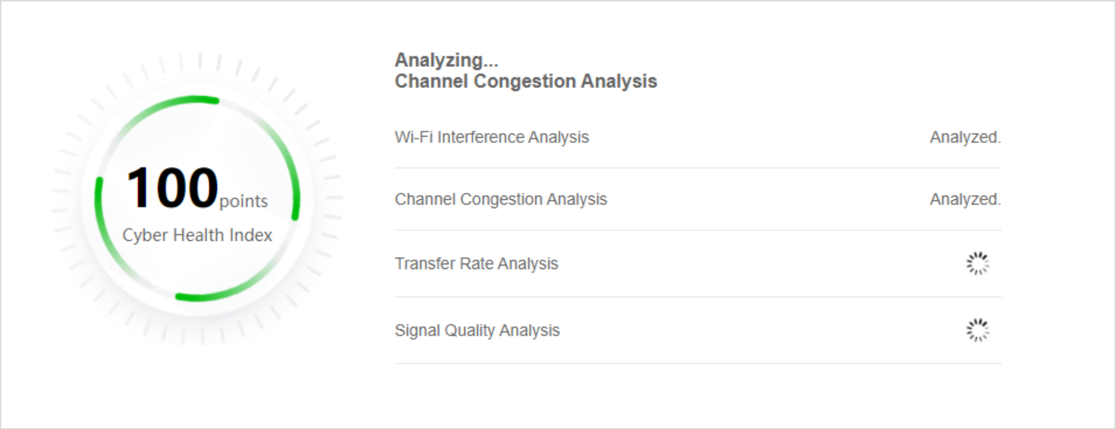
If the device network connection is abnormal, you can use **Quick Diagnosis** to diagnose the problem. Take corresponding measures according to the diagnosis results below.

- No Ethernet cable inserted: Please check if the Ethernet cable is connected to the router's WAN port.
- Network disconnected: Check if broadband configuration is correct, if uplink Wi-Fi is connected to the network, and if uplink route bridged is connected to the network.
- Relaying failed: Please check relay Wi-Fi password.
- Dial-up disconnected: Check if the physical link of router is normal.
- Incorrect user name or password: Check if broadband configuration or password is correct.
- Dialing timed out: Check if the broadband dial-up server is running normally.
- IP conflict: The IP address obtained by WAN port is in the same network segment as the LAN port. Please edit LAN port IP address in LAN configuration.

2.1.4 Quick Optimization

Go to **More→Wi-Fi Settings→Quick Optimization**.

The system can analyze the external Wi-Fi interference and link congestion of the current working channel. If the health index is lower than 100, you can optimize the current network to the optimal status through **Quick Optimization**.



Analyzing...
Channel Congestion Analysis

Wi-Fi Interference Analysis	Analyzed.
Channel Congestion Analysis	Analyzed.
Transfer Rate Analysis	
Signal Quality Analysis	

Figure 2-3 Quick Optimization

2.1.5 Check Port Status

Check port status on the right side of Overview page.

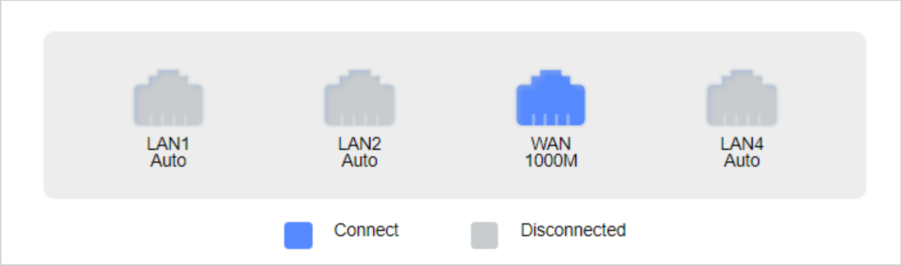


Figure 2-4 Port Status

2.1.6 Download Hik-Connect

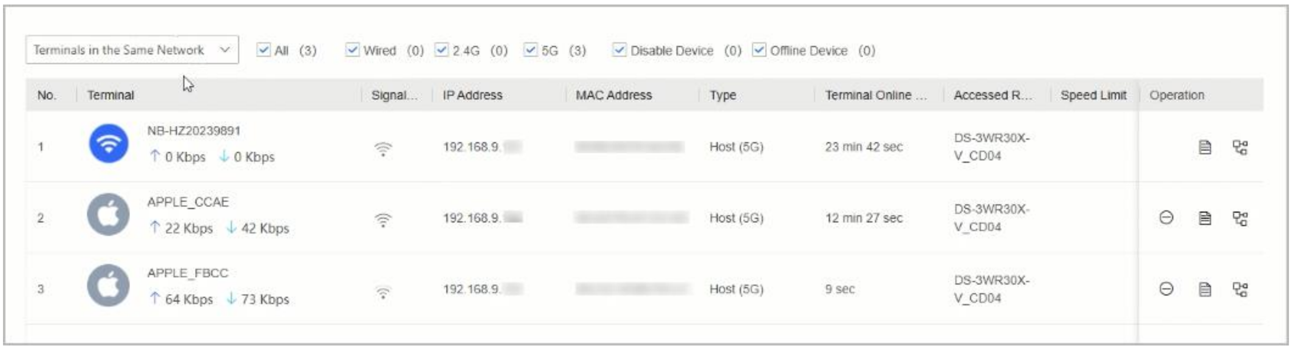
Scan the QR code at the bottle of the interface to download Hik-Connect application to manage router devices.

Chapter 3 Terminal Management

Parents can add terminals connected to router's Wi-Fi to the list, so that family members (especially minors) can develop correct online habits.

3.1 Check Terminal Information

Click **Terminal** on the home page to view and manage online, offline, and disabled terminals.



Terminals in the Same Network ∨ ☑ All (3) ☑ Wired (0) ☑ 2.4G (0) ☑ 5G (3) ☑ Disable Device (0) ☑ Offline Device (0)

No.	Terminal	Signal...	IP Address	MAC Address	Type	Terminal Online ...	Accessed R...	Speed Limit	Operation
1	NB-HZ20239891 ↑ 0 Kbps ↓ 0 Kbps		192.168.9.[redacted]	[redacted]	Host (5G)	23 min 42 sec	DS-3WR30X-V_CD04		
2	APPLE_CCAE ↑ 22 Kbps ↓ 42 Kbps		192.168.9.[redacted]	[redacted]	Host (5G)	12 min 27 sec	DS-3WR30X-V_CD04		⊖
3	APPLE_FBCC ↑ 64 Kbps ↓ 73 Kbps		192.168.9.[redacted]	[redacted]	Host (5G)	9 sec	DS-3WR30X-V_CD04		⊖

Figure 3-1 Terminal List

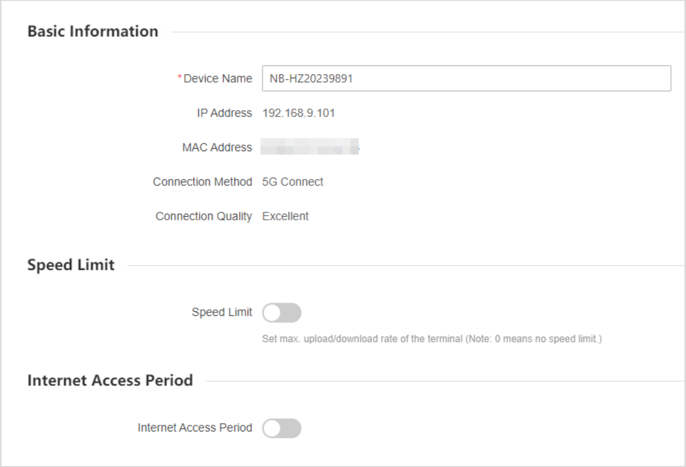
3.2 Restrict Internet Access

Click ⊖ to restrict the current terminal.

Optional: To remove the network connection limit of the terminal, check **Offline & Disabled** and click ⊖ .

3.3 Limit Terminal Network

Click to 🗎 view current terminal details and configure terminal connection status.



Basic Information

*Device Name	NB-HZ20239891
IP Address	192.168.9.101
MAC Address	[redacted]
Connection Method	5G Connect
Connection Quality	Excellent

Speed Limit

Speed Limit ○

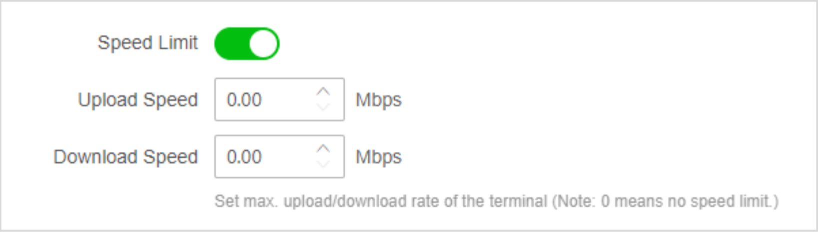
Set max. upload/download rate of the terminal (Note: 0 means no speed limit.)

Internet Access Period

Internet Access Period ○

Figure 3-2 Terminal Details

- **Speed Limit**: The network speed of the current terminal can be limited.



Speed Limit

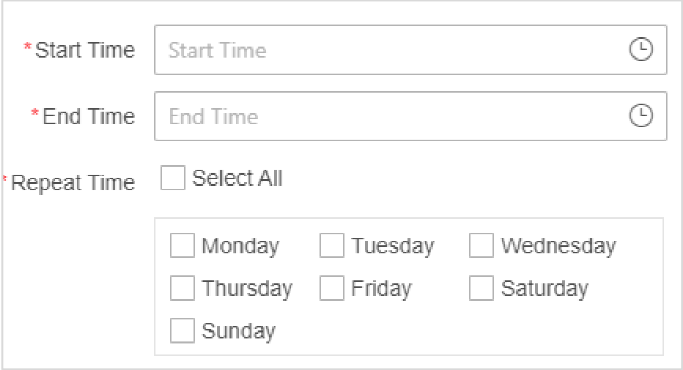
Upload Speed 0.00 Mbps

Download Speed 0.00 Mbps

Set max. upload/download rate of the terminal (Note: 0 means no speed limit.)

Figure 3-3 Limit Speed

- **Internet Access Period**: The time period during which the current terminal can connect to the network. Out of the set time period, the terminal can connect to Wi-Fi, but the network cannot be connected. Up to 3 items can be set.



*Start Time: Start Time

*End Time: End Time

*Repeat Time: □ Select All

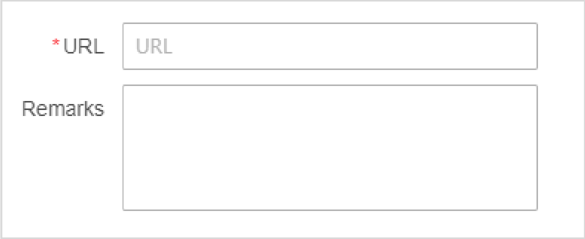
□ Monday □ Tuesday □ Wednesday

□ Thursday □ Friday □ Saturday

□ Sunday

Figure 3-4 Set Internet Time Period

- **Filter URL**: Set a domain name that is prohibited from accessing the current terminal. Up to 16 items can be set.



*URL: URL

Remarks

Figure 3-5 Add URL

Chapter 4 Internet Settings

4.1 Wi-Fi Settings

Set Wi-Fi parameters and functions, such as timed switch, quick optimization, and guest network.

4.1.1 Basic Settings

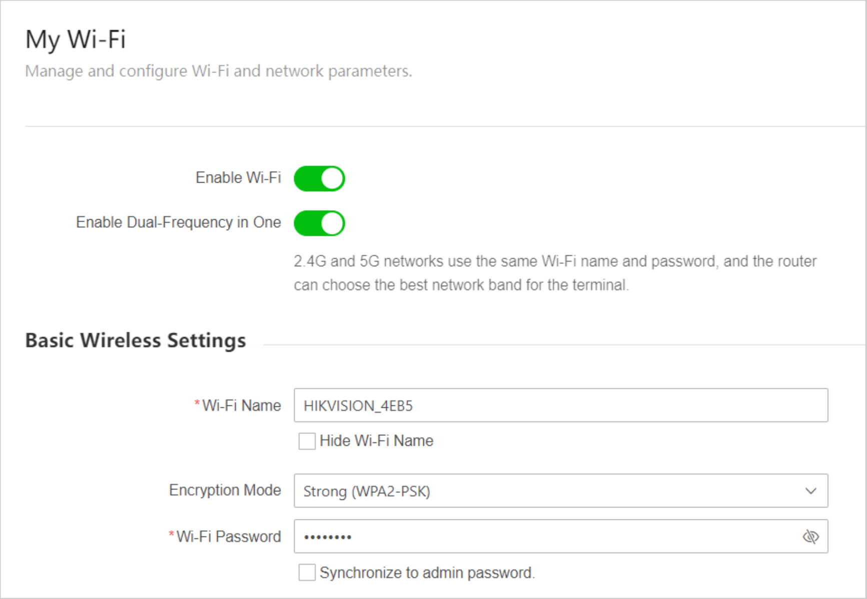
Step 1 Click **My Wi-Fi**.

Step 2 Make sure Wi-Fi is enabled.

Step 3 Configure the parameters.

Table 4-1 Basic Parameter Description

Parameter	Description
Enable Wi-Fi	Enable or disable the Wi-Fi network.
Enable Dual-Frequency in One	● Enable: 2.4 G or 5 G networks are recommended automatically according to signal strength and distance. ● Disable: 2.4 G and 5 G networks can be set separately.
Enable Network	When **Dual-Frequency in One** is disabled, you can choose to enable 2.4 G and 5 G networks separately.
Wi-Fi Name	Set the device Wi-Fi name for other terminals to search.
Hide Wi-Fi Name	If selected, this Wi-Fi cannot be searched by terminals. You need to enter Wi-Fi name manually for connection. This feature can enhance network security.
Encryption Mode	It supports **Hybrid Strong**, **Hybrid**, **Strong**, and **None** (Allow all connections). **Note** Make sure the access terminal is supported when using **Hybrid Strong**. If the connection problem persists, please switch to **Hybrid** or other methods.
Wi-Fi Password	8 to 63 characters are allowed, including digits, uppercase letters, lowercase letters, or special characters.
Synchronize to Admin Password	Set the **Wi-Fi Password** as the **Admin Password**.



My Wi-Fi

Manage and configure Wi-Fi and network parameters.

Enable Wi-Fi

Enable Dual-Frequency in One

2.4G and 5G networks use the same Wi-Fi name and password, and the router can choose the best network band for the terminal.

Basic Wireless Settings

*Wi-Fi Name: HIKVISION_4EB5

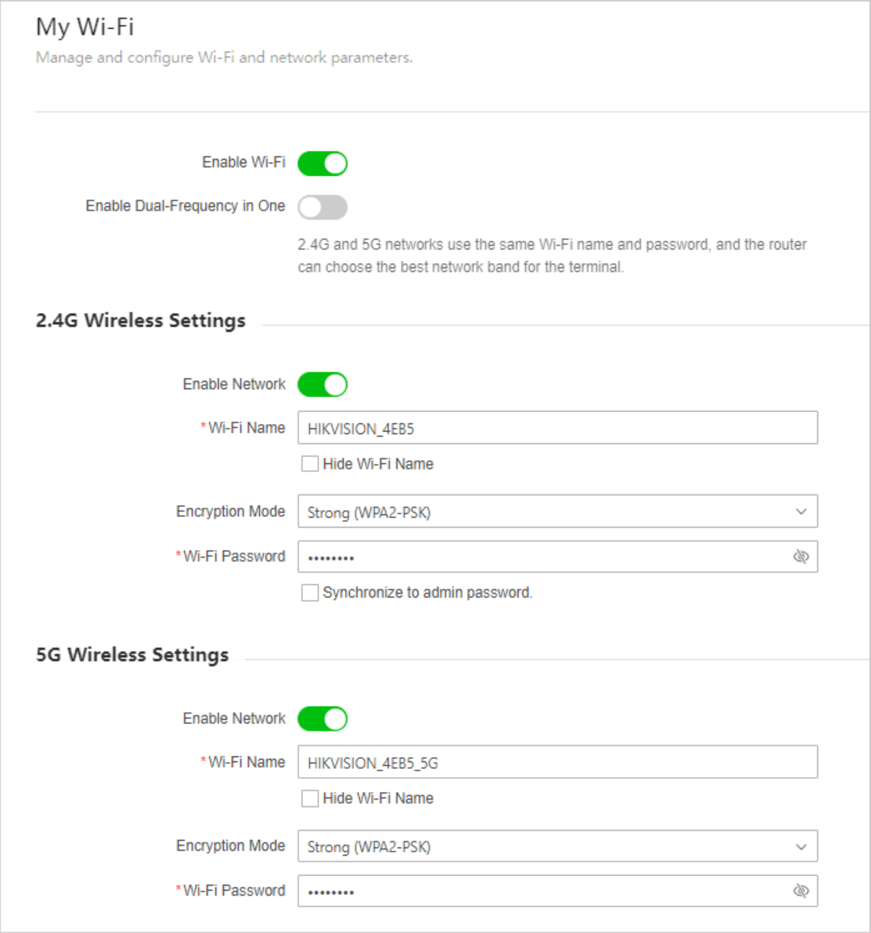
□ Hide Wi-Fi Name

Encryption Mode: Strong (WPA2-PSK)

*Wi-Fi Password: ••••••••

□ Synchronize to admin password.

Figure 4-1 Enable Dual-Frequency in One



My Wi-Fi

Manage and configure Wi-Fi and network parameters.

Enable Wi-Fi

Enable Dual-Frequency in One

2.4G and 5G networks use the same Wi-Fi name and password, and the router can choose the best network band for the terminal.

2.4G Wireless Settings

Enable Network

*Wi-Fi Name: HIKVISION_4EB5

□ Hide Wi-Fi Name

Encryption Mode: Strong (WPA2-PSK)

*Wi-Fi Password: ••••••••

□ Synchronize to admin password.

5G Wireless Settings

Enable Network

*Wi-Fi Name: HIKVISION_4EB5_5G

□ Hide Wi-Fi Name

Encryption Mode: Strong (WPA2-PSK)

*Wi-Fi Password: ••••••••

Figure 4-2 Disable Dual-Frequency in One

Step 4 Click **Save**.

4.1.2 Advanced Settings

Step 1 Go to **More→Wi-Fi Settings→Advanced Wi-Fi Settings**.

Note

The function varies with models. The actual interface prevails.

Step 2 Configure the parameters.

Table 4-2 Advanced Parameter Description

Parameter		Description
2.4/5 G Wireless Settings	Wireless Channel	Wireless signal is used as a data channel of transmission medium. If **Auto** is selected, the router will select an optimal channel according to the surrounding environment.
	Wireless Mode	Set the wireless working mode. The default selection is recommended.
	Channel Width	Set the channel width occupied for wireless data transmission.
Wireless Advanced Settings	TWT	After **TWT** is enabled, resource scheduling between devices will be optimized automatically, so as to reduce random competition, increase device sleeping time, and reduce power consumption.
	MU-MIMO	After **MU-MIMO** is enabled, you can communicate with multiple terminals to improve the online experience.
	OFDMA	After **OFDMA** is enabled, multi-user reuse channel resources, which will improve transmission efficiency in multi-user environment and reduce network delay.
Wi-Fi Signal Strength		The enhanced wireless signal is suitable for covering large area or partitions.

Step 3 Click **Save**.

4.1.3 Scheduled Wi-Fi On/Off

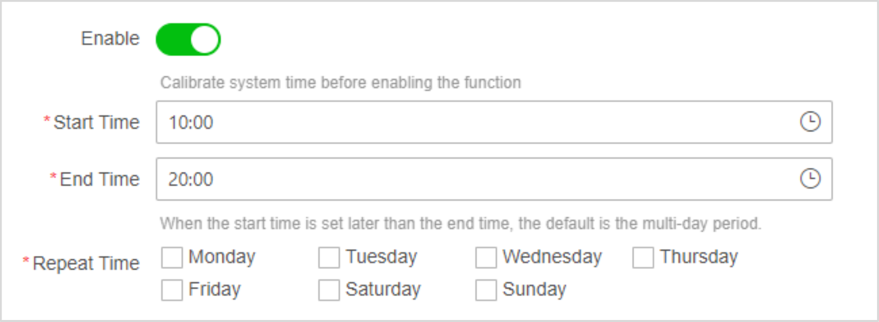
Set a period during when the Wi-Fi will be disabled automatically.

Step 1 Go to **More→Wi-Fi Settings→Scheduled Wi-Fi On/Off**.

Step 2 Check **Enable**.

Step 3 Select **Start Time** and **End Time**.

Step 4 Select **Repeat Time** (Monday to Sunday).



Enable

Calibrate system time before enabling the function

*Start Time 10:00

*End Time 20:00

When the start time is set later than the end time, the default is the multi-day period.

*Repeat Time □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday

Figure 4-3 Timed Wi-Fi

Step 5 Click **Save**.

Note

Before enabling this function, check if the router system time is correct.

4.1.4 Guest Network

Set a Wi-Fi network for guests, which can guarantee host network data and information security, and also meet the network needs of guests.

Step 1 Go to **More**→**Wi-Fi Settings**→**Guest Network**.

Step 2 Check **Enable**.

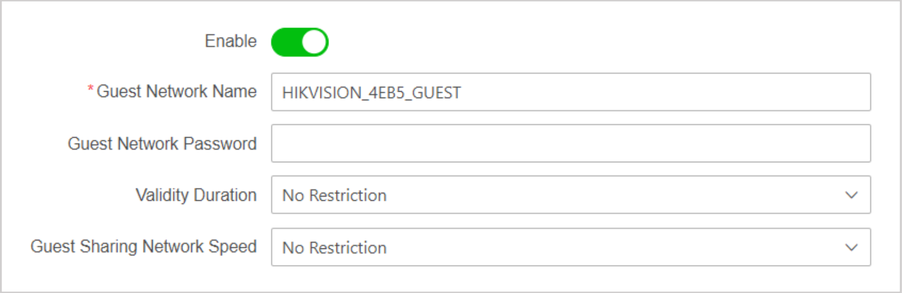
Step 3 Set the following parameters.

- **Guest Network Name**: Set a Wi-Fi name that is different with the host network name.
- **Guest Network Password**: Set the password for connecting the Guest Network.
- Validity Duration: It supports No Restriction, 4h, 8h, or 24h.
- **Guest Sharing Network Speed**: It supports to customize as desire.

Step 4 Click **Save**.

Note

- If you don’t set a **Guest Network Password**, the **Guest Network** will be available without a password.
- Before enabling, check if router is connected. Otherwise, the function cannot take effect.



Enable ●

*Guest Network Name: HIKVISION_4EB5_GUEST

Guest Network Password:

Validity Duration: No Restriction

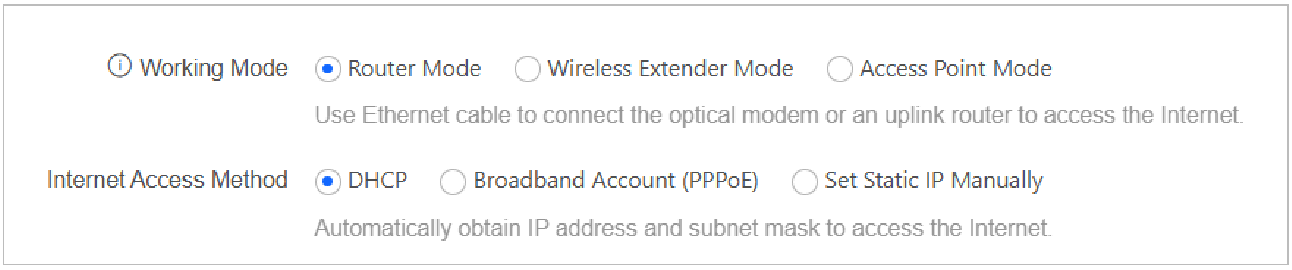
Guest Sharing Network Speed: No Restriction

Figure 4-4 Set Guest Network

4.2 Broadband Settings

4.2.1 Basic Settings

Go to **My Broadband**→**Basic Settings** to set router working mode.



Working Mode: ● Router Mode ○ Wireless Extender Mode ○ Access Point Mode

Use Ethernet cable to connect the optical modem or an uplink router to access the Internet.

Internet Access Method: ● DHCP ○ Broadband Account (PPPoE) ○ Set Static IP Manually

Automatically obtain IP address and subnet mask to access the Internet.

Figure 4-5 Working Mode

Router Mode

Your router will create a new Wi-Fi network or replace the old router. In this mode, the WAN port of the router can connect to a modem or an uplink router via an Ethernet cable.

Step 1 Go to **My Broadband**→**Basic Settings**, and select the working mode as **Router Mode**.

Step 2 Select **Internet Access Method**.

Table 4-3 Internet Access Method Description

Method	Description
DHCP	The router will automatically get IP address, subnet mask, gateway, DNS and other information. You do not need to configure. Note If static DNS is enabled, you need to enter the preferred DNS information. Not enabled by default.
Broadband Account (PPPoE)	Dial up via broadband account (telecom, mobile, and network connection). Note ● If you have an old router that can connect to the network normally, you can migrate data in PPPoE mode by connecting to the old router. ● If static DNS is enabled, you need to enter the preferred DNS information. Not enabled by default.
Set Static IP Manually	It is not recommended unless your ISP has provided an IP address and other information.

Step 3 Click **Save**.

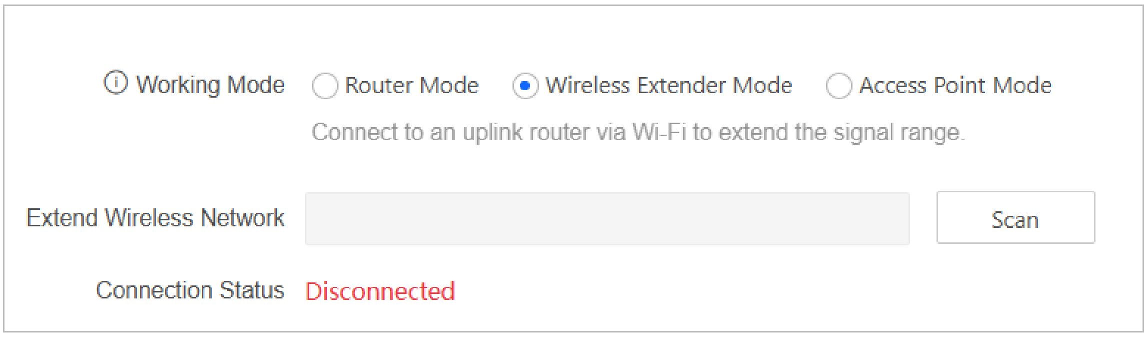
Wireless Extender Mode

Your router will be connected to the uplink router via Wi-Fi wirelessly to expand the Wi-Fi coverage of the uplink router.

Note

- Make sure the DHCP server is enabled for uplink routing.
- Make sure the router WAN port is not connected to other devices using an Ethernet cable.
- In this mode, functions such as terminal management and LAN settings will be hidden. Wi-Fi cannot be configured.

Step 1 Go to **My Broadband**→**Basic Settings** and select the working mode as the **Wireless Extender Mode**.



ⓘ Working Mode ○ Router Mode ● Wireless Extender Mode ○ Access Point Mode

Connect to an uplink router via Wi-Fi to extend the signal range.

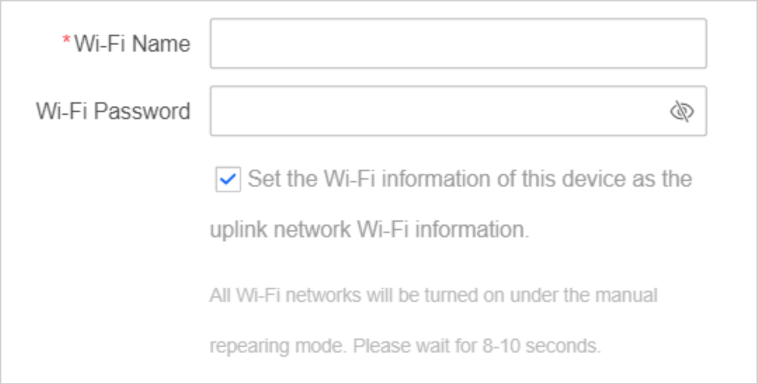
Extend Wireless Network

Connection Status Disconnected

Figure 4-6 Wireless Extender Mode

Step 2 Click **Scan** to select the network to expand the signal range and enter the Wi-Fi password.

Step 3 (Optional) Click **Add Manually** to enter the network name and password to expand the signal range.



*Wi-Fi Name

Wi-Fi Password

☑ Set the Wi-Fi information of this device as the uplink network Wi-Fi information.

All Wi-Fi networks will be turned on under the manual repearing mode. Please wait for 8-10 seconds.

Figure 4-7 Add Manually

Step 4 Click **Save**.

Step 5 Click **Ok**.

Access Point Mode

The user can connect to the uplink router via wired connection, and expand the network interface. Terminal management, LAN settings, etc. will be hidden.

Note

- Make sure network mode of uplink router is not DHCP mode.
- After the router is switched to bridge or all-purpose relay mode, the enabled visitor network will be disabled.
- After switching from bridge mode to route mode, the connected device needs to reconnect the router. Otherwise, the network connection may fail.

Step 1 Go to **My Broadband**→**Basic Settings** and select the working mode as **Bridge Mode**.

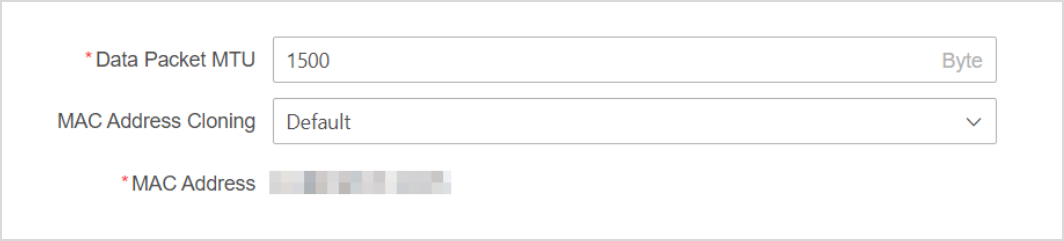
Step 2 Connect the WAN port of your router and the LAN port of the uplink router.

Step 3 Click **Save**.

4.2.2 Advanced Settings

Go to **My Broadband→Advanced Settings**. It is recommended to maintain the default configuration.

- Data Package MTU: Set the maximum transmission unit (MTU). The default value is 1480 in **PPPoE** mode, 1500 in **DHCP** and **Set Static IP Manually** mode.
- MAC Address Cloning: It can solve the broadband limit and enable router to share network. You can select default MAC address, or clone the MAC address of the management PC to the WAN port, or configure the MAC address manually.



*Data Packet MTU: 1500 Byte

MAC Address Cloning: Default

*MAC Address: [redacted]

Figure 4-8 Advanced Settings

4.3 Network Settings

Select **More→Network Settings** to set router network parameters.

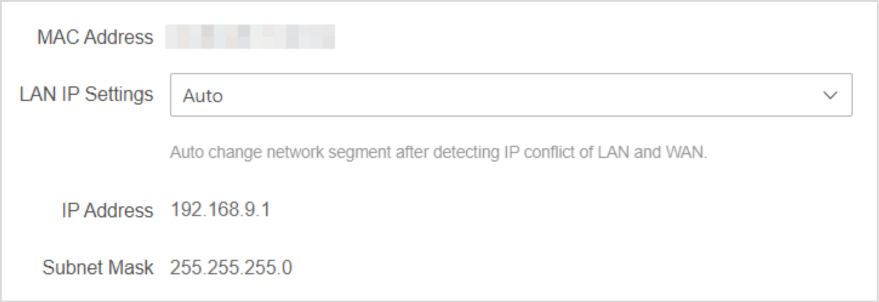
4.3.1 LAN Settings

LAN port IP settings can be auto or manual, and both have LAN-WAN conflict detection mechanism, detecting whether the IP obtained by WAN port is in the same network segment with the IP address of LAN port. It is usually in auto mode.

Go to **More→Network Settings→LAN Settings.**

- **Auto**: After conflict is detected, the LAN port IP address will be automatically changed to other network segment.
- **Manual**: After conflict is detected, you can manually edit the LAN port IP address.

After the IP address of the LAN is edited, the device connected to the router will be redistributed.



MAC Address: [redacted]

LAN IP Settings: Auto

Auto change network segment after detecting IP conflict of LAN and WAN.

IP Address: 192.168.9.1

Subnet Mask: 255.255.255.0

Figure 4-9 LAN Settings

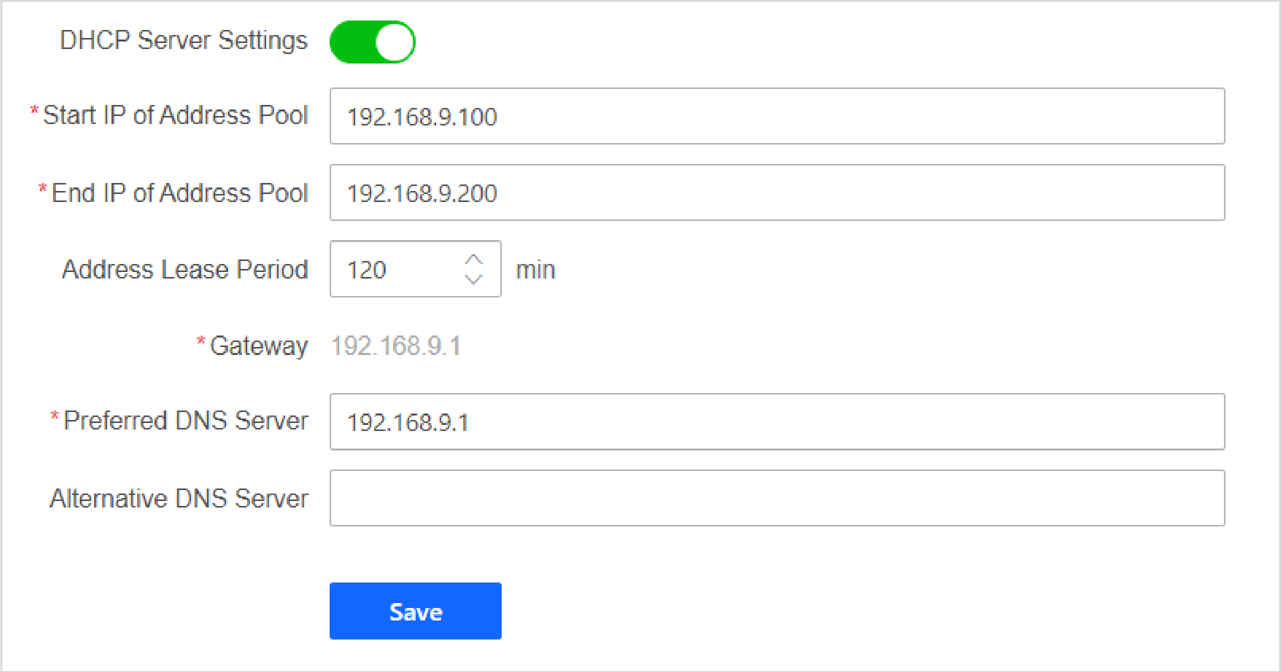
4.3.2 DHCP Server Settings

DHCP server can be enabled or disabled according your need. After it is enabled, the router can automatically distribute network parameters such as IP address, subnet mask, and DNS to network devices in the LAN.

Go to **More→Network Settings→DHCP Server Settings.**

Table 4-4 Parameter Description

Parameter	Description
Start/End IP of Address Pool	The start/end address of the IP address automatically allocated by DHCP server. **Note** DHCP address pool IP address should be in the same network segment as LAN port IP address.
Address Lease Period	The effective time of auto-distributing IP address. The device needs to get the IP address again after the time exceeded.
Gateway	The IP address of the router LAN port cannot be edited.
Preferred/Alternative DNS Server	Domain name parses server address.



DHCP Server Settings: enabled

*Start IP of Address Pool: 192.168.9.100

*End IP of Address Pool: 192.168.9.200

Address Lease Period: 120 min

*Gateway: 192.168.9.1

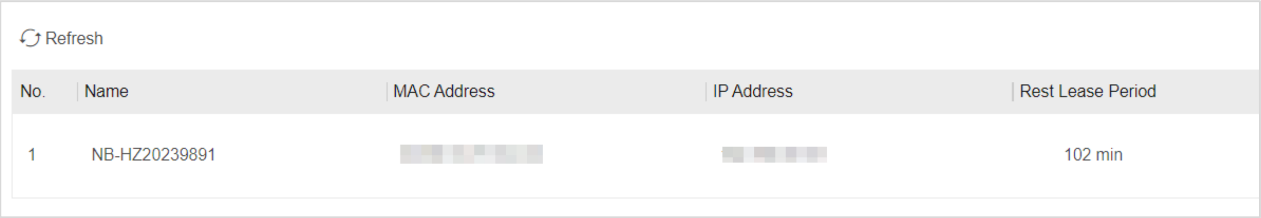
*Preferred DNS Server: 192.168.9.1

Alternative DNS Server:

Figure 4-10 DHCP Server

4.3.3 DHCP Client List

Go to **More**→**Network Settings**→**DHCP Client List**. Check the list of terminals that obtain IP addresses through a DHCP server.



No.	Name	MAC Address	IP Address	Rest Lease Period
1	NB-HZ20239891	[redacted]	[redacted]	102 min

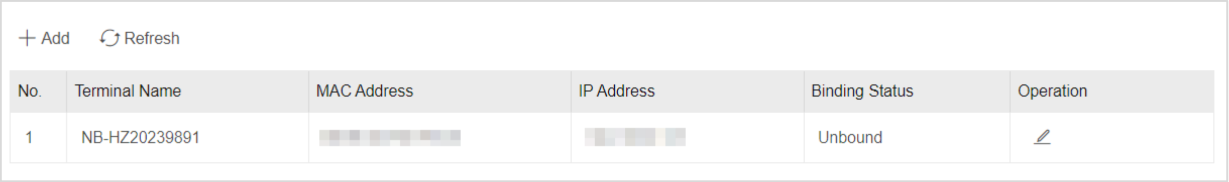
Figure 4-11 DHCP Client List

4.3.4 Bind IP and MAC

Bind IP address to terminal MAC address, and distribute fixed IP address to terminal device. It can ensure that users' valid IP address is not misappropriated or abused, and can also be protected from ARP attack.

Go to **More**→**Network Settings**→**Bind IP and MAC.**

- Click ✎ to edit the bound terminal.



No.	Terminal Name	MAC Address	IP Address	Binding Status	Operation
1	NB-HZ20239891	[redacted]	[redacted]	Unbound	✎

Figure 4-12 Terminal Binding List

- Click + Add to bind a new terminal.

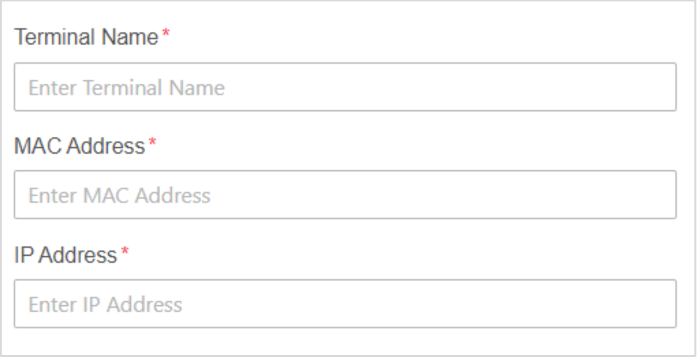
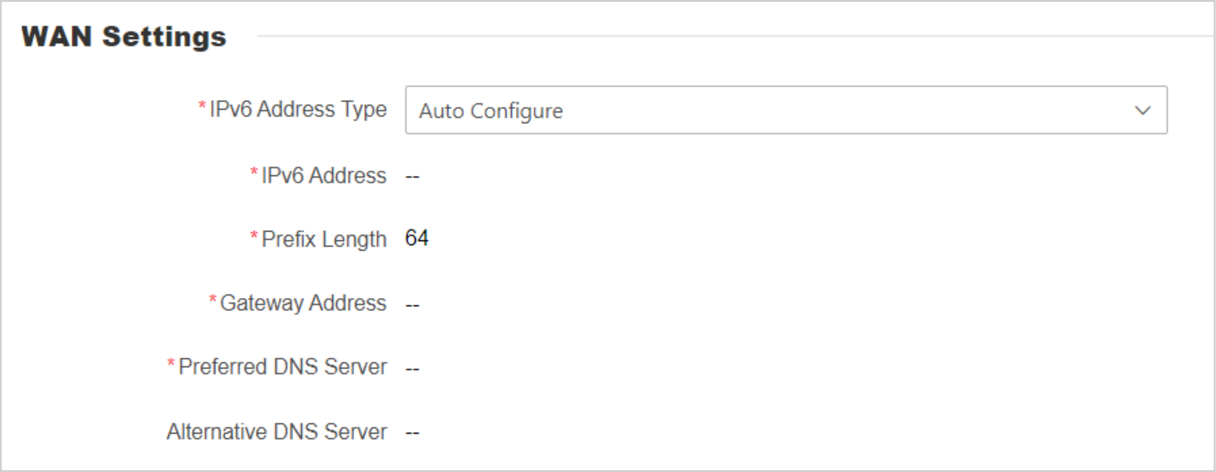

Terminal Name*
Enter Terminal Name
MAC Address*
Enter MAC Address
IP Address*
Enter IP Address

Figure 4-13 Add Binding

4.3.5 IPv6

Go to **More**→**Network Settings**→**IPv6.** You can configure WAN connection mode and LAN address distribution mode.



WAN Settings

* IPv6 Address Type: Auto Configure

* IPv6 Address: --

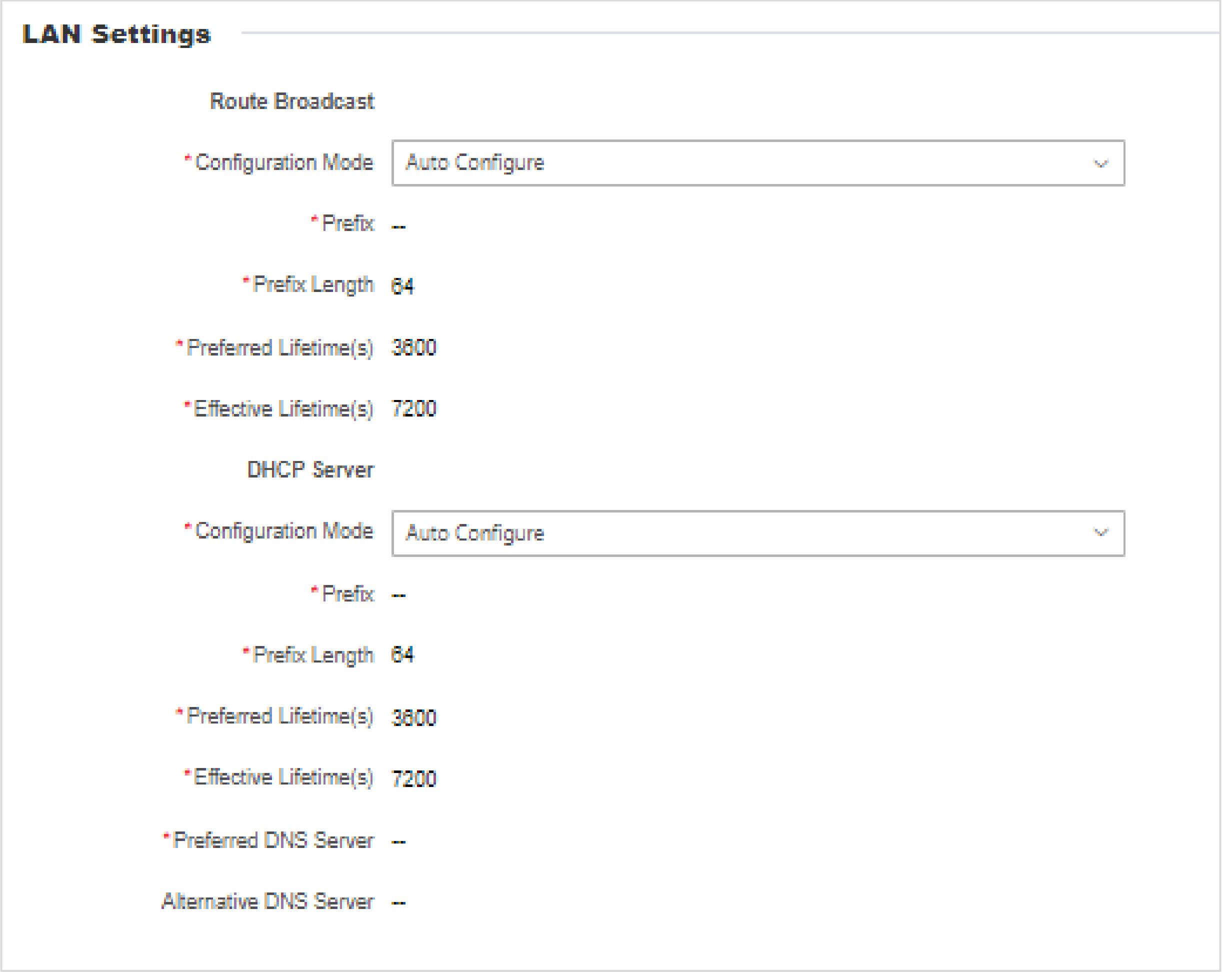
* Prefix Length: 64

* Gateway Address: --

* Preferred DNS Server: --

Alternative DNS Server: --

Figure 4-14 IPv6-WAN Configuration



LAN Settings

Route Broadcast

* Configuration Mode: Auto Configure

* Prefix: --

* Prefix Length: 64

* Preferred Lifetime(s): 3600

* Effective Lifetime(s): 7200

DHCP Server

* Configuration Mode: Auto Configure

* Prefix: --

* Prefix Length: 64

* Preferred Lifetime(s): 3600

* Effective Lifetime(s): 7200

* Preferred DNS Server: --

Alternative DNS Server: --

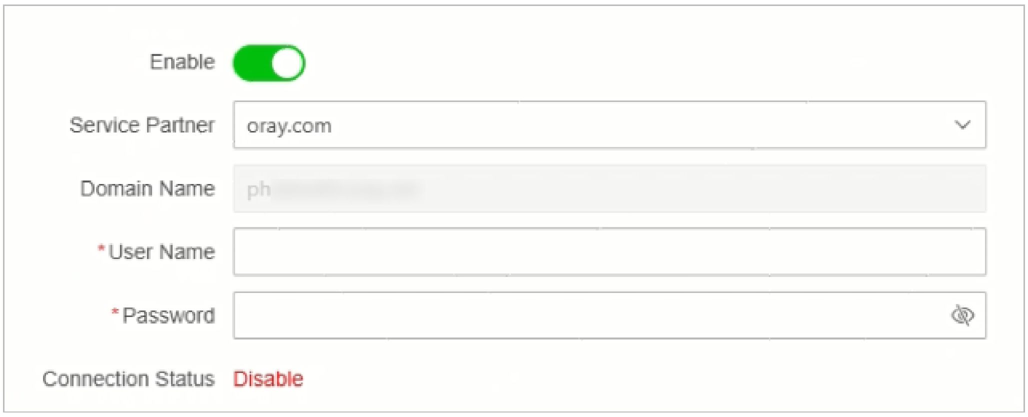
Figure 4-15 IPv6-LAN Configuration

4.3.6 DDNS

DDNS is an extended version of DNS (Domain Name System) that supports dynamically updating the mapping relationship between domain names and IP addresses. It allows users to access dynamically changing public IP addresses through a fixed domain name.

Go to **More→Network Settings→DDNS.**

The server partner is only supported with ORAY. Please set your user name and password.



Enable ●

Service Partner: oray.com

Domain Name: ph[redacted]

*User Name:

*Password:

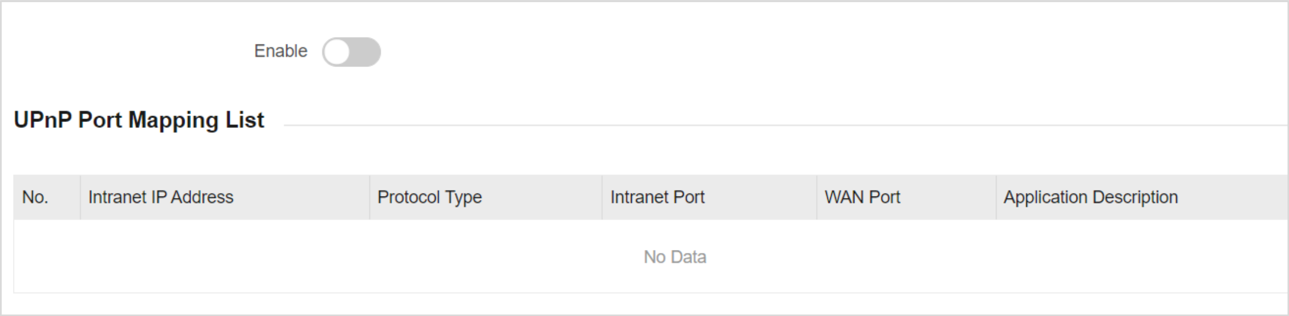
Connection Status: Disable

Figure 4-16 Set DDNS

4.3.7 UPnP

Enabling UPNP (UniversalPlugandPlay, general plug-and-play), the internal network host can request the router to map the port automatically through the UPNP protocol. When using software such as P2P that supports UPNP protocol, the download speed can be increased to improve network stability.

Go to **More→Network Settings→UPnP.**



Enable ○

UPnP Port Mapping List

No.	Intranet IP Address	Protocol Type	Intranet Port	WAN Port	Application Description
No Data					

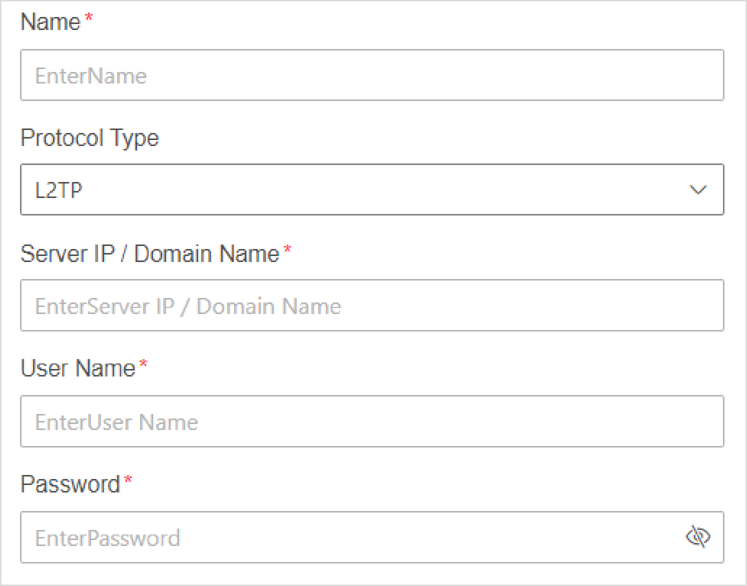
Figure 4-17 UPnP

4.3.8 VPN

After connecting to the VPN server, you can easily and securely access the internal network resources of the VPN server through the Internet.

Step 1 Go to **More→Network Settings→VPN**.

Step 2 Click **ADD** and enter required information to add VPN.



Name*

EnterName

Protocol Type

L2TP

Server IP / Domain Name*

EnterServer IP / Domain Name

User Name*

EnterUser Name

Password*

EnterPassword

Figure 4-18 Add VPN

Note

Support to select L2TP or PPTP as protocol type.

Step 3 Click **Save**.

Step 4 (Optional) **Shunt by Intelligent VPN** allows to connect the selected server or device's data diversion to the VPN channel.

- **Shunt by Server Address**: The router will transmit data with a specified service address as the destination address through a VPN link.
- **Shunt by Device**: The router will transmit data from devices with specified MAC addresses or selected online devices through a VPN link.

Note

- **Name** allows 1~128 bytes.
- Support at least 8 rules at the same time.
- The flow rule takes effect independently.

4.3.9 VLAN

In the uplink network environment provided by the ISP, a fixed VLAN is configured when assigning addresses. So it is required that the router supports the corresponding VALN on the WAN side, and at the same time, the LAN side needs to specify the corresponding VLAN ID for the business in order to obtain the IP address.

Note

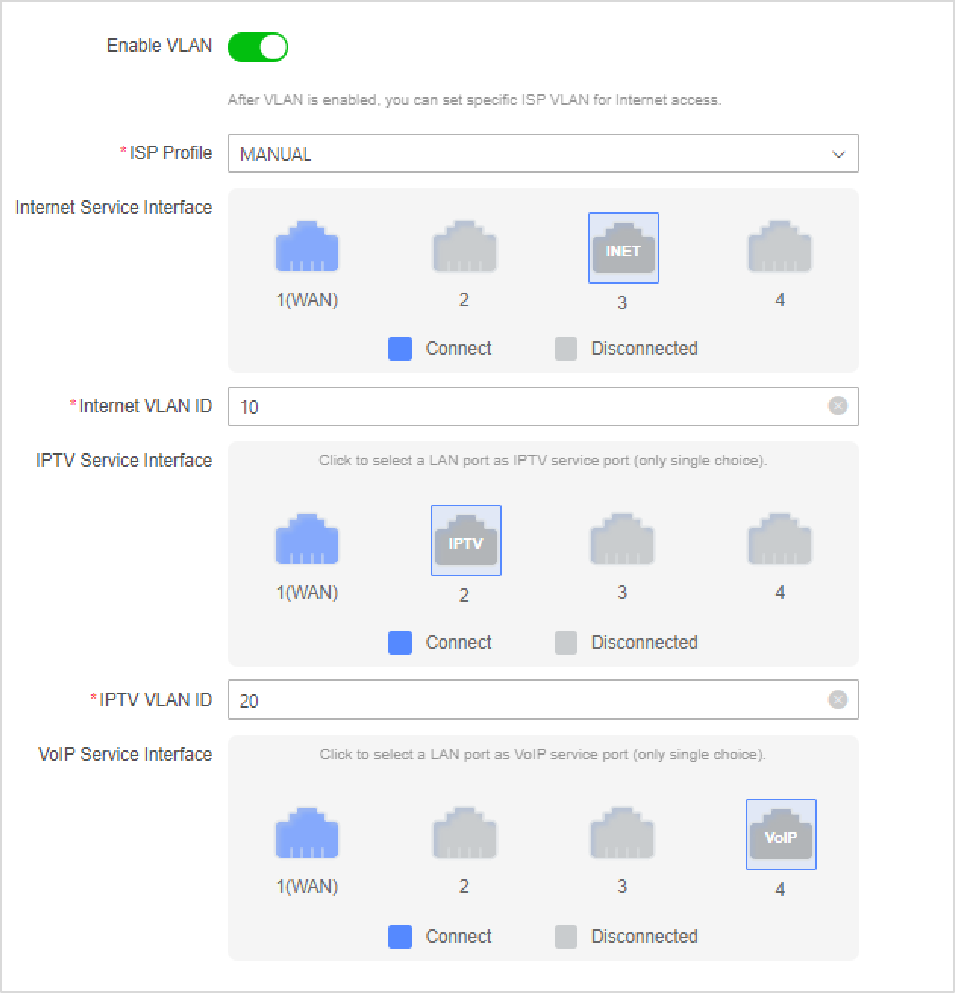
The function is only available for some models. The actual interface prevails.

Step 1 Go to **More**→**Network Settings**→**VLAN**.

Step 2 Enable VLAN.

Step 3 Select your **ISP Profile**. The **Internet VLAN ID** will be set by defaults unless you choose MANUAL as your ISP.

Step 4 (Optional) If you choose MANUAL as your ISP, you need to set **Internet Service Interface**, **IPTV Service Interface**, and **VoIP Service Interface** independently, and set their VLAN ID.



Enable VLAN ●

After VLAN is enabled, you can set specific ISP VLAN for Internet access.

*ISP Profile: MANUAL

Internet Service Interface

*Internet VLAN ID: 10

IPTV Service Interface

Click to select a LAN port as IPTV service port (only single choice).

*IPTV VLAN ID: 20

VoIP Service Interface

Click to select a LAN port as VoIP service port (only single choice).

Figure 4-19 Set MANUAL

Step 5 Click **Save**.

Note

- After VLAN is enabled, the WAN port will be fixed to network port 1 by default. Please reconnect the Ethernet cable to port 1.
- A LAN port can only be set for one kind of service when you configure MANUAL parameter.
- VLAN ID should be set within 5~4094.

4.3.10 Mesh

Mesh networking helps with activating and paring a new router to extend the old router's Wi-Fi range.

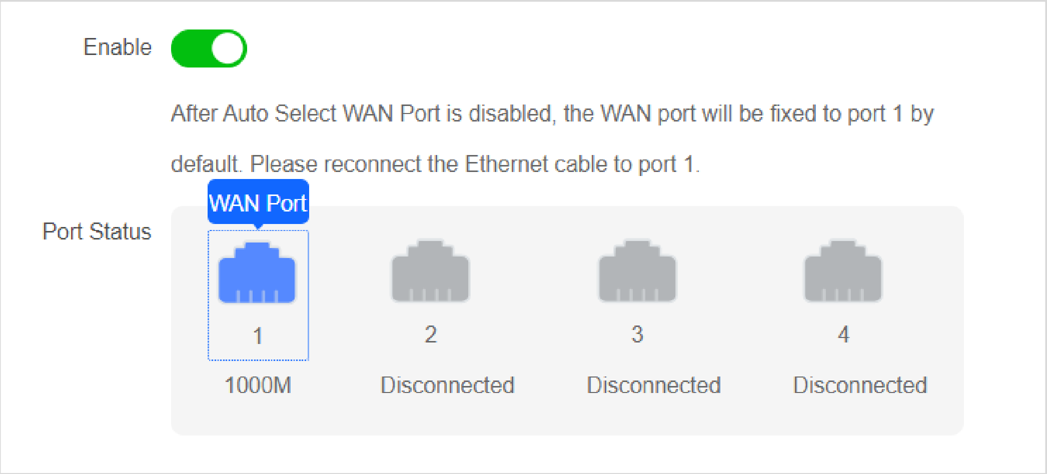
Go to **More**→**Network Settings**→**Mesh** to enable this function.

The details about operation steps refer to **Quick Networking Guidance** on the page or ***1.2.2 Extend Wi-Fi Range***.

4.3.11 Auto Select WAN Port

The four network ports of the router are adaptive to WAN or LAN by default.

Go to **More**→**Network Settings**→**Auto Select WAN Port** to disable this function, the WAN port will be fixed to network port 1.



Enable

After Auto Select WAN Port is disabled, the WAN port will be fixed to port 1 by default. Please reconnect the Ethernet cable to port 1.

Port Status

Figure 4-20 Auto Select WAN Port

Note

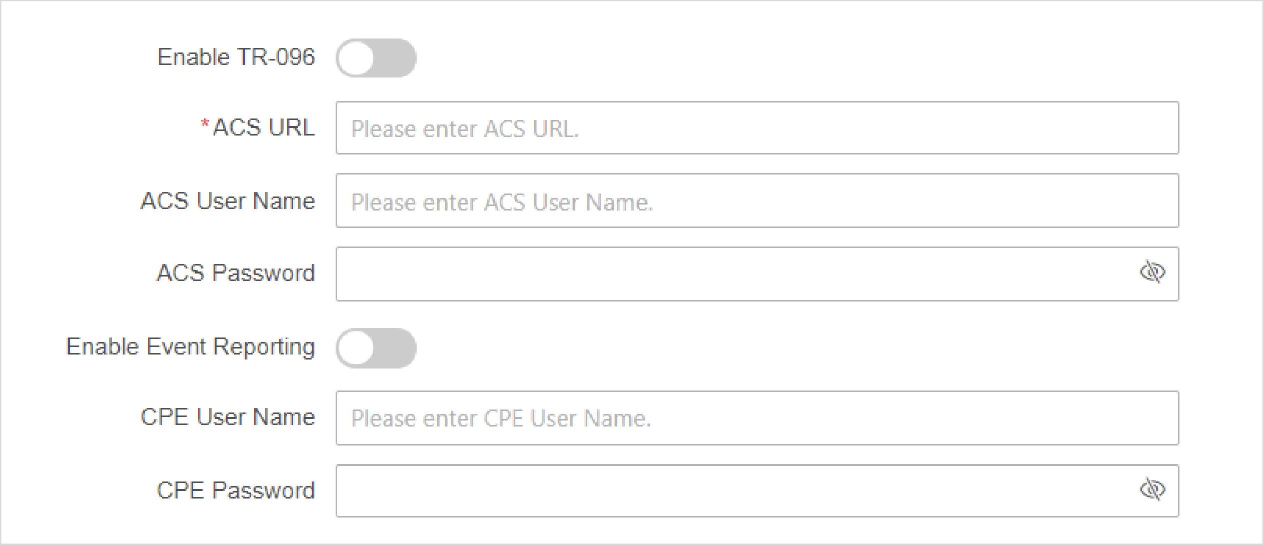
Reconnect the Ethernet cable to port 1 if you disable this function.

4.3.12 TR-069

The CPE WAN Management Protocol (TR-069) is a technical specification that allows the auto-configuration server (ACS) to configure, connect, and diagnose the customer-premises equipment

(CPE) connected to an Internet Protocol (IP) network, achieving remote management for your router.

Go to **More→Network Settings→TR-069** to enable this function.



Enable TR-096

*ACS URL: Please enter ACS URL.

ACS User Name: Please enter ACS User Name.

ACS Password

Enable Event Reporting

CPE User Name: Please enter CPE User Name.

CPE Password

Figure 4-21 Configure TR069

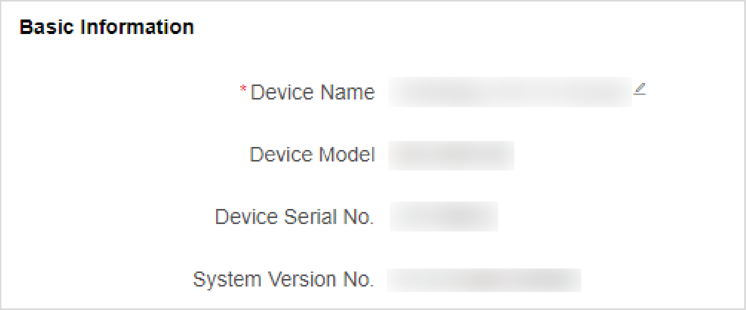
- **Enable TR-096**: Enable/disable TR-069. The router will send a session setup request to the ACS if TR-096 is enabled. TR-069 is disabled by default.
- **ACS URL**: The ACS server IP address or domain name is required. The length range is 1~255 characters.
- **ACS User Name**: The user name authenticated by the ACS after receiving a session setup request from the router. The length range is 1~256 characters.
- **ACS Password**: The password authenticated by the ACS. The length range is 1~64 characters.
- **Enable Event Reporting**: After it is enabled, the router will report events to the ACS within the set interval time.
- **Report Interval**: The interval time for event reporting. The value range is 5~3600 seconds.
- **CPE User Name**: The user name authenticated by the CPE after receiving a connection request from the ACS. The user name has been specified on the ACS. The length range is 1~256 characters.
- **CPE Password**: The password authenticated by the CPE after receiving a connection request from the ACS. The password has been specified on the ACS. The length range is 1~64 characters.

Chapter 5 Router Management

5.1 Device Information

Click **More**→**Basic Information** to view basic device information and network information.

Basic Information: View device model, serial No., system version, and customize device name.



Basic Information

*Device Name	[redacted]
Device Model	[redacted]
Device Serial No.	[redacted]
System Version No.	[redacted]

Figure 5-1 Basic Information

Network Information: Check device network IP address, subnet mask, gateway, and DNS server information.

5.2 System Settings

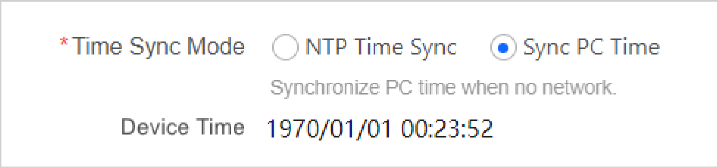
Click **More**→**System Settings** to perform time sync, indicator, etc.

5.2.1 System Time

Time Sync

Sync device system time with network time to ensure system time accuracy. The default configuration is for general user.

- **Sync PC time**: Support for use when no network.



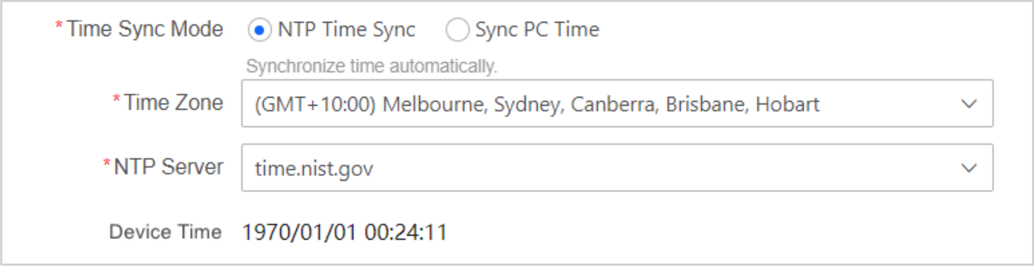
*Time Sync Mode ○ NTP Time Sync ● Sync PC Time

Synchronize PC time when no network.

Device Time 1970/01/01 00:23:52

Figure 5-2 Sync PC Time

- **NTP Time Sync**: Synchronize time automatically with network.



*Time Sync Mode ● NTP Time Sync ○ Sync PC Time

Synchronize time automatically.

*Time Zone (GMT+10:00) Melbourne, Sydney, Canberra, Brisbane, Hobart

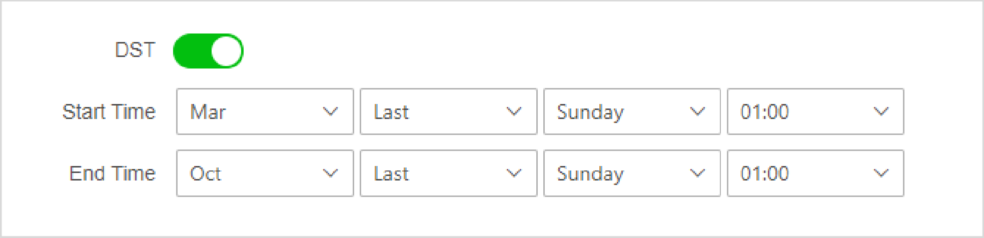
*NTP Server time.nist.gov

Device Time 1970/01/01 00:24:11

Figure 5-3 NTP Time Sync

DST

Support configuring the start and end times of daylight saving time (DST). After being turned on, once the system time reaches the start time of DST, it will shift back by 1 hour; once the system time reaches the end time of DST, it will offset forward by 1 hour.



DST

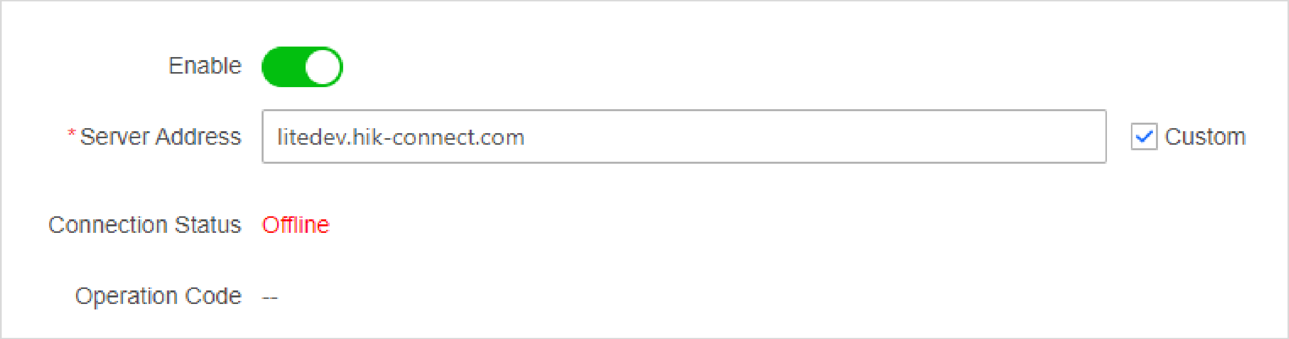
Start Time Mar Last Sunday 01:00

End Time Oct Last Sunday 01:00

Figure 5-4 DST

5.2.2 Cloud Management

Cloud based network management is supported.



Enable

*Server Address litedev.hik-connect.com ☑ Custom

Connection Status Offline

Operation Code --

Figure 5-5 Cloud Management

5.2.3 Indicator

You can enable or disable the device indicator via Web page switch.

5.3 Security Settings

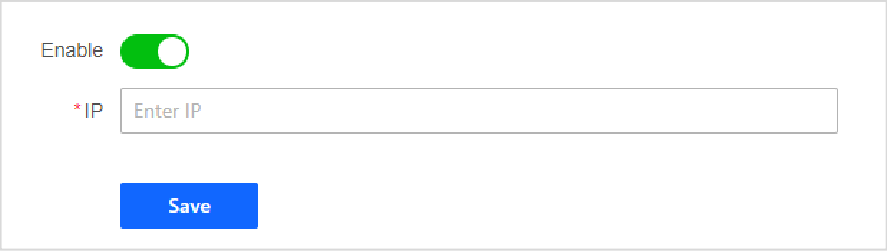
Select **More**→**Security Settings** to configure router security.

5.3.1 Firewall

The firewall is a safety barrier between the Internet and the home LAN. After the firewall is enabled, the device will filter the data entering the LAN from the Internet to avoid network attacks from external networks, thus protecting the security of internal network users and data. It is recommended to keep it on.

5.3.2 DMZ

Set the local area network (LAN) host as the DMZ host, then the external network can access the host. For example, you can set the web server and FTP server as the DMZ host to access the DMZ host via the Internet. Enter the IP address of the DMZ host when enabling DMZ.


Enable ●

*IP Enter IP

Figure 5-6 Set DMZ

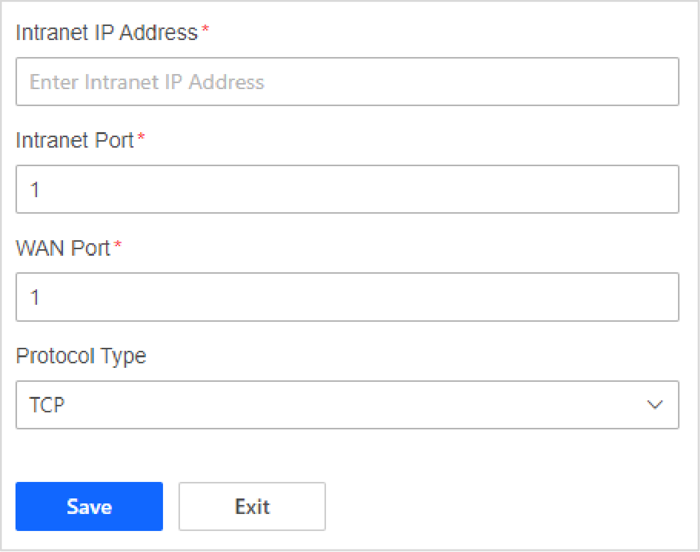
Note

Port mapping is only used to map the specified port. DMZ refers to mapping all ports, and directly exposes the host to the gateway. It is easier than port mapping, but it is less secure.

5.3.3 Port Mapping

Map the specific port of a LAN host to a WAN IP address and port for easy access from the public network.

The IP address, IP port, and external port information are required to add the mapping port.



Intranet IP Address*

Enter Intranet IP Address

Intranet Port*

1

WAN Port*

1

Protocol Type

TCP

Figure 5-7 Add Port Mapping

5.3.4 Remote Web

After the remote web function is enabled, the device can be managed by inputting the WAN port IP of the router through the HTTPS protocol. Once enabled, there is a risk of being attacked by hackers, and long-term activation is not recommended.

Caution

After **Remote Web** is enabled, the router is at risk of attack. Please close the remote web in a timely manner.

5.3.5 WPS

The WPS key of the router can be used to connect the terminal device to the network of the router with no password, or to connect your router to the uplink devices with no password.

Note

- Make sure WPS is supported by the connected device or uplink router.
- Make sure the route is activated.

Step 1 Put the terminal device within 1 meter of the router.

Step 2 Enable WLAN and tap the network to access.

Step 3 Press and hold the WPS button of the router frame for 1~3 seconds. The router's indicator flashes blue, which means it is pairing.

Note

Long press for more than 5s to achieve secure relay to other routers with WPS mode enabled.

5.4 System Maintenance

Select **More→System Maintenance** to upgrade, backup, restore the device to factory, log, etc.

5.4.1 Software Upgrade

Select **More→System Maintenance→Software Upgrade**.

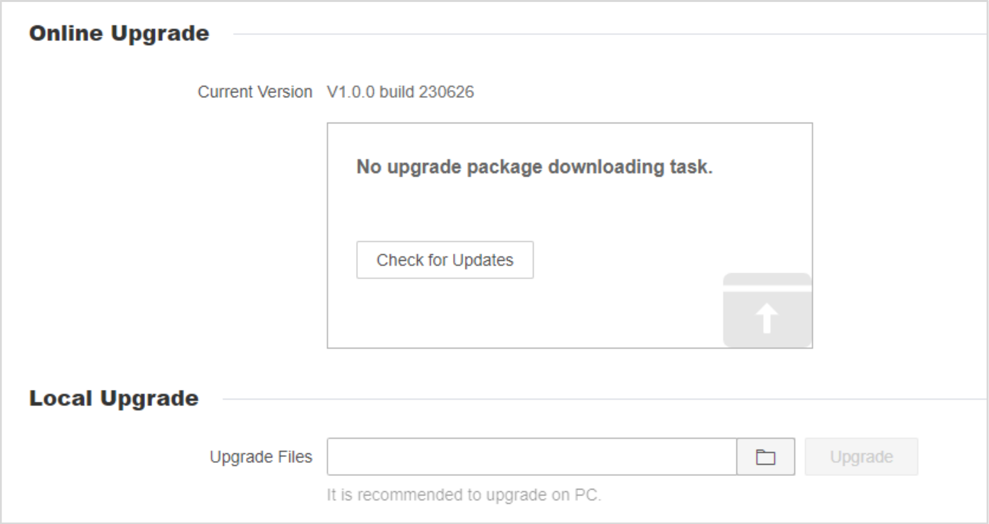
Auto Upgrade

The function is enabled by default. After **Auto Upgrade** is enabled, every day from 2:00 to 5:30 in the morning, when the WAN port traffic is less than a certain threshold and a new version is detected, the device will automatically upgrade to the new version.

Manual Upgrade

Online upgrade and local upgrade are supported.

- **Online Upgrade**: Click **Check for Updates** after the new version is detected online.
- **Local Upgrade**: Import local upgrade package file, and click **Upgrade**.



Online Upgrade

Current Version V1.0.0 build 230626

No upgrade package downloading task.

Local Upgrade

Upgrade Files

It is recommended to upgrade on PC.

Figure 5-8 Manual Upgrade

Caution

Do not power off the device during upgrade.

5.4.2 Reboot Device

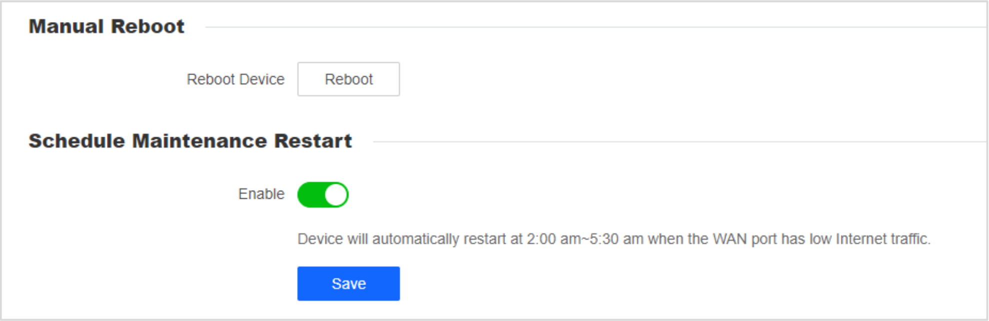
Select **More→System Maintenance→Reboot Device**.

Manual Reboot

Click **Reboot** to restart the device manually.

Scheduled Restart

The status is disabled by default. After **Scheduled Restart** is enabled, the device will automatically restart every day from 3:00 to 5:00 in the morning when the WAN port traffic is less than a certain threshold. During device restart, all connections will be disconnected.



Manual Reboot

Reboot Device: Reboot

Schedule Maintenance Restart

Enable: ●

Device will automatically restart at 2:00 am~5:30 am when the WAN port has low Internet traffic.

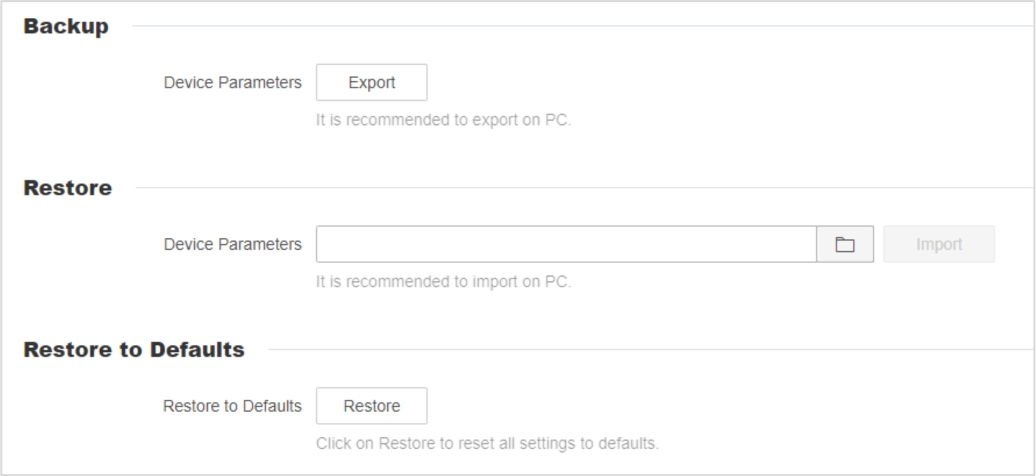
Save

Figure 5-9 Timed Restart

5.4.3 Backup and Restore

Select **More**→**System Maintenance**→**Backup and Restore**.

- **Backup**: Click **Export** to export the router configuration file to local.
- **Restore**: Import the exported configuration file to the device, and restore the previous configuration.
- **Restore to default**: Restore all settings of the device to factory status.



Backup

Device Parameters: Export

It is recommended to export on PC.

Restore

Device Parameters: Import

It is recommended to import on PC.

Restore to Defaults

Restore to Defaults: Restore

Click on Restore to reset all settings to defaults.

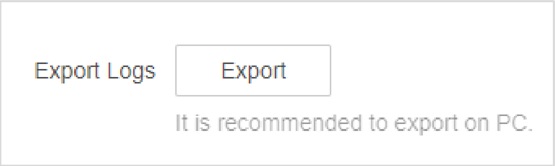
Figure 5-10 Backup and Restore

Note

Restoring previous configuration does not include restoring device management IP address and password.

5.4.4 Log Management

Select **More**→**System Maintenance**→**Logs** to manage logs.



Export Logs Export

It is recommended to export on PC.

Figure 5-11 Log Management

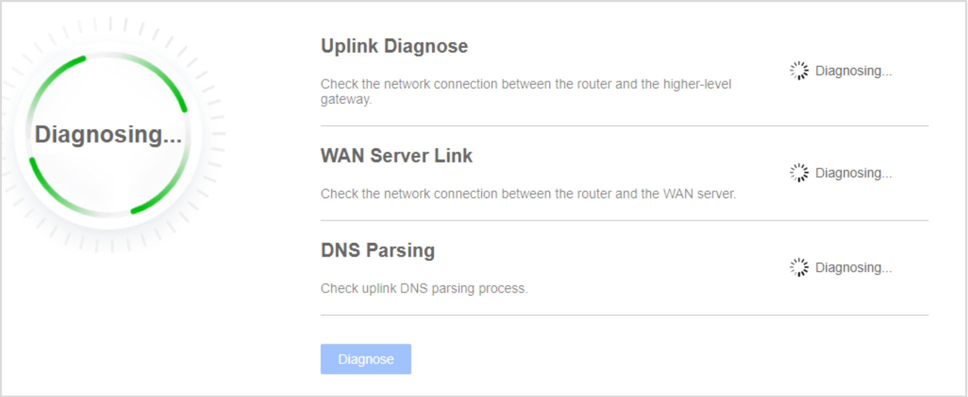
Click **Export** to export the log information of the device to the local computer.

Note

The exported log file is only available for viewing and using by maintenance personnel.

5.4.5 Diagnosis

Select **More**→**System Maintenance**→**Diagnose**. Click **Diagnose** to check the router network connection status. Please check the connection status and select whether to upload the result to cloud server.



Diagnosing...

Uplink Diagnose

Check the network connection between the router and the higher-level gateway.

Diagnosing...

WAN Server Link

Check the network connection between the router and the WAN server.

Diagnosing...

DNS Parsing

Check uplink DNS parsing process.

Diagnosing...

Diagnose

Figure 5-12 Diagnosis Network

5.5 Password Management

Table 5-1 Password Manegement

Operation	Description
Check Wi-Fi Password	Click 👁 on the Oerview page.
Modify Wi-Fi Password	Go to **My Wi-Fi→Basic Wireless Settings**.
Modify Admin Password	Click **Modify Password** in the upper-right corner of the page.
Forget Admin Password	Press reset button for 8s, and activate your router again to set new admin password.

See Far, Go Further