HIKVISION

1200Mbps 4G LTE Router

User Guide

Legal Information

About this Manual

The Manual 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 Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (https://www.hikvision.com/).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL 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 MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Applicable Models

This guide is applicable to the model: DS-3WR4G12C

Symbol Conventions

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

Item	Presentation	Example
Cascading Menus	>	Click **Status** > **Device Status**
Parameter and value	Bold	Set **User Name** to **Tom**.
UI control	Bold	On the **Policy** page, click the **OK** button.
Variable	Italic	Format: *XX:XX:XX:XX:XX:XX*
Message	“ ”	The “Success” message appears.

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

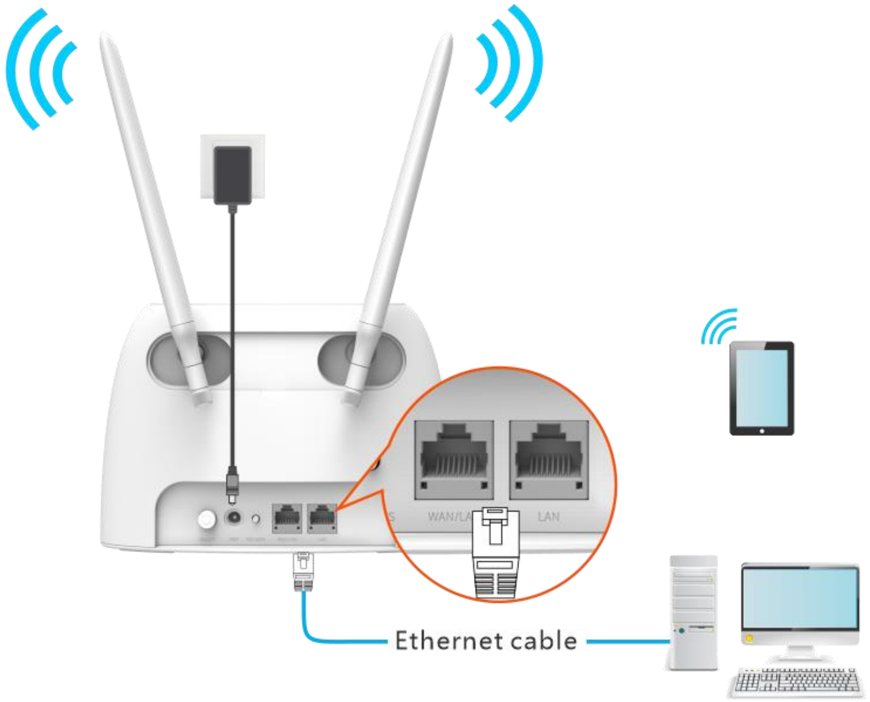
Symbol	Description
ℹ **Note**	Provides additional information to emphasize or supplement important points of the main text.
⚠ **Caution**	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.

TABLE OF CONTENTS

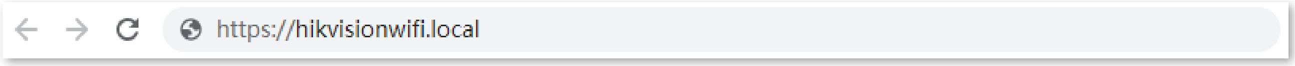
Chapter 1 Web UI

1.1 Log in to the web UI

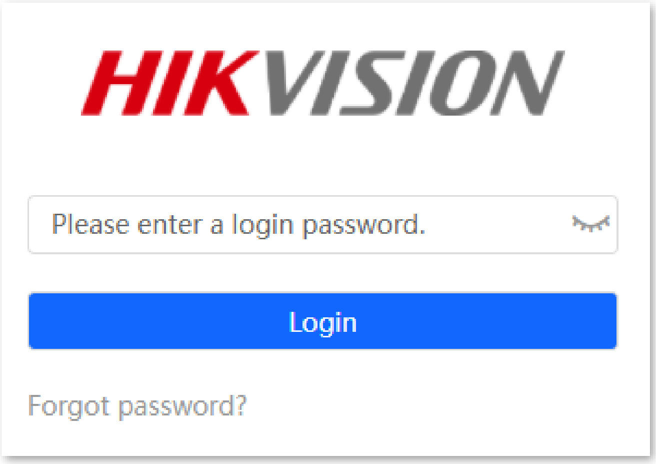
Step 1 Connect your smartphone to the Wi-Fi network, or connect your computer to a LAN port of the router (By default, the WAN/LAN and LAN port are both LAN ports).



Step 2 Start a web browser on the device connected to the router, and visit **https://hikvisionwifi.local**.


https://hikvisionwifi.local

Step 3 Enter the login password, and click **Login**.

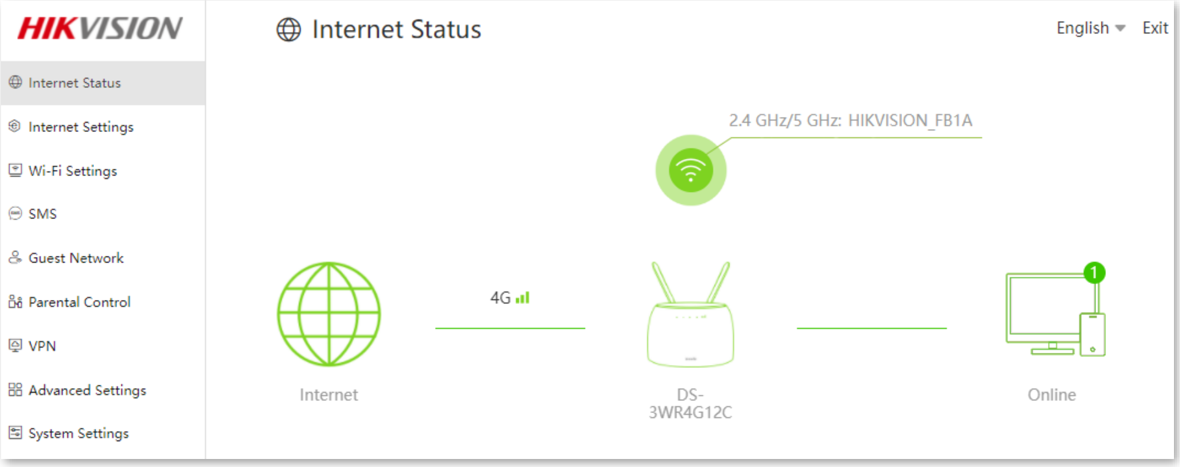


Note

If the above page does not appear, try the following solutions:

- Ensure that the router is powered on properly.
- Ensure that the computer is connected to a LAN port of the router, and the computer is set to obtain an IP address automatically.
- Restore the router to factory settings and try again.

The following page appears.

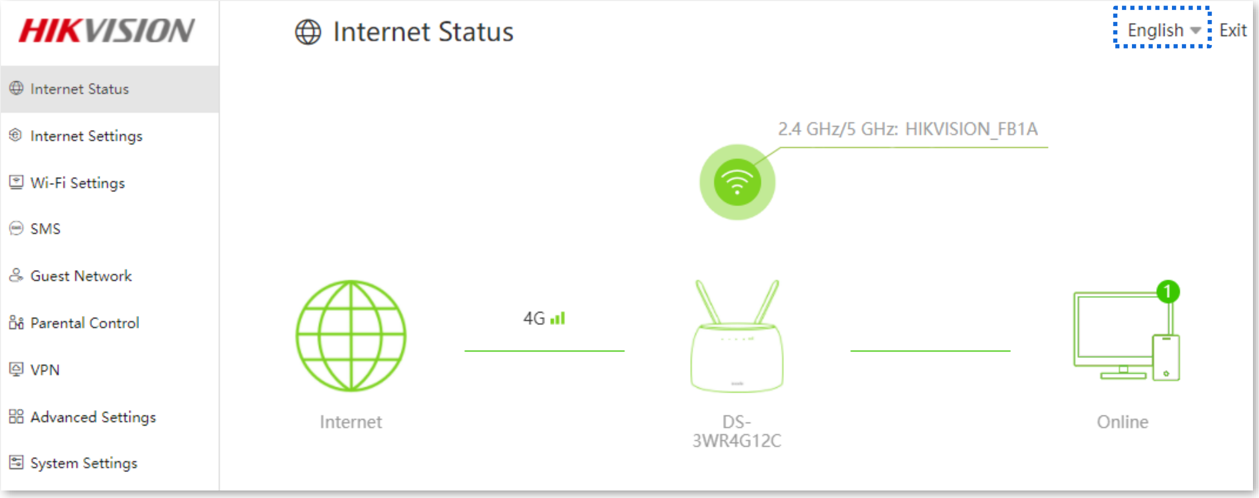


1.2 Log out of the web UI

If you Log in to the web UI of the router and perform no operation within 5 minutes, the router logs you out automatically. You can also log out by clicking **Exit** at the top right corner of the web UI.

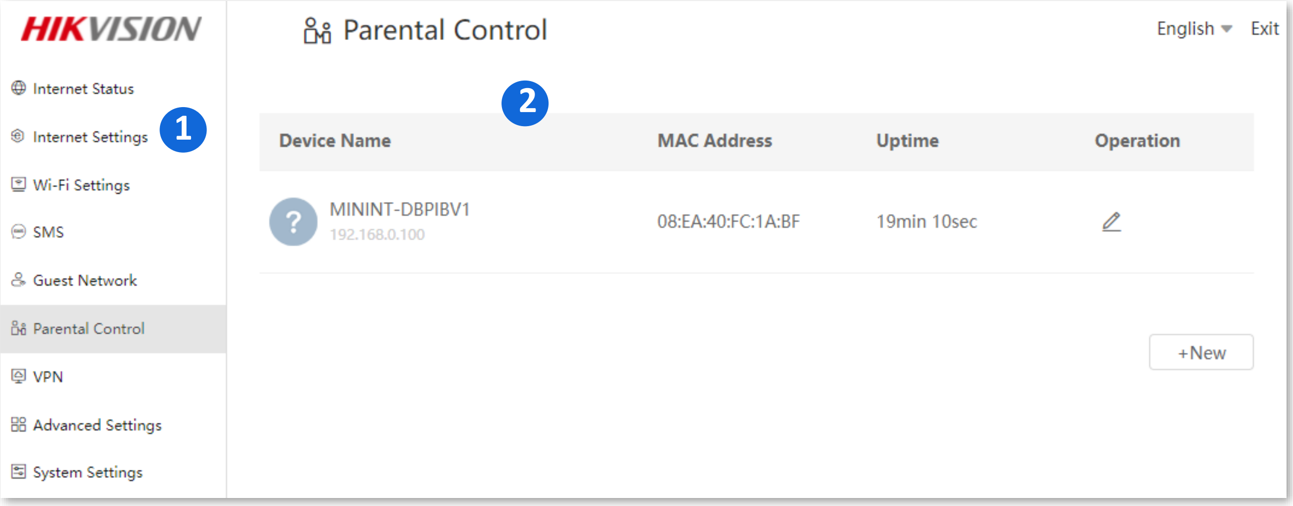
1.3 Change the language

The default language displayed is **English**. You can select another language from the drop-down list in the upper right corner.



1.4 Web UI layout

The web UI of the router consists of two sections, including the navigation bar and the configuration area. See the following figure.



Device Name	MAC Address	Uptime	Operation
MININT-DBPIBV1 192.168.0.100	08:EA:40:FC:1A:BF	19min 10sec	

SN	Name	Description
1	Navigation bar	It is used to display the function menu of the router. Users can select functions in the navigation bar and the configuration page appears in the configuration area.
2	Configuration area	It is used to modify or view your configurations.

Chapter 2 Internet status

Log in to the web UI of the router and choose **Internet Status** to enter the page. On this page, you can:

- View the internet status
- View wireless information
- View system information
- View online device information

2.1 Internet status

Note

The router supports both 3G/4G router mode and wireless router mode, and function may differ under different modes. Refer to Operating mode to set the operating mode of the router.

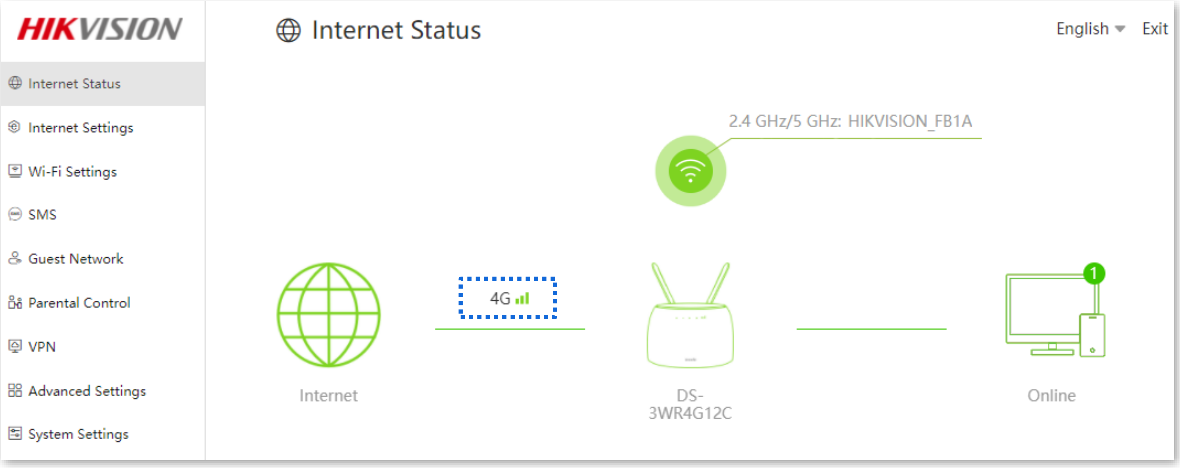
2.1.1 Under 3G/4G router mode

To view the internet status:

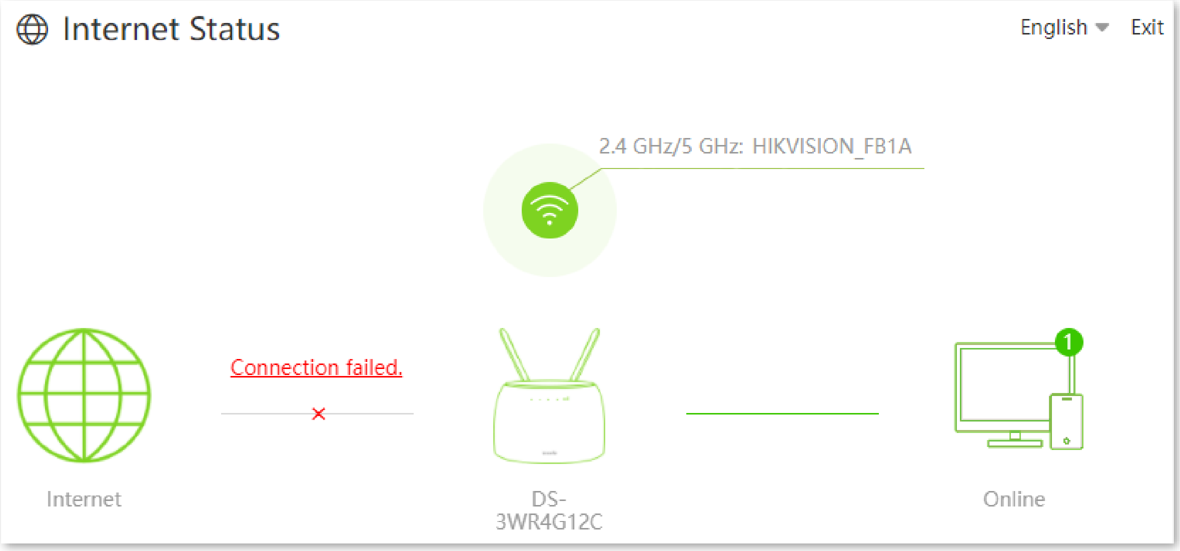
Step 1 Log in to the web UI of the router.

Step 2 Choose **Internet Status**.

When the connection between the Internet and the router is shown as below, the router is connected to the internet successfully.



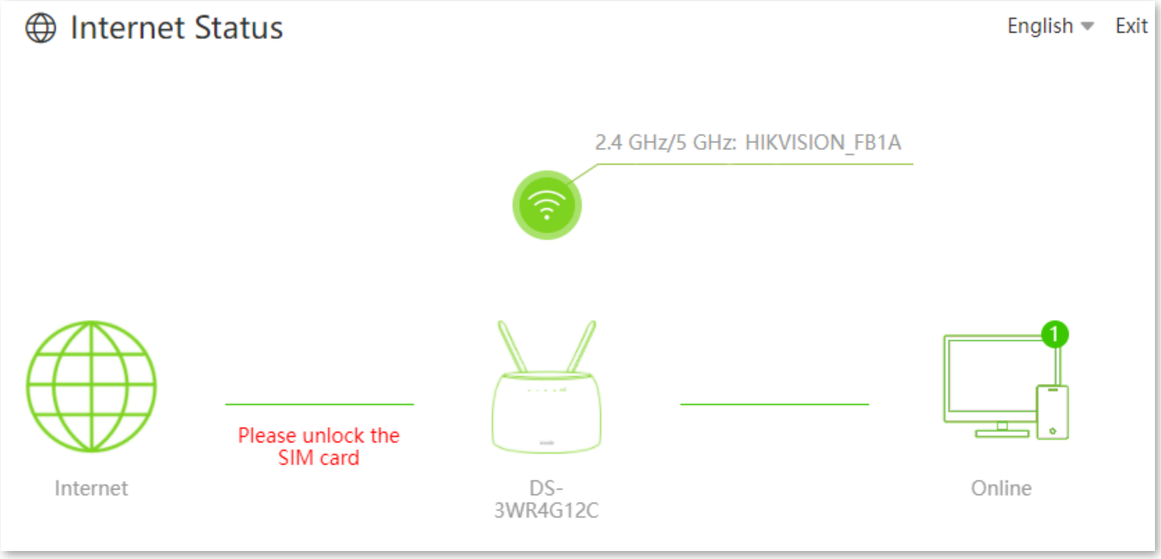
When a red cross and "Connection failed." are shown between the Internet and the Router, it indicates that the internet connection is abnormal.



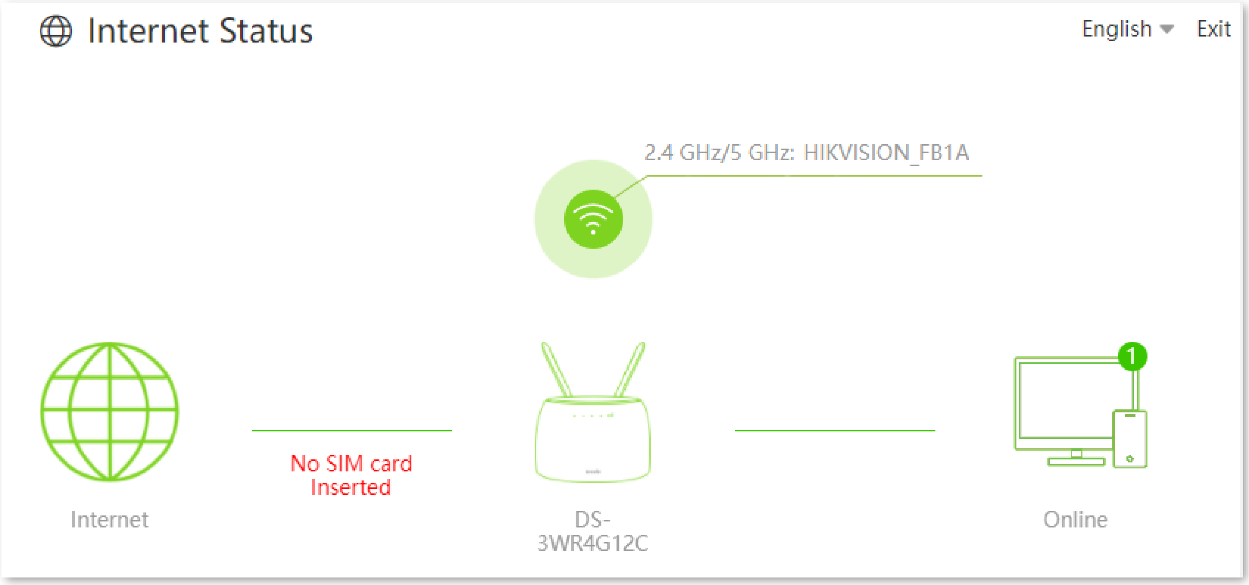
Try the following solutions:

- Choose **Internet Settings**, and ensure that the **Mobile Data** and **Data Roaming** functions are enabled, and the mobile data option is set to **4G Preferred**.
- Choose **Internet Settings**, and ensure that the dial-up settings parameters are identified by the router automatically. If not, check whether the SIM card is inserted properly, or refer to create an APN profile manually to access the internet to configure the router.
- If the SIM card is identified successfully but no internet access is available, your SIM card may have run out of money. Contact your ISP for more help.

When a red cross and "Please unlock the SIM card" are shown between the Internet and the Router, it indicates that the SIM card is locked. Refer to Unlock the SIM card in the web UI.



When a red cross and “No SIM card inserted” are shown between the Internet and the Router, ensure the SIM card is inserted properly.



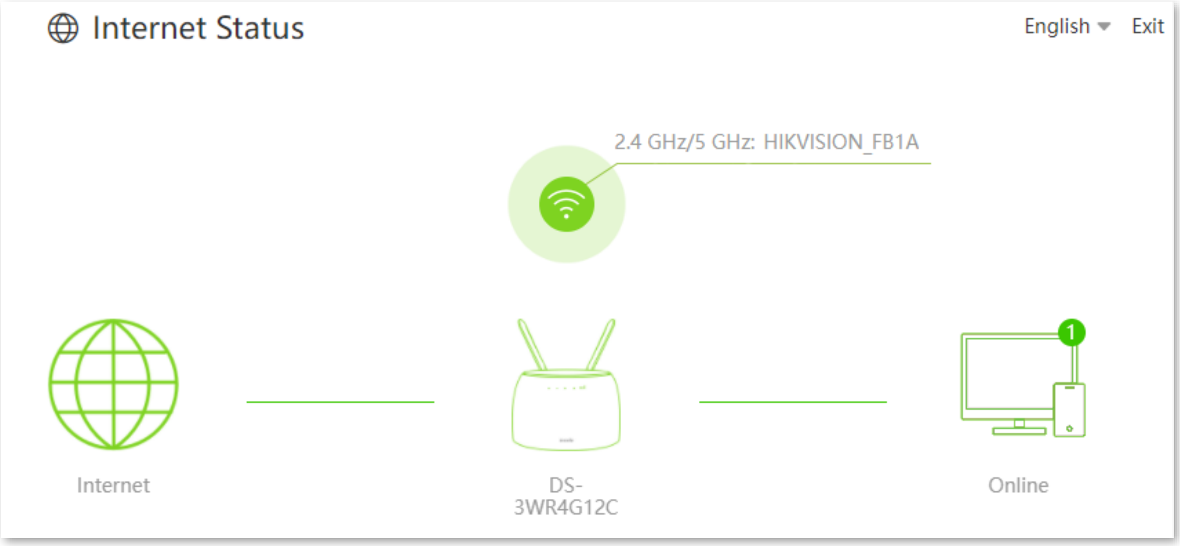
2.1.2 Under wireless router mode

To view the internet status:

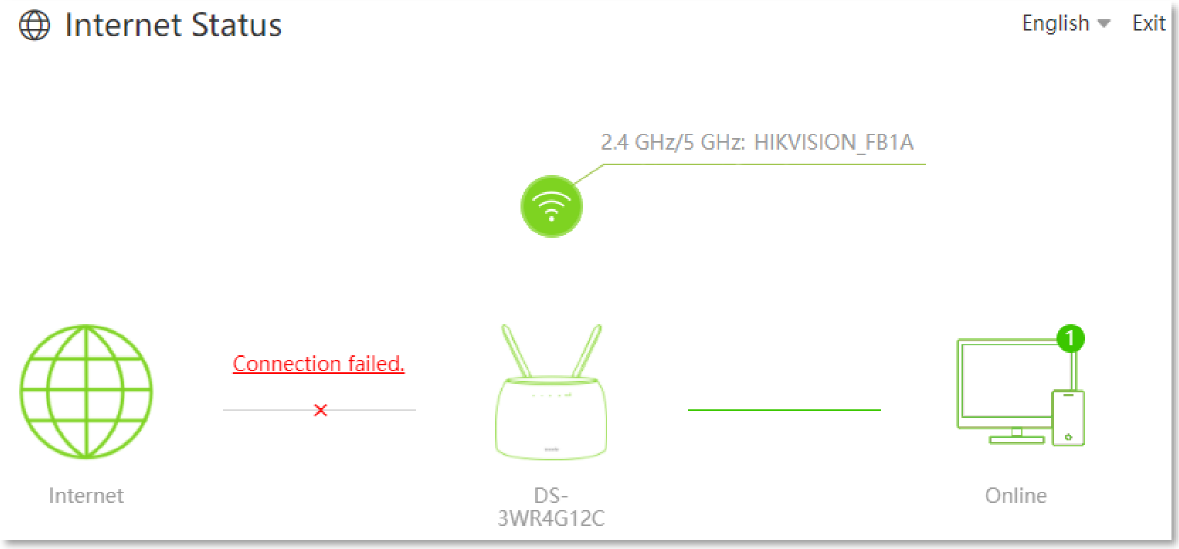
Step 1 Log in to the web UI of the router.

Step 2 Choose **Internet Status**.

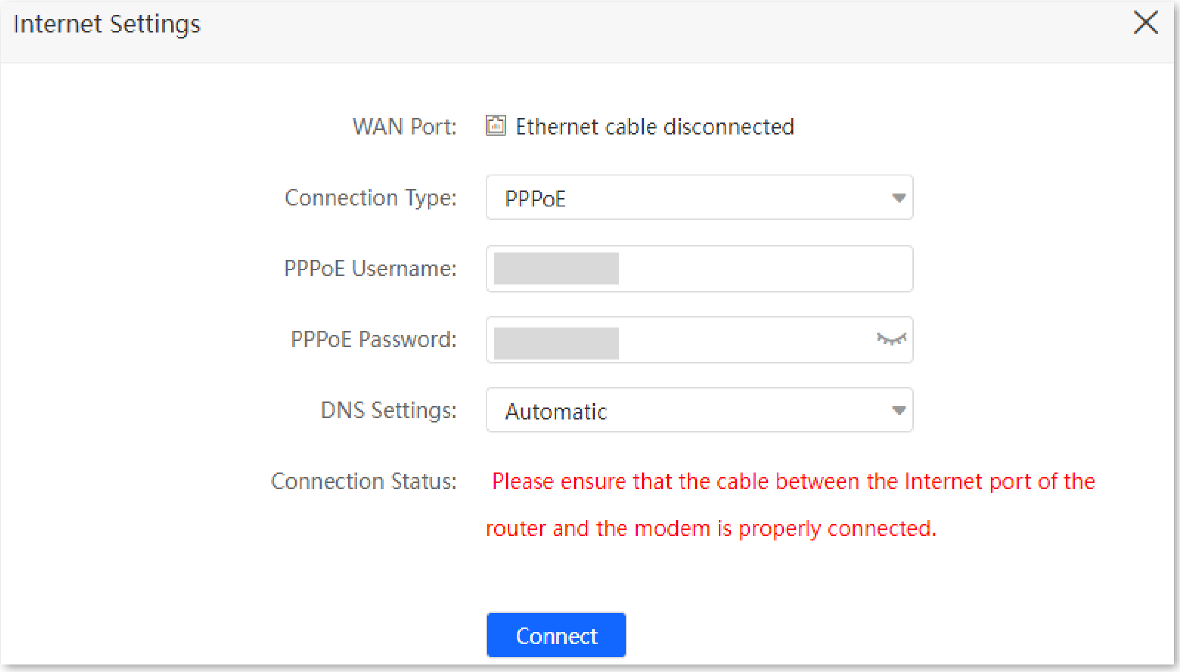
When the **Internet** and **DS-3WR4G12C** is connected as shown below, the router is connected to the internet successfully and you can access the internet via the router.



When a red cross and "Connection failed." are shown between the **Internet** and the **DS-3WR4G12C**, it indicates that the internet connection is abnormal. Please click Connection failed. to choose the **Internet Settings** page and refer to the following scenarios and solutions.



When "Please ensure that the cable between the Internet port of the router and the modem is properly connected" is shown on the page, ensure that the Ethernet cable between the WAN/LAN port of the router and the modem is connected properly. If the problem persists, contact the technical support for help.



Internet Settings

WAN Port: Ethernet cable disconnected

Connection Type: PPPoE

PPPoE Username: [redacted]

PPPoE Password: [redacted]

DNS Settings: Automatic

Connection Status: Please ensure that the cable between the Internet port of the router and the modem is properly connected.

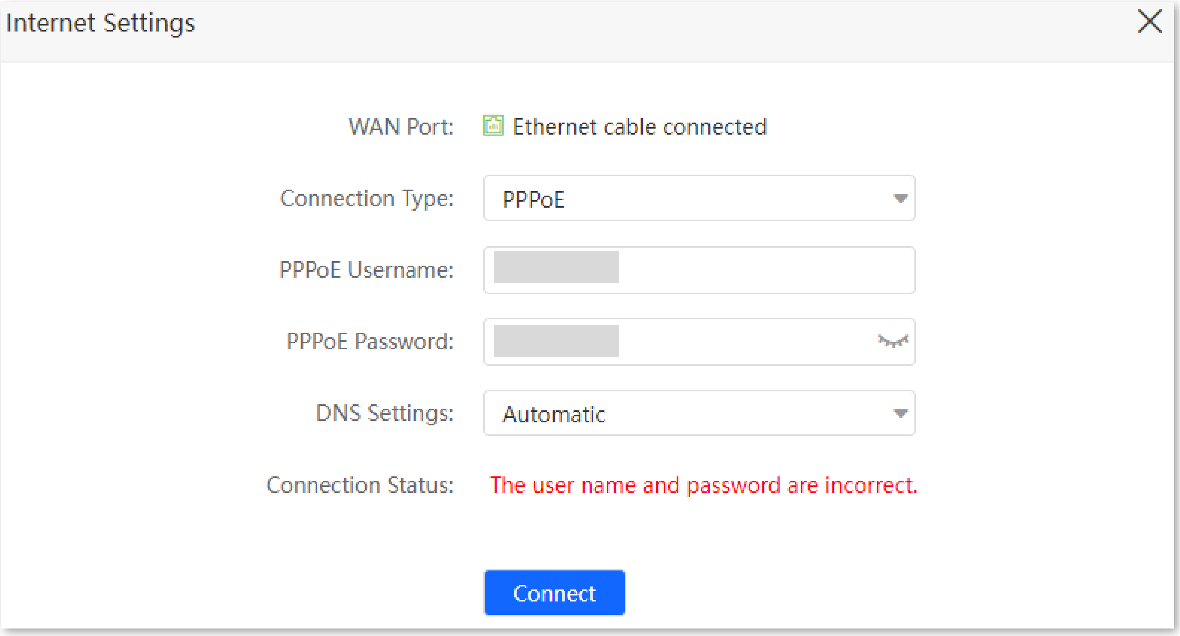
When “The user name and password are incorrect.” is shown on the page, it indicates that the user name and password you entered are incorrect. Please re-enter the user name and password.

Note

Please consider the following tips when entering the user name and password:

- Pay attention to case sensitivity, such as “Z” and “z”.
- Pay attention to the difference between similar letters and numbers, such as “I” and “1”.
- Ensure the completeness of account parameters, such as “0755000513@163.gd”, not “0755000513”.
- If the user name and password are correct, but the problem persists, try change the MAC address of the WAN port. Refer to details in Change the MAC address of the WAN port.

If the problem persists, contact your ISP for help.



Internet Settings

WAN Port: Ethernet cable connected

Connection Type: PPPoE

PPPoE Username: [redacted]

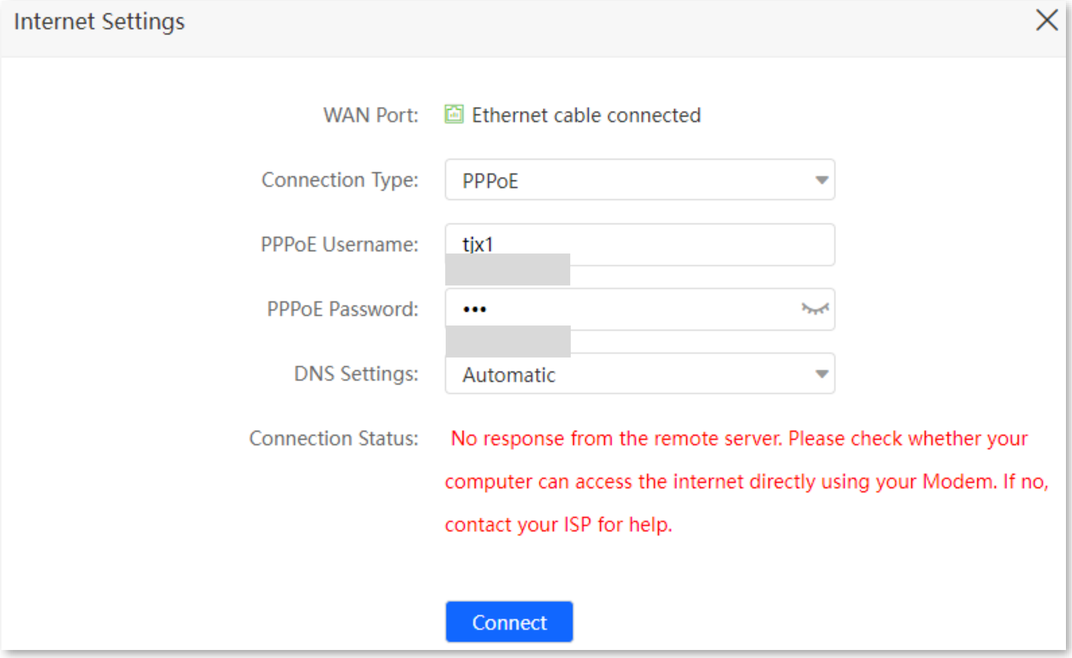
PPPoE Password: [redacted]

DNS Settings: Automatic

Connection Status: The user name and password are incorrect.

When “No response from the remote server. Please check whether your computer can access the internet directly using your Modem. If no, contact your ISP for help.” is shown on the page as below, try the following methods:

- Ensure that you choose the proper connection type. Contact your ISP for any doubt about the connection type.
- Power off the router for several minutes, then power it on and try again.
- Change the MAC address of the WAN port. Refer to details in Change the MAC address of the WAN port.
- If the problem persists, contact your ISP for help.



Internet Settings

WAN Port: Ethernet cable connected

Connection Type: PPPoE

PPPoE Username: tjx1 [redacted]

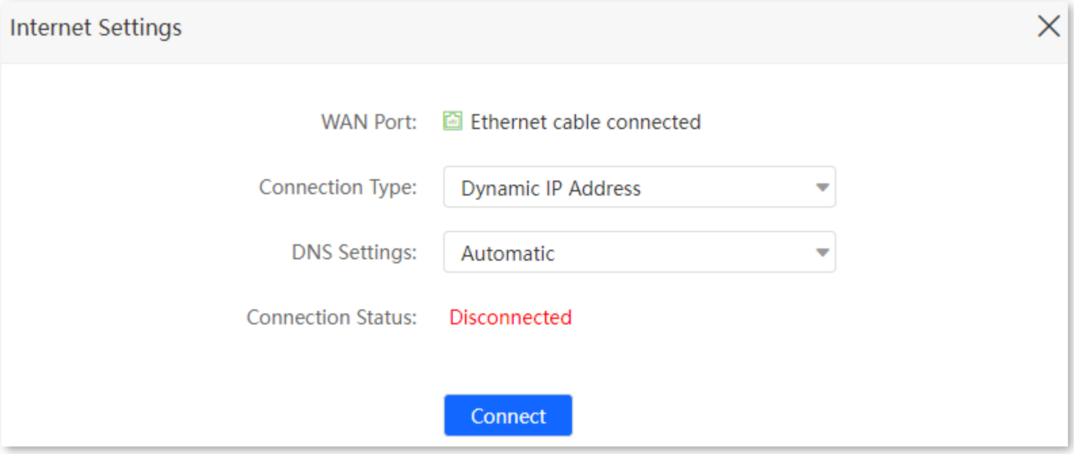
PPPoE Password: ••• [redacted]

DNS Settings: Automatic

Connection Status: No response from the remote server. Please check whether your computer can access the internet directly using your Modem. If no, contact your ISP for help.

When “Disconnected” is shown on the page as below, try the following methods:

- Modify the MAC address of WAN port by referring to Change the MAC address of the WAN port.
- Use another device to configure the router.
- Ensure that your internet service does not expire.
- If the problem persists, contact Hikvision technical support.



Internet Settings

WAN Port: Ethernet cable connected

Connection Type: Dynamic IP Address

DNS Settings: Automatic

Connection Status: Disconnected

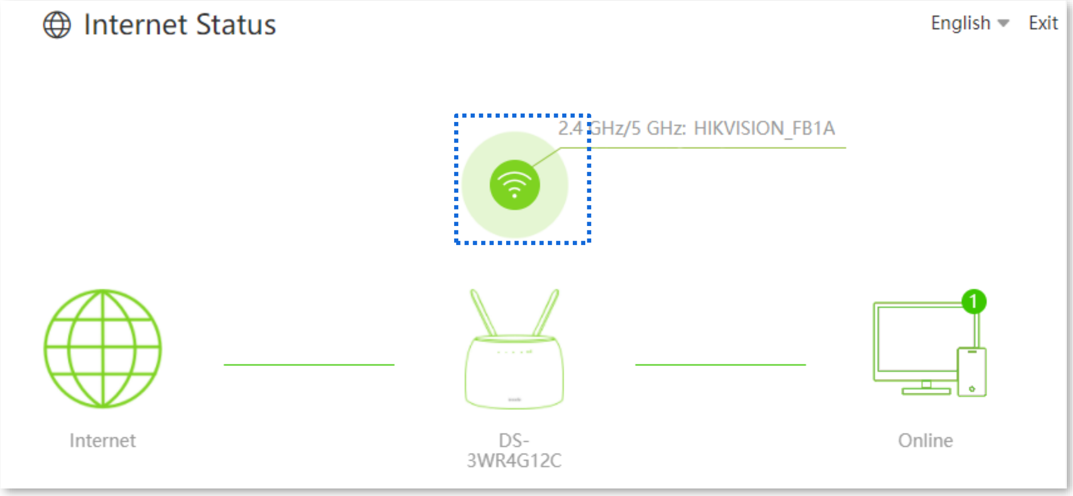
2.2 Wireless information

To view or configure the wireless information:

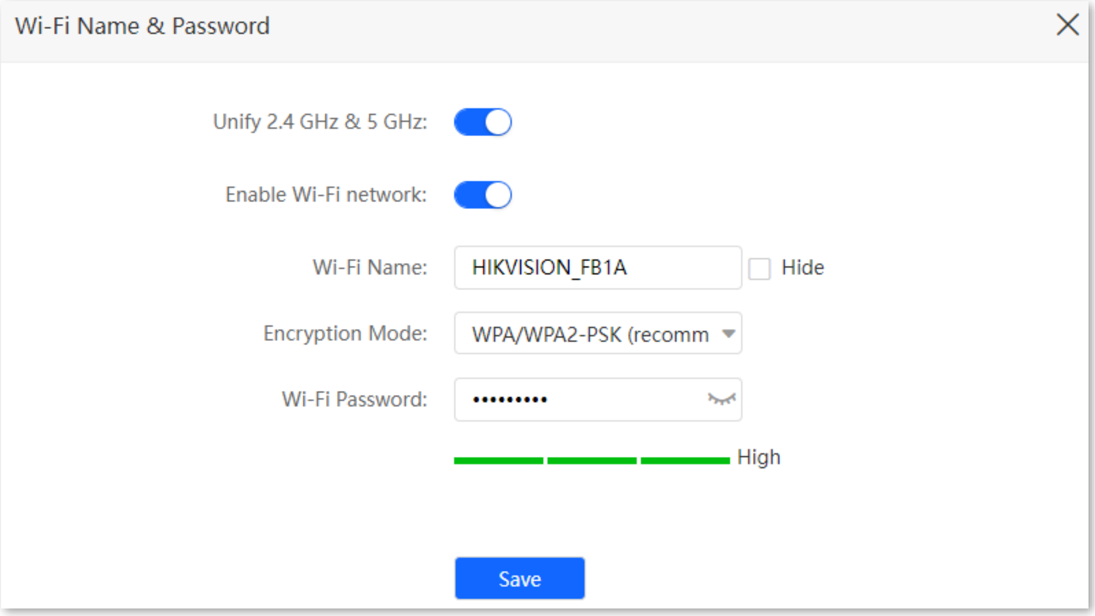
Step 1 Log in to the web UI of the router.

Step 2 Choose **Internet Status**.

Step 3 Click 🛜.



You can change wireless parameters as required.


Wi-Fi Name & Password

Unify 2.4 GHz & 5 GHz: ●

Enable Wi-Fi network: ●

Wi-Fi Name: HIKVISION_FB1A □ Hide

Encryption Mode: WPA/WPA2-PSK (recomm

Wi-Fi Password: •••••••••

High

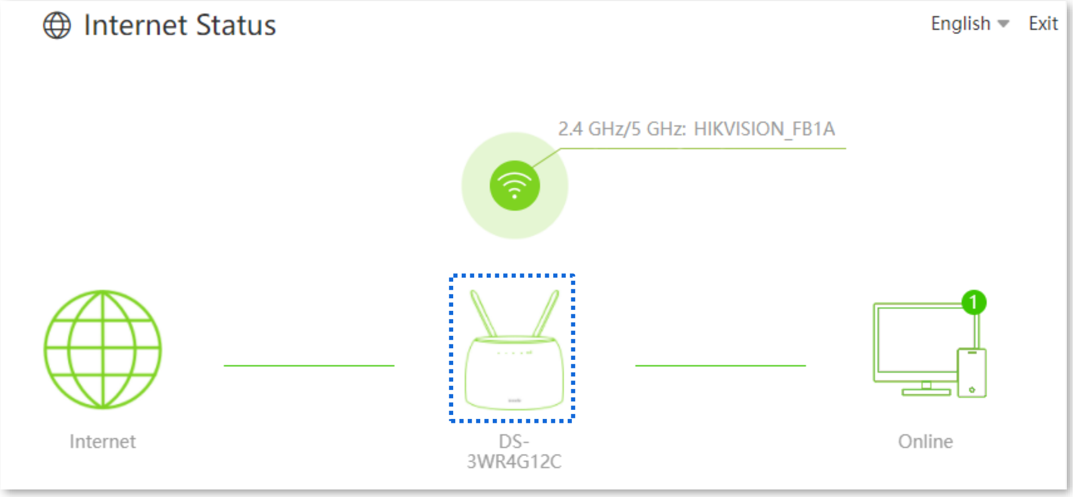
2.3 System information

To view the system information:

Step 1 Log in to the web UI of the router.

Step 2 Choose Internet Status.

Step 3 Click .

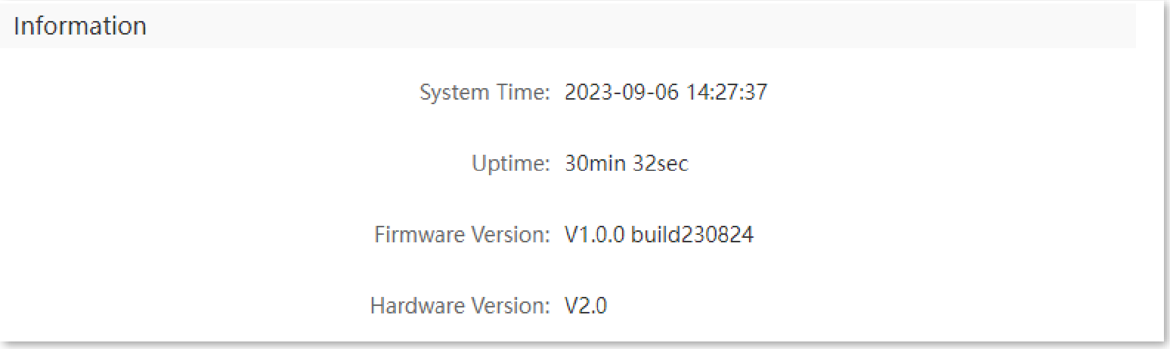


Note

For detailed description of parameters on this page, refer to System status.

2.3.1 Basic information

In this part, you can view the basic information of the router, such as system time, uptime, firmware version and hardware version.



Information

System Time: 2023-09-06 14:27:37

Uptime: 30min 32sec

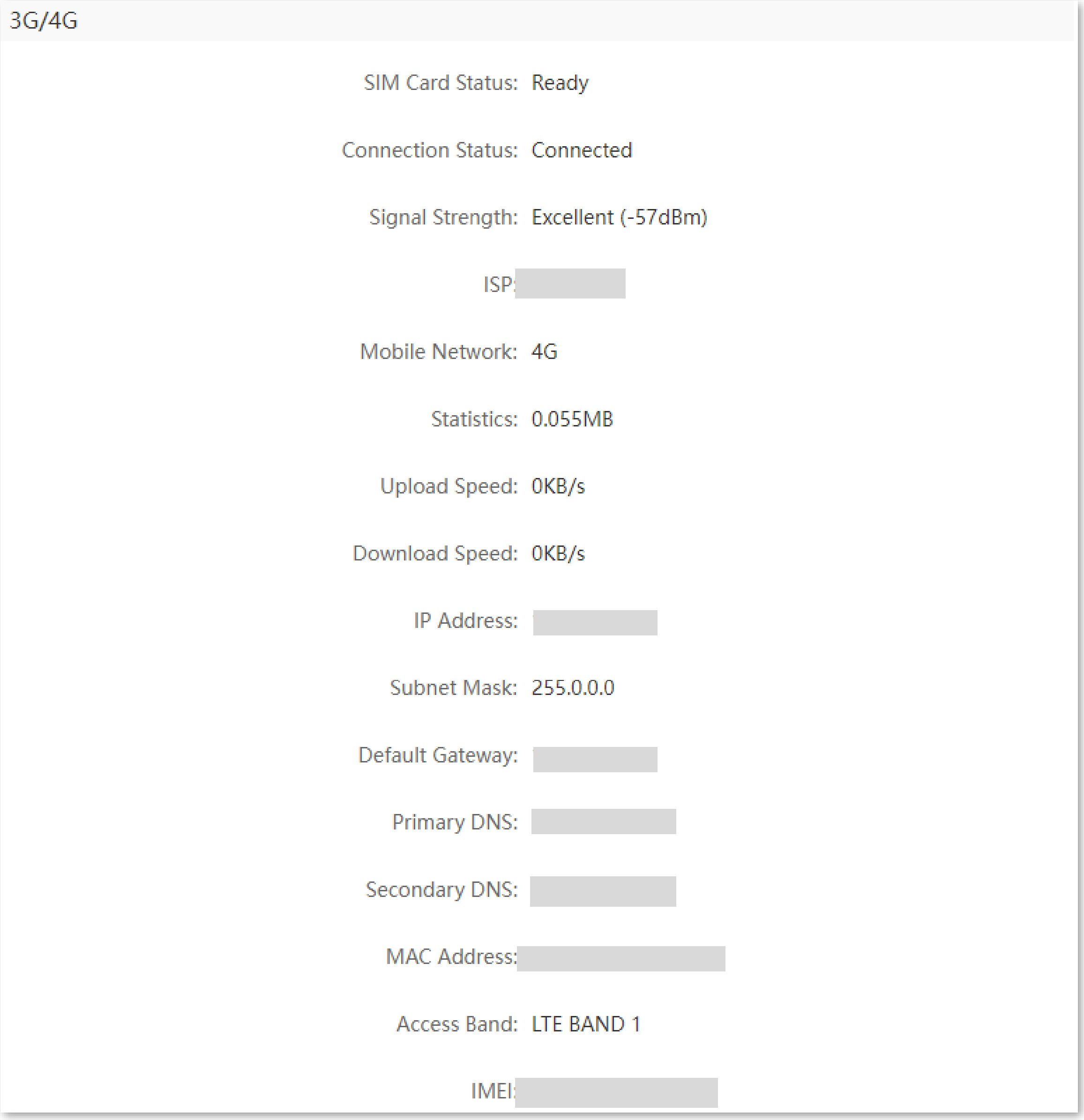
Firmware Version: V1.0.0 build230824

Hardware Version: V2.0

2.3.2 Connection status

3G/4G router mode

Under the 3G/4G router mode, you can view the information of the SIM card and 3G/4G network in this part.



3G/4G

SIM Card Status: Ready

Connection Status: Connected

Signal Strength: Excellent (-57dBm)

ISP: [redacted]

Mobile Network: 4G

Statistics: 0.055MB

Upload Speed: 0KB/s

Download Speed: 0KB/s

IP Address: [redacted]

Subnet Mask: 255.0.0.0

Default Gateway: [redacted]

Primary DNS: [redacted]

Secondary DNS: [redacted]

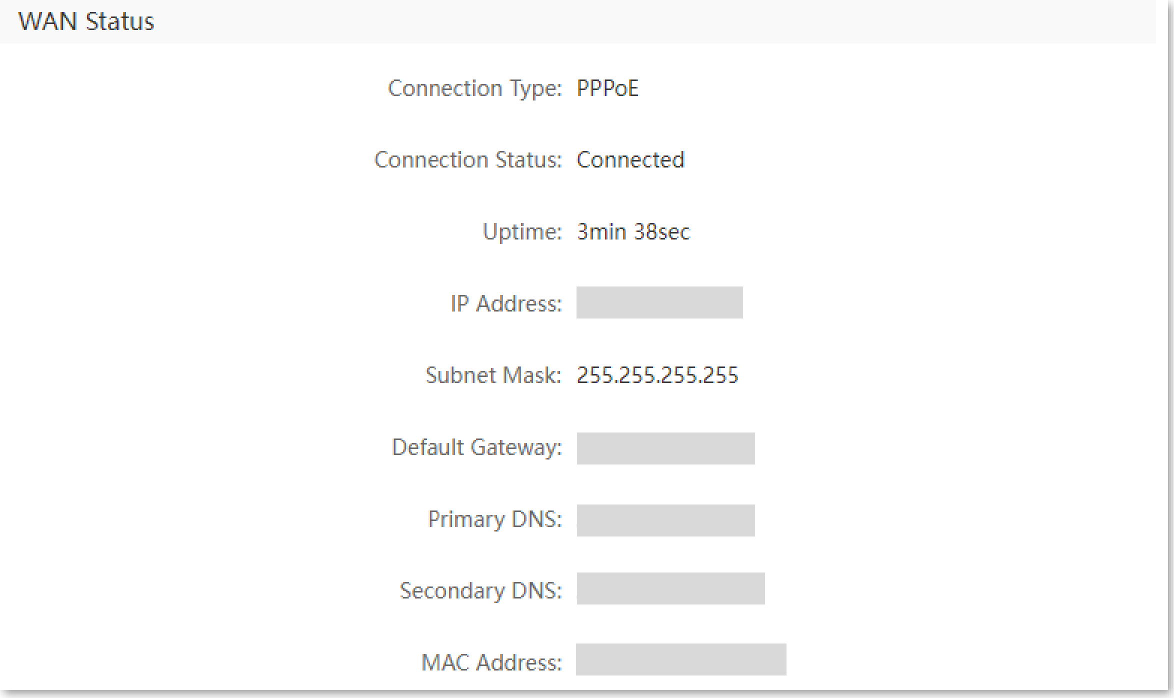
MAC Address: [redacted]

Access Band: LTE BAND 1

IMEI: [redacted]

Wireless router mode

Under the wireless router mode, you can view the information of the WAN port, including connection type, connection status and uptime.



WAN Status

Connection Type: PPPoE

Connection Status: Connected

Uptime: 3min 38sec

IP Address: [redacted]

Subnet Mask: 255.255.255.255

Default Gateway: [redacted]

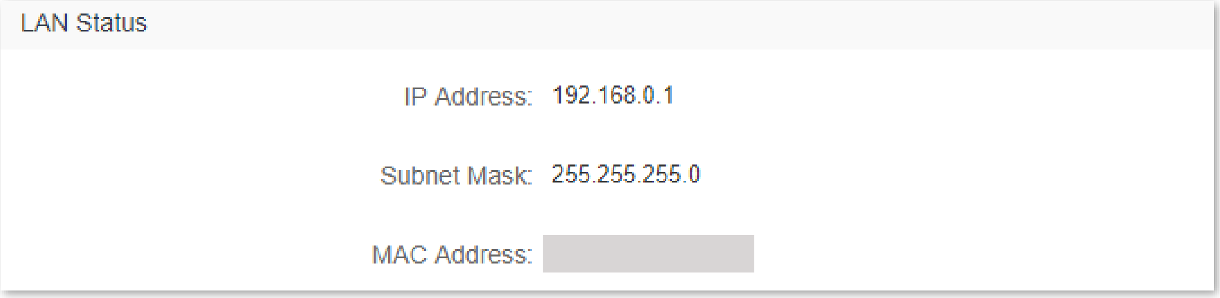
Primary DNS: [redacted]

Secondary DNS: [redacted]

MAC Address: [redacted]

2.3.3 LAN status

In this part, you can view the LAN information, such as LAN IPv4 address, subnet mask and MAC address.



LAN Status

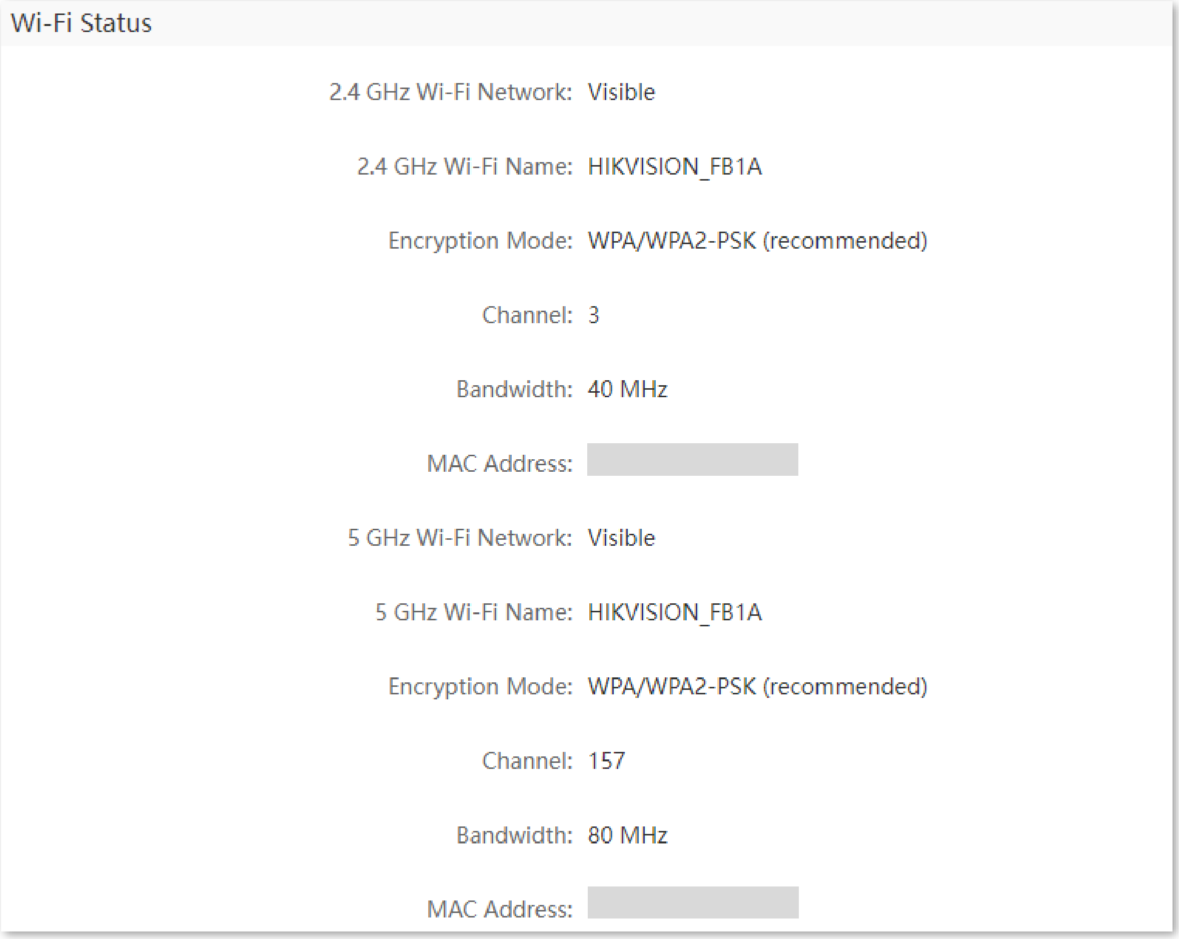
IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

MAC Address: [redacted]

2.3.4 Wi-Fi status

In this part, you can view the information of 2.4 GHz and 5 GHz Wi-Fi networks, including the visibility, Wi-Fi name and encryption mode.



Wi-Fi Status

2.4 GHz Wi-Fi Network: Visible

2.4 GHz Wi-Fi Name: HIKVISION_FB1A

Encryption Mode: WPA/WPA2-PSK (recommended)

Channel: 3

Bandwidth: 40 MHz

MAC Address: [redacted]

5 GHz Wi-Fi Network: Visible

5 GHz Wi-Fi Name: HIKVISION_FB1A

Encryption Mode: WPA/WPA2-PSK (recommended)

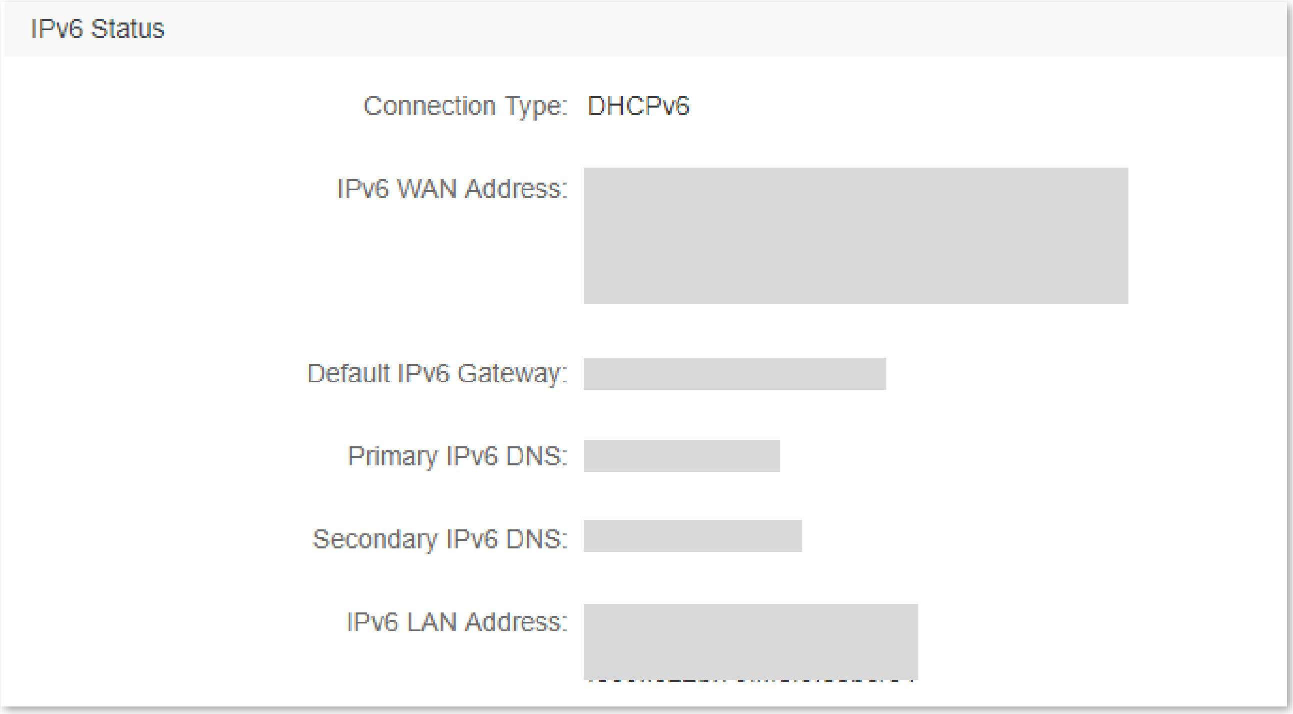
Channel: 157

Bandwidth: 80 MHz

MAC Address: [redacted]

2.3.5 IPv6 status

This part is only displayed when the IPv6 function is enabled. You can view the information of IPv6 connection, including connection type, IPv6 WAN address and IPv6 LAN address.



IPv6 Status

Connection Type: DHCPv6

IPv6 WAN Address: [redacted]

Default IPv6 Gateway: [redacted]

Primary IPv6 DNS: [redacted]

Secondary IPv6 DNS: [redacted]

IPv6 LAN Address: [redacted]

2.4 Online device information

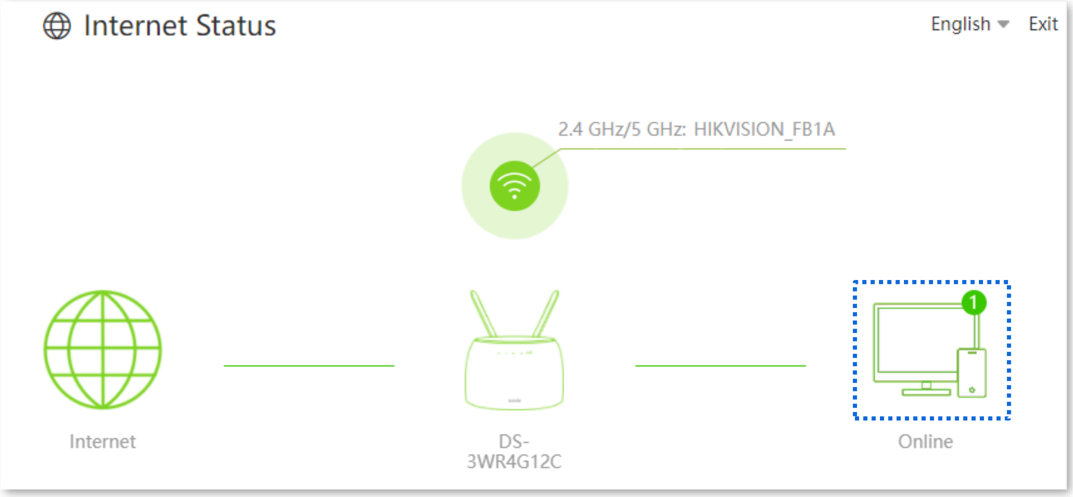
On this page, you can view the information of devices connected to the router, including the upload speed, download speed and access type. You can also view and add devices to the blacklist.

To access the page:

Step 1 Log in to the web UI of the router.

Step 2 Choose **Internet Status**.

Step 3 Click 🖥.

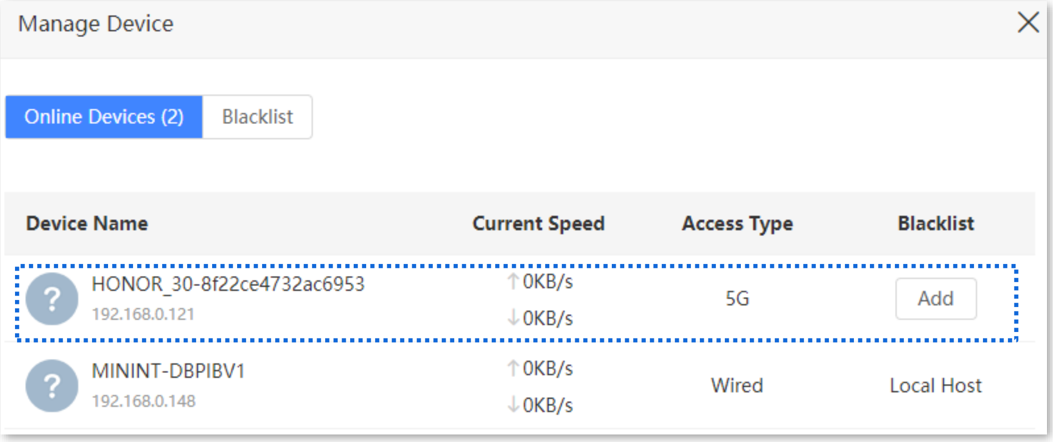


2.4.1 Add devices to the blacklist

Adding devices to the blacklist to block the internet access.

Step 1 Choose **Online Devices**, and target the device to be added.

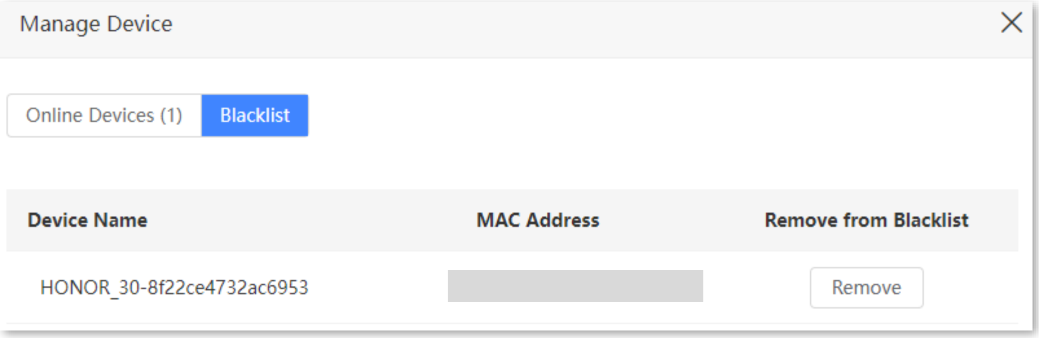
Step 2 Click **Add**.


Manage Device

Online Devices (2) | Blacklist

Device Name	Current Speed	Access Type	Blacklist
HONOR_30-8f22ce4732ac6953 192.168.0.121	↑0KB/s ↓0KB/s	5G	Add
MININT-DBPIBV1 192.168.0.148	↑0KB/s ↓0KB/s	Wired	Local Host

Click **Blacklist**, you can find the device already in the blacklist.



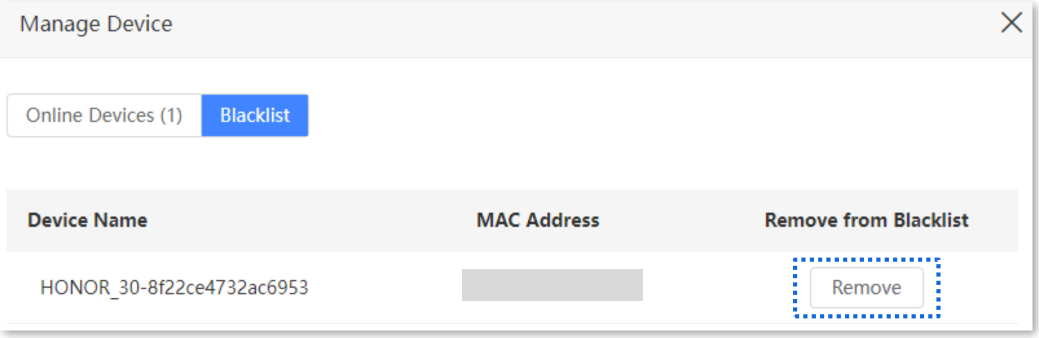
Device Name	MAC Address	Remove from Blacklist
HONOR_30-8f22ce4732ac6953	[redacted]	Remove

2.4.2 Remove devices from the blacklist

To remove devices from the blacklist:

Step 1 Choose **Blacklist**, and target the device to be removed from the blacklist.

Step 2 Click **Remove**.



Device Name	MAC Address	Remove from Blacklist
HONOR_30-8f22ce4732ac6953	[redacted]	Remove

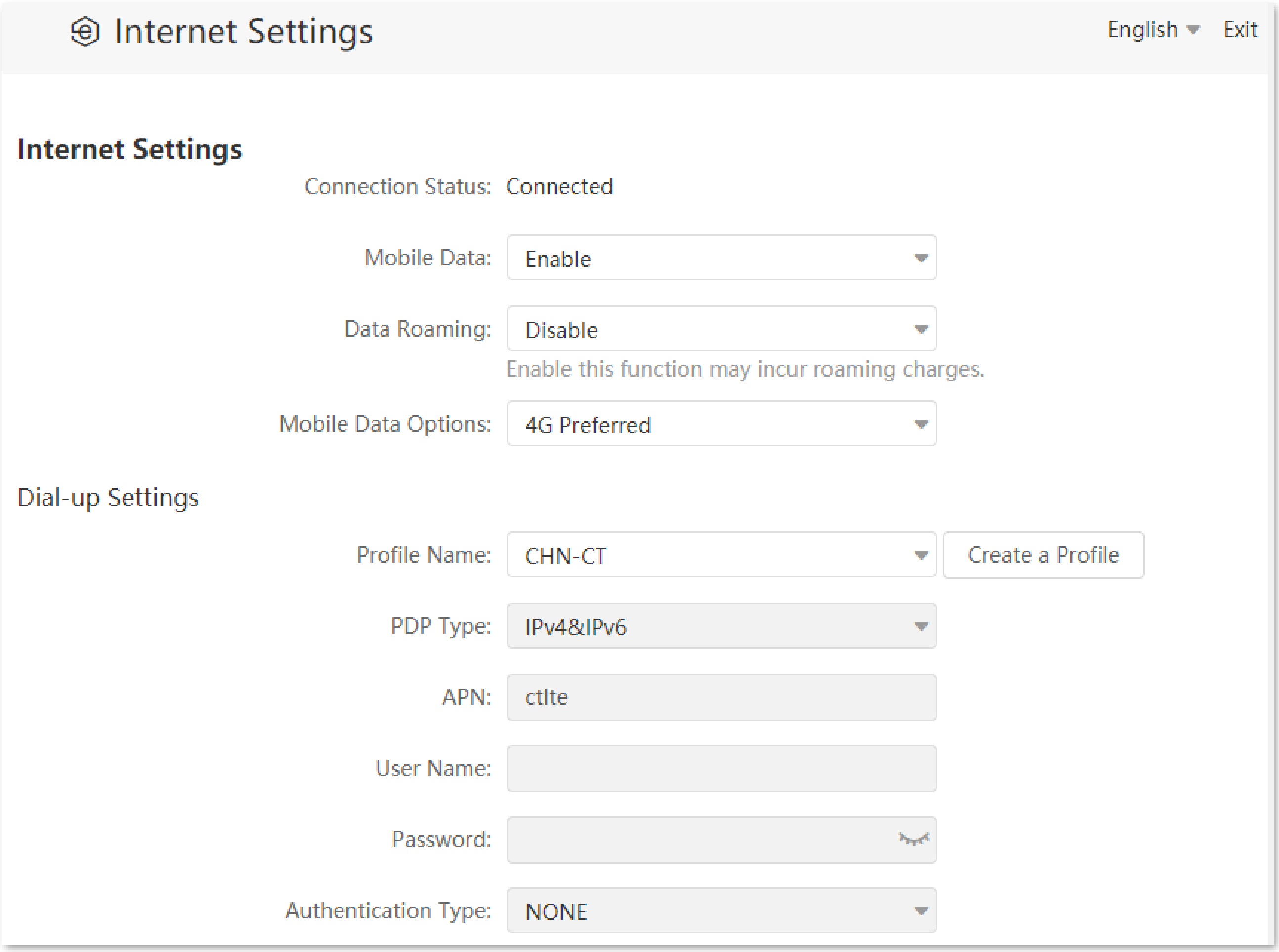
Chapter 3 Internet settings

By configuring the internet settings, you can achieve the shared internet access (IPv4) for multiple users within the LAN. The router supports accessing the internet under both 3G/4G router mode and wireless router mode, and the configuring procedures differ.

3.1 Access the internet with a SIM card

If you are configuring the router for the first time or after restoring it to factory settings, refer to the quick installation guide to configure the internet access. After then, you can change the internet settings by following instructions here.

To access the configuration page, Log in to the web UI of the router, and choose **Internet Settings**.



Internet Settings

Internet Settings

Connection Status: Connected

Mobile Data: Enable

Data Roaming: Disable

Enable this function may incur roaming charges.

Mobile Data Options: 4G Preferred

Dial-up Settings

Profile Name: CHN-CT

PDP Type: IPv4&IPv6

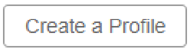
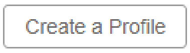
APN: ctlte

User Name:

Password:

Authentication Type: NONE

Table 3-1 Parameter description

Parameter	Description
Connection Status	It specifies the internet connection status of the SIM card.
Mobile Data	It is used to enable or disable the mobile data traffic. When it is disabled, you cannot access the internet through the router.
Data Roaming	It is used to enable or disable data roaming for the SIM card inserted in the router. Data roaming means the data usage produced when you are outside the coverage of your ISP. You can disable data roaming to avoid roaming data usage and charges.
Mobile Data Options	It specifies the mobile network type for internet access.
Profile Name	Generally, all these parameters are predefined in the SIM card. The router will identify these parameters automatically, which cannot be changed, and use them for dial-up. If the router fails to identify these parameters of your SIM card, you must enter them manually by clicking  Create a Profile and dial up for internet access. **Note** If the router cannot identify these parameters, contact your ISP for them.
PDP Type	
APN	
User Name	
Password	
Authentication Type	
 Create a Profile	It is used to create an APN dial-up profile when the router fails to identify these parameters automatically.

3.1.2 Change mobile network preference

When you are already able to access the internet with a SIM card, you can also change the preference towards mobile data, data roaming and preferred network type.

Assume that you are using the router outside the coverage of the ISP of your SIM card and want to use 4G network only.

Configuring procedure:

Step 1 Log in to the web UI of the router.

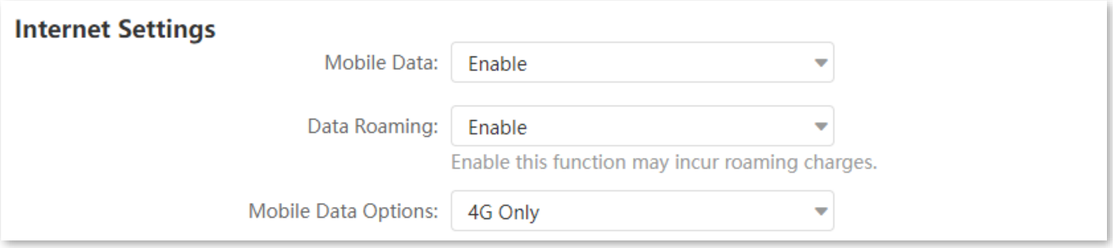
Step 2 Choose **Internet Settings**.

Step 3 Set **Mobile Data** to **Enable**.

Step 4 Set **Data Roaming** to **Enable**.

Step 5 Set **Mobile Data Option** to **4G Only**.

Step 6 Click **Connect** at the bottom.



Internet Settings

Mobile Data: Enable

Data Roaming: Enable

Enable this function may incur roaming charges.

Mobile Data Options: 4G Only

After the configuration, refresh the configuration page. When the **Connected** is shown in **Connection Status,** you can use the 4G network only to access the internet outside the coverage of your ISP.

3.1.3 Create an APN profile manually to access the internet

If the router cannot identify APN parameters automatically and access the internet, you can add a new APN profile manually for dial-up. Contact your ISP for these parameters.

Configuring procedure:

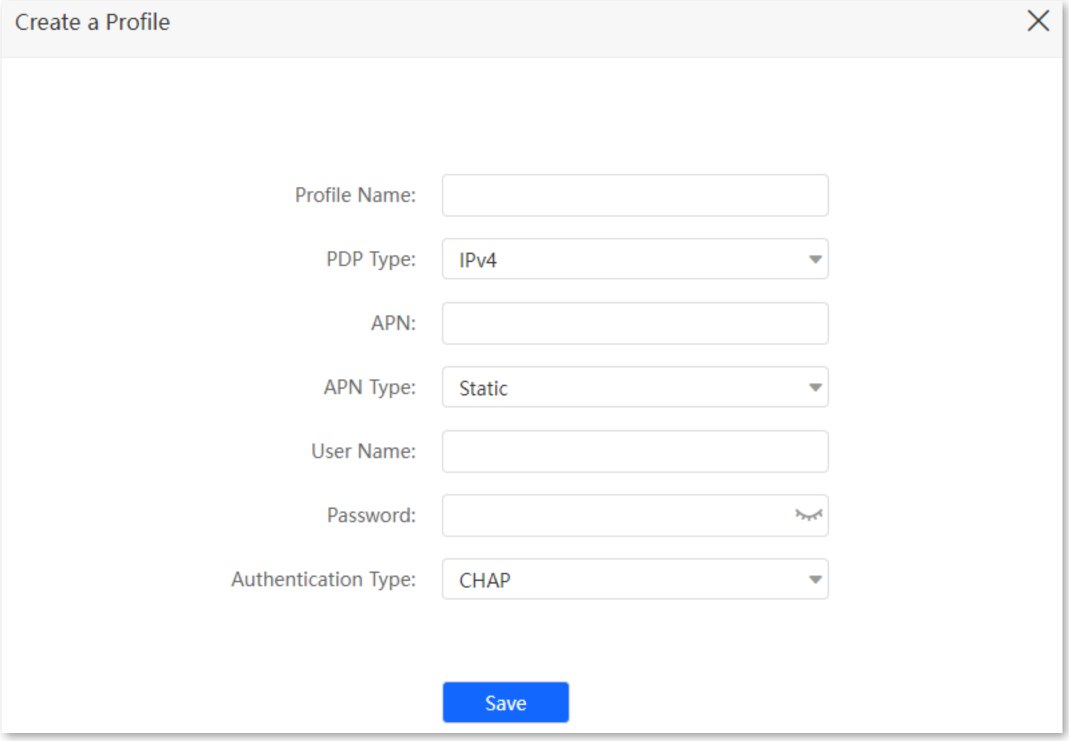
Step 1 Log in to the web UI of the router.

Step 2 Choose **Internet Settings**.

Step 3 Click Create a Profile .

Step 4 Enter required parameters inquired from your ISP.

Step 5 Click **Save**.



Create a Profile

Profile Name:

PDP Type: IPv4

APN:

APN Type: Static

User Name:

Password:

Authentication Type: CHAP

Wait a moment; the router will use the parameters you entered to dial up for internet access. When **Connected** is shown in **Connection Status,** you can access the internet with the APN profile you create.

3.2 Access the internet through the WAN port

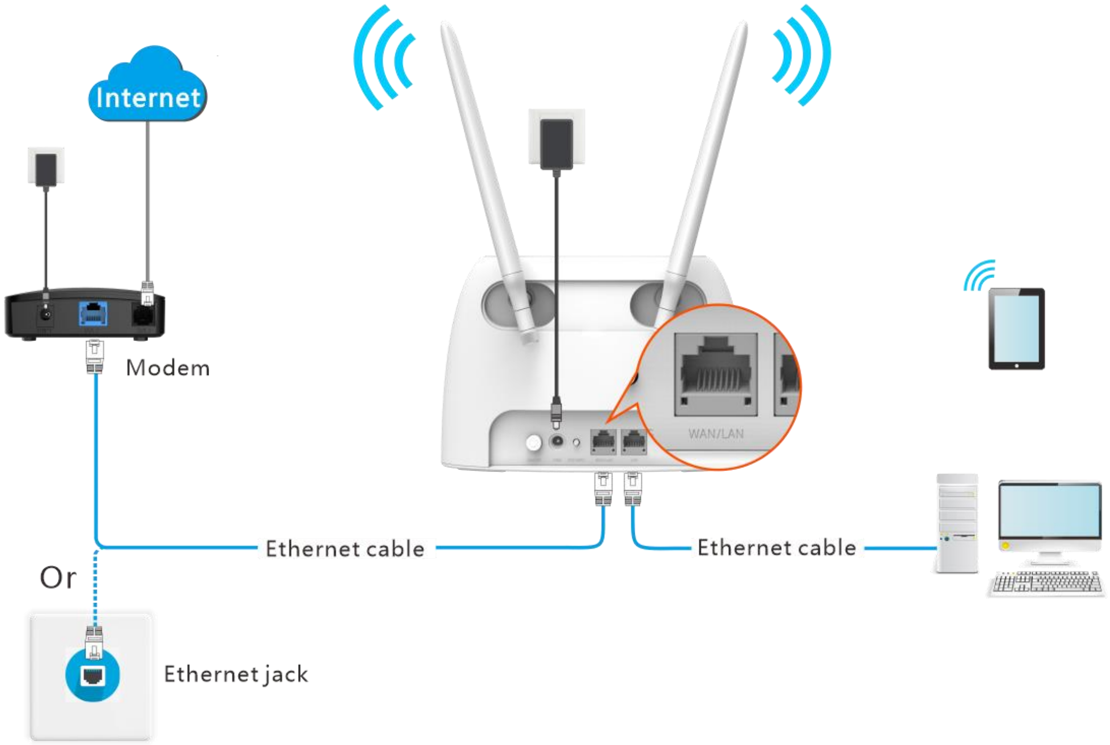
If you want to connect your broadband to the router to access the internet, you can set the router to wireless router mode (refer to Operating mode) and access the internet through the WAN port.

Note

Parameters for accessing the internet are provided by your ISP. Contact your ISP for any doubt.

3.2.1 Access the internet with a PPPoE account

If the ISP provides you with PPPoE user name and password, you can choose this connection type to access the internet. The application scenario is shown below.



Configuring procedure:

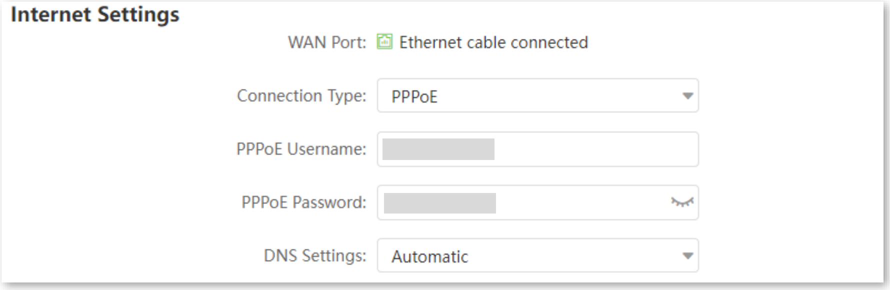
Step 1 Log in to the web UI of the router.

Step 2 Choose **Internet Settings**.

Step 3 Set **Connection Type** to **PPPoE**.

Step 4 Enter the **PPPoE Username** and **PPPoE Password** provided by your ISP.

Step 5 Click **Connect**.



Internet Settings

WAN Port: Ethernet cable connected

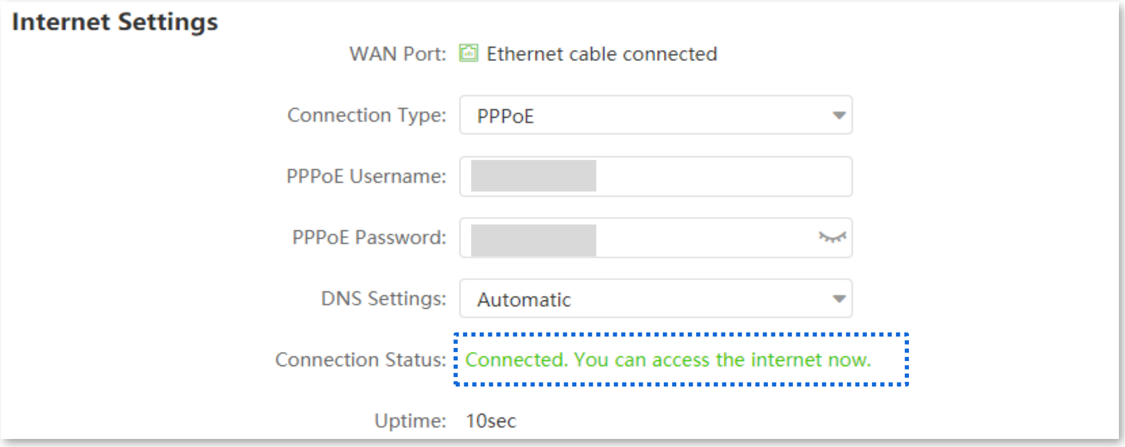
Connection Type: PPPoE

PPPoE Username: [redacted]

PPPoE Password: [redacted]

DNS Settings: Automatic

Wait a moment until the **Connection Status** turns “Connected. You can access the internet now.”, and you can access the internet.



Internet Settings

WAN Port: Ethernet cable connected

Connection Type: PPPoE

PPPoE Username: [redacted]

PPPoE Password: [redacted]

DNS Settings: Automatic

Connection Status: Connected. You can access the internet now.

Uptime: 10sec

Note

If you fail to access the internet, try the following methods:

- If “No response from the remote server. Please check whether your computer can access the internet directly using your Modem. If no, contact your ISP for help.” is shown on the page, you are recommended to choose access the internet through dynamic IP address.
- If the problem persists, refer to View the internet status to find a solution.

Table 3-2 Parameter description

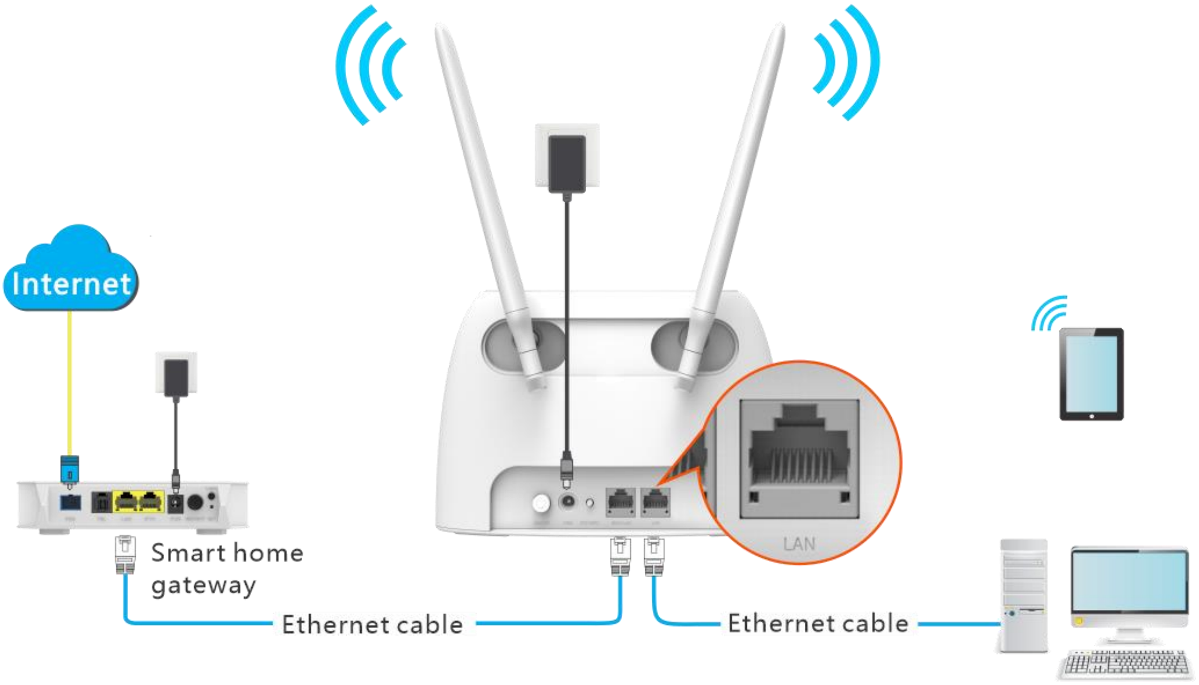
Parameter	**Description**
PPPoE Username	When PPPoE is chosen as the connection type, you need to enter the user name and password provided by your ISP to access the internet.
PPPoE Password	
DNS Settings	It specifies the obtaining method of WAN port DNS address, which is **Automatic** by default. ● **Automatic**: The router obtains a DNS server address from the DHCP server of the upstream network automatically. ● **Manual**: The DNS server address is configured manually.
Connection Status	It specifies the internet connection status. ● When "Connected. You can access the internet now." is shown here, the router is connected to the internet successfully. ● When other information is shown here, the router fails to connect to the internet. Please take corresponding measures according to the information shown here.
Uptime	It specifies the duration since the router is connected to the internet.

3.2.2 Access the internet through dynamic IP address

Generally, accessing the internet through dynamic IP address is applicable in the following situations:

- Your ISP does not provide PPPoE user name or password, or any information including IP address, subnet mask, default gateway or DNS server.
- You have a router with internet access and want to add a DS-3WR4G12C as the other one.

The application scenario is shown below.



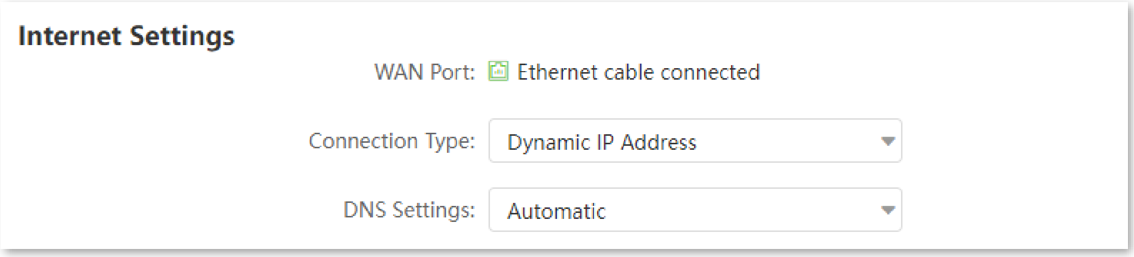
Configuring procedure:

Step 1 Log in to the web UI of the router.

Step 2 Choose **Internet Settings**.

Step 3 Set **Connection Type** to **Dynamic IP Address**.

Step 4 Click **Connect**.



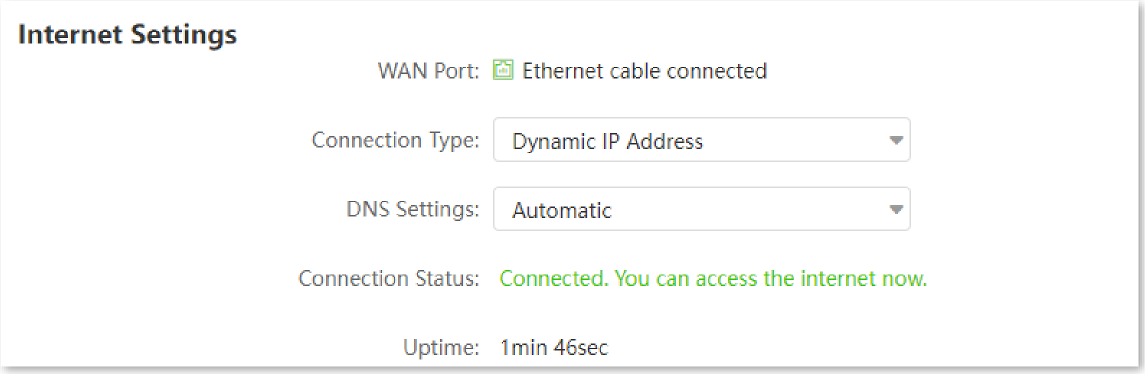
Internet Settings

WAN Port: Ethernet cable connected

Connection Type: Dynamic IP Address

DNS Settings: Automatic

Wait a moment until the **Connection Status** turns "Connected. You can access the internet now.", and you can access the internet.



Internet Settings

WAN Port: Ethernet cable connected

Connection Type: Dynamic IP Address

DNS Settings: Automatic

Connection Status: Connected. You can access the internet now.

Uptime: 1min 46sec

If you fail to access the internet, refer to View the internet status to find a solution.

Table 3-3 Parameter description

Parameter	Description
DNS Settings	It specifies the obtaining method of WAN port DNS address, which is **Automatic** by default. ● **Automatic**: The router obtains a DNS server address from the DHCP server of the upstream network automatically. ● **Manual**: The DNS server address is configured manually.
Connection Status	It specifies the internet connection status. ● When "Connected. You can access the internet now." is shown here, the router is connected to the internet successfully. ● When other information is shown here, the router fails to connect to the internet. Please take corresponding measures according to the information shown here.
Uptime	It specifies the duration since the router is connected to the internet.

3.2.3 Access the internet with static IP address information

When your ISP provides you with information including IP address, subnet mask, default gateway and DNS server, you can choose this connection type to access the internet.

Configuring procedure:

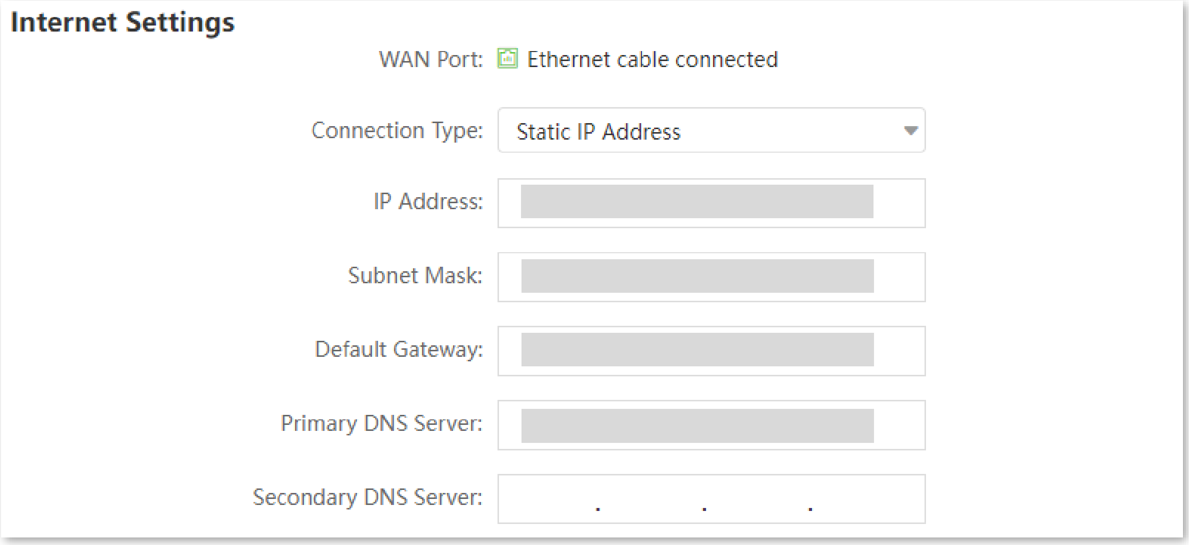
Step 1 Log in to the web UI of the router.

Step 2 Choose **Internet Settings**.

Step 3 Set **Connection Type** to **Static IP Address**.

Step 4 Enter **IP Address**, **Subnet Mask**, **Default Gateway** and **Primary/Secondary DNS Server** provided by your ISP.

Step 5 Click **Connect**.



Internet Settings

WAN Port: Ethernet cable connected

Connection Type: Static IP Address

IP Address:

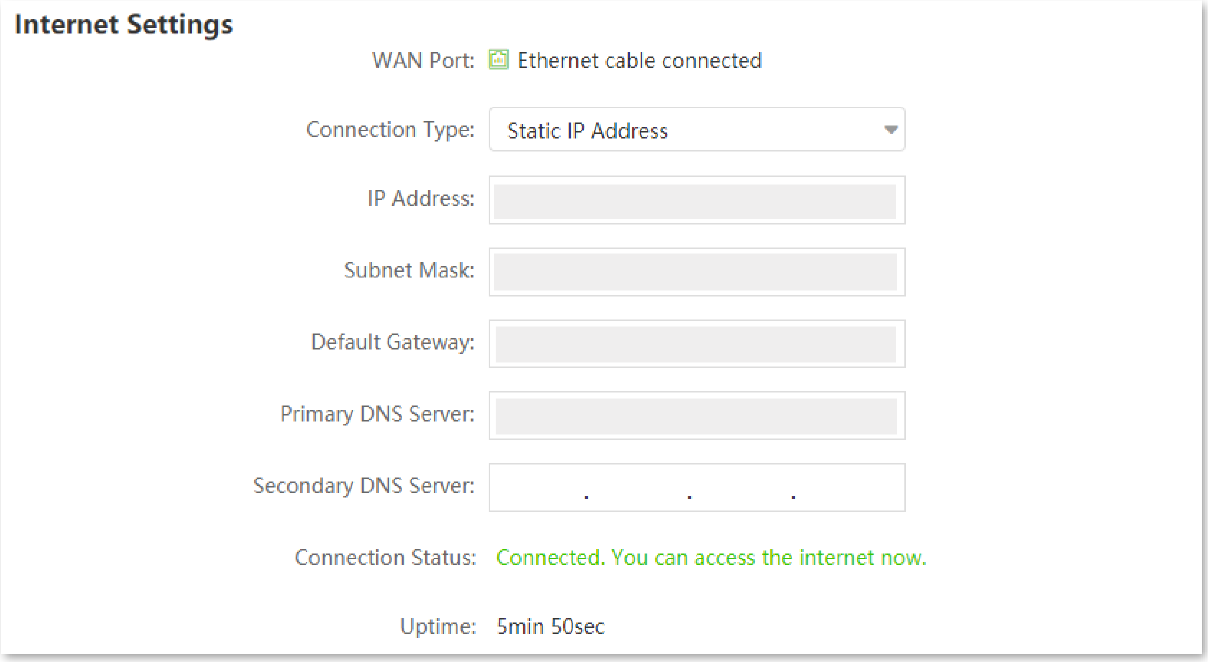
Subnet Mask:

Default Gateway:

Primary DNS Server:

Secondary DNS Server: . . .

Wait a moment until the **Connection Status** turns “Connected. You can access the internet now.”, you can access the internet.



Internet Settings

WAN Port: Ethernet cable connected

Connection Type: Static IP Address

IP Address:

Subnet Mask:

Default Gateway:

Primary DNS Server:

Secondary DNS Server: . . .

Connection Status: Connected. You can access the internet now.

Uptime: 5min 50sec

If you fail to access the internet, refer to refer to View the internet status to find a solution.

Table 3-4 Parameter description

Parameter	Description
IP Address	When static IP address is chosen as the connection type, enter the fixed IP address information provided by your ISP. **Note** If your ISP only provides one DNS server, you can leave the secondary DNS server blank.
Subnet Mask	
Default Gateway	
Primary DNS Server	
Secondary DNS Server	

Parameter	Description
Connection Status	It specifies the internet connection status. ● When “Connected. You can access the internet now.” is shown here, the router is connected to the internet successfully. ● When other information is shown here, the router fails to connect to the internet. Please take corresponding measures according to the information shown here.
Uptime	It specifies the duration since the router is connected to the internet.

3.3 Set failover connection

3.3.1 Overview

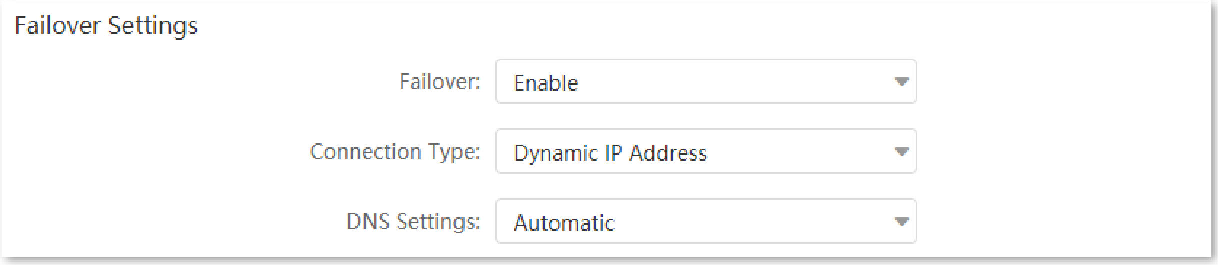
The router can work under either 3G/4G router mode or wireless router mode. By configuring the failover function, you can set parameters of the operating mode other than the current one. If the internet access under the current operating mode fails, the router switches to the other mode automatically, therefore ensuring an uninterrupted internet access for clients under the router.

Note

Before setting the failover function, ensure that you insert a SIM card into the router, and connect the WAN port of the router to the internet at the same time.

To access the configuration page, Log in to the web UI of the router, and choose **Internet Settings**, and find the **Failover Settings** part. This function is disabled by default.

- When the failover function is enabled under the 3G/4G router mode, the page is shown as below. You can configure the failover connection by referring to **Access the internet through the WAN port**.



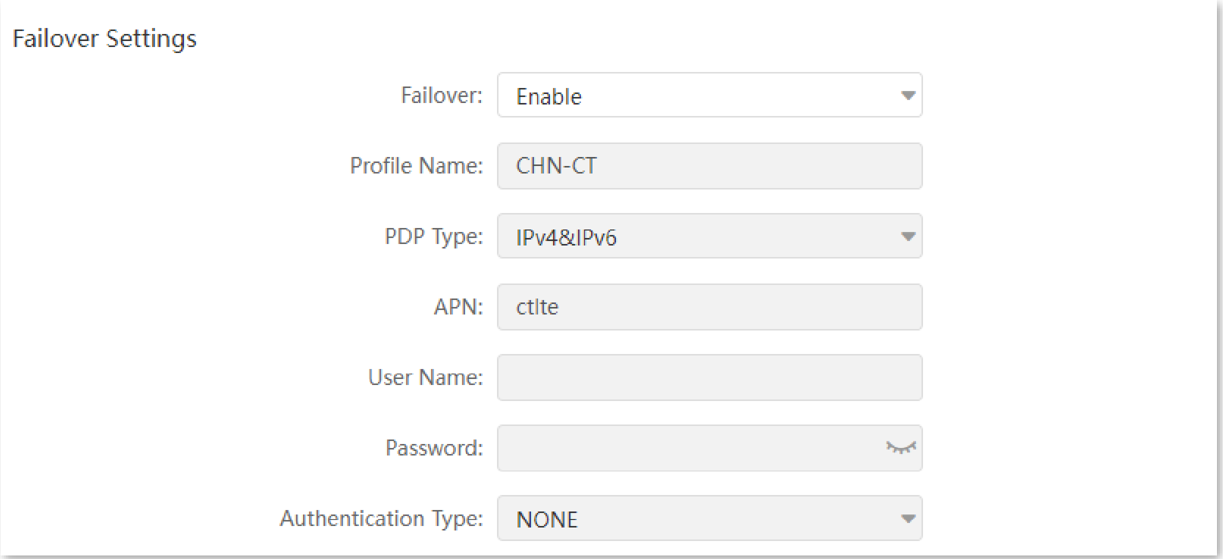
Failover Settings

Failover: Enable

Connection Type: Dynamic IP Address

DNS Settings: Automatic

- When the failover function is enabled under the wireless router mode, the page is shown as below. You can configure the failover connection by referring to **Access the internet with a SIM card**.



Failover Settings

Failover: Enable

Profile Name: CHN-CT

PDP Type: IPv4&IPv6

APN: ctlte

User Name:

Password:

Authentication Type: NONE

3.3.2 Set up failover connection

Scenario: You used to insert a SIM card in the router to access the internet, but you install a smart home gateway after subscribing to the broadband service recently.

Goal: Set the router to access the internet through the broadband, and use the SIM card as backup in case of broadband failure.

Solution: Connect the broadband to the router and insert the SIM card into the router, and configure the failover function.

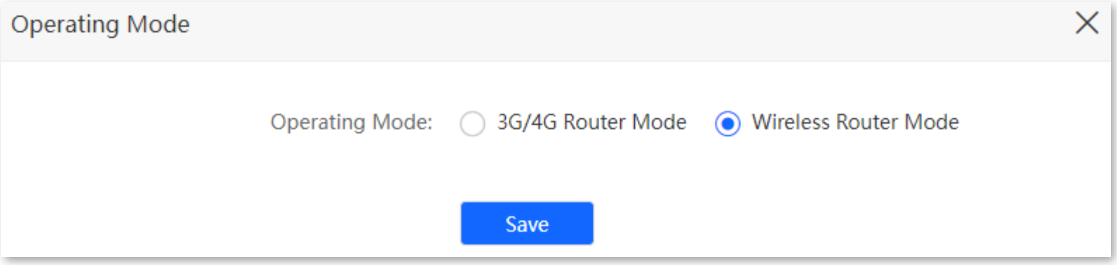
Assume that the ISP provides a PPPoE user name and PPPoE password for setting up internet connection.

Configuring procedures:

Step 1 Log in to the web UI of the router.

Step 2 Change operating mode.

1) Choose **Advanced Settings** > **Operating Mode**.
2) Choose **Wireless Router Mode**, and click **Save**.



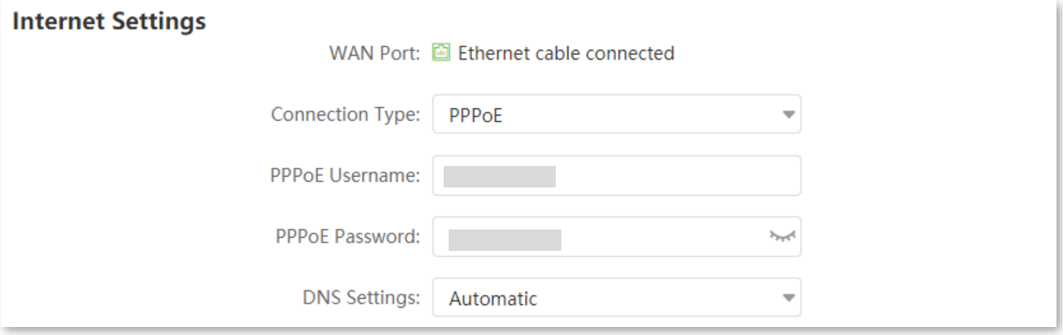
Operating Mode

Operating Mode: ○ 3G/4G Router Mode ● Wireless Router Mode

Wait for the router to reboot to enable the setting.

Step 3 Configure internet access.

1) Connect the **WAN/LAN** port of the router to the LAN port of your smart home gateway.
2) Log in to the web UI of the router, and choose **Internet Settings**.
3) Set **Connection Type** to **PPPoE**, and enter the **PPPoE Username** and **PPPoE Password** provided by your ISP.



Internet Settings

WAN Port: Ethernet cable connected

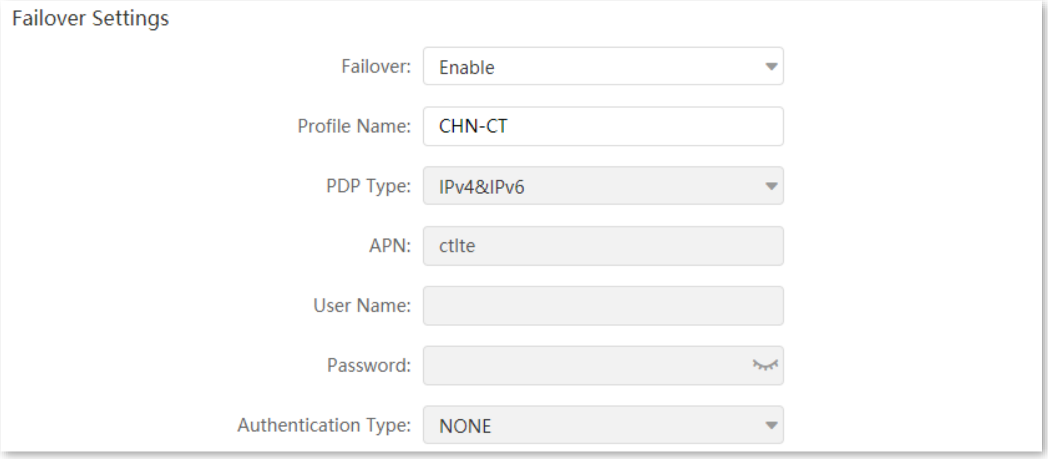
Connection Type: PPPoE

PPPoE Username:

PPPoE Password:

DNS Settings: Automatic

4) Set **Failover** to **Enable**, and the router will fill parameters concerning 3G/4G internet access automatically.



Failover Settings

Failover:	Enable
Profile Name:	CHN-CT
PDP Type:	IPv4&IPv6
APN:	ctlte
User Name:	
Password:	
Authentication Type:	NONE

5) Click **Connect** on the bottom.

When the **Connection Status** turns Connected. You can access the internet now., the router is connected to the internet successfully and you can enjoy uninterrupted internet access guaranteed by both the broadband and SIM card.

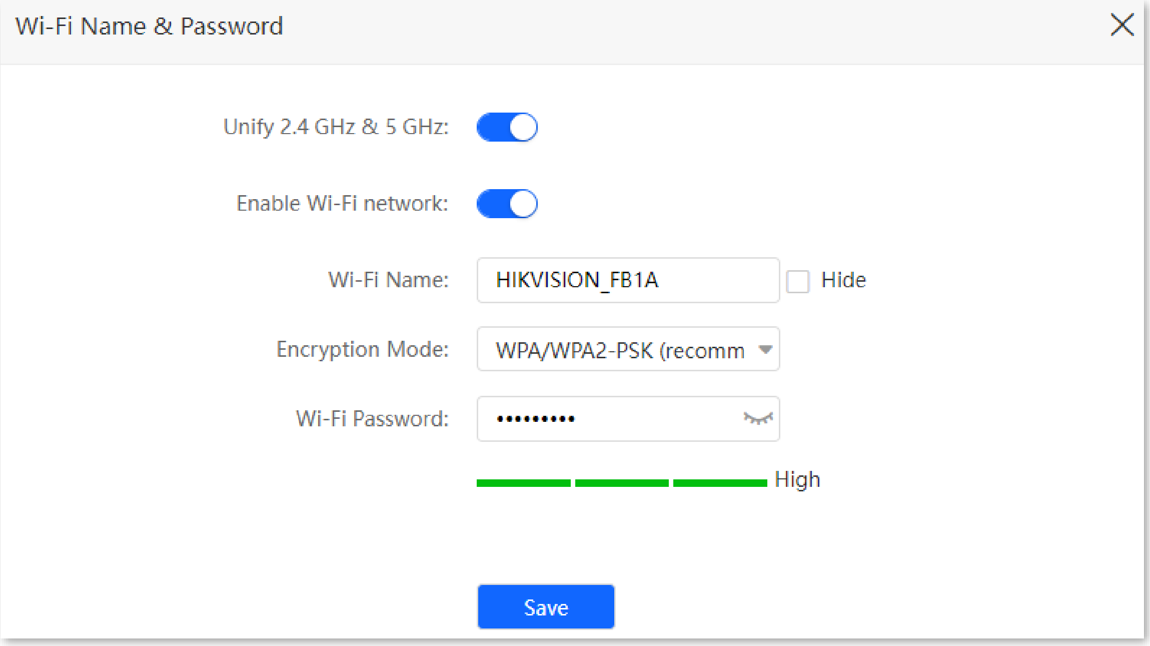
Chapter 4 Wi-Fi settings

4.1 Wi-Fi name & password

4.1.1 Overview

To access the configuration page, Log in to the web UI of the router, and choose **Wi-Fi Settings** > **Wi-Fi Name & Password**.

On this page, you can configure basic Wi-Fi parameters, such as the Wi-Fi name and password.



Wi-Fi Name & Password

Unify 2.4 GHz & 5 GHz: ● on

Enable Wi-Fi network: ● on

Wi-Fi Name: HIKVISION_FB1A □ Hide

Encryption Mode: WPA/WPA2-PSK (recomm

Wi-Fi Password: •••••••••

High

Table 4-1 Parameter description

Parameter	Description
Unify 2.4 GHz & 5 GHz	It is used to enable or disable the Unify 2.4 GHz & 5 GHz function, which is enabled by default. When this function is enabled, the 2.4 GHz and 5 GHz Wi-Fi networks share the same SSID and password. Devices connected to the Wi-Fi network will use the network with better connection quality automatically.
Enable Wi-Fi network	It is used to enable or disable the Wi-Fi networks of the router.
2.4 GHz Network	You can enable or disable the 2.4 GHz network and 5 GHz network separately when the Unify 2.4 GHz & 5 GHz function is disabled. ● If the wireless devices, such as smartphones, are far away from the router, or blocked from the router by a wall, it is recommended to connect to the 2.4 GHz network. ● If the wireless devices are close to the router, it is recommended to connect to the 5 GHz network.
5 GHz Network	

Parameter	Description
Wi-Fi Name	It specifies the Wi-Fi network name (SSID) of the corresponding Wi-Fi network.
Hide	It is used to hide the Wi-Fi name of the Wi-Fi network, to improve the security level of the Wi-Fi network. When this function is enabled, the Wi-Fi network is invisible to wireless devices. You need to enter the Wi-Fi name of the network on your wireless devices (such as a smartphone) manually if you want to join the network.
Encryption Mode	It specifies the encryption modes supported by the router, including: ● **None**: It indicates that the Wi-Fi network is not encrypted and any clients can access the network without a password. This option is not recommended as it leads to low network security. ● **WPA-PSK**: The network is encrypted with WPA-PSK/AES, which has a better compatibility than WPA2-PSK. ● **WPA2-PSK**: The network is encrypted with WPA2-PSK/AES, which has a higher security level than WPA-PSK. ● **WPA/WPA2-PSK (recommended)**: It indicates that WPA-PSK and WPA2-PSK are adopted to encrypt the network, providing both security and compatibility.
Wi-Fi Password	It specifies the password for connecting to the Wi-Fi network. You are strongly recommended to set a Wi-Fi password for security. **Note** It is recommended to use the combination of digits, uppercase letters, lowercase letters, and special symbols in the password to enhance the security of the Wi-Fi network.

4.1.2 Separate the 2.4 GHz Wi-Fi name from 5 GHz Wi-Fi name

The router supports both 2.4 GHz and 5 GHz Wi-Fi networks, which are unified and only one Wi-Fi name is displayed by default. If you want to separate the Wi-Fi names of the two networks, follow the procedures below.

Configuring procedure:

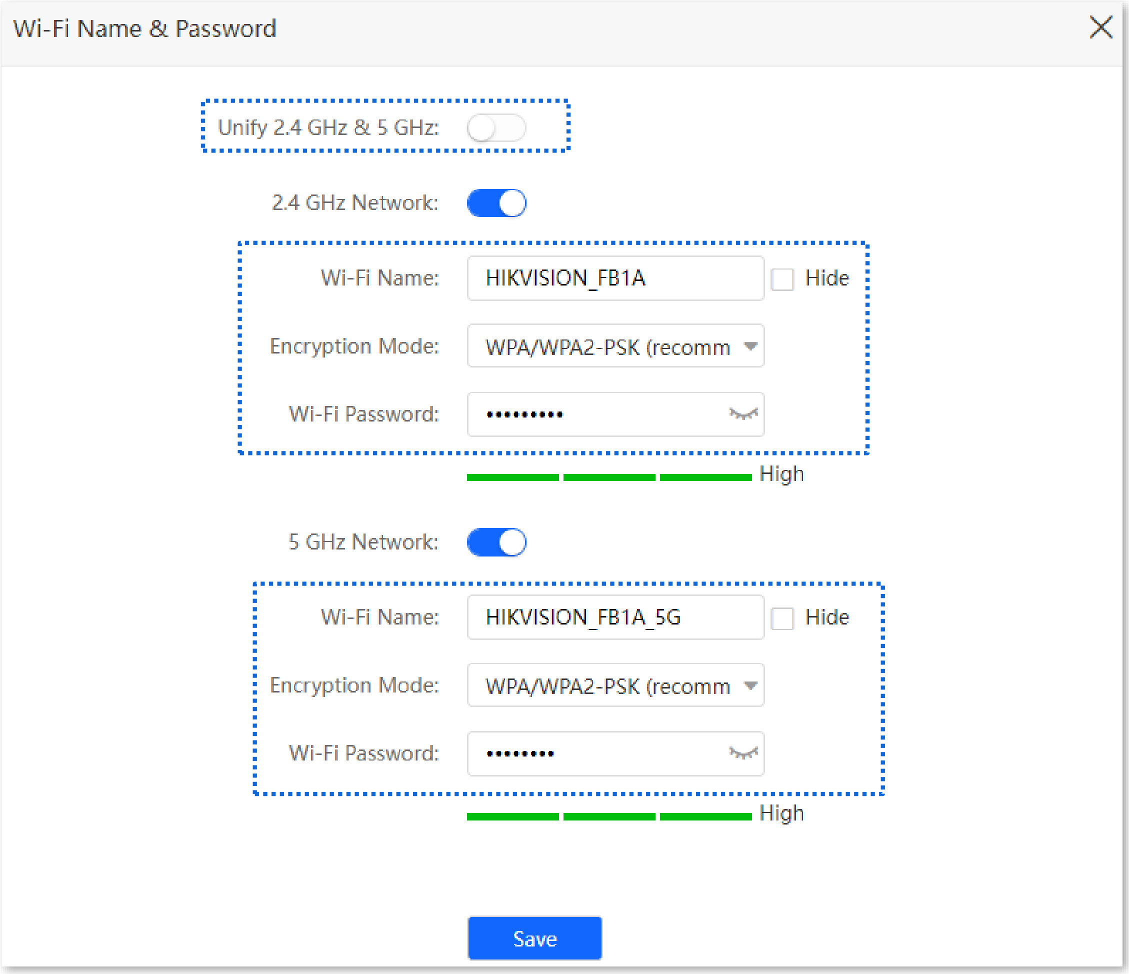
Step 1 Log in to the web UI of the router.

Step 2 Choose **Wi-Fi Settings** > **Wi-Fi Name & Password**.

Step 3 Disable **Unify 2.4 GHz & 5 GHz**.

Step 4 Customize the **Wi-Fi Name** and **Wi-Fi Password** of each Wi-Fi network.

Step 5 Click **Save**.



Wi-Fi Name & Password

Unify 2.4 GHz & 5 GHz: ○

2.4 GHz Network: ●

Wi-Fi Name: HIKVISION_FB1A □ Hide

Encryption Mode: WPA/WPA2-PSK (recomm

Wi-Fi Password: •••••••••

High

5 GHz Network: ●

Wi-Fi Name: HIKVISION_FB1A_5G □ Hide

Encryption Mode: WPA/WPA2-PSK (recomm

Wi-Fi Password: ••••••••

High

When completing the configurations, you can connect to the either the 2.4 GHz or 5 GHz Wi-Fi networks of the router to access the internet.

4.1.3 Change the Wi-Fi name and Wi-Fi password

The router supports both 2.4 GHz and 5 GHz Wi-Fi networks.

Assume that you want to change the 2.4 GHz Wi-Fi name and password to **John_Doe_2.4GHz** and **Hikvision+WiFi24,** and the 5 GHz Wi-Fi name and password to **John_Doe_5GHz** and **Hikvision+WiFi5**. Both networks adopt **WPA/WPA2-PSK (recommended)** as the encryption type.

Configuring procedure:

Step 1 Log in to the web UI of the router.

Step 2 Choose **Wi-Fi Settings** > **Wi-Fi Name & Password**.

Step 3 Disable **Unify 2.4 GHz & 5 GHz**.

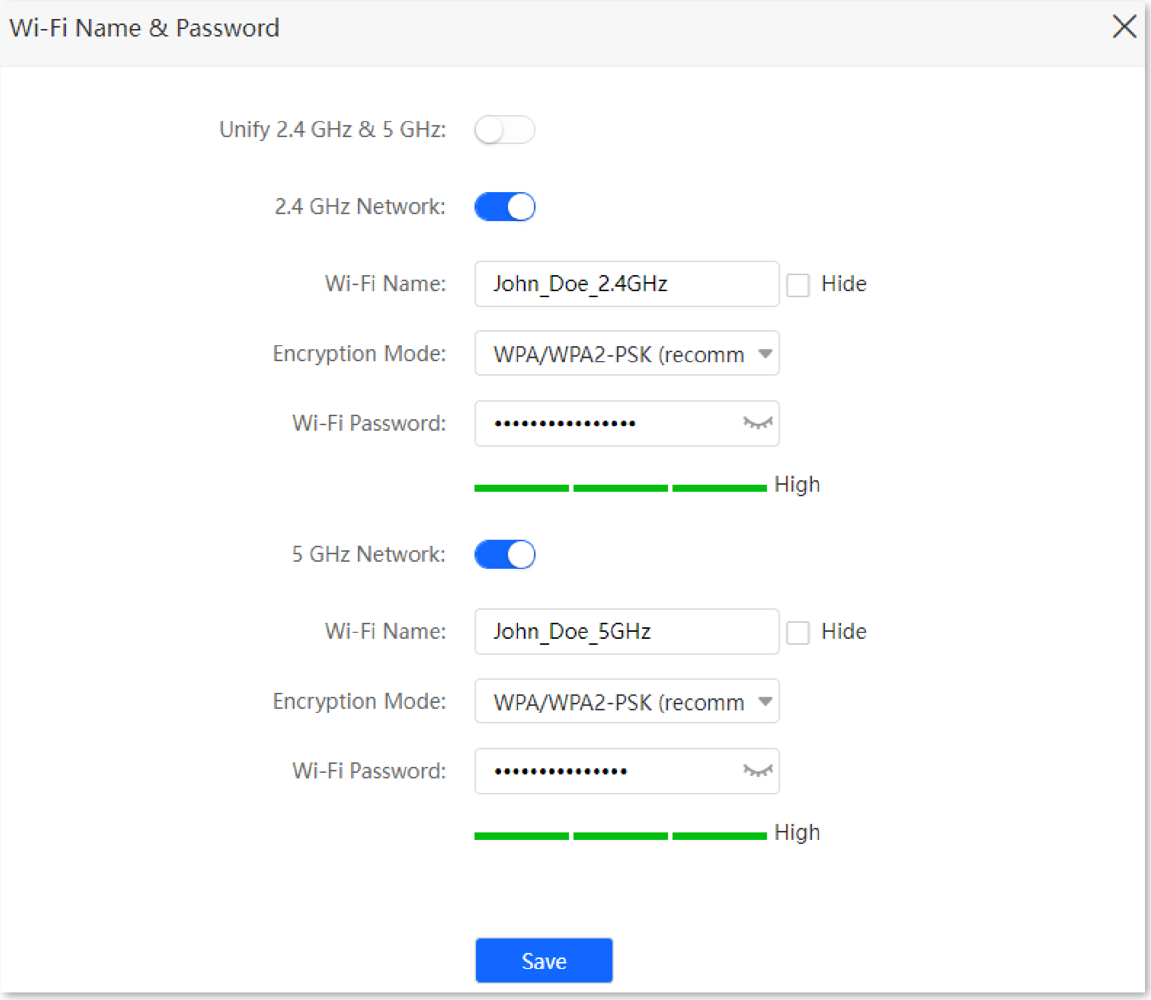
Step 4 Change the parameters of the 2.4 GHz network.

1) Change the **Wi-Fi Name** of the 2.4 GHz network, which is **John_Doe_2.4GHz** in this example.
2) Choose an **Encryption Mode**, which is **WPA/WPA2-PSK (recommended)** in this example.
3) Change the **Wi-Fi Password** of the 2.4 GHz network, which is **Hikvision+WiFi24** in this example.

Step 5 Change the parameters of the 5 GHz network.

1) Change the **Wi-Fi Name** of the 5 GHz network, which is **John_Doe_5GHz** in this example.
2) Choose an **Encryption Mode**, which is **WPA/WPA2-PSK (recommended)** in this example.
3) Change the **Wi-Fi Password** of the 5 GHz network, which is **Hikvision+WiFi5** in this example.

Step 6 Click **Save**.



Wi-Fi Name & Password

Unify 2.4 GHz & 5 GHz: ○

2.4 GHz Network: ●

Wi-Fi Name: John_Doe_2.4GHz □ Hide

Encryption Mode: WPA/WPA2-PSK (recomm

Wi-Fi Password: ••••••••••••••••

High

5 GHz Network: ●

Wi-Fi Name: John_Doe_5GHz □ Hide

Encryption Mode: WPA/WPA2-PSK (recomm

Wi-Fi Password: •••••••••••••••

High

When completing the configurations, you can connect your wireless devices to any Wi-Fi networks of the router to access the internet.

4.1.4 Hide the Wi-Fi network

The hidden Wi-Fi networks are invisible to wireless devices, thus improving the security of the networks.

Configuring procedure:

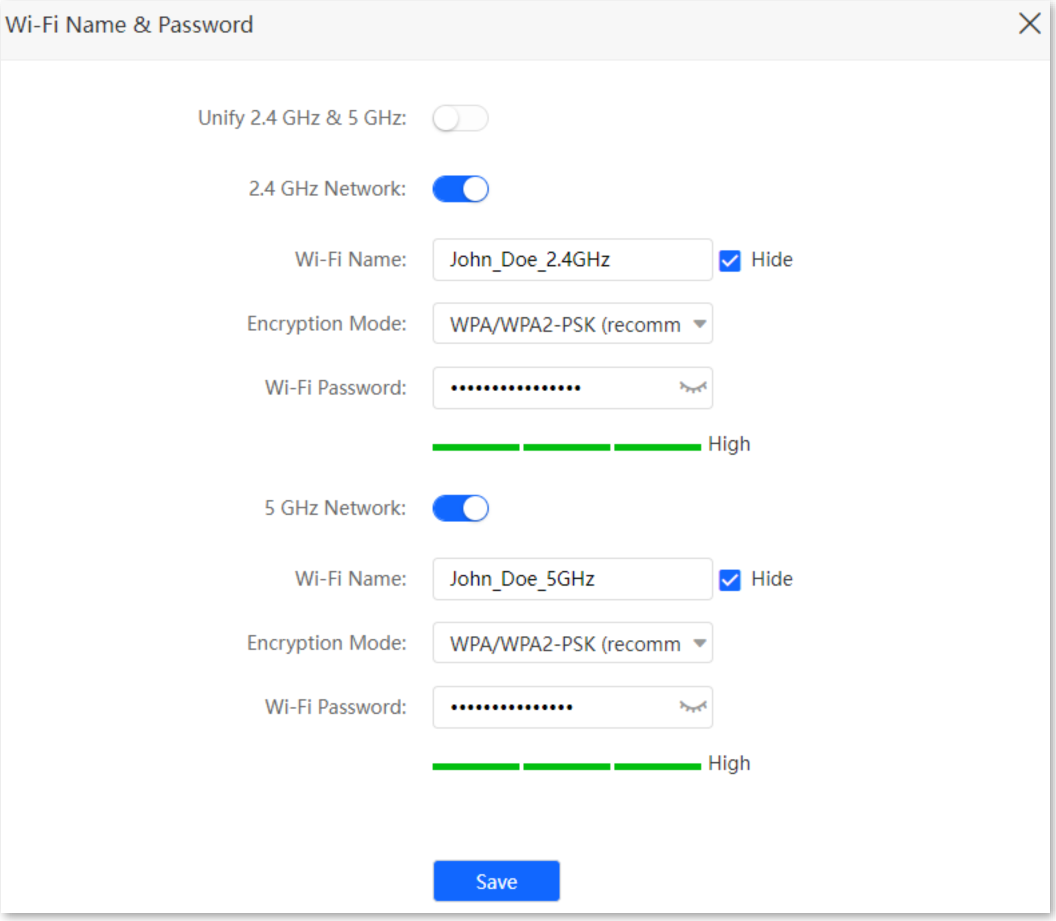
Step 1 Log in to the web UI of the router.

Step 2 Choose **Wi-Fi Settings** > **Wi-Fi Name & Password**.

Step 3 Disable **Unify 2.4 GHz & 5GHz**.

Step 4 Tick **Hide** of the target network.

Step 5 Click **Save**.



Wi-Fi Name & Password

Unify 2.4 GHz & 5 GHz: ○

2.4 GHz Network: ●

Wi-Fi Name: John_Doe_2.4GHz ☑ Hide

Encryption Mode: WPA/WPA2-PSK (recomm

Wi-Fi Password: ••••••••••••••••

High

5 GHz Network: ●

Wi-Fi Name: John_Doe_5GHz ☑ Hide

Encryption Mode: WPA/WPA2-PSK (recomm

Wi-Fi Password: •••••••••••••••

High

When configuration is completed, the corresponding Wi-Fi network name is invisible to wireless devices.

4.1.5 Connect to a hidden Wi-Fi network

When a Wi-Fi network is hidden, you need to enter the Wi-Fi parameters manually and connect to it.

Assume that the Unify 2.4 GHz & 5 GHz function is enabled and the parameters are:

- Wi-Fi name: Jone_Doe
- Encryption type: WPA/WPA2-PSK (recommended)
- Wi-Fi password: Hikvision+WiFi245

Note

If you do not remember the wireless parameters of the Wi-Fi network, Log in to the web UI of the router and choose **Wi-Fi Settings** > **Wi-Fi Name & Password** to find them.

Procedures for connecting to the Wi-Fi network on your wireless device (Example: iPhone):

Step 1 Tap **Settings** on your phone, and choose **WLAN**.

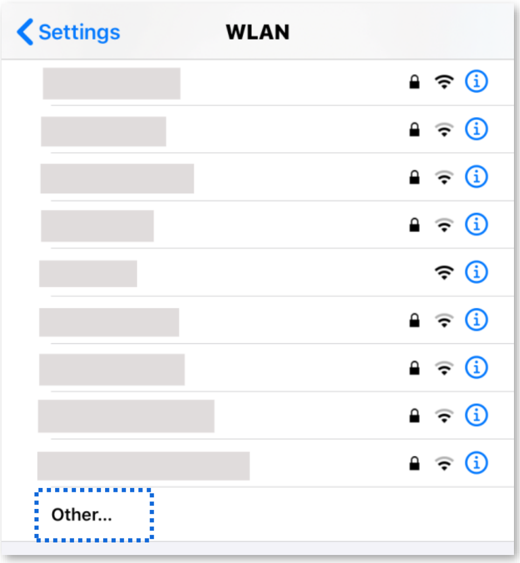
Step 2 Enable **WLAN**.

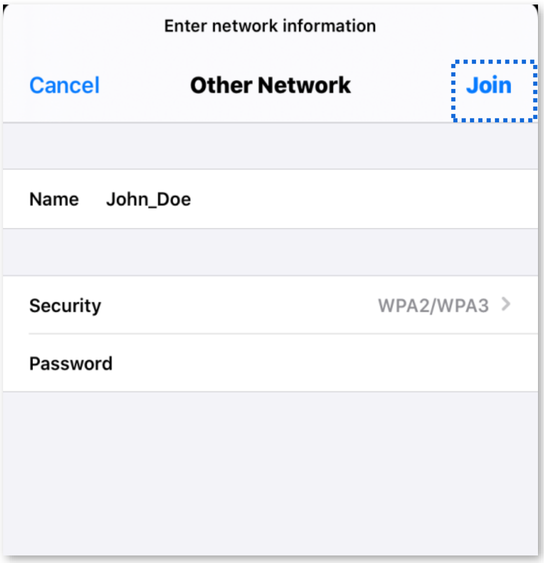
Step 3 Scroll the Wi-Fi list to the bottom, and tap **Other…**.

Step 4 Enter the Wi-Fi name and password, which are **John_Doe** and **Hikvision+WiFi245** in this example.

Step 5 Set security to **WPA2/WPA3** (If WPA2/WPA3 is not available, choose WPA2).

Step 6 Tap **Join**.




Enter network information

Name John_Doe

Security WPA2/WPA3

Password

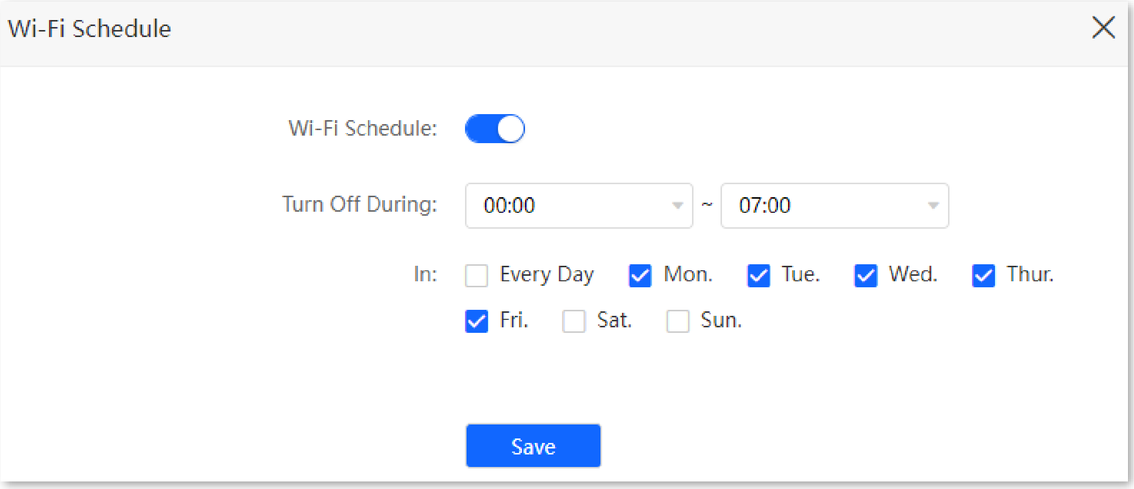
When completing the configurations, you can connect to the hidden Wi-Fi network to access the internet.

4.2 Wi-Fi schedule

4.2.1 Overview

This Wi-Fi Schedule function allows you to disable the Wi-Fi networks of the router at specified period.

To access the configuration page, Log in to the web UI of the router, and choose **Wi-Fi Settings** > **Wi-Fi Schedule**. This function is disabled by default. When it is enabled, the page is shown as below.



Wi-Fi Schedule

Wi-Fi Schedule: ●

Turn Off During: 00:00 ~ 07:00

In: □ Every Day ☑ Mon. ☑ Tue. ☑ Wed. ☑ Thur. ☑ Fri. □ Sat. □ Sun.

Note

To make the Wi-Fi schedule function work properly, please ensure the system time is synchronized with the internet time. Refer to Sync the system time with the internet time for configuration.

Table 4-2 Parameter description

Parameter	Description
Wi-Fi Schedule	It is used to enable or disable the Wi-Fi schedule function.
Turn Off During	It specifies the period when the Wi-Fi networks are disabled.
In	It specifies the day(s) on which the Wi-Fi networks are disabled during the specified period.

4.2.2 An example of configuring Wi-Fi schedule

Assume that you want to disable the Wi-Fi network from 22:00 to 07:00 every day.

Configuring procedure:

Step 1 Log in to the web UI of the router.

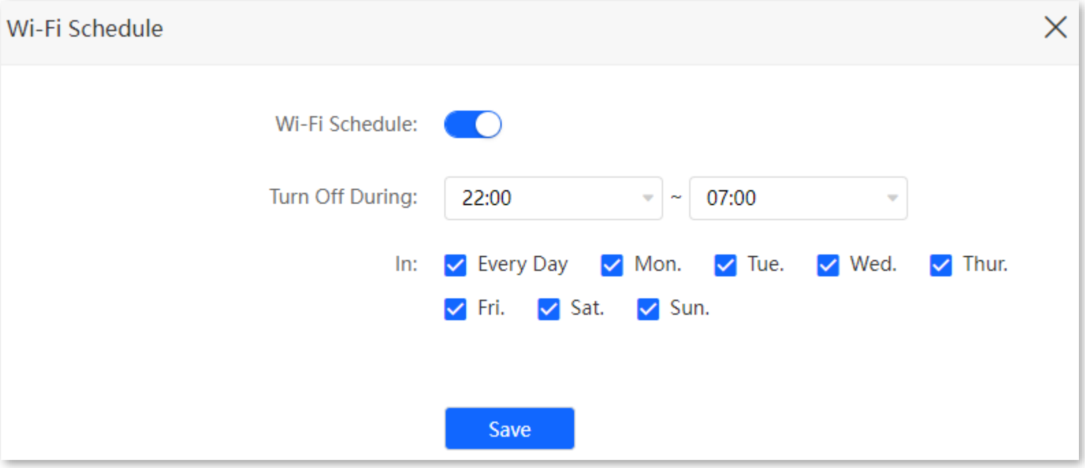
Step 2 Choose **Wi-Fi Settings** > **Wi-Fi Schedule**.

Step 3 Enable **Wi-Fi Schedule**.

Step 4 Set a period for the Wi-Fi networks to be disabled, which is **22:00-07:00** in this example.

Step 5 Set the days when the function works, which is **Every Day** in this example.

Step 6 Click **Save**.



Wi-Fi Schedule

Wi-Fi Schedule: ●

Turn Off During: 22:00 ~ 07:00

In: ☑ Every Day ☑ Mon. ☑ Tue. ☑ Wed. ☑ Thur.
☑ Fri. ☑ Sat. ☑ Sun.

When the configuration is completed, the Wi-Fi networks will be disabled from 22:00 to 7:00 every day.

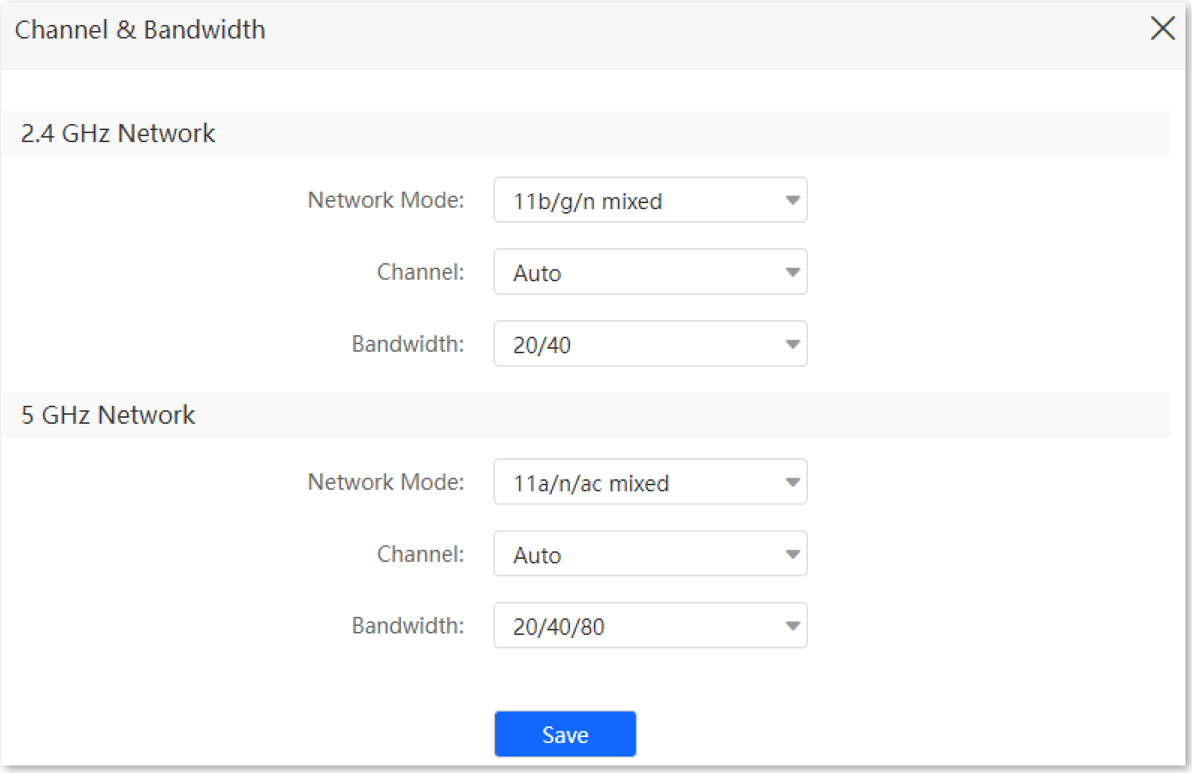
4.3 Channel & bandwidth

In this section, you can change network mode, wireless channel, and wireless bandwidth of 2.4 GHz and 5 GHz Wi-Fi networks.

To access the configuration page, Log in to the web UI of the router, and choose **Wi-Fi Settings** > **Channel & Bandwidth**.

Note

In order not to influence the wireless performance, it is recommended to maintain the default settings on this page without professional instructions.



Channel & Bandwidth

2.4 GHz Network

Network Mode: 11b/g/n mixed

Channel: Auto

Bandwidth: 20/40

5 GHz Network

Network Mode: 11a/n/ac mixed

Channel: Auto

Bandwidth: 20/40/80

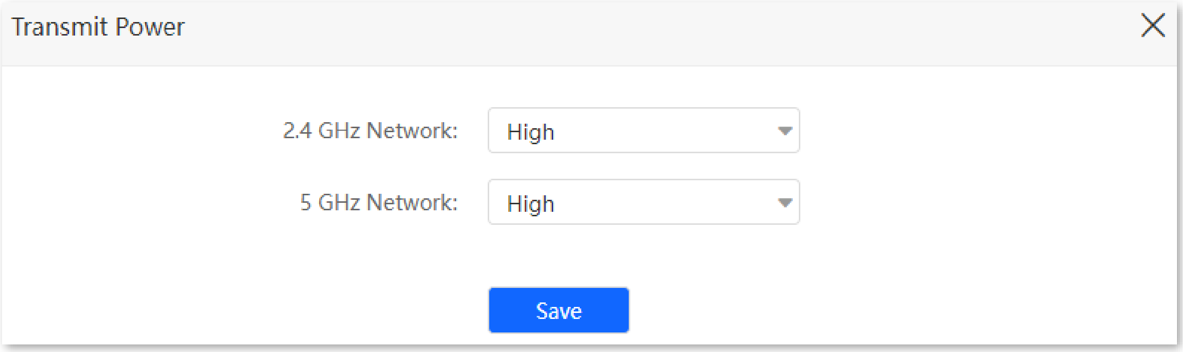
Table 4-3 Parameter description

Parameter	Description
Network Mode	It specifies various protocols adopted for wireless transmission. 2.4 GHz Wi-Fi network supports 11n, 11b/g mixed and 11b/g/n mixed modes. ● **11n**: It indicates that devices compliant with IEEE 802.11n protocol can connect to the 2.4 GHz Wi-Fi network of the router. ● **11b/g mixed**: It indicates that devices compliant with IEEE 802.11b or IEEE 802.11g protocol can connect to the 2.4 GHz Wi-Fi network of the router. ● **11b/g/n mixed**: It indicates that all devices can connect to the router if they are compliant with IEEE 802.11b or IEEE 802.11g protocol, or work at 2.4 GHz with IEEE 802.11n protocol. 5 GHz Wi-Fi network supports 11ac, 11a/n/ac mixed modes. ● **11ac**: It indicates that devices complaint with IEEE 802.11ac protocol can connect to the router. ● **11a/n/ac mixed**: It indicates that all devices that are compliant with IEEE 802.11a or IEEE 802.11ac protocol, or work at 5 GHz with IEEE 802.11n protocol can connect to the router.
Channel	It specifies the channel in which the Wi-Fi network works. By default, the wireless channel is **Auto**, which indicates that the router selects a channel for the Wi-Fi network automatically. You are recommended to choose a channel with less interference for better wireless transmission efficiency. You can use a third-party tool to scan the Wi-Fi signals nearby to understand the channel usage situations.
Bandwidth	It specifies the bandwidth of the wireless channel of a Wi-Fi network. Please change the default settings only when necessary. ● **20**: It indicates that the channel bandwidth used by the router is 20 MHz. ● **40**: It indicates that the channel bandwidth used by the router is 40 MHz. ● **20/40**: It specifies that a router can switch its channel bandwidth between 20 MHz and 40 MHz based on the ambient environment. This option is available only at 2.4 GHz. ● **80**: It indicates that the channel bandwidth used by the router is 80 MHz. This option is available only at 5 GHz. ● **20/40/80**: It specifies that a router can switch its channel bandwidth among 20 MHz, 40 MHz, and 80 MHz based on the ambient environment. This option is available only at 5 GHz.

4.4 Transmit power

In this module, you can adjust the wall-penetration capability and wireless coverage of the router by setting the transmit power.

To access the configuration page, Log in to the web UI of the router, and choose **Wi-Fi Settings** > **Transmit Power**.



Transmit Power

2.4 GHz Network: High

5 GHz Network: High

Table 4-4 Parameter description

Parameter	**Description**
Transmit Power	It specifies the mode of signal strength. The default mode is **High**. ● **High**: It is typically used to meet wireless coverage requirements in large or multi-barrier environments. ● **Medium**: It is typically used to meet wireless coverage requirements in medium-area or less-obstacle environments. ● **Low**: It is typically used to meet wireless coverage requirements in small area or barrier-free environments. **Note** It is recommended to choose the **Low** mode if the network experience is satisfactory enough under this mode.

4.5 WPS

4.5.1 Overview

The WPS function enables wireless devices, such as smartphones, to connect to Wi-Fi networks of the router quickly and easily.

To access the configuration page, Log in to the web UI of the router, and choose **Wi-Fi Settings** > **WPS**.

Note

This function is only applicable to WPS-enabled wireless devices.

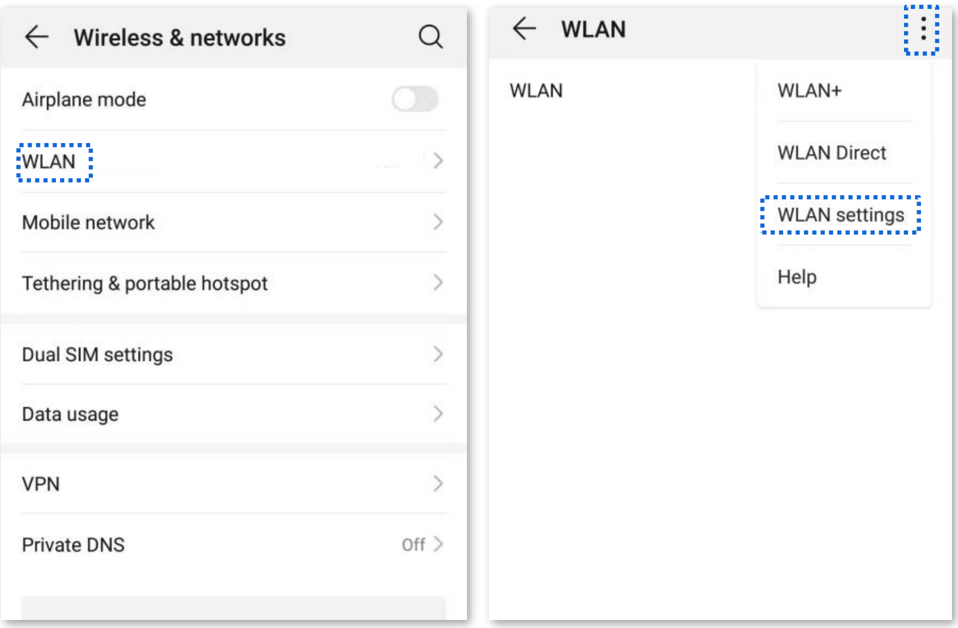
4.5.2 Connect devices to the Wi-Fi network using the WPS button

Configuring procedure:

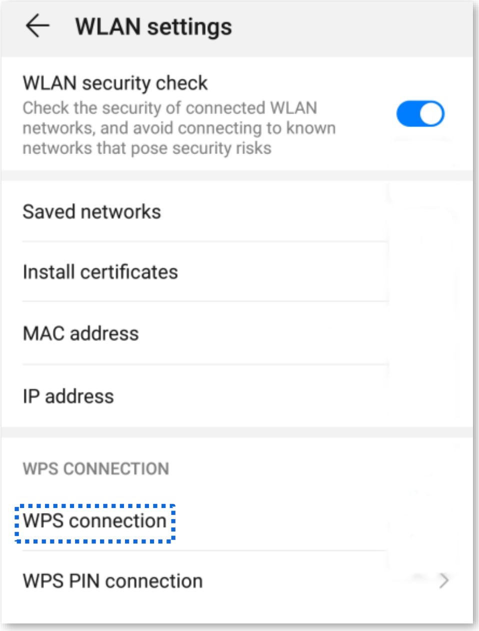
Step 1 Find the **RST/WPS** button on the rear panel of the router, and hold it down for 1 to 3 seconds. The Wi-Fi indicator blinks slow.

Step 2 Configure the WPS function on your wireless devices **within 2 minutes**. Configurations on various devices may differ (Example: HUAWEI P10).

1) Find **Settings** on the phone.
2) Choose **WLAN**.
3) Tap ⋮, and choose **WLAN settings**.



4) Choose **WPS connection**.



WLAN settings

WLAN security check

Check the security of connected WLAN networks, and avoid connecting to known networks that pose security risks

Saved networks

Install certificates

MAC address

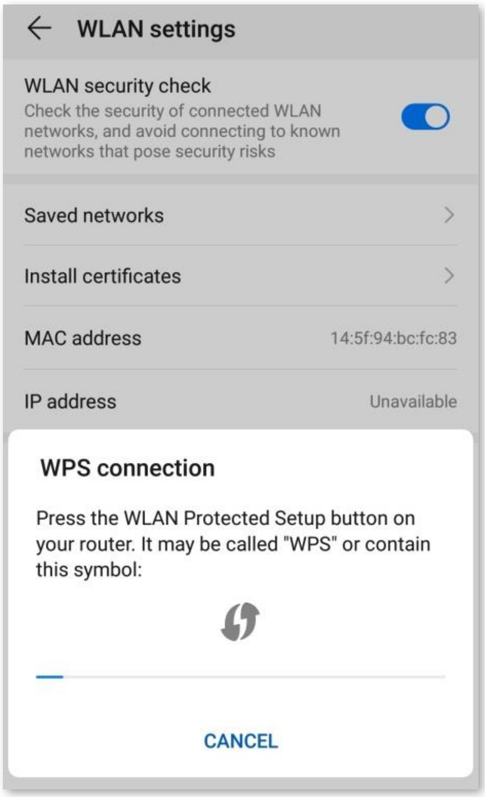
IP address

WPS CONNECTION

WPS connection

WPS PIN connection

Wait a moment until the WPS negotiation is completed, and the phone is connected to the Wi-Fi network.



WLAN settings

WLAN security check

Check the security of connected WLAN networks, and avoid connecting to known networks that pose security risks

Saved networks

Install certificates

MAC address 14:5f:94:bc:fc:83

IP address Unavailable

WPS connection

Press the WLAN Protected Setup button on your router. It may be called "WPS" or contain this symbol:

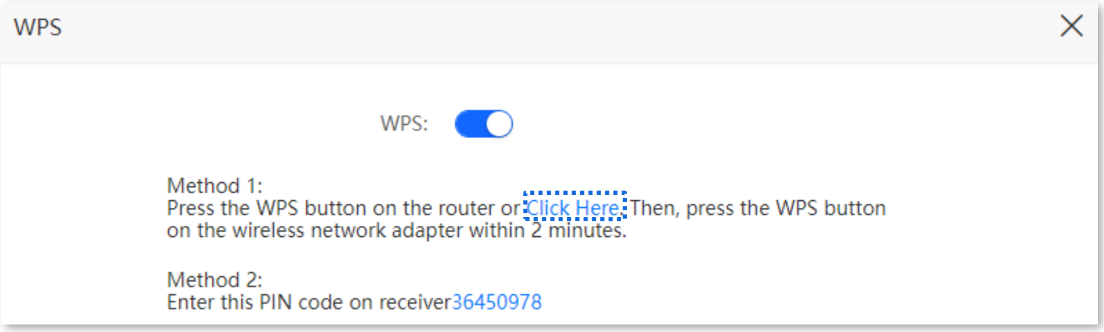
4.5.3 Connect devices to the Wi-Fi network through the web UI of the router

Configuring procedure:

Step 1 Log in to the web UI of the router.

Step 2 Choose **Wi-Fi Settings** > **WPS**.

Step 3 Click Click Here below **Method 1**.



WPS

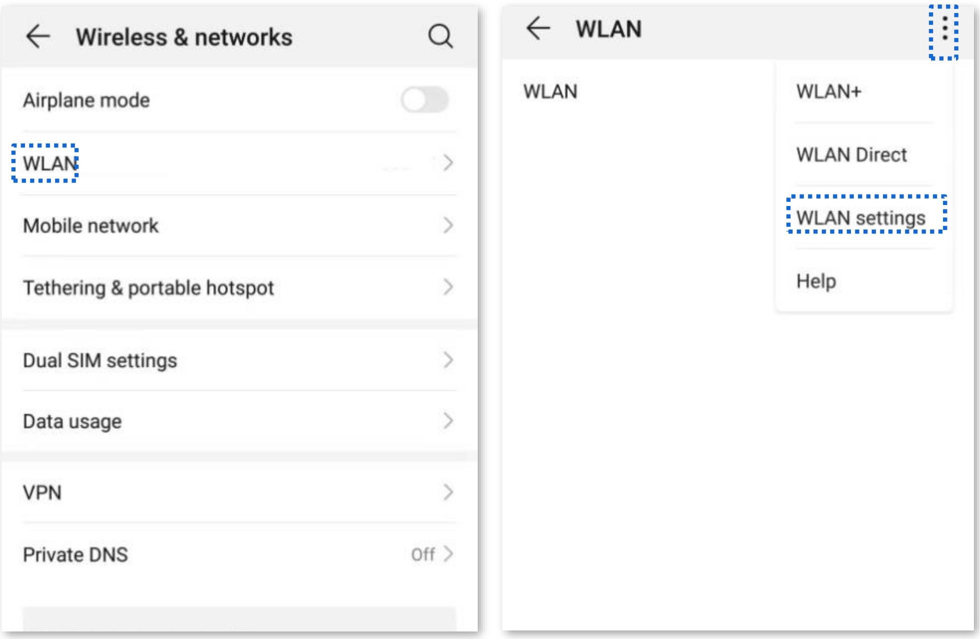
WPS: ●

Method 1:
Press the WPS button on the router or Click Here. Then, press the WPS button on the wireless network adapter within 2 minutes.

Method 2:
Enter this PIN code on receiver36450978

Step 4 Configure the WPS function on your wireless devices **within 2 minutes**. Configurations on various devices may differ (Example: HUAWEI P10).

1) Find **Settings** on the phone.
2) Choose **WLAN**.
3) Tap ⋮, and choose **WLAN settings**.



Wireless & networks

Airplane mode

WLAN

Mobile network

Tethering & portable hotspot

Dual SIM settings

Data usage

VPN

Private DNS Off

WLAN

WLAN

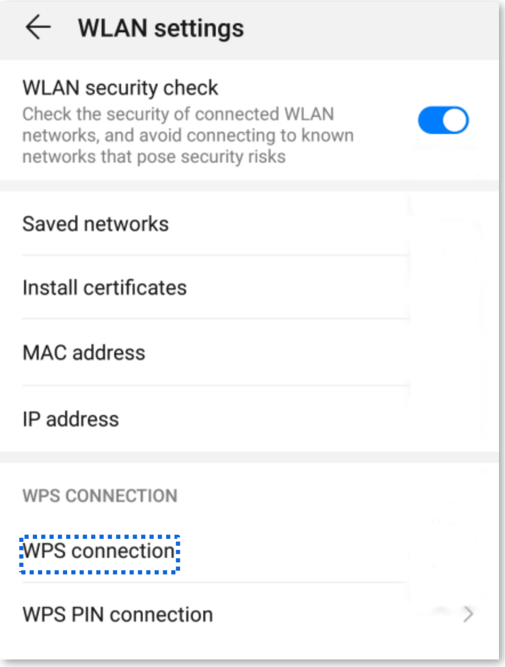
WLAN+

WLAN Direct

WLAN settings

Help

4) Choose **WPS connection**.



WLAN settings

WLAN security check

Check the security of connected WLAN networks, and avoid connecting to known networks that pose security risks

Saved networks

Install certificates

MAC address

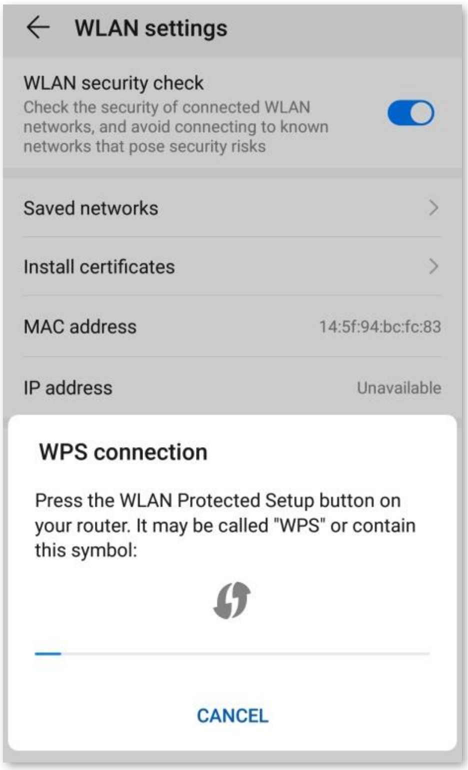
IP address

WPS CONNECTION

WPS connection

WPS PIN connection

Wait a moment until the WPS negotiation is completed, and the phone is connected to the Wi-Fi network.



WLAN settings

WLAN security check

Check the security of connected WLAN networks, and avoid connecting to known networks that pose security risks

Saved networks

Install certificates

MAC address 14:5f:94:bc:fc:83

IP address Unavailable

WPS connection

Press the WLAN Protected Setup button on your router. It may be called "WPS" or contain this symbol:

CANCEL

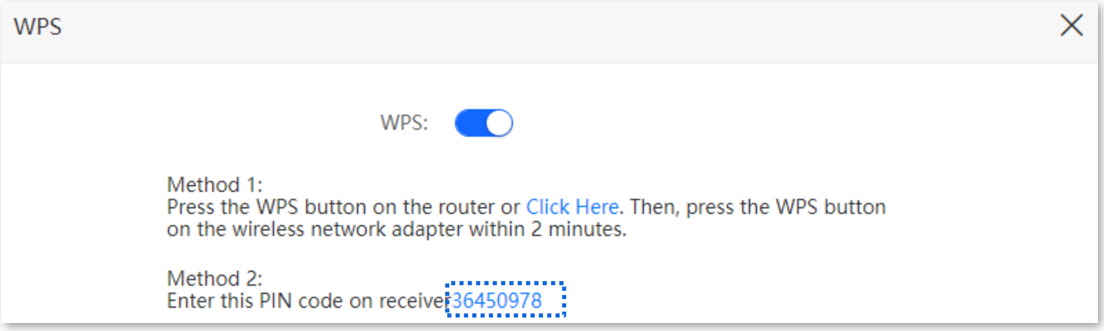
4.5.4 Connect devices to the Wi-Fi network using the PIN code of the router

Note

The router only supports WPS connection by entering the PIN code on wireless devices, which is usually used on Wi-Fi network adapters. Please refer to the user guide of the Wi-Fi network adapter for configuration details.

Configuring procedure:

Step 1 Find the PIN code of the router by logging in to the web UI of the router, and choose **Wi-Fi Settings** > **WPS**. The PIN code is shown under **Method 2**.



Method 1:
Press the WPS button on the router or Click Here. Then, press the WPS button on the wireless network adapter within 2 minutes.

Method 2:
Enter this PIN code on receive 36450978

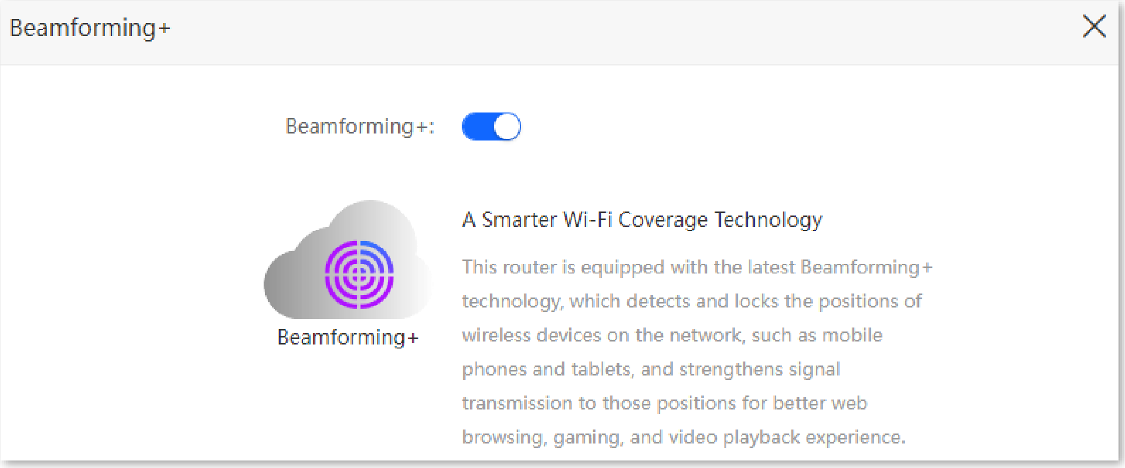
Step 2 Enter the PIN code on the wireless device that supports WPS connection using the PIN code.

Wait a moment until the WPS negotiation is completed, and the wireless device is connected to the Wi-Fi network.

4.6 Beamforming+

Beamforming+ is a radio wave technology written into IEEE 802.11ac standard. Traditionally, the router broadcasts the data in all directions when broadcasting a Wi-Fi signal. With beamforming, the router transmits radio signal in the direction of the client, thus creating a stronger, faster and more reliable wireless communication. This function is enabled by default.

To access the configuration page, Log in to the web UI of the router, and choose **Wi-Fi Settings** > **Beamforming+**.



Beamforming+: ●

A Smarter Wi-Fi Coverage Technology

This router is equipped with the latest Beamforming+ technology, which detects and locks the positions of wireless devices on the network, such as mobile phones and tablets, and strengthens signal transmission to those positions for better web browsing, gaming, and video playback experience.

The following figure shows the wireless transmission when **Beamforming+** is enabled.

The following figure shows the wireless transmission when **Beamforming+** is disabled.

4.7 AP mode (wireless router mode)

Note

This function is only available under the wireless router mode. Refer to Operating mode to set the operating mode of the router.

When you have a smart home gateway which only provides wired internet access, you can set the router to work in AP mode to provide wireless coverage.

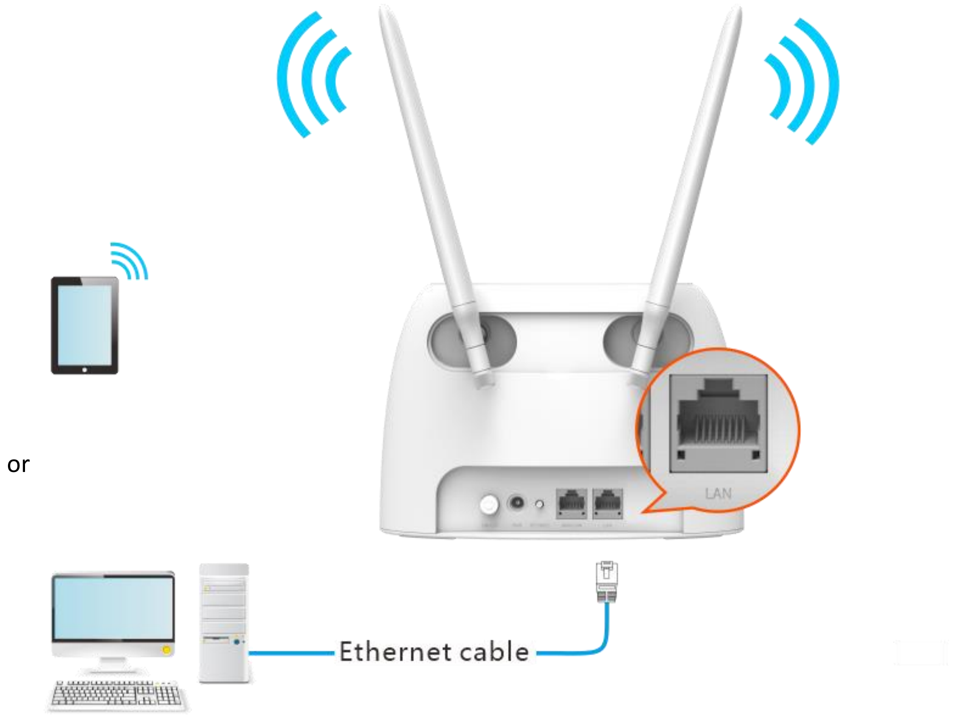
Note

When the router is set to AP mode:

- Every physical port can be used as a LAN port.
- The LAN IP address of the router will be changed. Please log in to web UI of the router by visiting **https://hikvisionwifi.local**.
- Functions, such as bandwidth control and virtual server, will be unavailable. Refer to the web UI for available functions.

Configuring procedure:

Step 1 Power on the router. Connect a computer to the LAN port of the router, or connect your smartphone to the Wi-Fi network of the router.

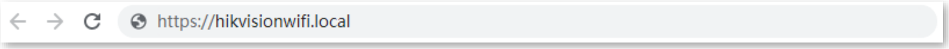


Note

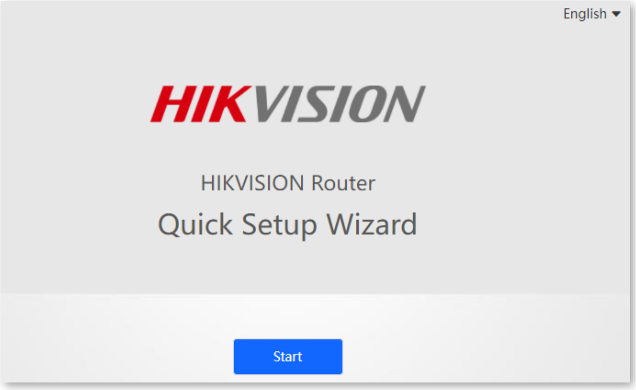
If you have finished the quick setup wizard before, start a web browser and visit **https://hikvisionwifi.local** and skip to **Step 3** to proceed with the configuration.

Step 2 Log in to the web UI of the router.

1) Start a web browser on the device connected to the router, and visit **https://hikvisionwifi.local**. A computer is used for illustration below.


https://hikvisionwifi.local

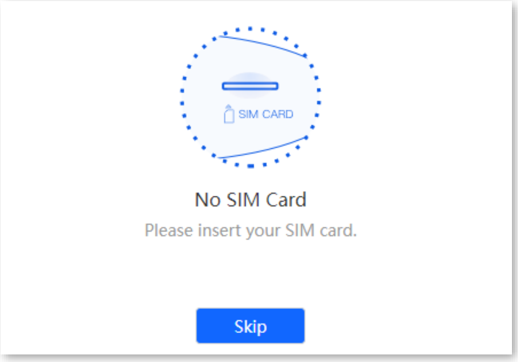
2) Click **Start**.


English

HIKVISION Router

Quick Setup Wizard

3) Click **Skip**.



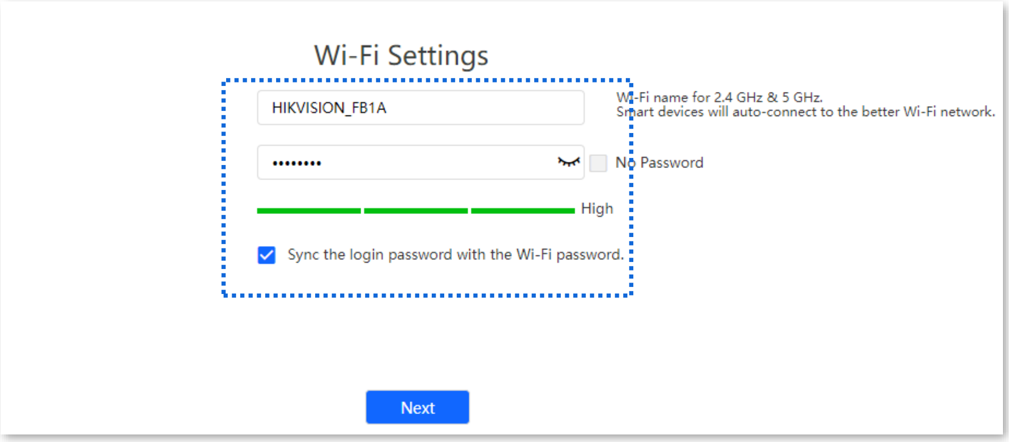
No SIM Card

Please insert your SIM card.

4) Set Wi-Fi and login password, and click **Next**.

Note

Ticking **Sync the login password with the Wi-Fi password**, the Wi-Fi password is set to the router login password.


Wi-Fi Settings

HIKVISION_FB1A

Wi-Fi name for 2.4 GHz & 5 GHz.
Smart devices will auto-connect to the better Wi-Fi network.

••••••••

□ No Password

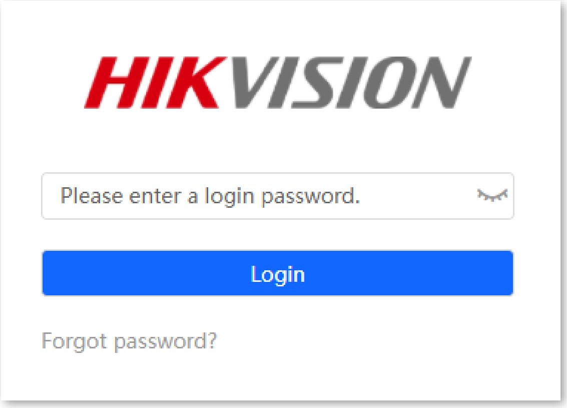
High

☑ Sync the login password with the Wi-Fi password.

5) Enter the login password you set, and click **Login**.

Note

You need to enter the Wi-Fi password of the wireless device to connect the Wi-Fi network of your router.

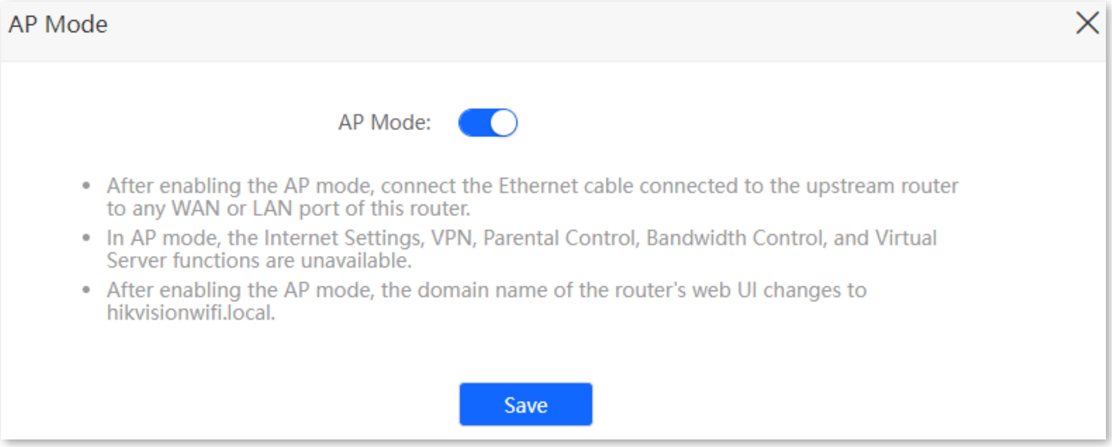


HIKVISION

Please enter a login password.

Step 3 Set the router to AP mode.

1) Choose **Wi-Fi Settings** > **AP Mode**.
2) Enable **AP Mode**.
3) Click **Save**.

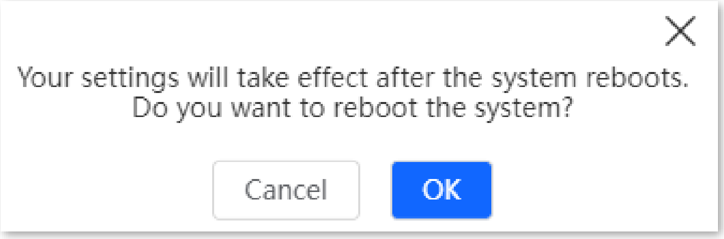


AP Mode

AP Mode: ●

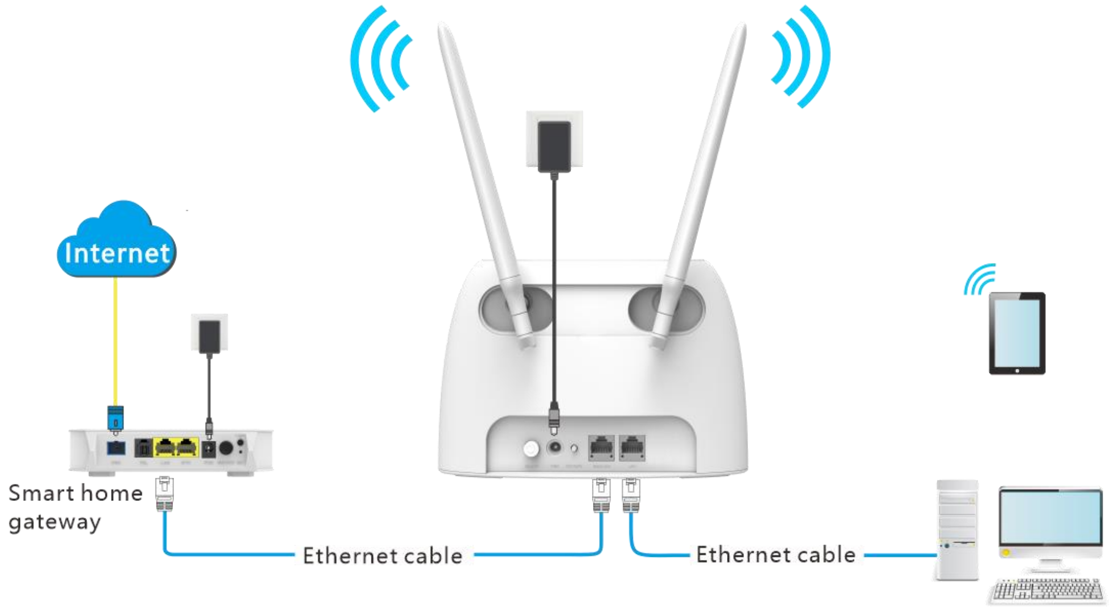
- After enabling the AP mode, connect the Ethernet cable connected to the upstream router to any WAN or LAN port of this router.
- In AP mode, the Internet Settings, VPN, Parental Control, Bandwidth Control, and Virtual Server functions are unavailable.
- After enabling the AP mode, the domain name of the router's web UI changes to hikvisionwifi.local.

Step 4 Click **OK**, and wait for the router to reboot.

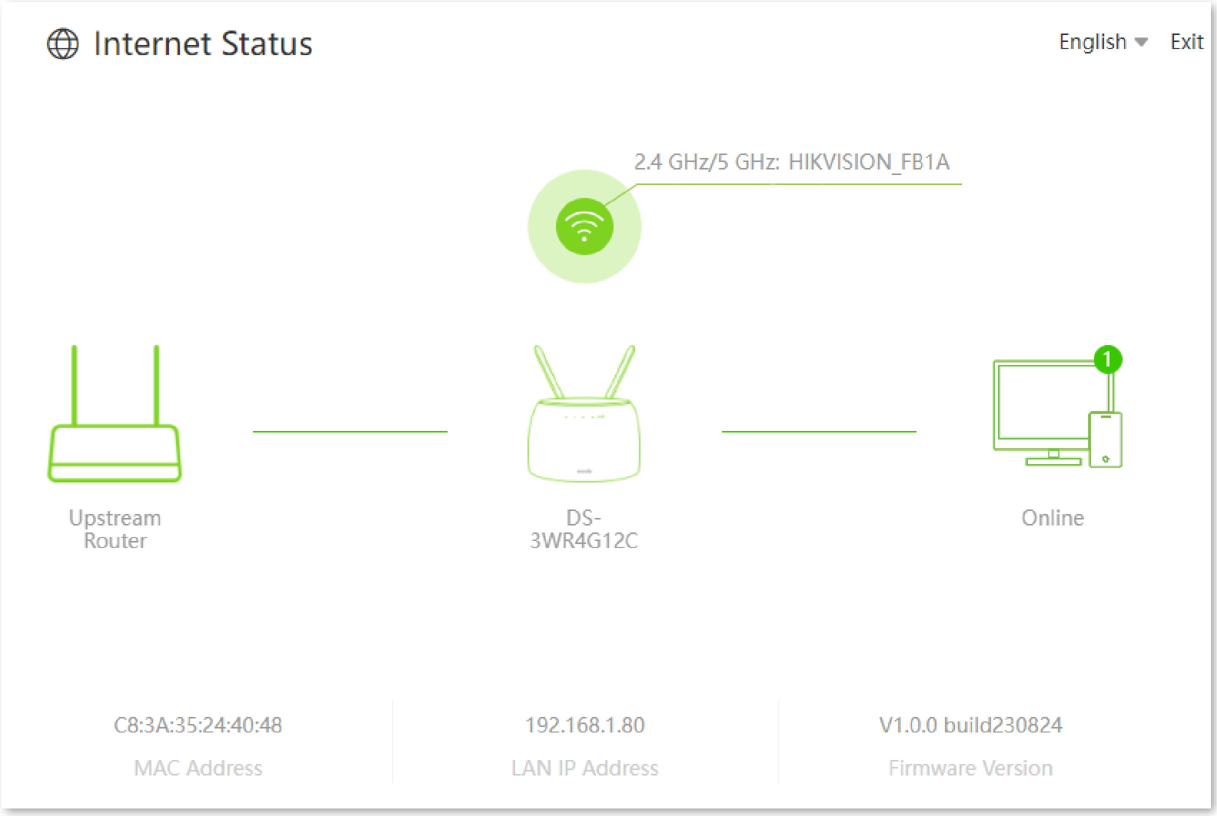


Your settings will take effect after the system reboots. Do you want to reboot the system?

Step 5 Connect the upstream device, such as a gateway, to any port of the router.



Log in to the web UI of the router again, and choose **Internet Status** to check if the AP mode is configured successfully.



Internet Status

English ▾ Exit

2.4 GHz/5 GHz: HIKVISION_FB1A

Upstream Router

DS-3WR4G12C

Online

1

C8:3A:35:24:40:48

MAC Address

192.168.1.80

LAN IP Address

V1.0.0 build230824

Firmware Version

Note

If there is another network device with the same login domain name (**https://hikvisionwifi.local**) with the router, log in to the upstream router and find the IP address obtained by the new router in the client list. Then you can Log in to the web UI of the router by visiting the IP address.

To access the internet, connect your computer to physical port, or connect your smartphone to the Wi-Fi network.

You can find the Wi-Fi name and password on the **Wi-Fi Settings** > **Wi-Fi Name & Password** page. If the network is not encrypted, you are recommended to set a Wi-Fi password on this page for security.

Note

If you cannot access the internet, try the following solutions:

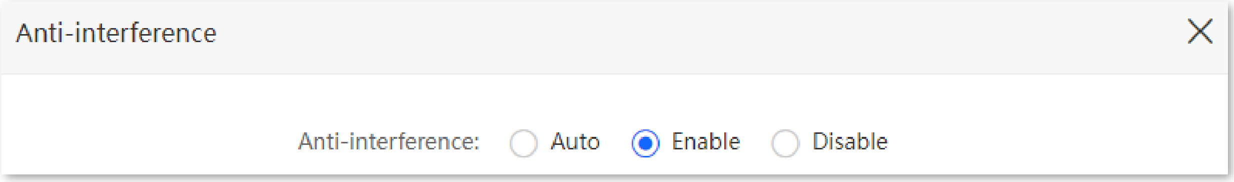
- Ensure that the existing router is connected to the internet successfully.
- Ensure that your wireless devices are connected to the correct Wi-Fi network of the new router.
- If the computer connected to the router cannot access the internet, ensure that the computer is configured to obtain an IP address and DNS sever automatically.

4.8 Anti-interference

The router supports anti-interference function. When you are experiencing unsatisfactory internet access, you can try to change the anti-interference settings to improve it.

To access the configuration page, Log in to the web UI of the router, and choose **Wi-Fi Settings** > **Anti-interference**.

The default setting is **Enable**.



Anti-interference

Anti-interference: ○ Auto ● Enable ○ Disable

- **Auto**: It indicates that the router will automatically adjust the receiving sensitivity according to the interference of the current environment.
- **Enable**: It indicates that the anti-interference ability of the router improves, but the Wi-Fi network coverage is reduced.
- **Disable**: It indicates that the wireless coverage of the router is improved. If the wireless interference in the environment is strong, it is recommended to select **Auto** or **Enable**.

Chapter 5 SMS (3G/4G router mode)

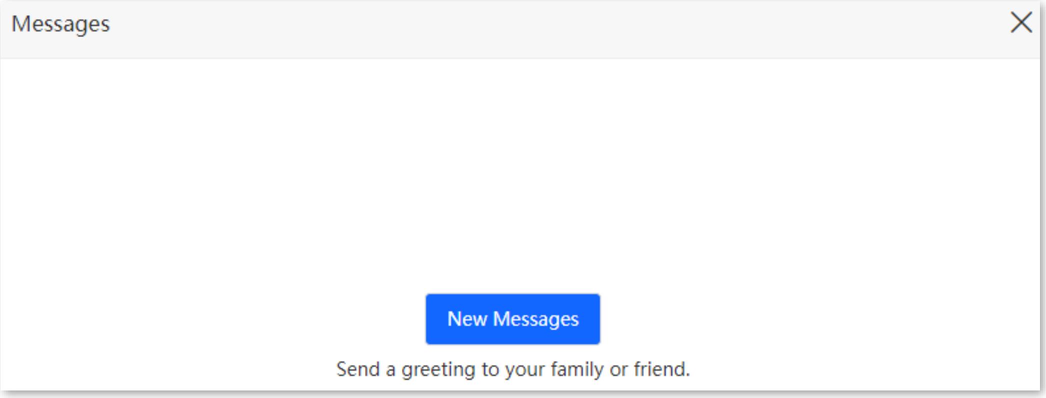
Note

This function is only available under the 3G/4G router mode. Refer to Operating mode to set the operating mode of the router.

5.1 Manage SMS messages

This router supports sending, receiving, and deleting SMS messages in the web UI of the router.

To access the page, Log in to the web UI of the router, and choose **SMS** > **Messages**.



5.1.1 Send SMS messages

Send SMS messages to a new phone number

Step 1 Log in to the web UI of the router.

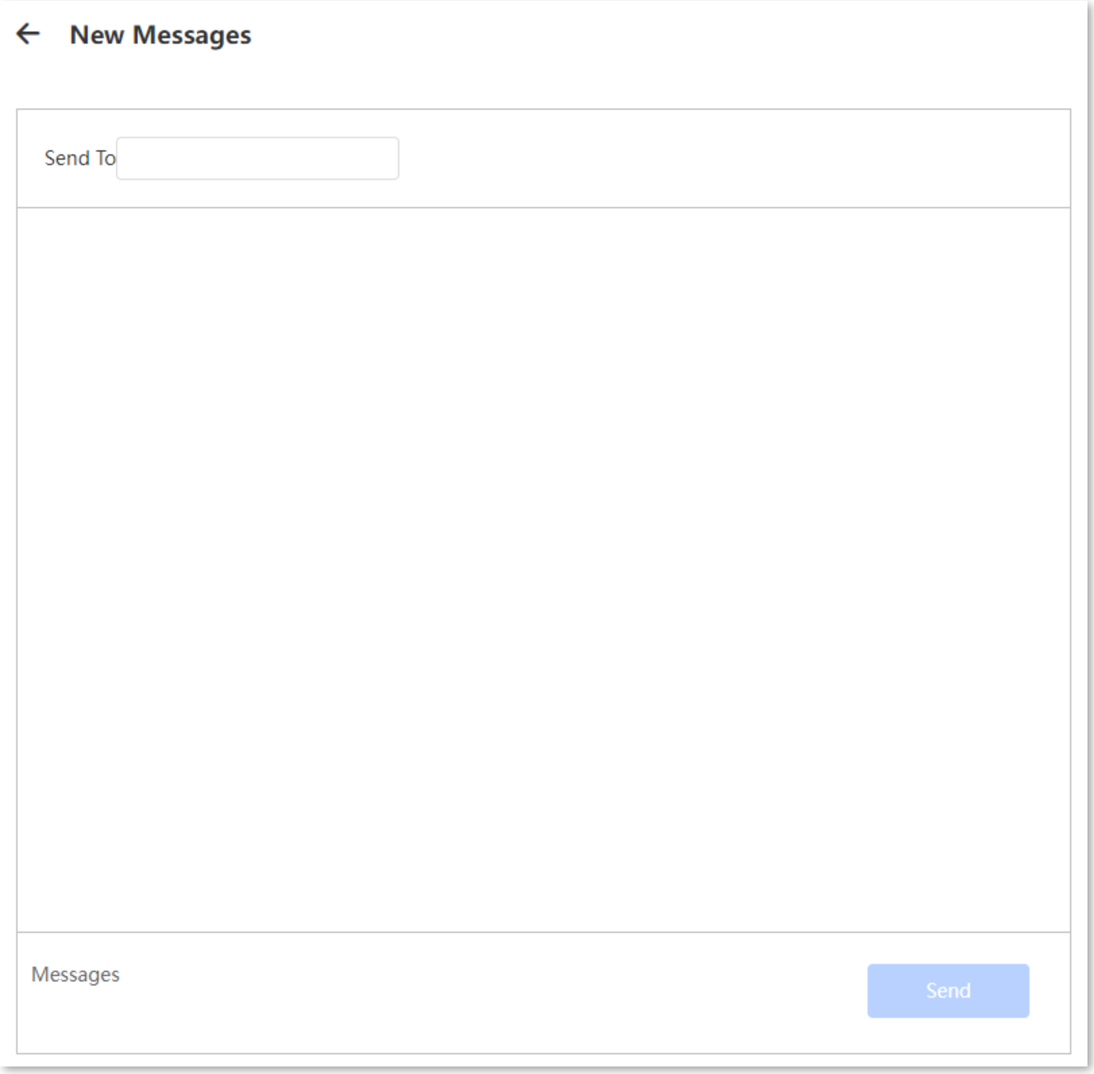
Step 2 Choose **SMS** > **Messages**.

Step 3 Click **New Message**.

Step 4 Enter the phone number in the **Send To** column.

Step 5 Enter the message content in the **Message** column at the bottom.

Step 6 Click **Send** at the bottom right corner.

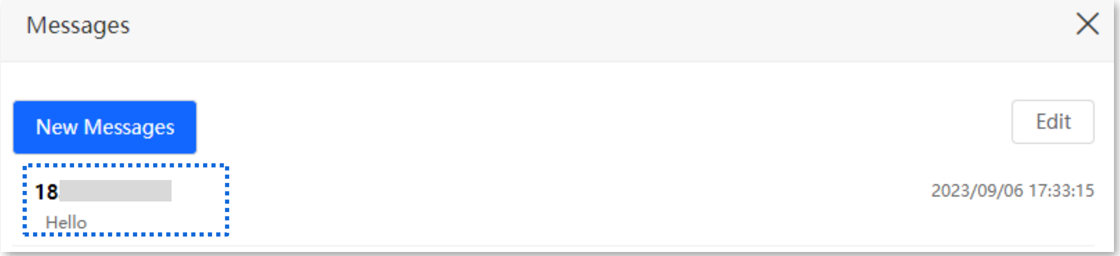


Send messages to an existing phone number

Step 1 Log in to the web UI of the router.

Step 2 Choose **SMS** > **Messages**.

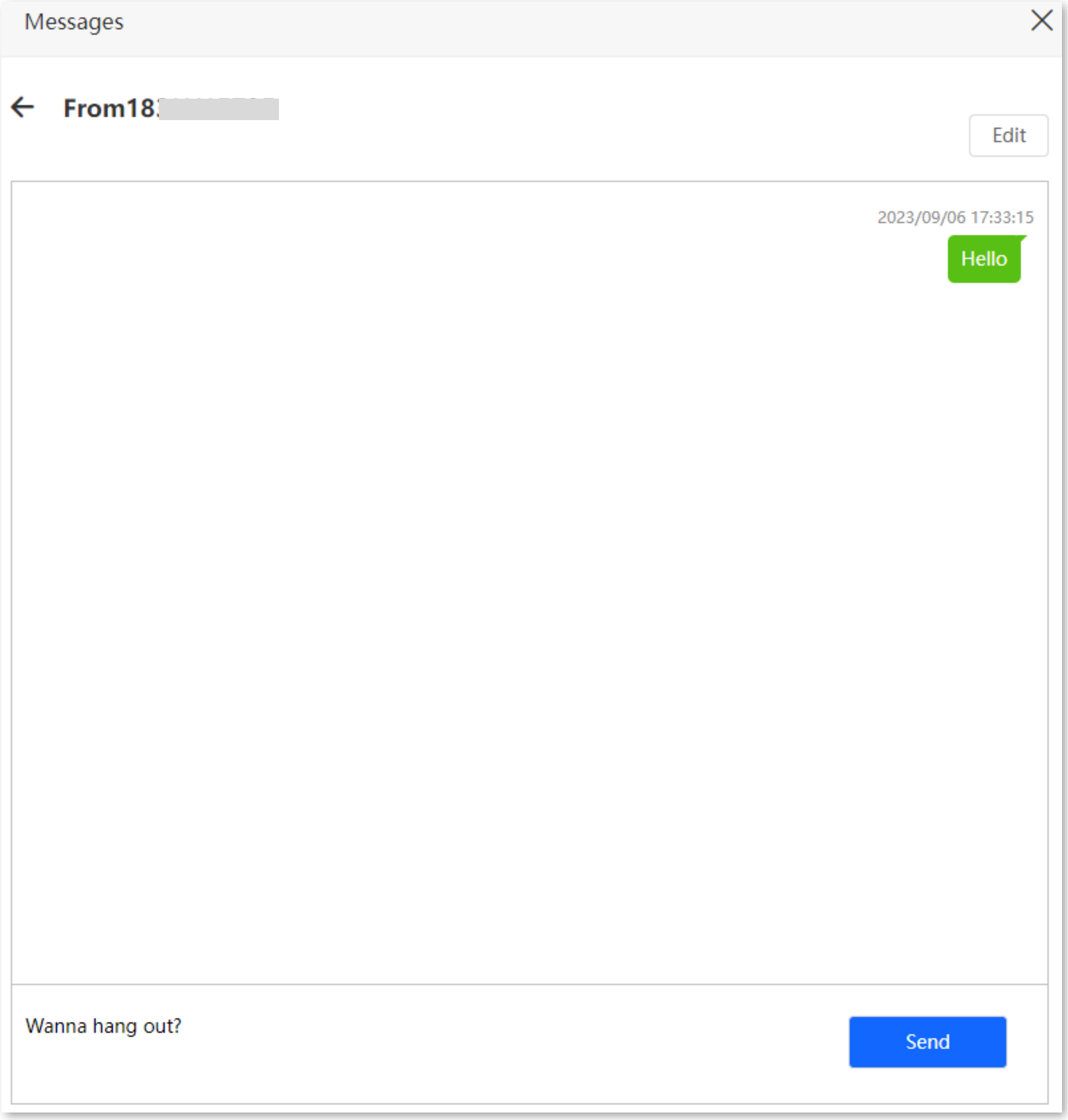
Step 3 Click the targeted phone number.



18[redacted]
Hello
2023/09/06 17:33:15

Step 4 Enter the message content in the **Message** column at the bottom.

Step 5 Click **Send**.



Messages

From18[redacted]

2023/09/06 17:33:15

Hello

Wanna hang out?

After the messages are sent, you can view them on the same page.

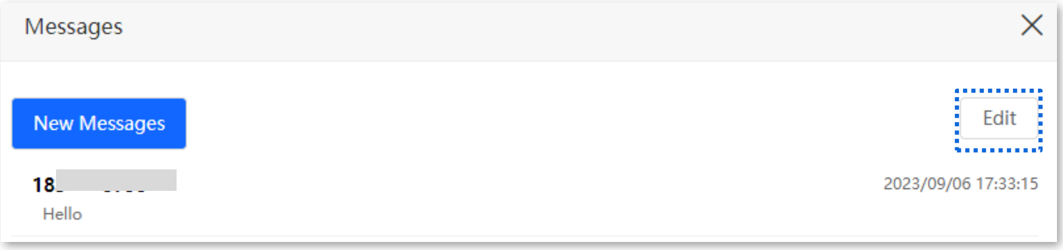
5.1.2 Delete SMS messages

Delete all messages of the same phone numbers

Step 1 Log in to the web UI of the router.

Step 2 Choose **SMS** > **Messages**.

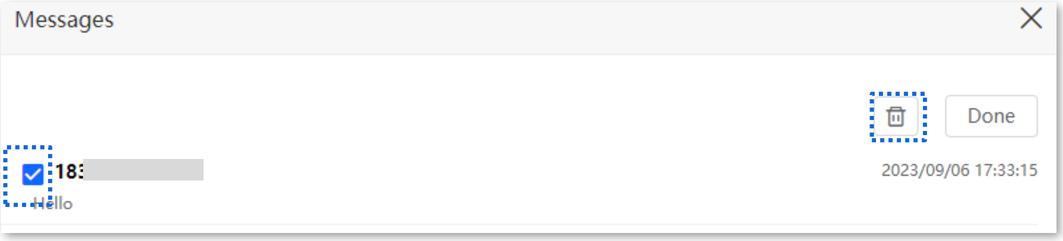
Step 3 Click **Edit** on the top right corner.



18[redacted]
Hello
2023/09/06 17:33:15

Step 4 Select one or more phone number to be deleted.

Step 5 Click 🗑 (click **Done** to cancel).



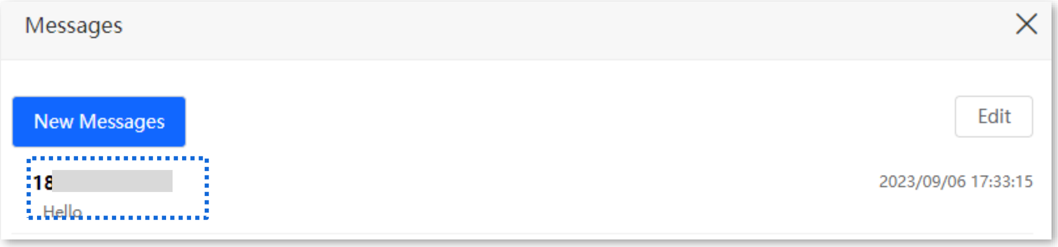
☑ 18[redacted]
Hello
2023/09/06 17:33:15

Delete certain messages of the same phone number

Step 1 Log in to the web UI of the router.

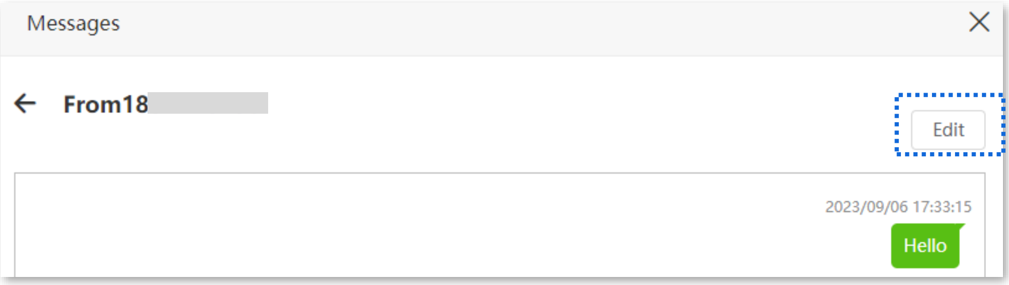
Step 2 Choose **SMS** > **Messages**.

Step 3 Click the targeted phone number.



18[redacted]
Hello
2023/09/06 17:33:15

Step 4 Click **Edit**.

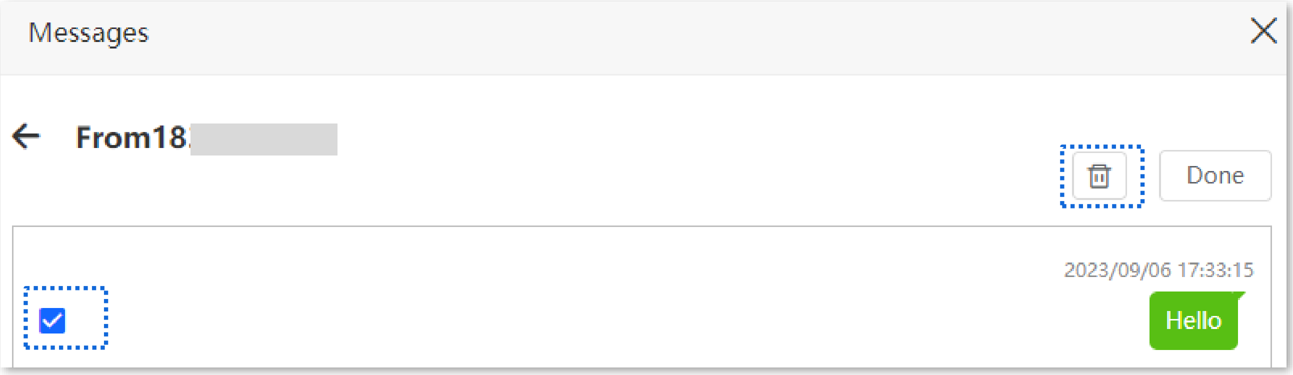


From18[redacted]

2023/09/06 17:33:15
Hello

Step 5 Select the messages to be deleted.

Step 6 Click 🗑 (click **Done** to cancel).



Messages

From18[redacted]

☑

2023/09/06 17:33:15

Hello

5.2 Set the message center number

Message center is the short message server for SMS messages. You will be unable to send SMS messages with a wrong message center number.

The router can automatically detect the message center number after you insert a SIM card. If you have problems in sending SMS messages, you are recommended to inquire your ISP for the message center number and change it in the web UI of the router if it is wrong.

Configuring procedure:

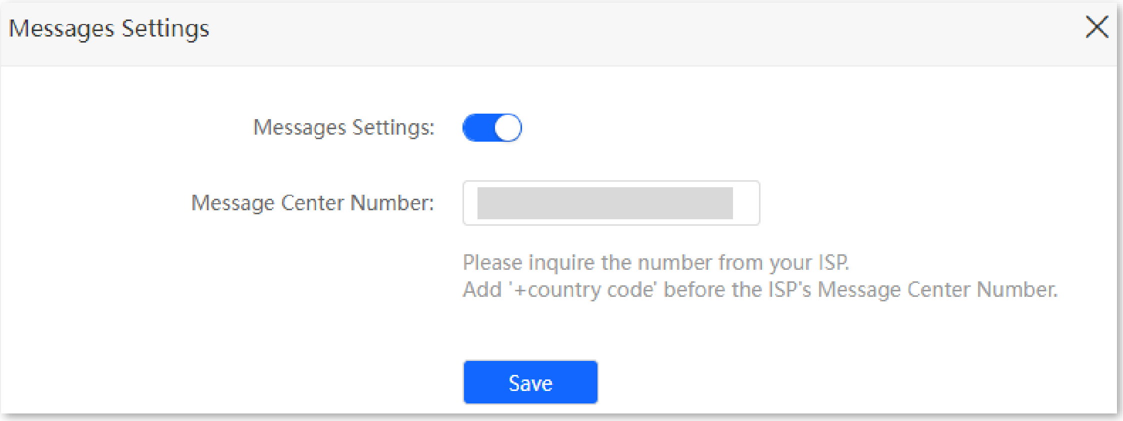
Step 1 Log in to the web UI of the router.

Step 2 Choose **SMS** > **Messages Settings**.

Step 3 Enable **Messages Settings**.

Step 4 Enter the correct **Message Center Number**.

Step 5 Click **Save**.



Messages Settings

Messages Settings: ●

Message Center Number:

Please inquire the number from your ISP.
Add '+country code' before the ISP's Message Center Number.

5.3 Inquire information by sending USSD commands

With **USSD** function, you can inquire specific information or perform specific operations by send a special code or command to your ISP.

Note

Such codes or commands are predetermined. You can contact your ISP to find those codes or commands.

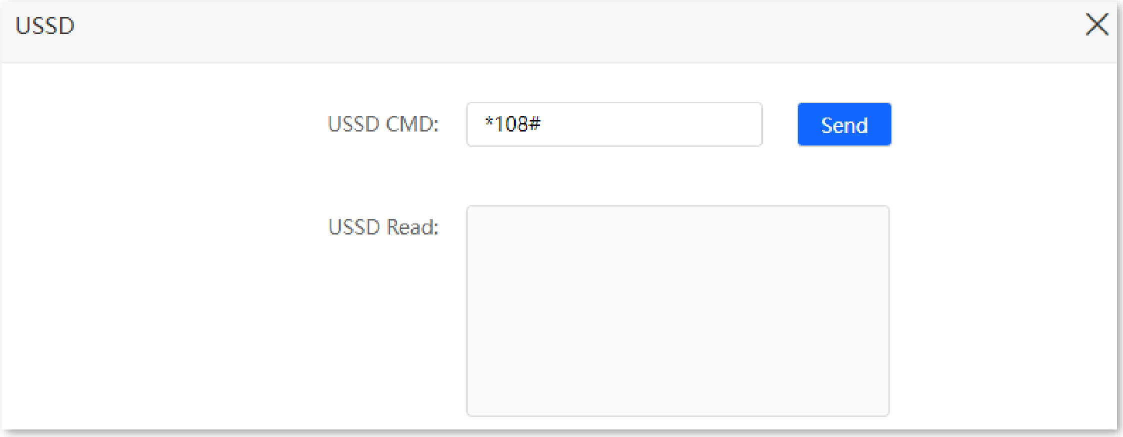
Configuring procedure:

Step 1 Log in to the web UI of the router.

Step 2 Choose **SMS** > **USSD**.

Step 3 Enter a **USSD CMD**, such as ***108#**.

Step 4 Click **Send**.


USSD

USSD CMD: *108#

USSD Read:

Wait a moment, you will get the desired information you want in the **USSD Read** box.

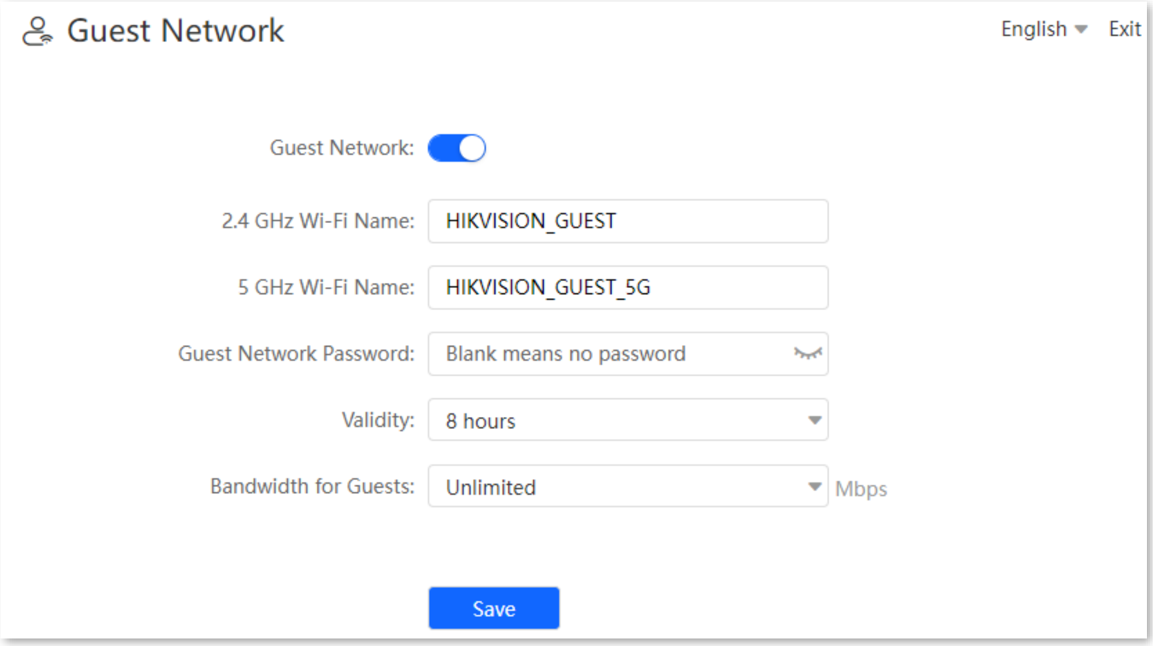
Chapter 6 Guest network

6.1 Overview

In this module, you can enable/disable the guest network function and change the Wi-Fi names and password of the guest networks.

A guest network can be set up with a shared bandwidth limit for visitors to access the internet, and isolated from the main network. It protects the security of the main network and ensures the bandwidth of your main network.

To access the configuration page, Log in to the web UI of the router and choose the **Guest Network**. This function is disabled by default. When it is enabled, the page is shown as below.



Guest Network

Guest Network: ●

2.4 GHz Wi-Fi Name: HIKVISION_GUEST

5 GHz Wi-Fi Name: HIKVISION_GUEST_5G

Guest Network Password: Blank means no password

Validity: 8 hours

Bandwidth for Guests: Unlimited Mbps

Table 6-1 Parameter description

Parameter	Description
Guest Network	It is used to enable or disable the guest network function.
2.4 GHz Wi-Fi Name	They specify the Wi-Fi name of the router's guest network. You can change the SSIDs (Wi-Fi names) as required. To distinguish the guest network from the main network, you are recommended to set different Wi-Fi network names.
5 GHz Wi-Fi Name	
Guest Network Password	It specifies the password for the router's two guest networks.
Validity	It specifies the validity of the guest networks. The guest network function will be disabled automatically out of the validity period.
Bandwidth for Guests	It allows you to specify the maximum upload and download speed for all devices connected to the guest networks. By default, the bandwidth is not limited.

6.2 An example of configuring the guest network

Scenario: A group of friends are going to visit your home and stay for about 8 hours.

Goal: Prevent the use of Wi-Fi network by guests from affecting the network speed of your computer for work purposes.

Solution: You can configure the guest network function and let your guests to use the guest networks.

Assume that the parameters you are going to set for the guest Wi-Fi network are:

- Wi-Fi names for 2.4 GHz and 5 GHz networks: John_Doe and John_Doe_5G
- Wi-Fi password for 2.4 GHz and 5 GHz networks: UmXmL9UK

Configuring procedure:

Step 1 Log in to the web UI of the router.

Step 2 Choose **Guest Network**, and enable the **Guest Network**.

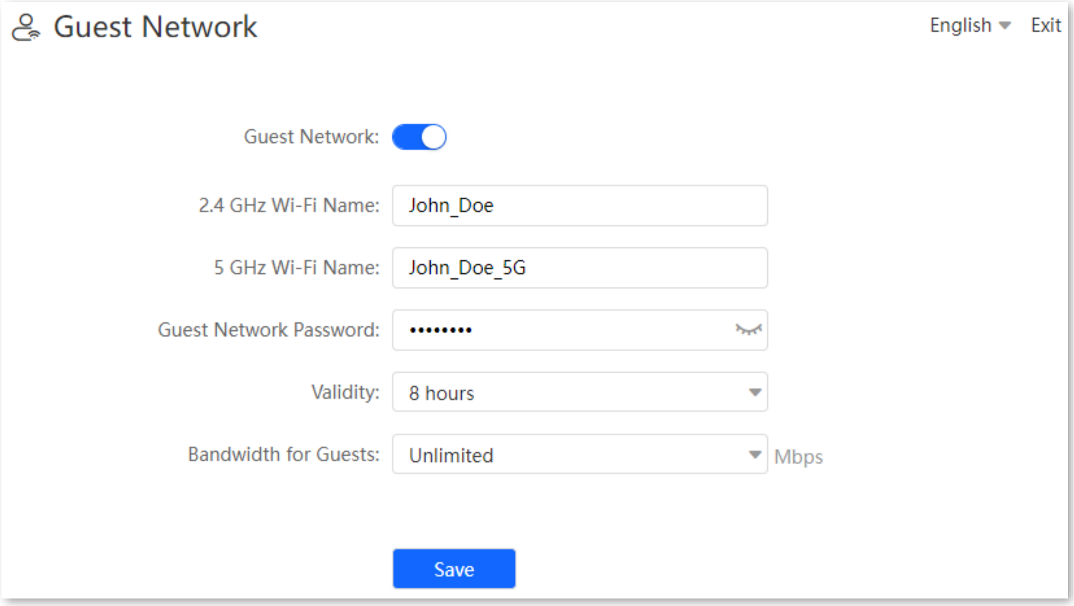
Step 3 Set the **2.4 GHz Wi-Fi Name**, which is **John_Doe** in this example.

Step 4 Set the **5 GHz Wi-Fi Name**, which is **John_Doe_5G** in this example.

Step 5 Set the **Guest Network Password**, which is **UmXmL9UK** in this example.

Step 6 Select a validity time from the **Validity** drop-down box, which is **8 hours** in this example.

Step 7 Click **Save**.



Guest Network: ●

2.4 GHz Wi-Fi Name: John_Doe

5 GHz Wi-Fi Name: John_Doe_5G

Guest Network Password: ••••••••

Validity: 8 hours

Bandwidth for Guests: Unlimited Mbps

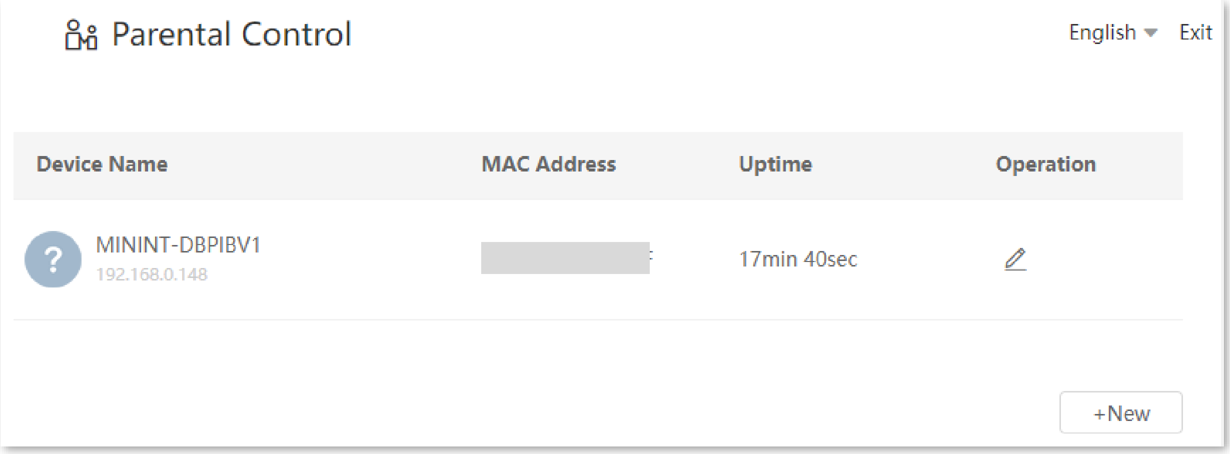
During the 8 hours after the configuration, guests can connect their wireless devices, such as smartphones, to **John_Doe** or **John_Doe_5G** to access the internet.

Chapter 7 Parental control

7.1 Overview

On the parental control page, you can view the information of online devices and configure their internet access options.

To access the configuration page, Log in to the web UI of the router, and choose **Parental Control**.



Parental Control

English ▾ Exit

Device Name	MAC Address	Uptime	Operation
MININT-DBPIBV1 192.168.0.148	[redacted]	17min 40sec	✎

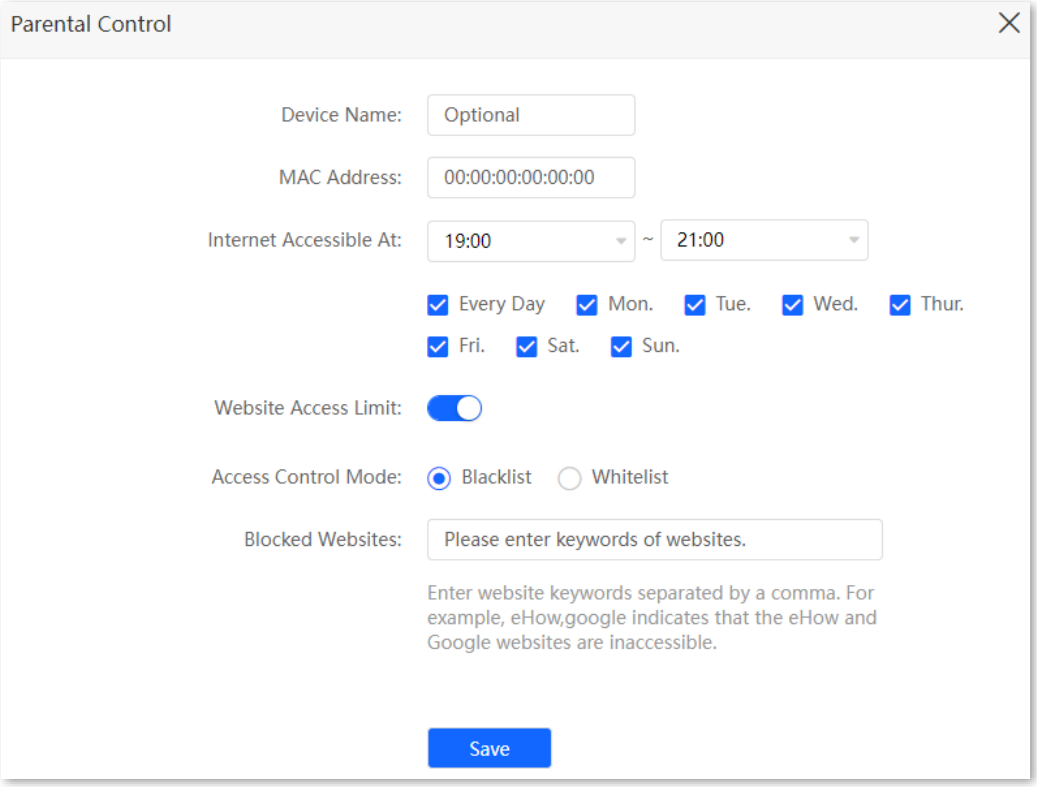
+New

Table 7-1 Parameter description

Parameter	Description
Device Name	It specifies the name of the online device.
MAC Address	It specifies the MAC address of the online device.
Uptime	It specifies the online duration of the device.
Operation	Available operations include: ● ✎ : Click to configure a parental control rule for the device. ● ✓ : Click to enable the configured rule. ● ⊘: Click to disable the configured rule.
+New	Click +New to add parental control rules for devices that are not connected to the router at the time.

7.2 Configure the parental control rule

Click ✎ or +New to edit or add a parental control rule. The +New button is used for illustration here.



Parental Control

Device Name: Optional

MAC Address: 00:00:00:00:00:00

Internet Accessible At: 19:00 ~ 21:00

☑ Every Day ☑ Mon. ☑ Tue. ☑ Wed. ☑ Thur.
☑ Fri. ☑ Sat. ☑ Sun.

Website Access Limit: ●

Access Control Mode: ● Blacklist ○ Whitelist

Blocked Websites: Please enter keywords of websites.

Enter website keywords separated by a comma. For example, eHow,google indicates that the eHow and Google websites are inaccessible.

Table 7-2 Parameter description

Parameter	Description
Device Name	It specifies the name of the device that the parental control rule applies to.
MAC Address	It specifies the MAC address of the device that the parental control rule applies to.
Internet Accessible At	It specifies the period during which the device can access the internet.
Website Access Limit	It is used to enable or disable the website access limit function.

Parameter	Description
Access Control Mode	When the website access limit function is enabled, there are two access control modes available. ● **Blacklist**: The device is blocked from accessing the websites specified in the rule during the specified period, but can access other websites. The device cannot access the internet at all out of the specified period. ● **Whitelist**: The device can access the websites specified in the rule during the specified period, but cannot access other websites. The device cannot access the internet at all out of the specified period.
Blocked Websites	They specify the websites that the device is blocked from accessing or allowed to access during the specified period.
Unblocked Websites	

7.3 An example of adding parental control rules

Scenario: The final exam for your kid is approaching and you want to configure the internet access through the router.

Goal: Your kid cannot access websites, such as Facebook, Twitter, Youtube and Instagram, during 8:00 to 22:00 on weekends using the computer in the room, and cannot access the internet from 22:00 to 8:00.

Solution: You can configure the parental control function to reach the goal.

Configuring procedure:

Step 1 Log in to the web UI of the router.

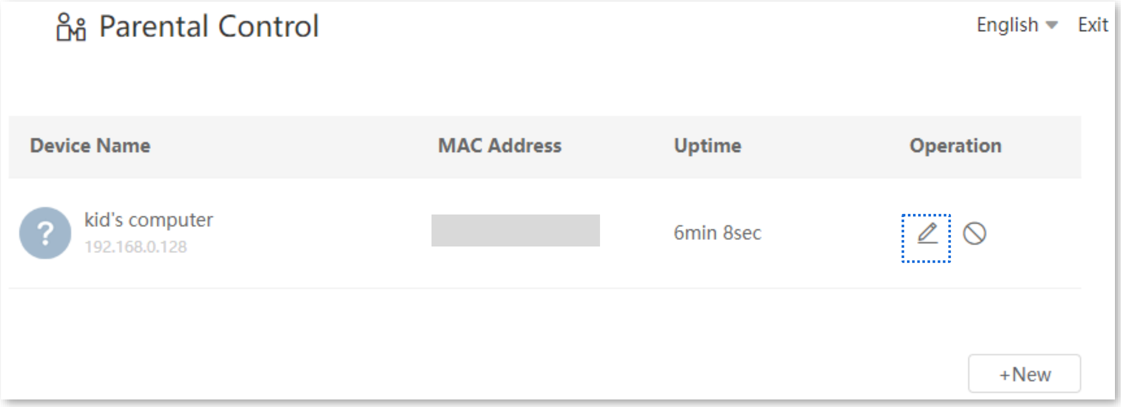
Step 2 Choose **Parental Control**.

Step 3 Configure the parental control rule.

1) Choose the device to which the rule applies, and click ✎ .

Note

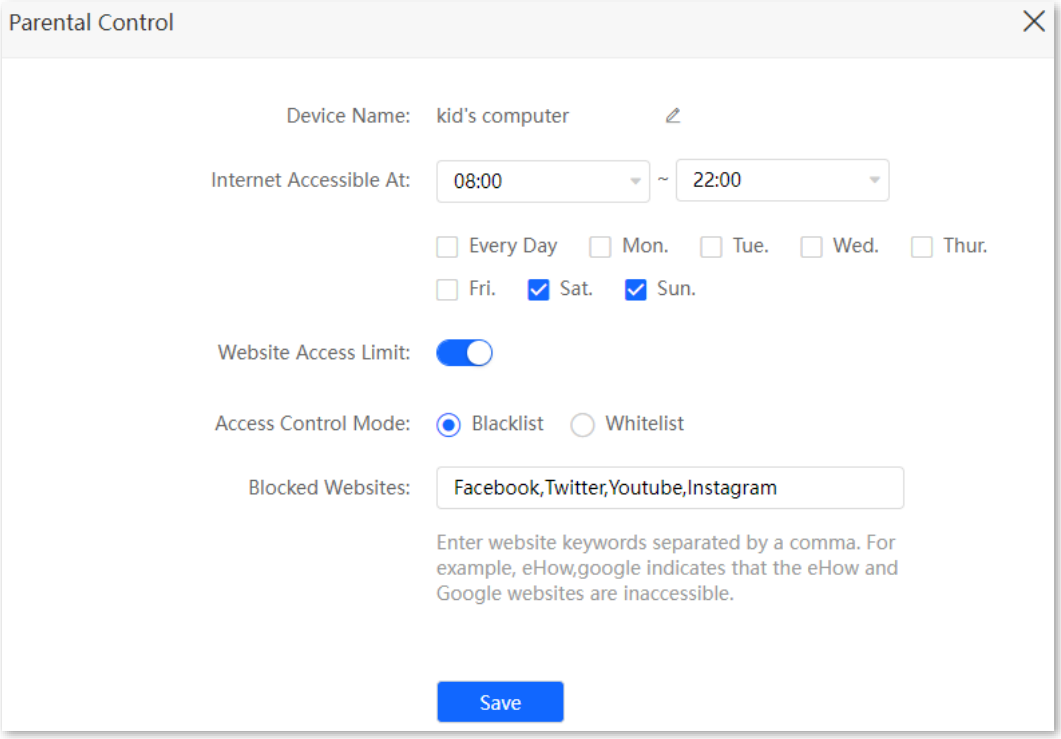
If the device to which the rule applies is not online at the time, you can click +New to add a parental control rule for the device.



Parental Control

Device Name	MAC Address	Uptime	Operation
kid's computer 192.168.0.128	[redacted]	6min 8sec	

2) Specify the period when the internet can be accessed, which is **8:00 ~ 22:00** in this example.
3) Tick the days when the rule is applied, which are **Sun.** and **Sat.** in this example.
4) Enable **Website Access Limit**, and choose **Blacklist**.
5) Set Blocked Websites, which is **Facebook,Twitter,Youtube,Instagram** in this example.
6) Click **Save**.



Parental Control

Device Name: kid's computer

Internet Accessible At: 08:00 ~ 22:00

□ Every Day □ Mon. □ Tue. □ Wed. □ Thur.
□ Fri. ☑ Sat. ☑ Sun.

Website Access Limit: ●

Access Control Mode: ● Blacklist ○ Whitelist

Blocked Websites: Facebook,Twitter,Youtube,Instagram

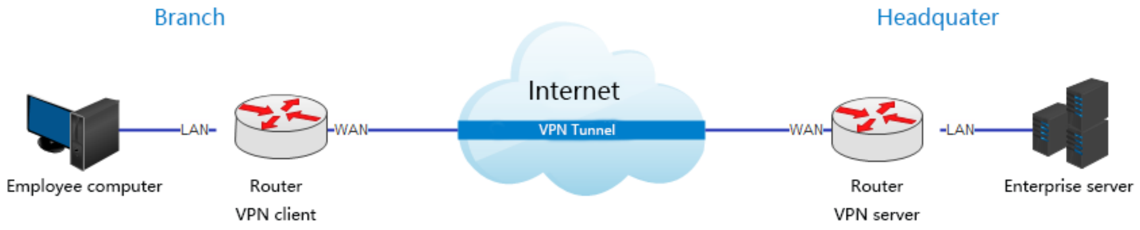
Enter website keywords separated by a comma. For example, eHow,google indicates that the eHow and Google websites are inaccessible.

After the configuration is completed, your kid can access any websites except for Facebook, Twitter, Youtube and Instagram from 8:00 to 22:00 on weekends, and your kid cannot access the internet at all between 22:00 to 8:00 on weekends.

Chapter 8 VPN

A VPN (Virtual Private Network) is a private network built on a public network (usually the Internet). This private network exists only logically and has no actual physical lines. VPN technology is widely used in corporate networks to share resources between corporate branches and headquarters, while ensuring that these resources are not exposed to other users on the internet.

The typology of a VPN network is shown below.

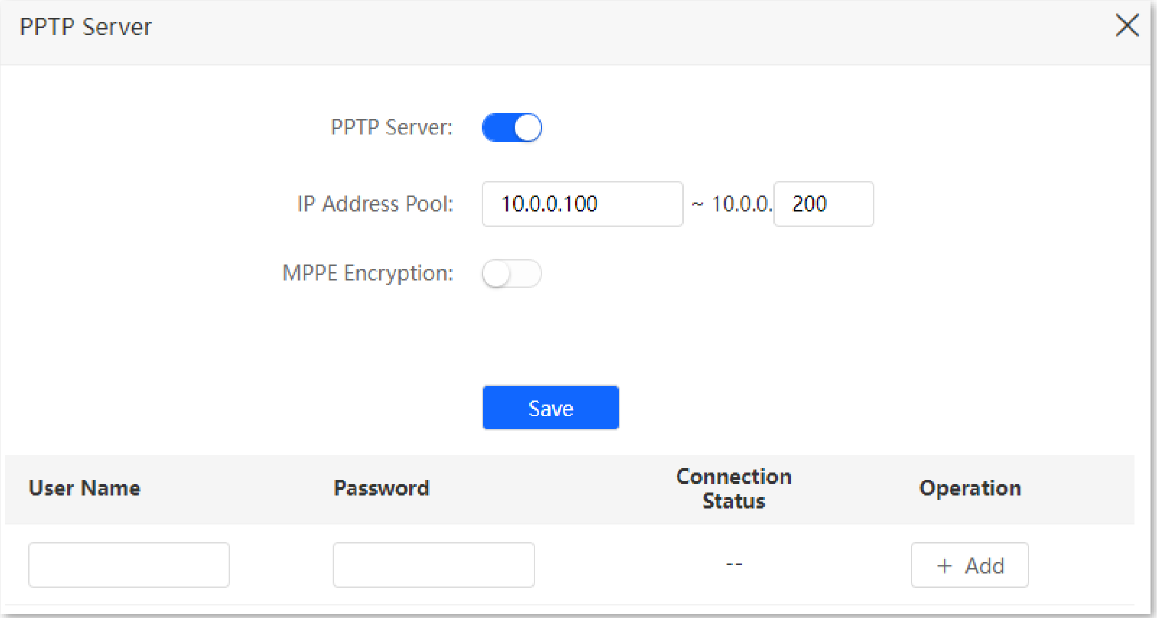


8.1 PPTP server

8.1.1 Overview

This router can function as a PPTP server and accept connections from PPTP clients.

To access the configuration page, Log in to the web UI of the router and choose **VPN** > **PPTP Server**. This function is disabled by default. When it is enabled, the page is shown as below.


PPTP Server

PPTP Server: ●

IP Address Pool: 10.0.0.100 ~ 10.0.0. 200

MPPE Encryption: ○

User Name	Password	Connection Status	Operation
		--	+ Add

Table 8-1 Parameter description

Parameter	Description
PPTP Server	It is used to enable or disabled the PPTP server. When it is enabled, the router functions as a PPTP server, which can accept the connections from PPTP clients.

Parameter	Description
IP Address Pool	It specifies the range of IP address range within which the PPTP server can assign to PPTP clients. It is recommended to keep the default settings.
MPPE Encryption	It is used to enable or disable 128-bit data encryption. The encryption settings should be the same between the PPTP server and PPTP clients. Otherwise, the communication cannot be achieved normally.
User Name	They specify the VPN user name and password, which the VPN user needs to enter when making PPTP dial-ups (VPN connections).
Password	
Connection Status	It specifies the connection status of the VPN connection.
Operation	Available operations include: + Add : It is used to add new PPTP user accounts. ⊘: It is used to disable the PPTP user account. ✓: It is used to enable the PPTP user account. 🗑: It is used to delete the PPTP user account.

8.1.2 Enable internet users to access resources of the LAN

Scenario: You have set up an FTP server within the LAN of the router.

Goal: Open the FTP server to internet users and enable them to access the resources of the FTP server from the internet.

Solution: You can configure the PPTP server function to reach the goal. Assume that:

- The user name and password that the PPTP server assigns to the client are both admin1.
- The WAN IP address of router is 113.88.112.220.
- The IP address of the FTP server is 192.168.0.136.
- The FTP server port is 21.
- The FTP login user name and password are both JohnDoe.

Note

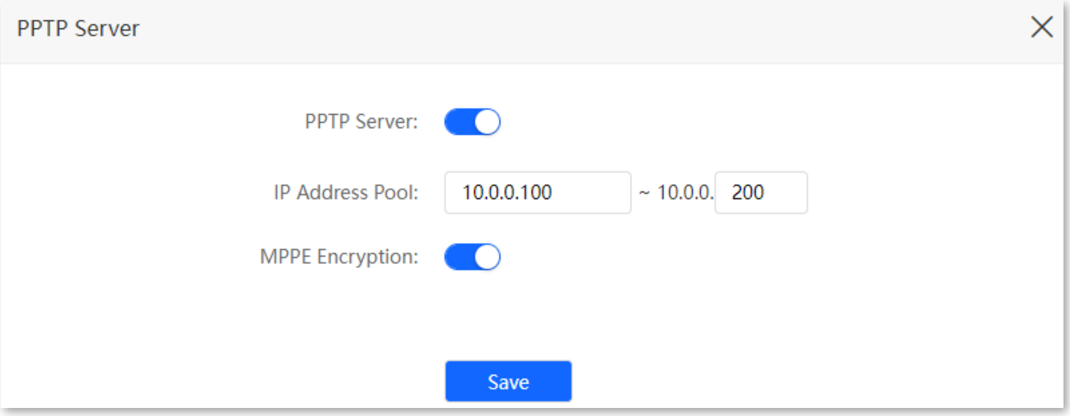
Please ensure the WAN IP address of router is a public network. This function may not work on a host with an IP address of a private network. Common IPv4 addresses are classified into class A, class B and class C. Private IP addresses of class A range from 10.0.0.0 to 10.255.255.255. Private IP addresses of class B range from 172.16.0.0-172.31.255.255. Private IP addresses of class C range from 192.168.0.0-192.168.255.255.

Configuring procedure:

Step 1 Log in to the web UI of the router.

Step 2 Enable the PPTP server function.

1) Choose **VPN** > **PPTP Server**.
2) Enable the **PPTP Server**.
3) Enable the **MPPE Encryption**, which means that the encryption digit remains the default value "128".
4) Click **Save**.



PPTP Server

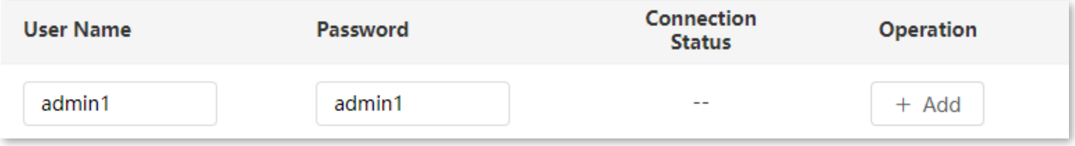
PPTP Server: ●

IP Address Pool: 10.0.0.100 ~ 10.0.0. 200

MPPE Encryption: ●

Step 3 Add PPTP user name and password.

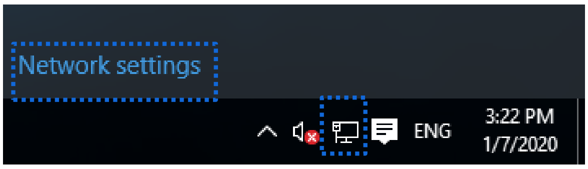
1) Set the **User Name** and **Password** of the PPTP server, which are both **admin1** in this example.
2) Click **+Add**.



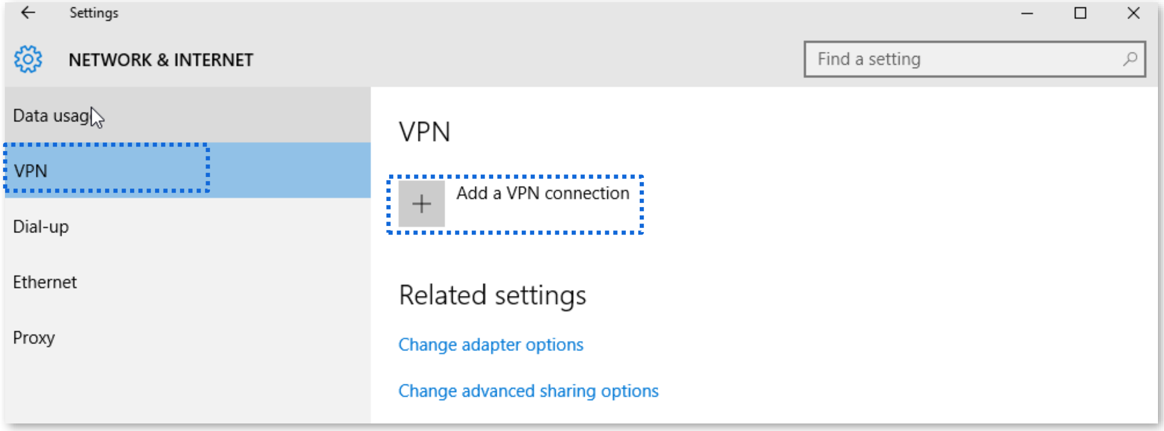
User Name	Password	Connection Status	Operation
admin1	admin1	--	+ Add

When completing the configurations, internet users can access the FTP server by following these steps (Windows 10 is used for illustration here):

Step 1 Click the 🖳 icon at the bottom right corner on the desktop, and then click **Network settings**.

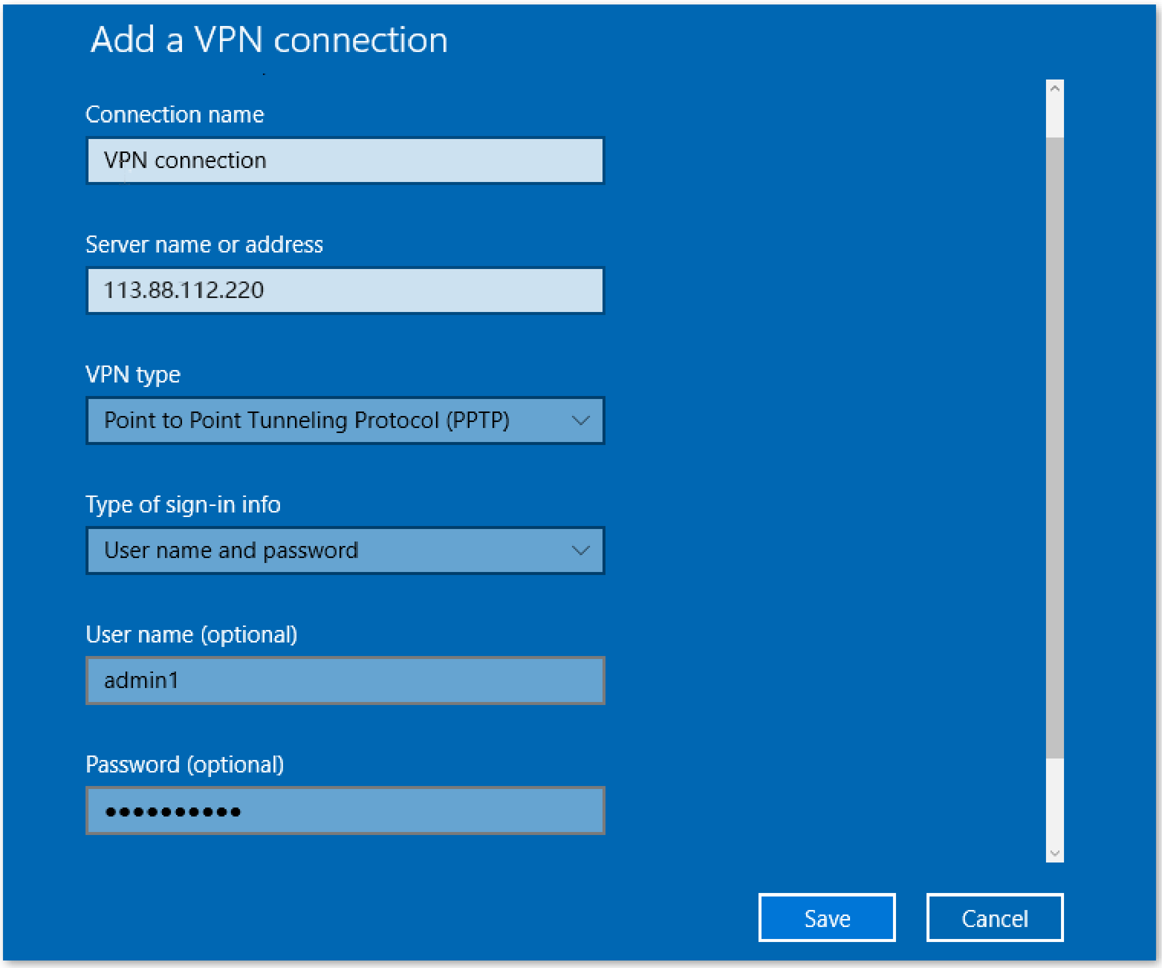


Step 2 Choose **VPN** on the left side, and click **Add a VPN connection**.



Step 3 Configure the VPN parameters.

1) Enter a connection name, such as **VPN connection**.
2) Enter the server address, which is **113.88.112.220** in this example.
3) Select a VPN type, which is **Point to Point Tunneling Protocol (PPTP)** in this example.
4) Select a type of sign-in info, which is **User name and password** in this example.
5) Enter the user name and password, which are both **admin1** in this example.
6) Click **Save**.



Add a VPN connection

Connection name: VPN connection

Server name or address: 113.88.112.220

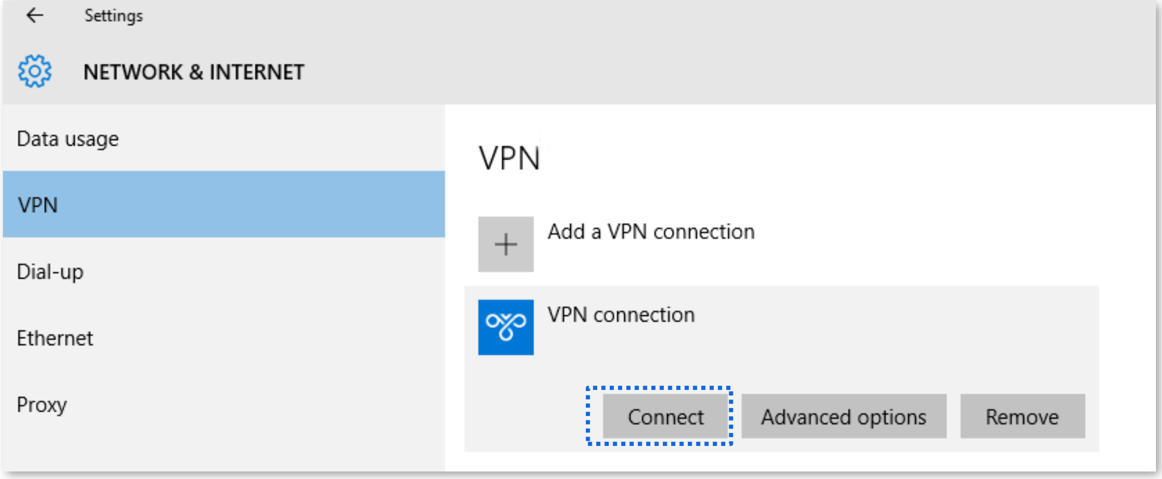
VPN type: Point to Point Tunneling Protocol (PPTP)

Type of sign-in info: User name and password

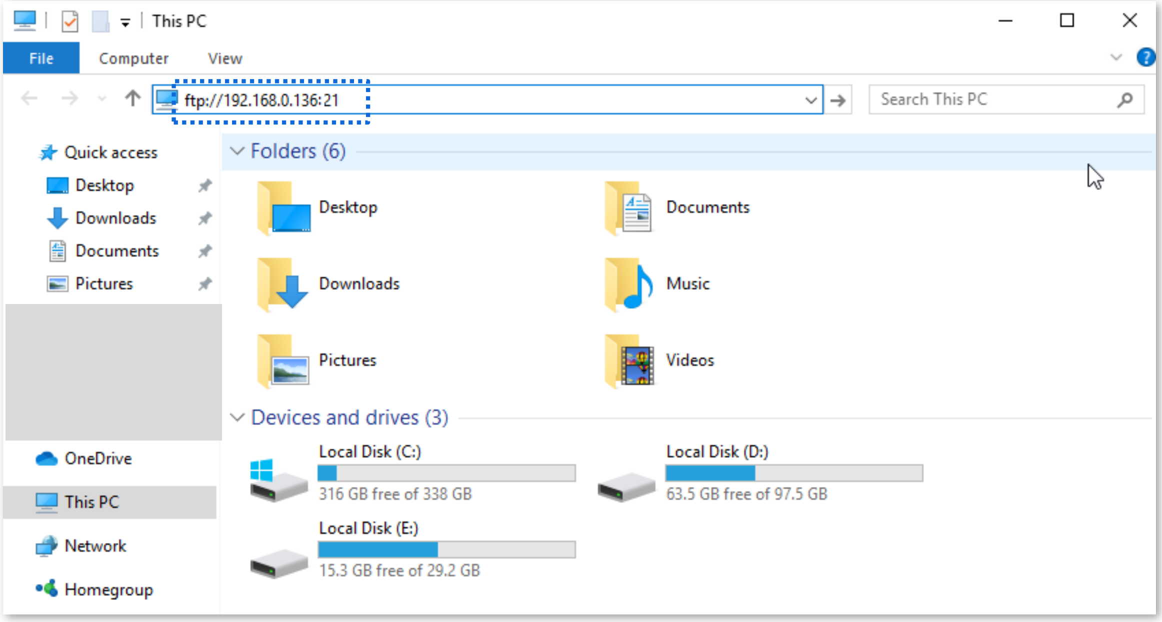
User name (optional): admin1

Password (optional): ●●●●●●●●●●

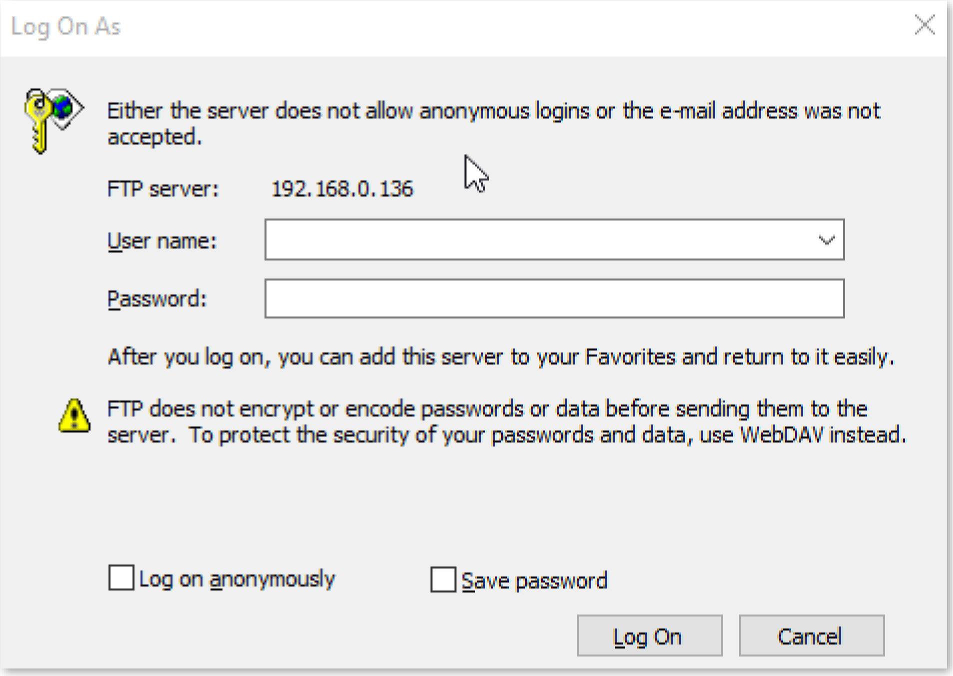
Step 4 Target the VPN connection added, and click **Connect**.



Step 5 Click the icon on the desktop, and enter the address in the address bar to access the FTP server, which is **ftp://192.168.0.136:21** in this example.



Step 6 Enter the user name and password for logging in to the FTP server, which are both **JohnDoe** in this example, and click **Log On**.



Log On As

Either the server does not allow anonymous logins or the e-mail address was not accepted.

FTP server: 192.168.0.136

User name:

Password:

After you log on, you can add this server to your Favorites and return to it easily.

FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use WebDAV instead.

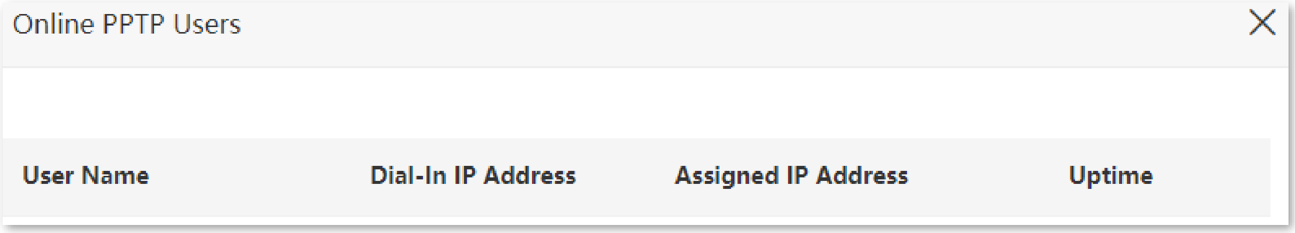
□ Log on anonymously □ Save password

By performing the steps above, you can access the resources on the FTP server.

8.2 Online PPTP users

When the PPTP server function is enabled, you can view the detailed information of VPN clients that establish connections with the PPTP server.

To access the configuration page, Log in to the web UI of the router and choose **VPN** > **Online PPTP Users**.



Online PPTP Users

User Name	Dial-In IP Address	Assigned IP Address	Uptime

Table 8-2 Parameter description

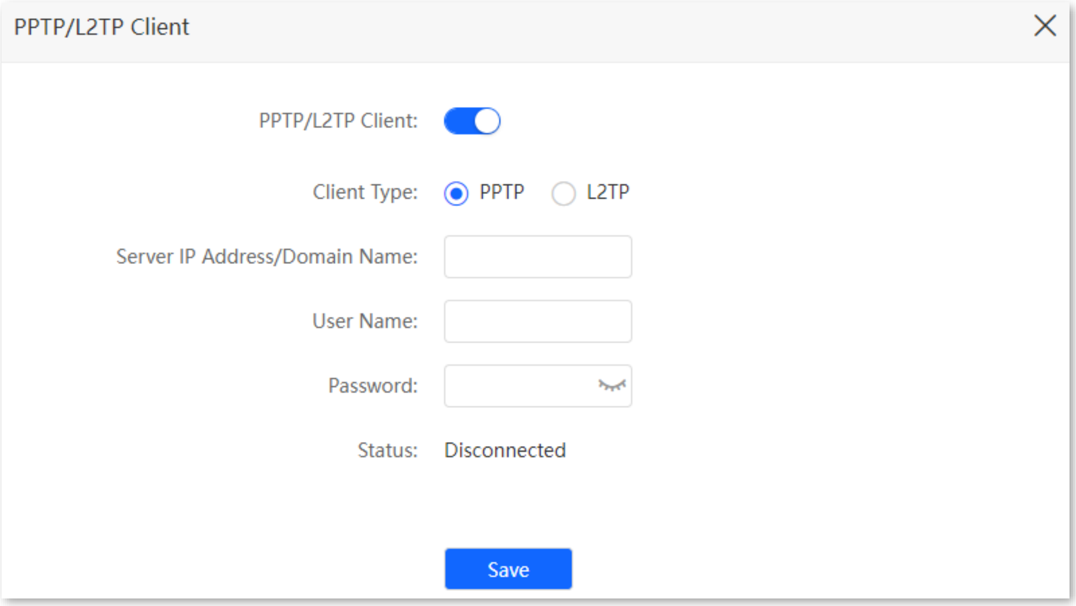
Parameter	Description
User Name	It specifies the VPN user name, which the VPN user uses when making PPTP dial-ups (VPN connection).
Dial-In IP Address	It specifies the IP address of the PPTP client. If the client is a router, it will be the IP address of the WAN port whose VPN function is enabled.
Assigned IP Address	It specifies the IP address that the PPTP server assigns to the client.
Uptime	It specifies the online time since the VPN connection succeeds.

8.3 PPTP/L2TP client

8.3.1 Overview

This router can function as a PPTP/L2TP client and connect to PPTP/L2TP servers.

The PPTP/L2TP client function is disabled by default. When it is enabled, the page is shown as below.



PPTP/L2TP Client

PPTP/L2TP Client: ●

Client Type: ● PPTP ○ L2TP

Server IP Address/Domain Name:

User Name:

Password:

Status: Disconnected

Table 8-3 Parameter description

Parameter	Description
PPTP/L2TP Client	It is used to enable or disable the PPTP/L2TP client function.
Client Type	It specifies the client type that the router serves as, either PPTP or L2TP. ● **PPTP**: When the router is connecting to a PPTP server, choose this option. ● **L2TP**: When the router is connecting to a L2TP server, choose this option.
Server IP Address/Domain Name	It specifies the IP address or domain name of the PPTP/L2TP server that the router connects to. Generally, when a router serves as the PPTP/L2TP server at the peer side, the domain name or IP address should be that of the WAN port whose PPTP/L2TP server function is enabled.
User Name	They specify the user name and password that the PPTP/L2TP server assigns to the PPTP/L2TP clients.
Password	
Status	It specifies the connection status of the VPN connection.

8.3.2 Access VPN resources with the router

Scenario: You have subscribed to the PPTP VPN service when purchasing the broadband service from your ISP.

Goal: Access the VPN resources of your ISP.

Solution: You can configure the PPTP/L2TP client function to reach the goal. Assume that:

- The IP address of the PPTP server is 113.88.112.220.
- The user name and password assigned by the PPTP server are both admin1.

Configuring procedure:

Step 1 Log in to the web UI of the router.

Step 2 Choose **VPN** > **PPTP/L2TP Client**.

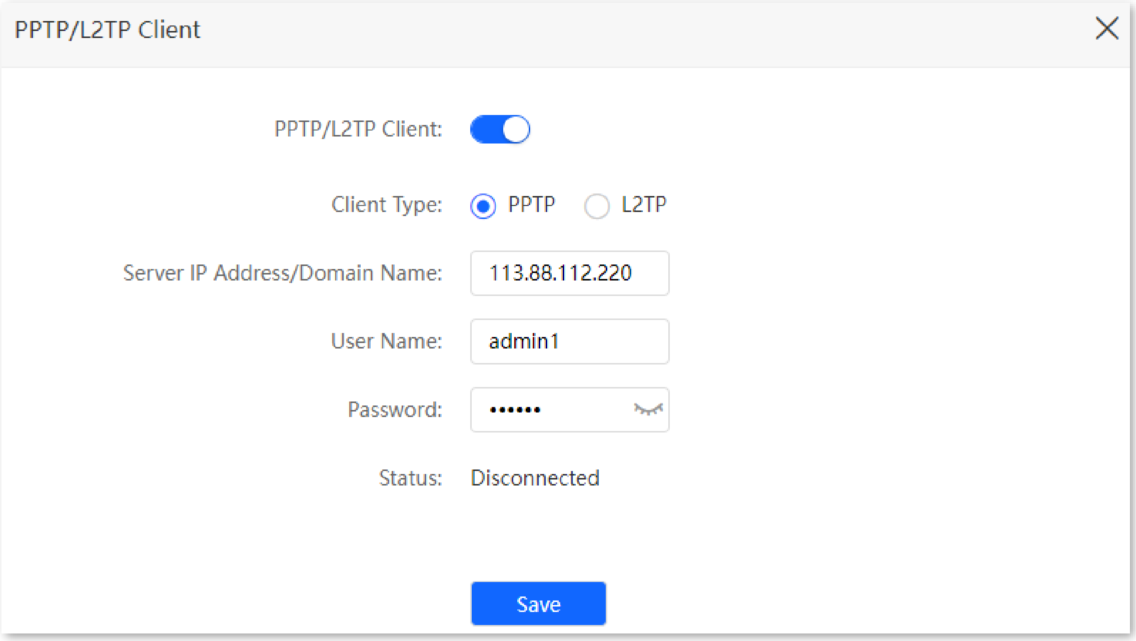
Step 3 Enable the **PPTP/L2TP Client**.

Step 4 Choose **PPTP** as the client type.

Step 5 Enter the **Server IP Address/Domain Name**, which is **113.88.112.220** in this example.

Step 6 Enter the **User Name** and **Password**, which are both **admin1** in this example.

Step 7 Click **Save**.



PPTP/L2TP Client

PPTP/L2TP Client: ●

Client Type: ◉ PPTP ○ L2TP

Server IP Address/Domain Name: 113.88.112.220

User Name: admin1

Password: ••••••

Status: Disconnected

When Connected is shown in **Status**, you can access the VPN resources of your ISP.

Chapter 9 IPv6 (wireless router mode)

Note

This function is only available under the wireless router mode. Refer to Operating mode to set the operating mode of the router.

This router supports IPv4 and IPv6 dual stack protocols. In the IPv6 part, you can:

- Connect to the IPv6 network of ISPs
- Configure the IPv6 tunnel and achieve communications between IPv6 islands
- Change IPv6 LAN settings

9.1 IPv6 WAN settings

9.1.1 Connect to the IPv6 network of ISPs

The router can access the IPv6 network of ISPs through three connection types. Choose the connection type by referring to the following chart.

Scenario	Connection Type
● The ISP does not provide any PPPoEv6 user name and password. ● The ISP does not provide information about IPv6 address. ● You have a router that can access IPv6 network.	DHCPv6
IPv6 service is included in the PPPoE user name and password.	PPPoEv6
The ISP provides you with a set of information including IPv6 address, subnet mask, default gateway and DNS server.	Static IPv6 address

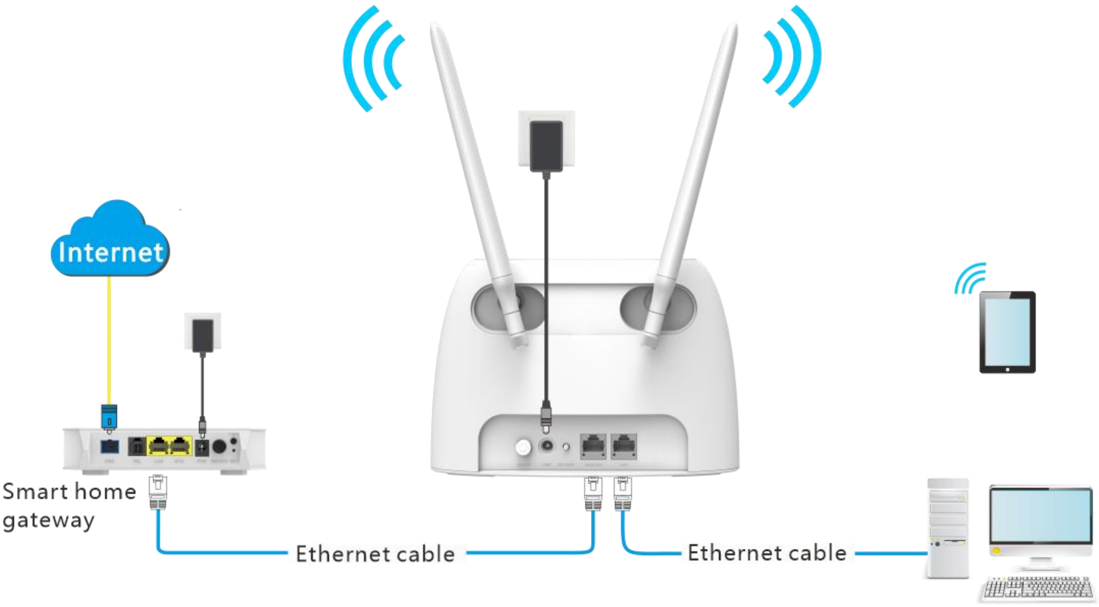
Note

Before configuring the IPv6 function, please ensure that you are within the coverage of IPv6 network and have already subscribed to the IPv6 internet service. Contact your ISP for any doubt about it.

DHCPv6

DHCPv6 enables the router to obtain IPv6 address from DHCPv6 server to access the internet, which is applicable in the following scenarios.

- The ISP does not provide any PPPoEv6 user name and password.
- The ISP does not provide information about IPv6 address.
- You have a router that can access IPv6 network.



Configuring procedure:

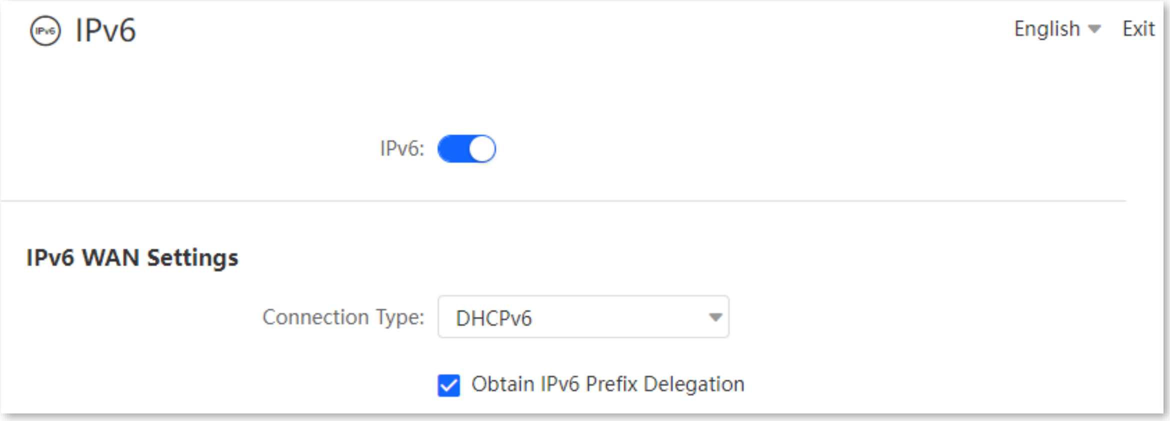
Step 1 Log in to the web UI of the router.

Step 2 Choose **IPv6**.

Step 3 Enable the **IPv6** function.

Step 4 Set **Connection Type** to **DHCPv6**.

Step 5 Click **Save**.



IPv6: ●

IPv6 WAN Settings

Connection Type: DHCPv6

☑ Obtain IPv6 Prefix Delegation

Table 9-1 Parameter description

Parameter	Description
Obtain IPv6 Prefix Delegation	When the option is selected, the LAN port of router obtains IPv6 prefix from its upstream device. It is recommended to keep the default setting (Selected). If the LAN port cannot obtain the PD prefix, it is because the upstream device does not support PD prefix delivery. Contact your ISP to solve this problem.

IPv6 network test:

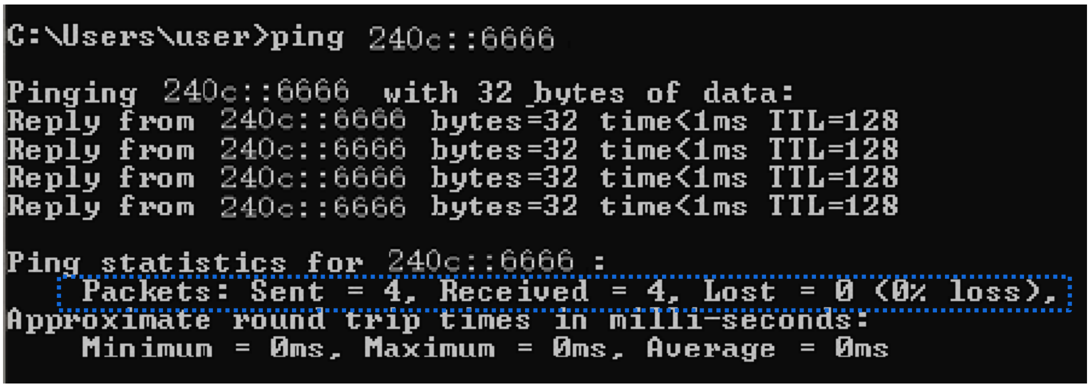
You can ping an IPv6 website (240c::6666 for example) to check whether the router accesses the IPv6 network successfully. The following steps are for your reference.

Step 1 On a computer connected to the router, press **Windows** + **R** to open the **Run** dialog box.

Step 2 Type **cmd** and then click **OK** to open a regular Command Prompt.

Step 3 Enter ping **240c::6666** and press **Enter**.

As shown in the following figure, if the number of packets received is not 0, the router accesses the IPv6 network successfully.



```
C:\Users\user>ping 240c::6666

Pinging 240c::6666 with 32 bytes of data:
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Reply from 240c::6666 bytes=32 time<1ms TTL=128

Ping statistics for 240c::6666 :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

If the IPv6 network test fails, try the following solutions:

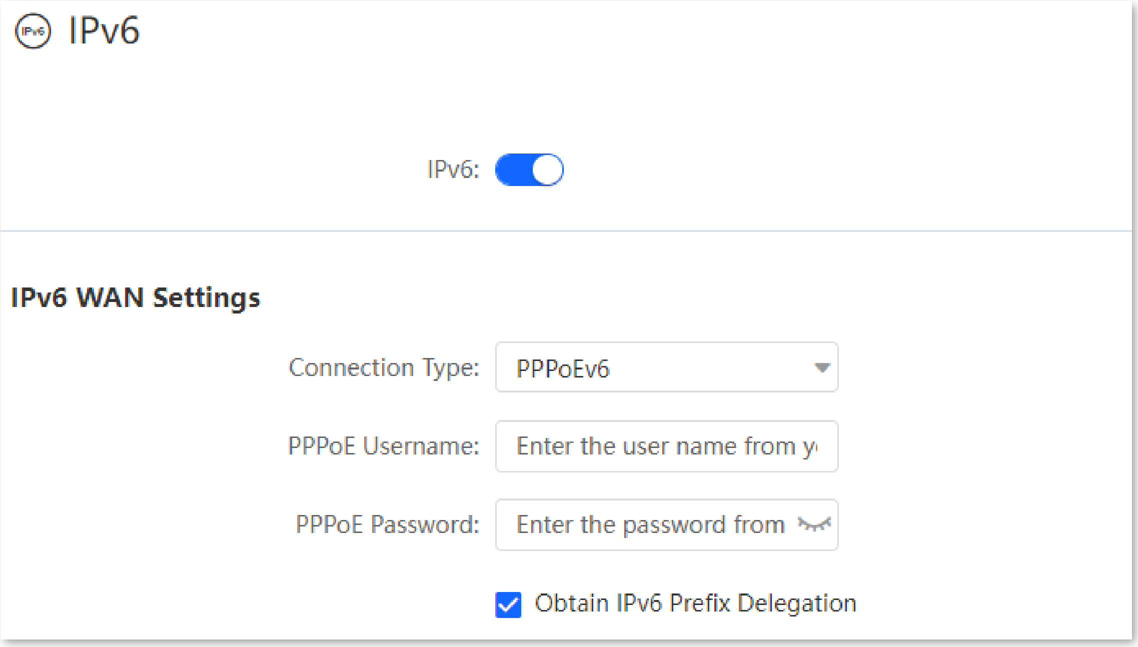
- Choose the **System Settings** > **System Status**, and move to the **IPv6 Status** part. Ensure that the IPv6 WAN address is a global unicast address.
- Ensure that devices connected to router obtain their IPv6 address through DHCPv6.
- Consult your ISP for help.

PPPoEv6

Overview

If your ISP provides you with the PPPoE user name and password with IPv6 service, you can choose PPPoEv6 to access the internet.

Log in to the web UI of the router, and choose the **IPv6**. When the connection type is set to **PPPoEv6**, the page is shown as below.



IPv6

IPv6: ●

IPv6 WAN Settings

Connection Type: PPPoEv6

PPPoE Username: Enter the user name from y

PPPoE Password: Enter the password from

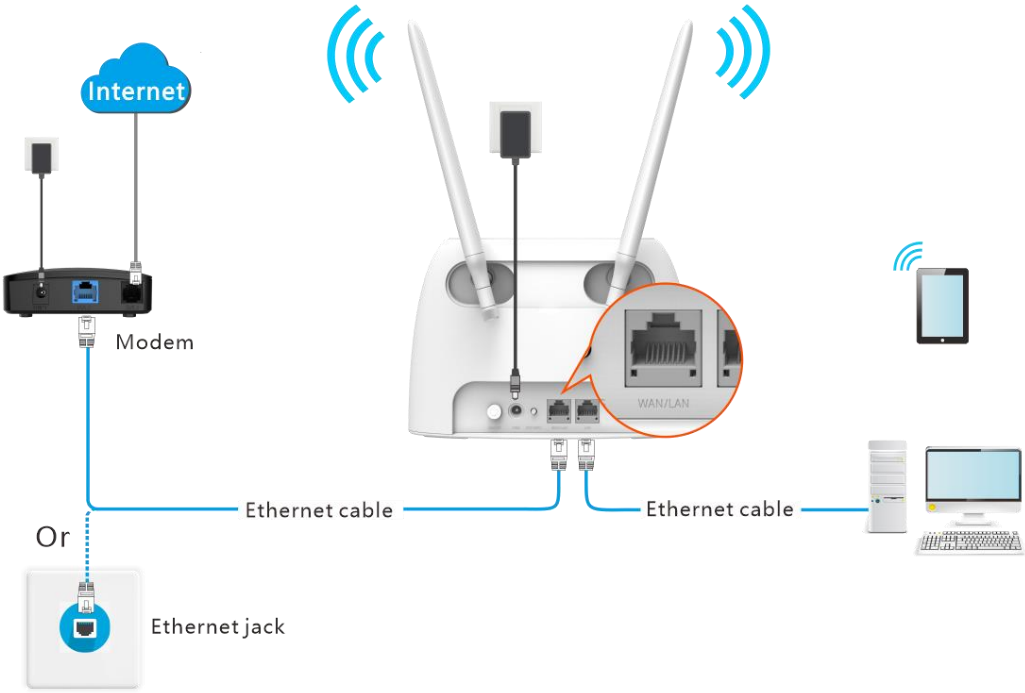
☑ Obtain IPv6 Prefix Delegation

Table 9-2 Parameter description

Parameter	Description
PPPoE Username PPPoE Password	They specify the PPPoE user name and password provided by your ISP. **Note** IPv4 and IPv6 services share the same PPPoE account.
Obtain IPv6 Prefix Delegation	When the option is selected, the LAN port of router obtains IPv6 prefix from its upstream device. It is recommended to keep the default setting (Selected). If the LAN port cannot obtain the PD prefix, it is because the upstream device does not support PD prefix delivery. Contact your ISP to solve this problem.

Access the internet through PPPoEv6

If the PPPoE account provided by your ISP includes IPv6 service, you can choose PPPoEv6 to access the IPv6 service. The application scenario is shown as below.



Configuring procedure:

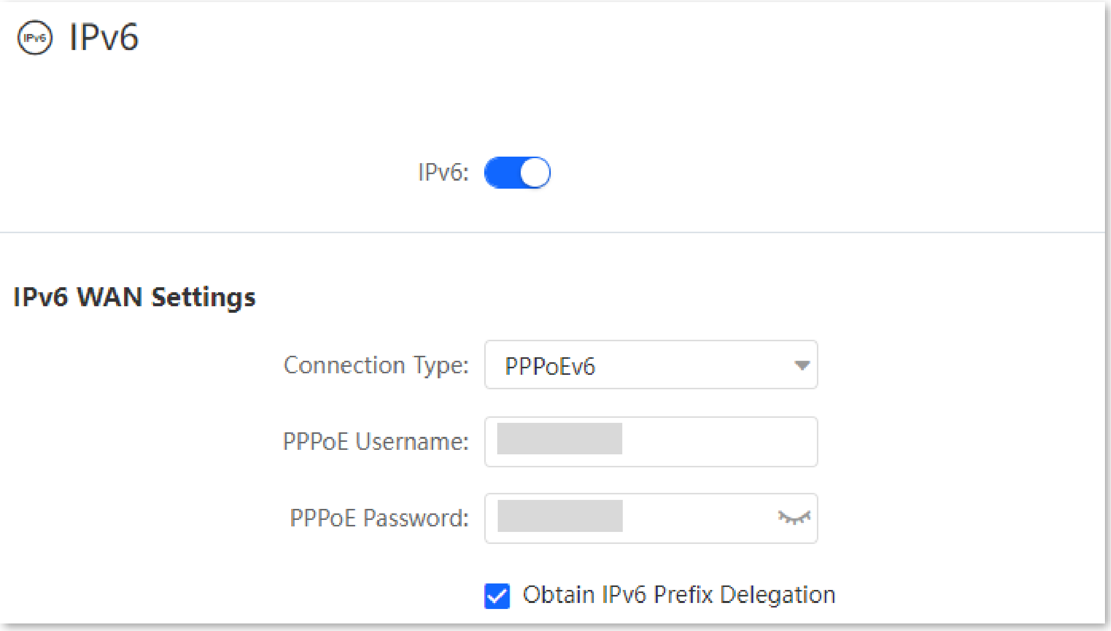
Step 1 Log in to the web UI of the router.

Step 2 Choose **IPv6**, and enable the **IPv6** function.

Step 3 Set **Connection Type** to **PPPoEv6**.

Step 4 Enter the **PPPoE Username** and **PPPoE Password**.

Step 5 Click **Save**.



IPv6

IPv6: ●

IPv6 WAN Settings

Connection Type: PPPoEv6

PPPoE Username:

PPPoE Password:

☑ Obtain IPv6 Prefix Delegation

IPv6 network test:

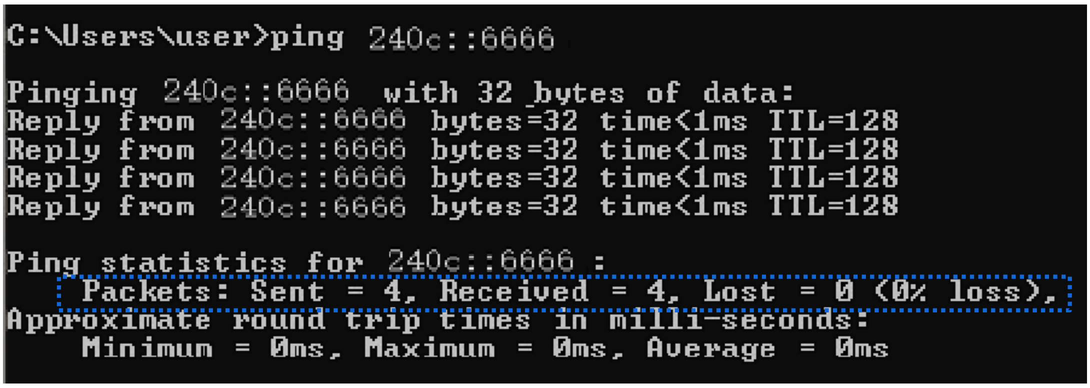
You can ping an IPv6 website (240c::6666 for example) to check whether the router accesses the IPv6 network successfully. The following steps are for your reference.

Step 1 On a computer connected to the router, press **Windows** + **R** to open the **Run** dialog box.

Step 2 Type **cmd** and then click **OK** to open a regular Command Prompt.

Step 3 Enter ping **240c::6666** and press **Enter**.

As shown in the following figure, if the number of packets received is not 0, the router accesses the IPv6 network successfully.



```
C:\Users\user>ping 240c::6666

Pinging 240c::6666 with 32 bytes of data:
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Reply from 240c::6666 bytes=32 time<1ms TTL=128

Ping statistics for 240c::6666 :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

If the IPv6 network test fails, try the following solutions:

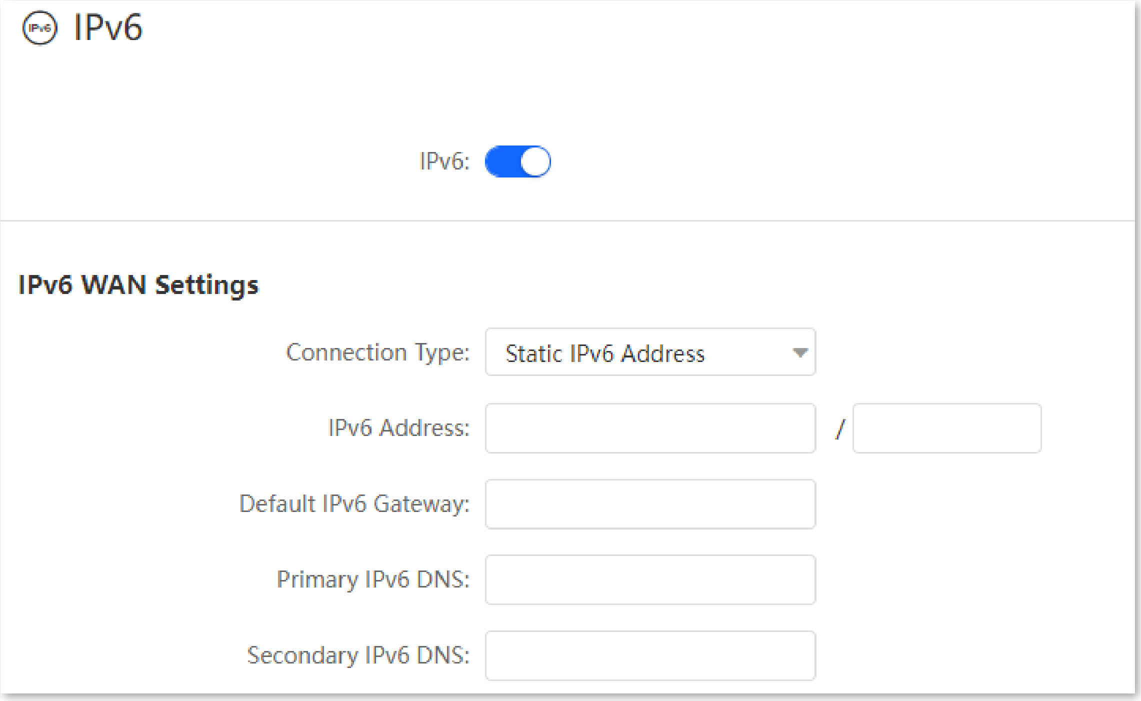
- Choose the **System Settings** > **System Status**, and move to the **IPv6 Status** part. Ensure that the IPv6 WAN address is a global unicast address.
- Ensure that devices connected to router obtain their IPv6 address through DHCPv6.
- Consult your ISP for help.

Static IPv6 Address

Overview

When your ISP provides you with information including IPv6 address, subnet mask, default gateway and DNS server, you can choose this connection type to access the internet with IPv6.

Log in to the web UI of the router, and choose the **IPv6**. When the connection type is set to **Static IPv6 Address**, the page is shown as below.



Connection Type: Static IPv6 Address

Table 9-3 Parameter description

Parameter	Description
IPv6 Address	They specify the fixed IP address information provided by your ISP. **Note** If your ISP only provides one DNS address, leave the secondary IPv6 DNS blank.
Default IPv6 Gateway	
Primary IPv6 DNS	
Secondary IPv6 DNS	

Access the internet through static IPv6 address

Configuring procedure:

Step 1 Log in to the web UI of the router.

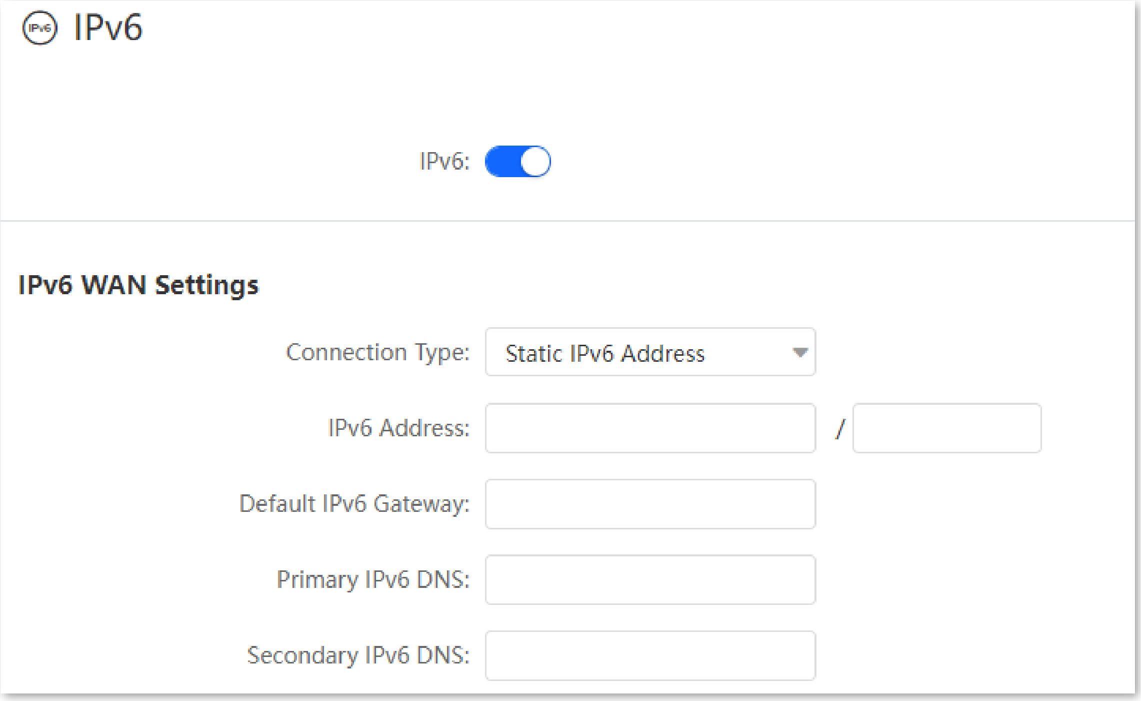
Step 2 Choose **IPv6**.

Step 3 Enable the **IPv6** function.

Step 4 Set the connection type to **Static IPv6 Address**.

Step 5 Enter the required parameters under IPv6 WAN settings.

Step 6 Click **Save**.



IPv6

IPv6: ●

IPv6 WAN Settings

Connection Type: Static IPv6 Address

IPv6 Address: /

Default IPv6 Gateway:

Primary IPv6 DNS:

Secondary IPv6 DNS:

IPv6 network test:

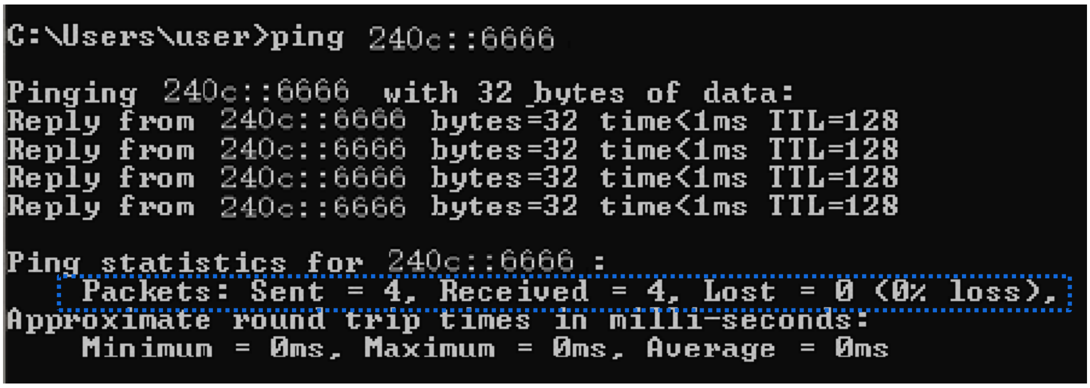
You can ping an IPv6 website (240c::6666 for example) to check whether the router accesses the IPv6 network successfully. The following steps are for your reference.

Step 1 On a computer connected to the router, press **Windows** + **R** to open the **Run** dialog box.

Step 2 Type **cmd** and then click **OK** to open a regular Command Prompt.

Step 3 Enter ping **240c::6666** and press **Enter**.

As shown in the following figure, if the number of packets received is not 0, the router accesses the IPv6 network successfully.



```
C:\Users\user>ping 240c::6666

Pinging 240c::6666 with 32 bytes of data:
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Reply from 240c::6666 bytes=32 time<1ms TTL=128

Ping statistics for 240c::6666 :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

If the IPv6 network test fails, try the following solutions:

- Ensure that you have entered the correct WAN IPv6 address.
- Ensure that devices connected to router obtain their IPv6 address through DHCPv6.
- Consult your ISP for help.

9.1.2 IPv6 tunnel

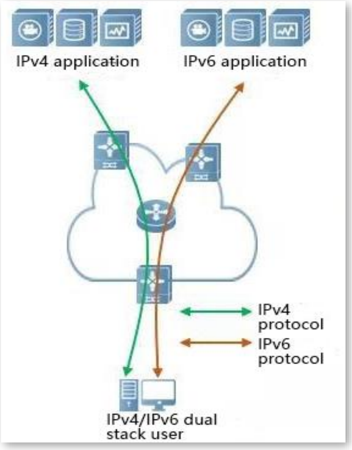
Overview

IPv6 transition mechanism

Before the IPv6 network is widely deployed, IPv6 stations are like isolated islands. Therefore, the dual stack and tunneling technologies are developed to achieve the communications between IPv6 islands.

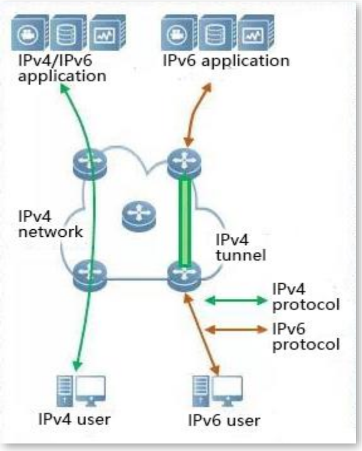
- Dual stack technology

  With the dual stack technology, nodes within the network support both IPv4 and IPv6 protocol stack. The source node selects different protocol stacks according to the different destination nodes, and the network device selects different protocol stacks for processing and forwarding according to the protocol type of the message. The dual-stack technology can realize the coexistence of IPv4 and IPv6 networks, but it cannot solve the problem of interoperability between IPv4 and IPv6 networks, nor can it solve the problem of IPv4 address exhaustion.



- Tunneling technology

  Tunneling technology is a technology for network transmission by encapsulating one IP protocol data packet in another IP protocol data packet, including data encapsulation, transmission, and decapsulation. IPv6 tunnel technology encapsulates IPv6 packets as data in IPv4 packets and communicates across IPv4 networks. With tunneling technology, you do not need to upgrade all devices to dual stacks. You only need the edge devices of IPv4 / IPv6 networks to implement dual stack and tunnel functions.



Manual and automatic tunnels

Generally, a tunnel consists of three parts: the tunnel start node, which encapsulates IPv6 packets; the tunnel end point, which decapsulates IPv6 packets; the tunnel, which is actually an IPv4 path, starts the encapsulated IPv6 packets from the tunnel. The node is transported to the end of the tunnel.

When the tunnel start node encapsulates an IPv6 packet in an IPv4 packet, it must determine the source and destination addresses of IPv4. The source address is the IPv4 address of the start node of the tunnel, and the destination address is the IPv4 address of the end of the tunnel.

Tunnels can be divided into manual tunnels and automatic tunnels based on how the tunnel end address is obtained.

- Manual tunnel

  The network boundary device cannot automatically obtain the IPv4 address of the tunnel endpoint. You need to manually configure the IPv4 address of the tunnel endpoint so that the packets can be sent to the tunnel endpoint correctly. It is usually used in the tunnel between routers.

- Automatic tunnel

  Network edge devices can automatically obtain the IPv4 address of the tunnel endpoint, without the need to manually configure the IPv4 address of the endpoint. In general, the IPv6 addresses at both ends of the tunnel are in the form of special IPv6 addresses with embedded IPv4 addresses. In this way, routing devices can extract IPv4 addresses from the destination IPv6 addresses in IPv6 packets. Automatic tunnels can be used from host to host, or from host to router.

6in4 tunnel

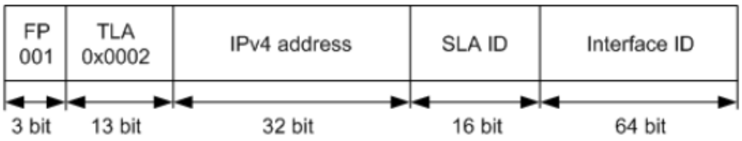
6in4 is a manual tunneling technology. It can implement IPv6 isolated island communication through manually configured tunnels without the network operator providing IPv6 interconnection services.

6to4 tunnel

6to4 is an automatic tunneling technology that enables communication between isolated IPv6 islands and between sites within the IPv6 backbone and IPv6 backbone networks without the network operator providing IPv6 interconnection services.

The 6to4 tunnel technology is used to establish a tunnel between edge routers at an IPv6 site. The edge router at the source site is the start node of the tunnel, and the edge router at the destination site is the end point of the tunnel.

The 6to4 tunnel technology uses a special IPv6 address, that is, a 6to4 address, which starts with 2002. The IPv4 address of the edge router is embedded in the prefix of this address. The address structure is shown in the figure below.



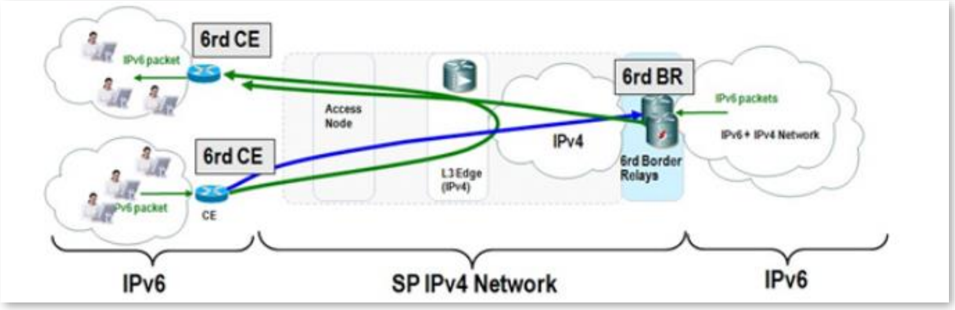
- FP: Format Prefix, which is 001

- TLA: Top Level Aggregator, which is 0x0002
- IPv4 address: The IPv4 address of the edge router
- SLA ID: Site Level Aggregator, namely the ID of subnet
- Interface ID: The ID of the interface

6rd tunnel

6RD (IPv6 Rapid Deployment) is an IPv6 network transition technology solution developed based on 6to4. It adds a 6RD BR (edge Relay, edge Relay Device) to an existing IPv4 network, establishes a 6in4 tunnel at the home gateway (6RD CE (Customer Edge)) and 6RD BR of IPv6 users, and provides IPv6 access to users.

The 6RD network typology is as follows.



As shown in the figure above, the 6RD tunnel technology is used to implement mutual access between IPv6 islands, and the BR can also be used to access the IPv6 network after the BR.

The main differences between 6RD and 6to4:

6RD does not need to use a specific address 2002::/16, it can use the network operator's own address block, which greatly increases the convenience of implementation.

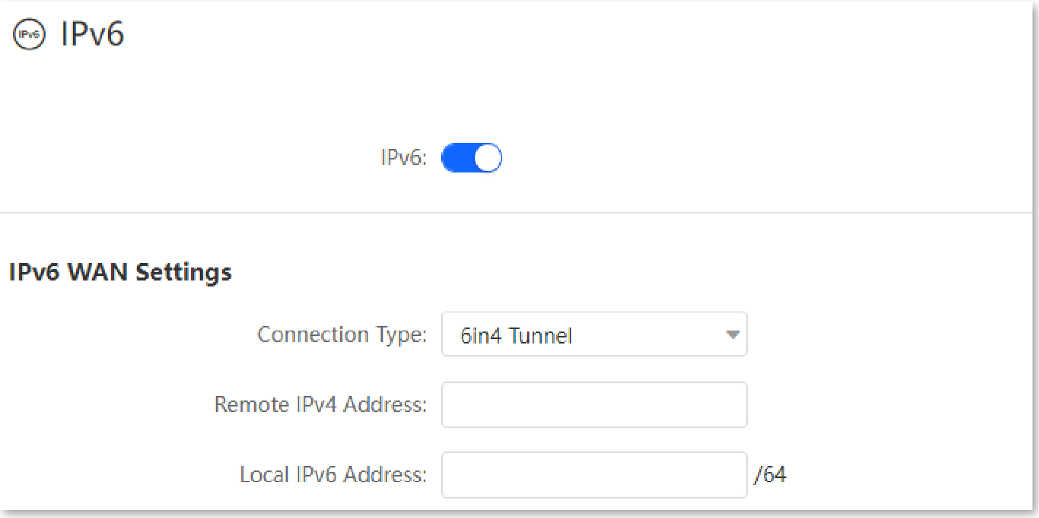
Configure IPv6 tunnel

Note

- Devices at both ends of the tunnel must support the dual stack protocol.
- The WAN IPv4 address of the routers must be a public IP address.

6in4 tunnel

Log in to the web UI of the router, and choose **IPv6**. Enable the **IPv6** function, set **Connection Type** to **6in4 Tunnel**, enter required parameters and save the configurations.



IPv6: on

IPv6 WAN Settings

Connection Type: 6in4 Tunnel

Remote IPv4 Address:

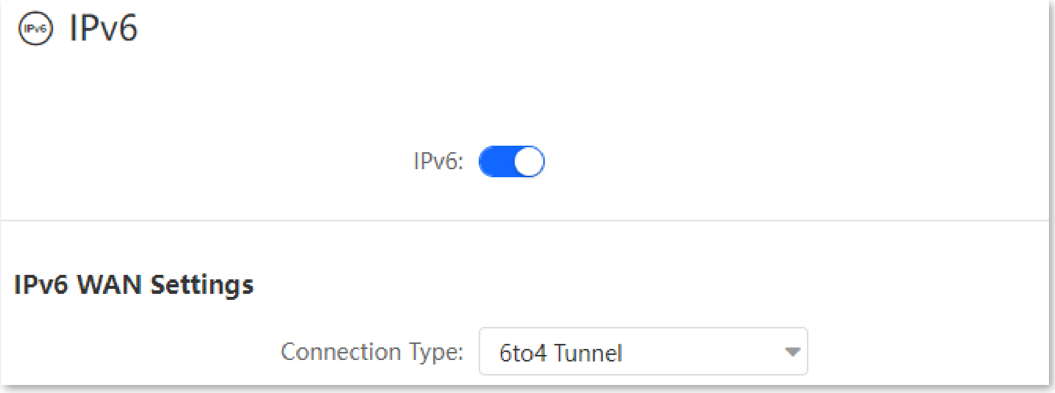
Local IPv6 Address: /64

Table 9-4 Parameter description

Parameter	Description
Remote IPv4 Address	It specifies the WAN IPv4 address of the dual stack router at the peer side.
Local IPv6 Address	It specifies the IPv6 address of the LAN, which needs to be customized.

6to4 tunnel

Log in to the web UI of the router, and choose **IPv6**. Enable the **IPv6** function, set the connection type to **6to4 Tunnel** and save the configurations.



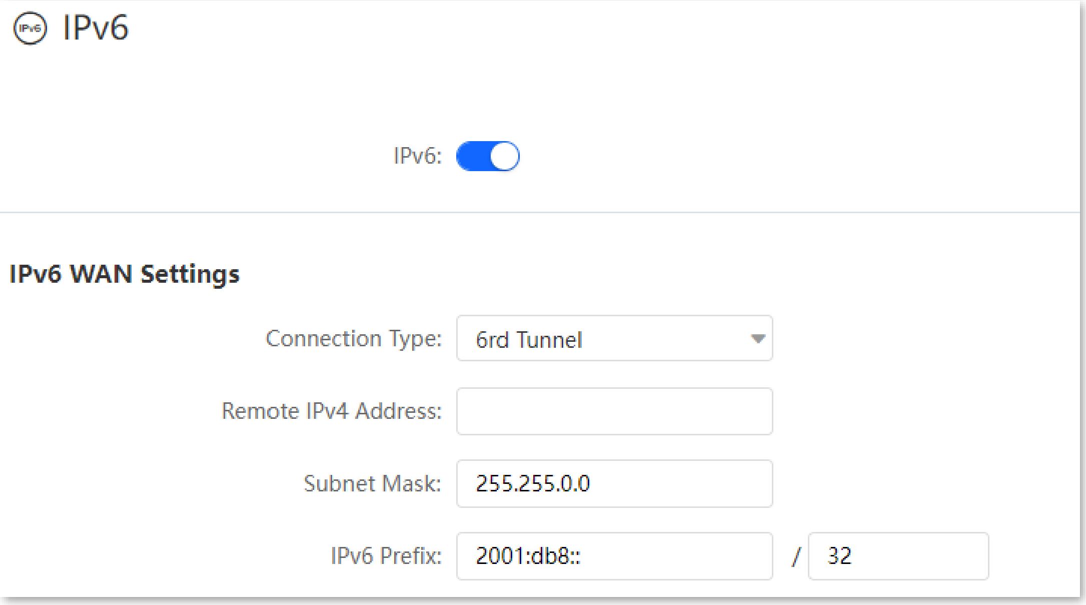
IPv6: on

IPv6 WAN Settings

Connection Type: 6to4 Tunnel

6rd tunnel

Log in to the web UI of the router, and choose **IPv6**. Enable the **IPv6** function, set the connection type to **6rd Tunnel**, enter required parameters and save the configurations.



IPv6

IPv6: ●

IPv6 WAN Settings

Connection Type: 6rd Tunnel

Remote IPv4 Address:

Subnet Mask: 255.255.0.0

IPv6 Prefix: 2001:db8:: / 32

Table 9-5 Parameter description

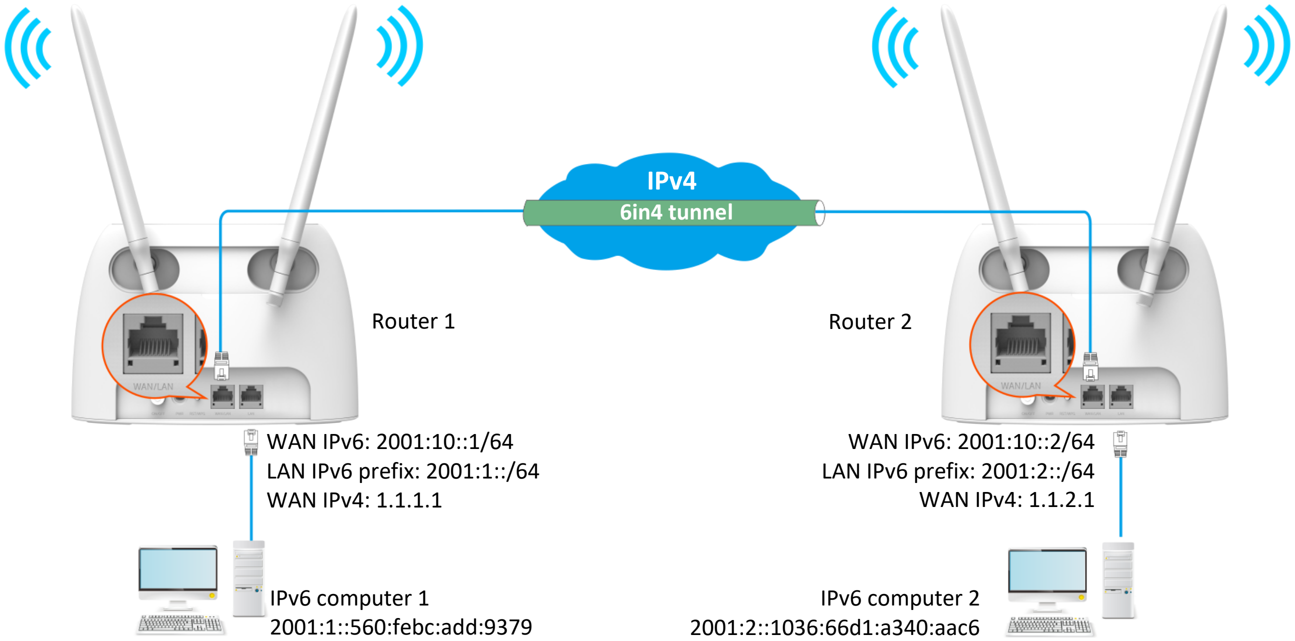
Parameter	Description
Remote IPv4 Address	It specifies the WAN IPv4 address of the dual stack router or 6rd BR at the peer side.
Subnet Mask	It specifies the subnet mask of the IPv4 network. The IPv4 network at both sides should be at the same network segment.
IPv6 Prefix	It specifies the IPv6 prefix of the network. ● When the 6rd tunnel is used to achieve the communication between isolated islands, users can customize the IPv6 prefix. ● If the 6rd tunnel is used to connect to the network of ISPs, contact your ISP for the IPv6 prefix.

Examples of IPv6 tunnel configuration

6in4 tunnel

As shown below, the two routers support dual stack protocol. To achieve the communication between the two hosts, you can configure the 6in4 tunnel.

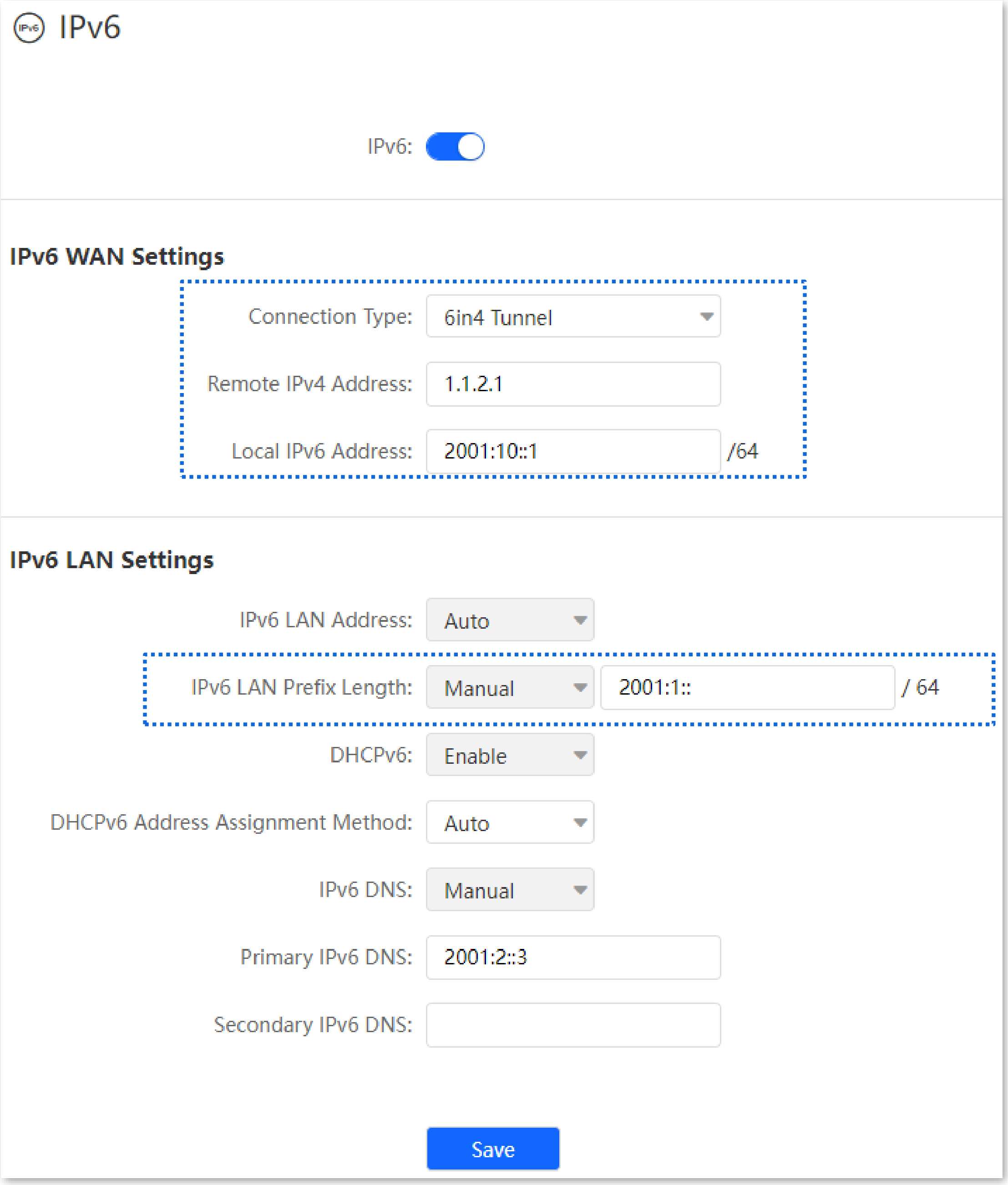
Assume that the two routers are connected to IPv4 network and obtain public IPv4 addresses.



Configuring procedure:

Step 1 Configure the **Router 1**.

1) Start a web browser on a device connected to the router 1 and visit **https://hikvisionwifi.local** to Log in to the web UI of the router.
2) Choose **IPv6**.
3) Enable the **IPv6** function.
4) Set the connection type to **6in4 Tunnel.**
5) Enter the WAN IPv4 address of the device at the peer side, which is **1.1.2.1** in this example.
6) Customize the local IPv6 address, which is **2001:10::1**/64 in this example.
7) Set the IPv6 LAN prefix length, which is **2001:1::**/64 in this example.
8) Click **Save**.



IPv6

IPv6: ●

IPv6 WAN Settings

Connection Type: 6in4 Tunnel

Remote IPv4 Address: 1.1.2.1

Local IPv6 Address: 2001:10::1 /64

IPv6 LAN Settings

IPv6 LAN Address: Auto

IPv6 LAN Prefix Length: Manual 2001:1:: / 64

DHCPv6: Enable

DHCPv6 Address Assignment Method: Auto

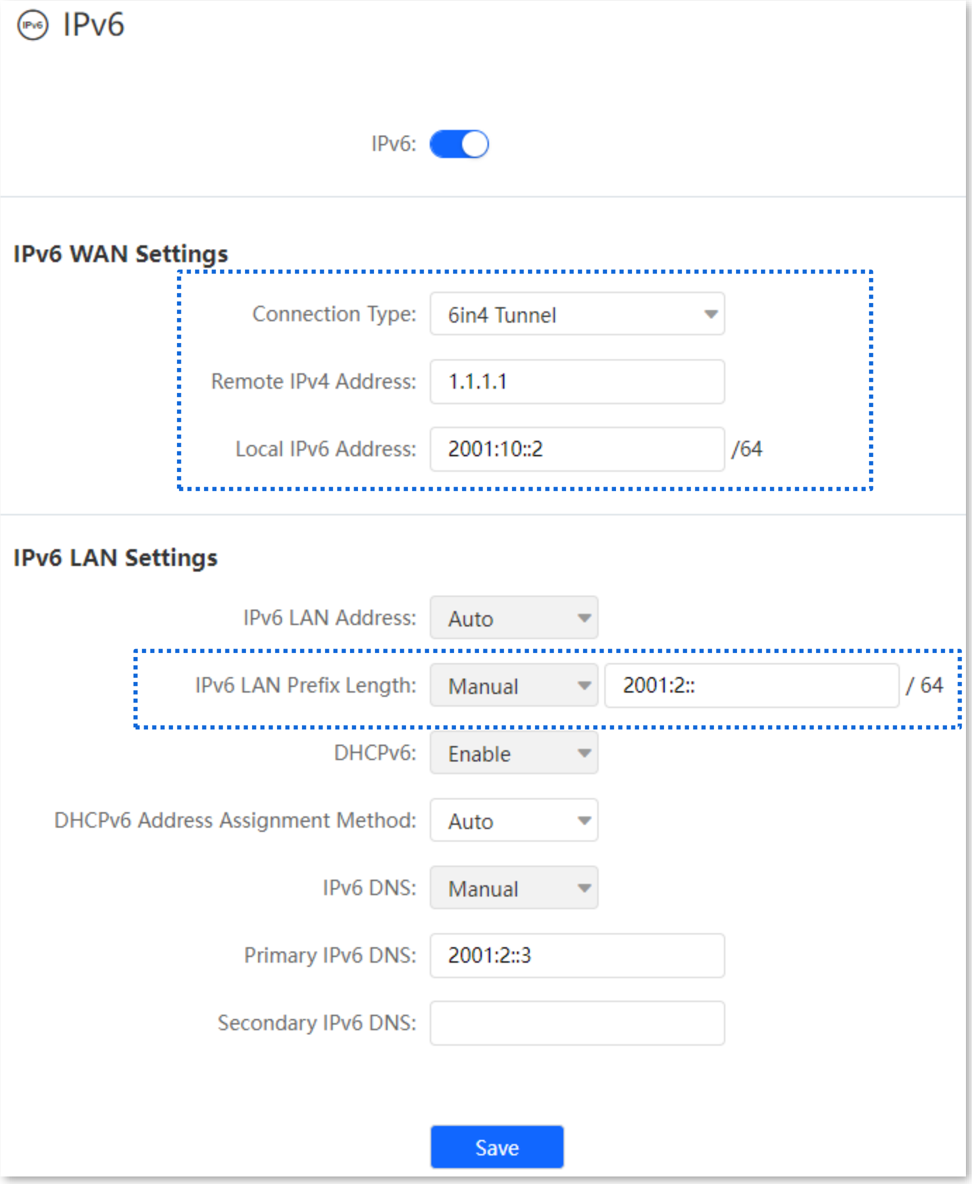
IPv6 DNS: Manual

Primary IPv6 DNS: 2001:2::3

Secondary IPv6 DNS:

Step 2 Configure the **Router 2**.

1) Start a web browser on a device connected to the router 2 and visit **https://hikvisionwifi.local** to Log in to the web UI of the router.
2) Choose **IPv6**, and enable the **IPv6** function.
3) Set the connection type to **6in4 Tunnel.**
4) Enter the WAN IPv4 address of the device at the peer side, which is **1.1.1.1** in this example.
5) Customize the local IPv6 address, which is **2001:10::2**/64 in this example.
6) Set the IPv6 LAN prefix length, which is **2001:2::**/64 in this example.
7) Click **Save**.



IPv6

IPv6: ●

IPv6 WAN Settings

Connection Type: 6in4 Tunnel

Remote IPv4 Address: 1.1.1.1

Local IPv6 Address: 2001:10::2 /64

IPv6 LAN Settings

IPv6 LAN Address: Auto

IPv6 LAN Prefix Length: Manual 2001:2:: / 64

DHCPv6: Enable

DHCPv6 Address Assignment Method: Auto

IPv6 DNS: Manual

Primary IPv6 DNS: 2001:2::3

Secondary IPv6 DNS:

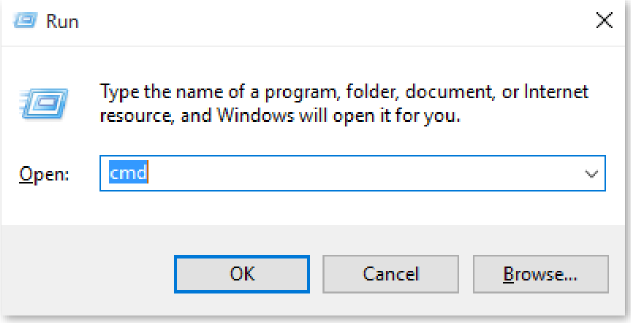
Verification

To verify whether the 6in4 tunnel is established successfully, you can ping each other on the two computers.

Now, ping computer 2 (IPv6 address: 2001:2::1036:66d1:a340:aac6) on computer 1.

Step 1 Use **Windows** + **R** shortcut to open the **Run** dialog window.

Step 2 Enter **cmd**, and click **OK**.

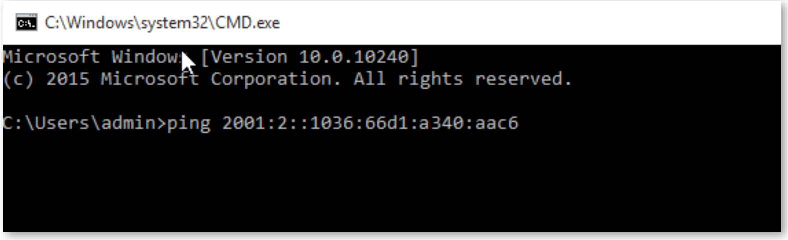


Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

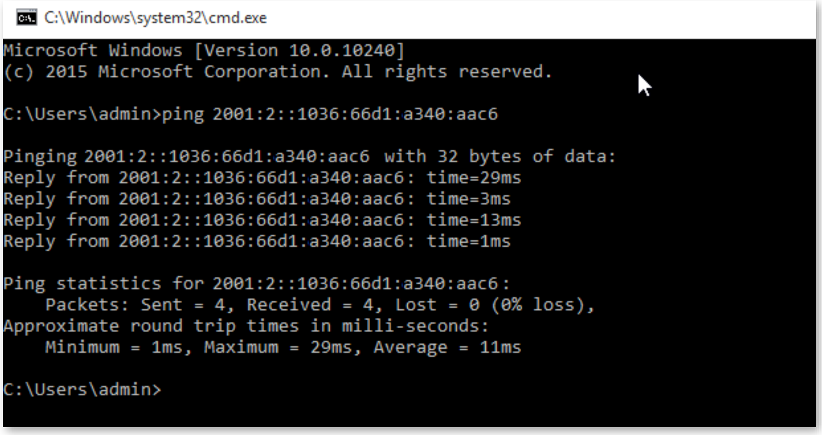
Open: cmd

Step 3 Enter the ping command, which is **ping 2001:2::1036:66d1:a340:aac6** in the example, and press **Enter**.



```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\admin>ping 2001:2::1036:66d1:a340:aac6
```

Wait a moment. The 6in4 tunnel configuration succeeds when the result is shown as below.

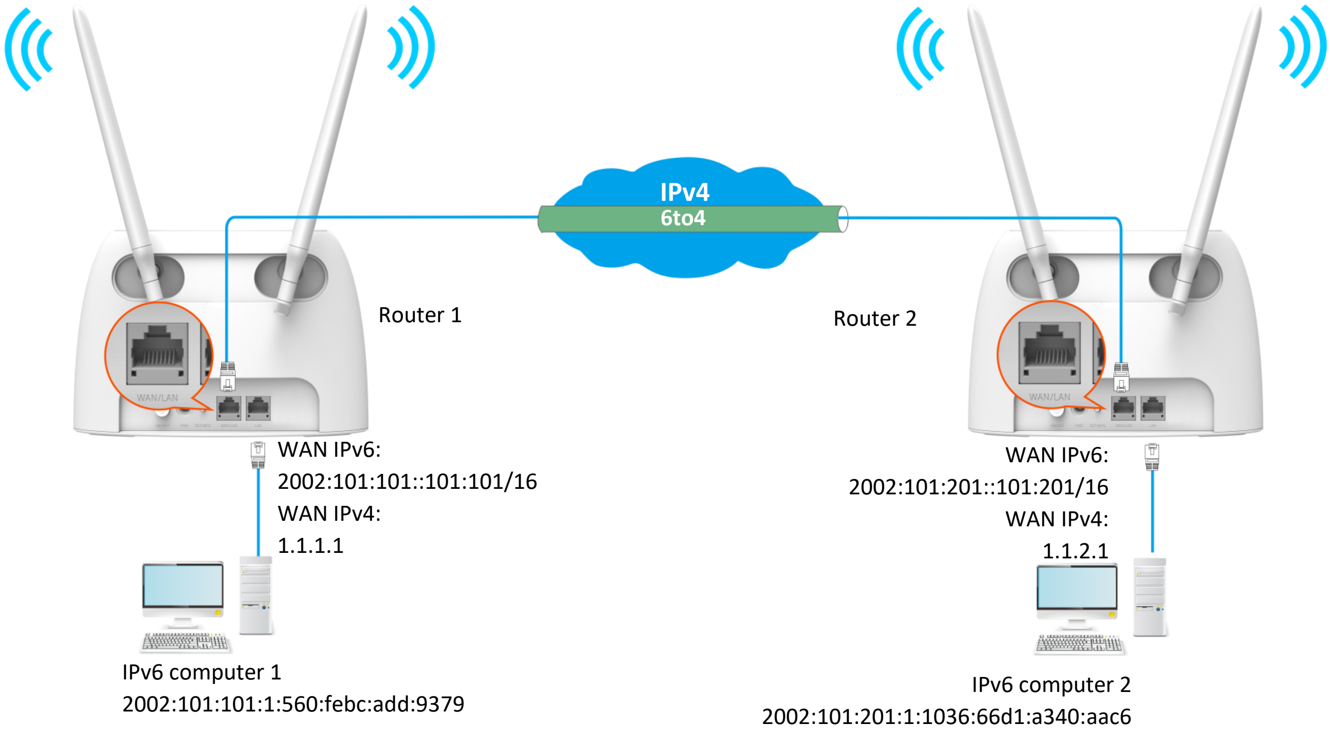


```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\admin>ping 2001:2::1036:66d1:a340:aac6

Pinging 2001:2::1036:66d1:a340:aac6 with 32 bytes of data:
Reply from 2001:2::1036:66d1:a340:aac6: time=29ms
Reply from 2001:2::1036:66d1:a340:aac6: time=3ms
Reply from 2001:2::1036:66d1:a340:aac6: time=13ms
Reply from 2001:2::1036:66d1:a340:aac6: time=1ms

Ping statistics for 2001:2::1036:66d1:a340:aac6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 29ms, Average = 11ms

C:\Users\admin>
```

6to4 tunnel

As shown below, the two routers support dual stack protocol. To achieve the communication between the two hosts, you can configure the 6to4 tunnel.

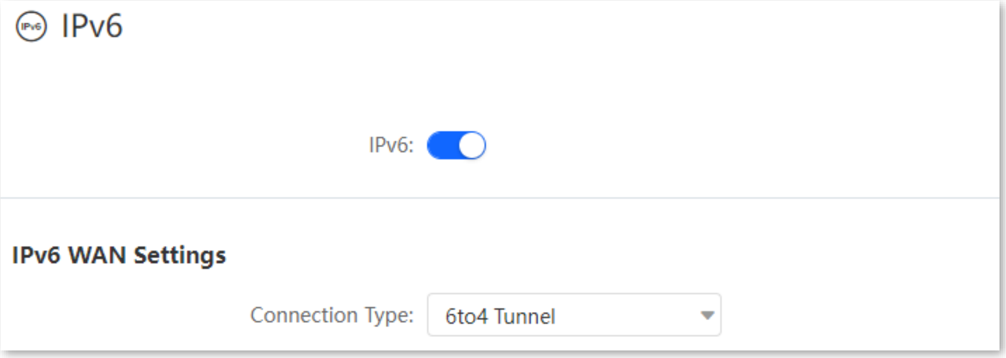
Assume that the two routers are connected to IPv4 network and obtain public IPv4 addresses.



Configuring procedure:

Step 1 Configure Router 1.

1) Start a web browser on a device connected to the router 1 and visit **https://hikvisionwifi.local** to Log in to the web UI of the router.
2) Choose **IPv6**.
3) Enable the **IPv6** function.
4) Set the connection type to **6to4 Tunnel.**
5) Click **Save**.



IPv6

IPv6: on

IPv6 WAN Settings

Connection Type: 6to4 Tunnel

Step 2 Repeat **Step 1** to set the connection type of Router 2 to **6to4**.

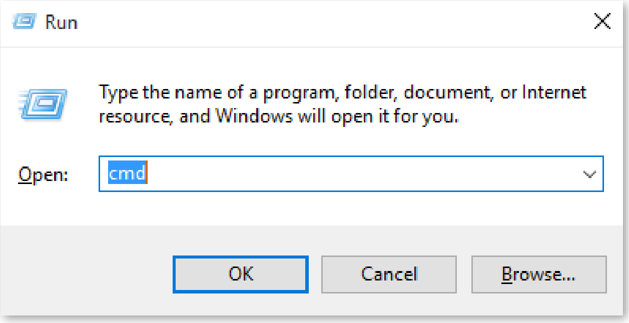
Verification

To verify whether the 6to4 tunnel is established successfully, you can ping each other on the two computers.

Now, ping computer 2 (IPv6 address: 2002:101:201:1:1036:66d1:a340:aac6) on computer 1.

Step 1 Use **Windows** + **R** shortcut to open the **Run** dialog window.

Step 2 Enter **cmd**, and click **OK**.

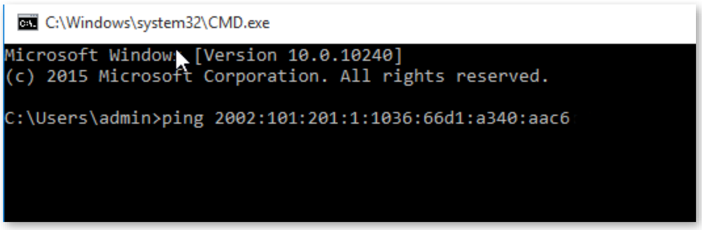


Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

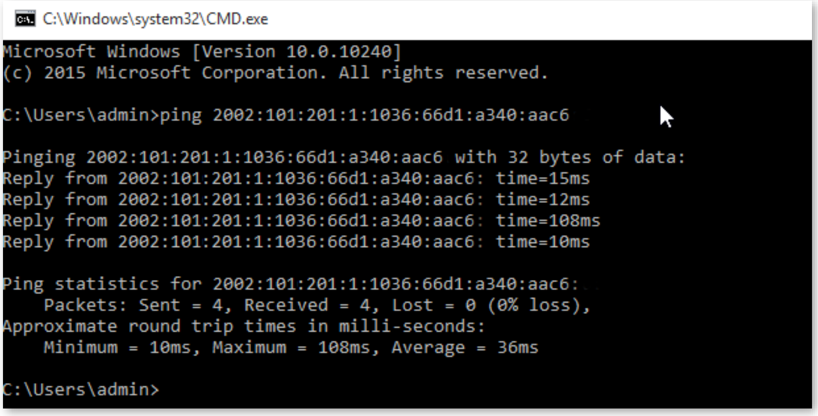
Step 3 Enter the ping command, which is **ping 2002:101:201:1:1036:66d1:a340:aac6** in the example and press **Enter**.



C:\Windows\system32\CMD.exe

```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\admin>ping 2002:101:201:1:1036:66d1:a340:aac6
```

Wait a moment. The 6to4 tunnel configuration succeeds when the result is shown as below.



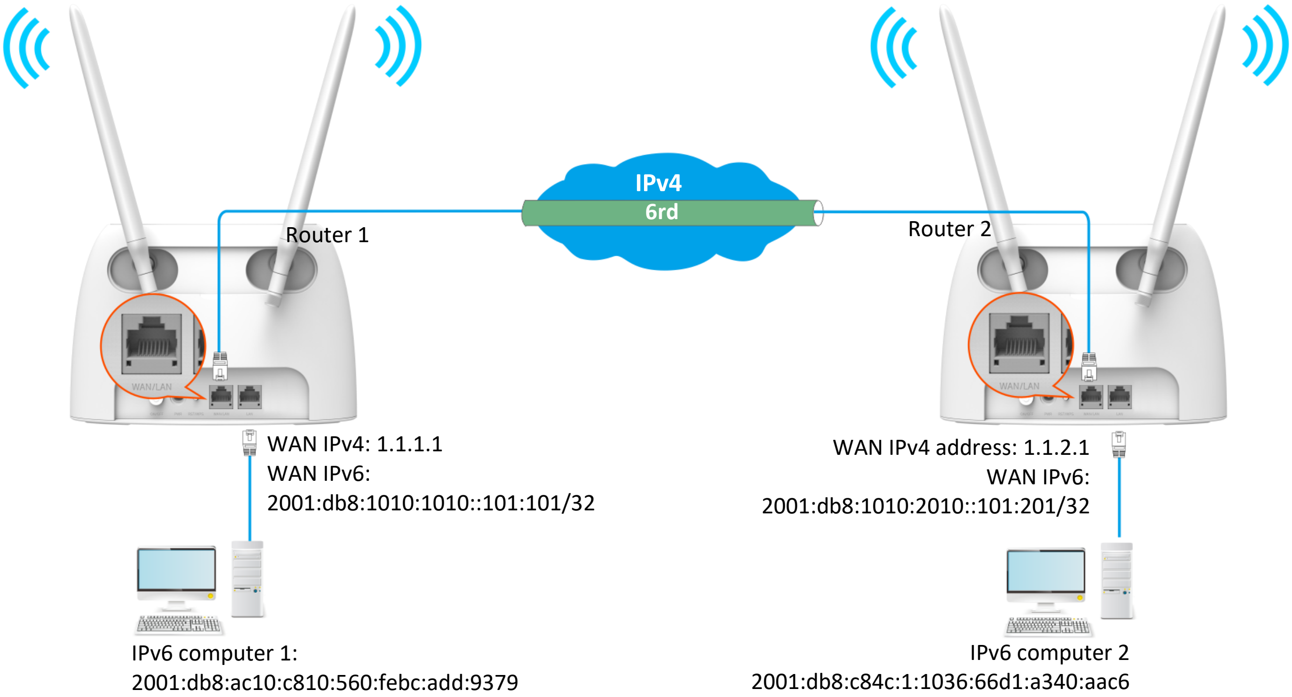
C:\Windows\system32\CMD.exe

```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\admin>ping 2002:101:201:1:1036:66d1:a340:aac6

Pinging 2002:101:201:1:1036:66d1:a340:aac6 with 32 bytes of data:
Reply from 2002:101:201:1:1036:66d1:a340:aac6: time=15ms
Reply from 2002:101:201:1:1036:66d1:a340:aac6: time=12ms
Reply from 2002:101:201:1:1036:66d1:a340:aac6: time=108ms
Reply from 2002:101:201:1:1036:66d1:a340:aac6: time=10ms

Ping statistics for 2002:101:201:1:1036:66d1:a340:aac6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 108ms, Average = 36ms

C:\Users\admin>
```

6rd tunnel

As shown below, the two routers support dual stack protocol. To achieve the communication between the two hosts, you can configure the 6rd tunnel.

Assume that the two routers are connected to IPv4 network and obtain public IPv4 addresses.


IPv4
6rd
Router 1
Router 2
WAN/LAN
WAN/LAN
WAN IPv4: 1.1.1.1
WAN IPv6:
2001:db8:1010:1010::101:101/32
WAN IPv4 address: 1.1.2.1
WAN IPv6:
2001:db8:1010:2010::101:201/32
IPv6 computer 1:
2001:db8:ac10:c810:560:febc:add:9379
IPv6 computer 2
2001:db8:c84c:1:1036:66d1:a340:aac6

Configuring procedure:

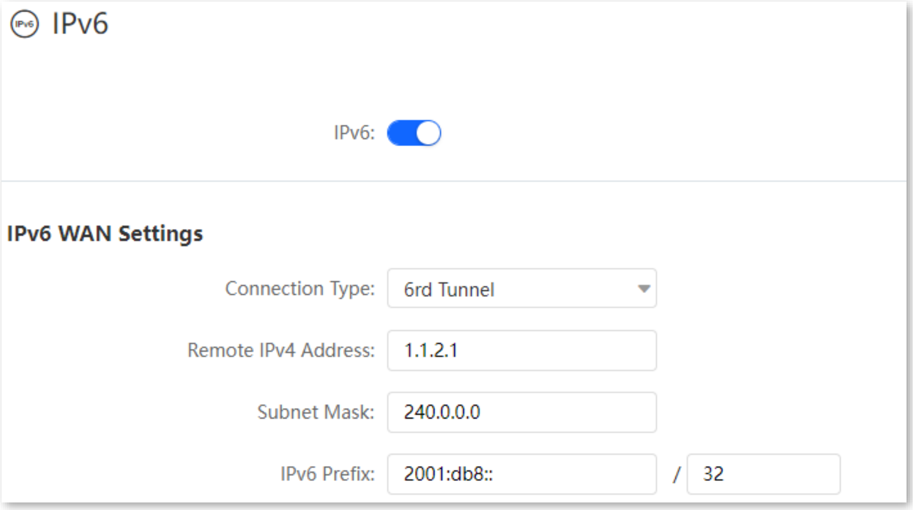
Note

Before configuring the 6rd tunnel, choose View system information to find the WAN IPv4 address of the router.

Step 1 Configure Router 1.

1) Start a web browser on a device connected to the router 1 and visit **https://hikvisionwifi.local** to Log in to the web UI of the router.
2) Choose **IPv6**.

3) Enable the **IPv6** function.
4) Set the connection type to **6rd Tunnel.**
5) Enter the WAN IPv4 address of the device at the peer side in **Remote IPv4 Address**, which is **1.1.2.1** in this example.
6) Enter the Subnet Mask of the IPv4 network. **240.0.0.0** is recommended.
7) Customize the **IPv6 Prefix** (the default is recommended).
8) Click **Save**.


IPv6

IPv6: on

IPv6 WAN Settings

Connection Type: 6rd Tunnel

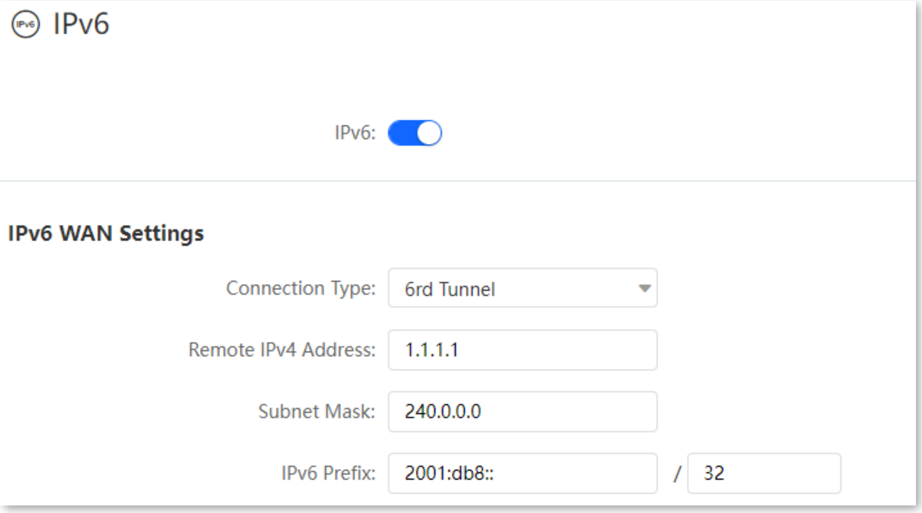
Remote IPv4 Address: 1.1.2.1

Subnet Mask: 240.0.0.0

IPv6 Prefix: 2001:db8:: / 32

Step 2 Configure Router 2.

1) Start a web browser on a device connected to the router 2 and visit **https://hikvisionwifi.local** to Log in to the web UI of the router.
2) Choose **IPv6**.
3) Enable the **IPv6** function.
4) Set the connection type to **6rd Tunnel**.
5) Enter the WAN IPv4 address of the device at the peer side in **Remote IPv4 Address**, which is **1.1.1.1** in this example.
6) Enter the **Subnet Mask** of the IPv4 network. **240.0.0.0** is recommended.
7) Customize the **IPv6 Prefix**(the default is recommended).
8) Click **Save**.


IPv6

IPv6: on

IPv6 WAN Settings

Connection Type: 6rd Tunnel

Remote IPv4 Address: 1.1.1.1

Subnet Mask: 240.0.0.0

IPv6 Prefix: 2001:db8:: / 32

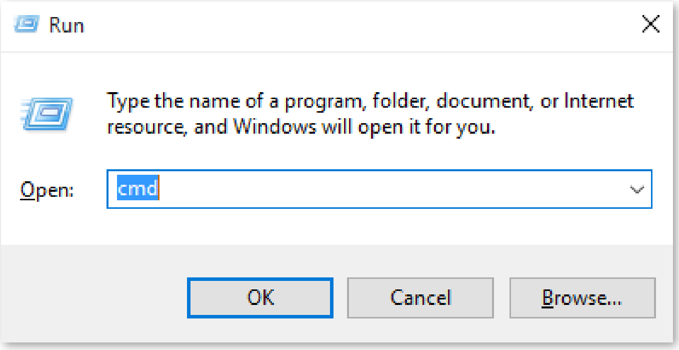
Verification

To verify whether the 6rd tunnel is established successfully, you can ping each other on the two computers.

Now, ping computer 2 (IPv6 address: 2001:db8:c84c:1:1036:66d1:a340:aac6) on computer 1.

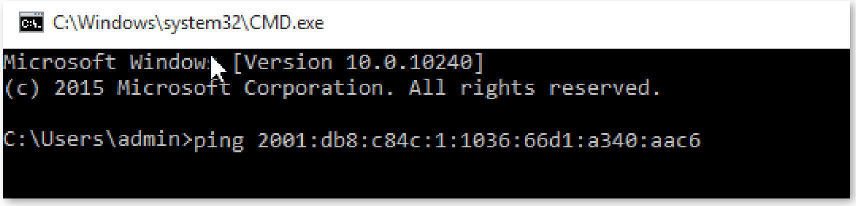
Step 1 Use **Windows** + **R** shortcut to open the **Run** dialog window.

Step 2 Enter **cmd**, and click **OK**.


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...

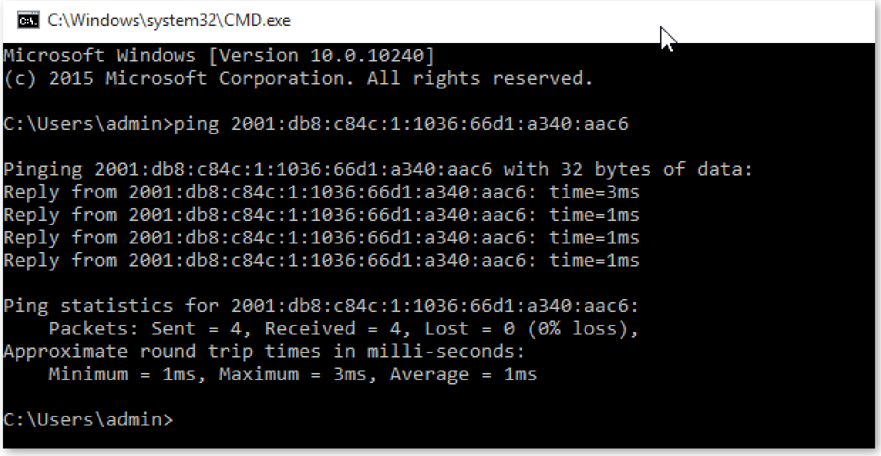
Open: cmd

Step 3 Enter the ping command, which is **ping 2001:db8:c84c:1:1036:66d1:a340:aac6** in the example and press **Enter**.



```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\admin>ping 2001:db8:c84c:1:1036:66d1:a340:aac6
```

Wait a moment. The 6rd tunnel configuration succeeds when the result is shown as below.

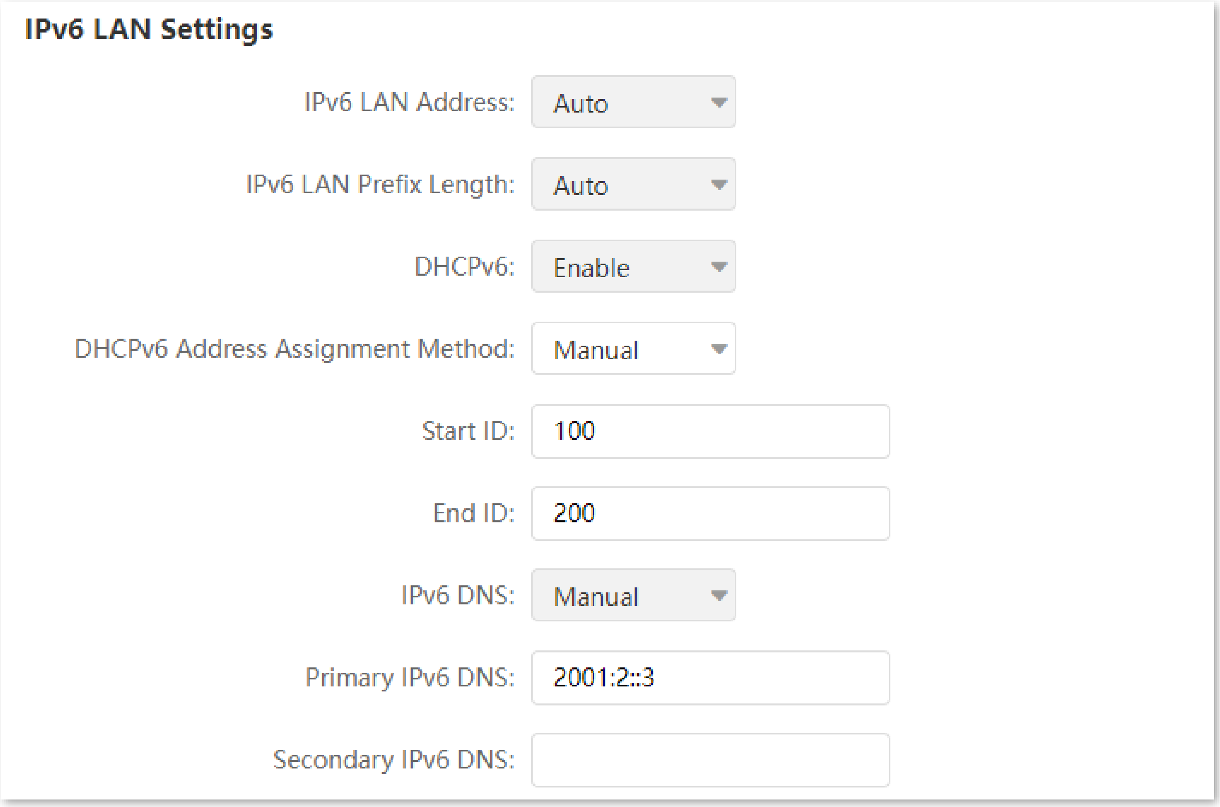


```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\admin>ping 2001:db8:c84c:1:1036:66d1:a340:aac6

Pinging 2001:db8:c84c:1:1036:66d1:a340:aac6 with 32 bytes of data:
Reply from 2001:db8:c84c:1:1036:66d1:a340:aac6: time=3ms
Reply from 2001:db8:c84c:1:1036:66d1:a340:aac6: time=1ms
Reply from 2001:db8:c84c:1:1036:66d1:a340:aac6: time=1ms
Reply from 2001:db8:c84c:1:1036:66d1:a340:aac6: time=1ms

Ping statistics for 2001:db8:c84c:1:1036:66d1:a340:aac6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms

C:\Users\admin>
```

9.2 IPv6 LAN settings

To access the page, Log in to the web UI of the router and choose **IPv6**.

You can change the IPv6 LAN settings here.



IPv6 LAN Settings

IPv6 LAN Address: Auto

IPv6 LAN Prefix Length: Auto

DHCPv6: Enable

DHCPv6 Address Assignment Method: Manual

Start ID: 100

End ID: 200

IPv6 DNS: Manual

Primary IPv6 DNS: 2001:2::3

Secondary IPv6 DNS:

Table 9-6 Parameter description

Parameter	**Description**
IPv6 LAN Address	It specifies two types of IPv6 LAN address assignment. ● **Auto**: The router generates the IPv6 address based on the LAN MAC address of the router. By default, the prefix has 64 digits. ● **Manual**: You need to set the IPv6 LAN address manually.
IPv6 LAN Prefix Length	It specifies two types IPv6 LAN prefix address assignment. ● **Auto**: The router obtains an LAN prefix from the upstream device. ● **Manual**: You need to set the IPv6 LAN prefix manually.
DHCPv6	DHCPv6 (Dynamic Host Configuration Protocol for IPv6) is used to assign IP addresses and prefix to IPv6 hosts on a network. It is the IPv6 equivalent of the DHCP for IPv4. This is also known as a stateful autoconfiguration.

Parameter	Description
DHCPv6 Address Assignment Method	It specifies the assignment type of IPv6 address information by the DHCPv6 server. ● **Auto**: Clients obtain their IPv6 address through Router Advertisement (Stateless Address Auto Configuration) and other parameters are allocated by the DHCPv6 server. ● **Manual**: The DHCPv6 server automatically assigns IPv6 addresses/prefixes and other network configuration parameters, such as DNS server addresses, to clients. The user needs to manually configure the start ID and the end ID.
Start ID	The configuration is required when the DHCPv6 address assignment method is set to Manual. They specify the range of the last segment of the IPv6 address that the DHCPv6 server assigns to the devices. Range: 1-ffff.
End ID	
IPv6 DNS	It specifies the LAN IPv6 DNS configuration method. ● **Auto**: Obtain the IPv6 DNS address from the upstream device. ● **Manual**: Configure the IPv6 DNS address manually.
Primary IPv6 DNS	Enter the fixed IPv6 DNS address provided by your ISP. **Note** If your ISP only provides one DNS server address, you can leave the secondary IPv6 DNS blank.
Secondary IPv6 DNS	

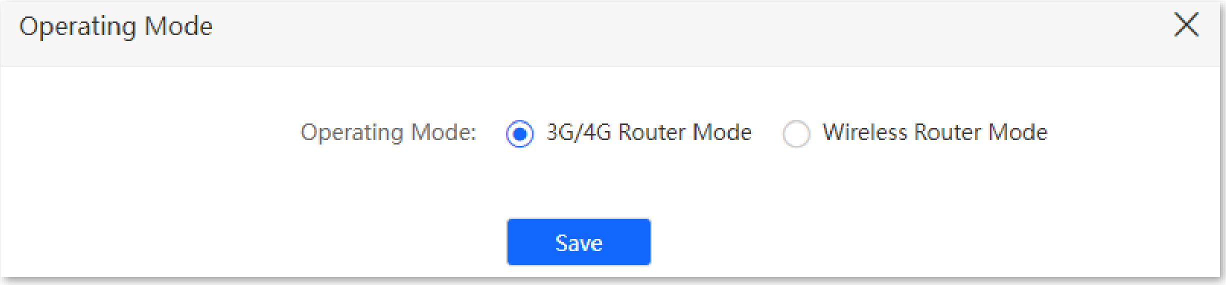
Chapter 10 Advanced settings

10.1 Operating mode

10.1.1 Overview

In addition to providing internet access with a SIM card, the router can also be connected to a broadband. By switching the operating mode, you can access the internet through the corresponding method. The default operating mode is 3G/4G router mode.

To access the configuration page, Log in to the web UI of the router and choose **Advanced Settings** > **Operating Mode**.



Operating Mode

Operating Mode: ● 3G/4G Router Mode ○ Wireless Router Mode

To access the internet:

- 3G/4G router mode: Refer to the quick installation guide or Access the internet with a SIM card.
- Wireless router mode: Refer to Access the internet through the WAN port.

10.1.2 Set the router to wireless router mode

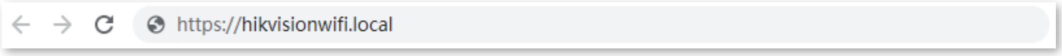
If you have already used the router and is able to access the web UI, choose the **Advanced Settings** > **Operating Mode** to change the operating mode.

If you are using the router for the first time, or the router is reset to factory settings, follow the steps below to set the router to wireless router mode.

Configuring procedure:

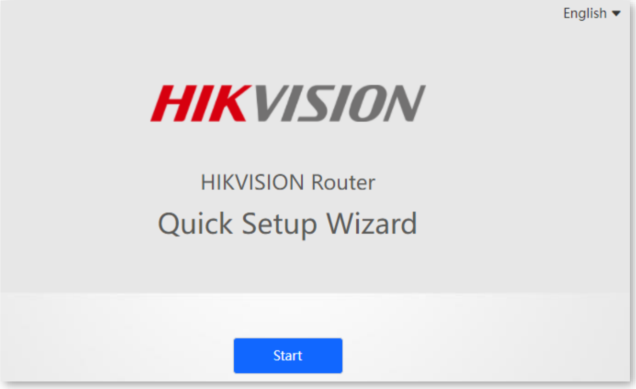
Step 1 Log in to the web UI of the router.

1) Connect your wireless device to the Wi-Fi network of your router, or connect a computer to the LAN port of the router.
2) Start a web browser on the device connected to the router, and visit **https://hikvisionwifi.local**. A computer is used for illustration below.

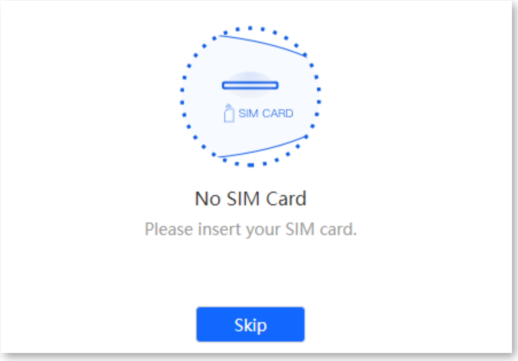


https://hikvisionwifi.local

3) Click **Start**.



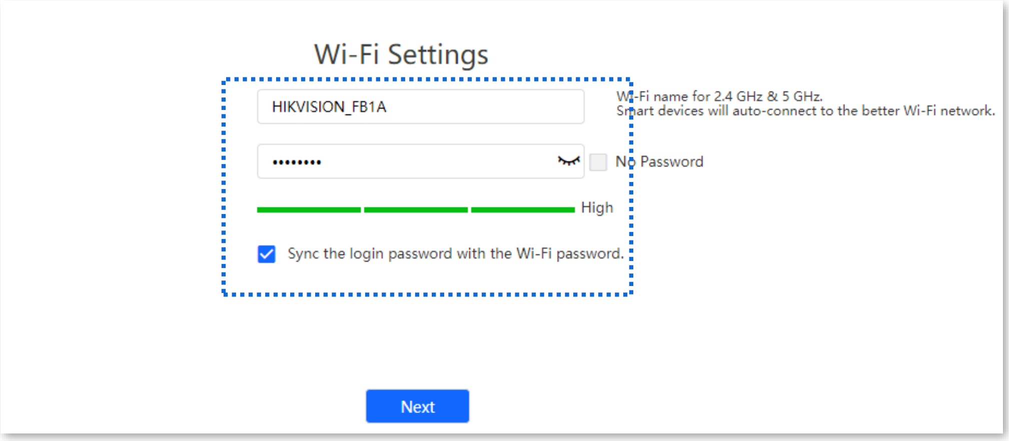
4) Click **Skip**.



5) Set Wi-Fi and login password, and click **Next**.

Note

Ticking **Sync the login password with the Wi-Fi password**, the Wi-Fi password is set to the router login password.


Wi-Fi Settings

HIKVISION_FB1A

Wi-Fi name for 2.4 GHz & 5 GHz.
Smart devices will auto-connect to the better Wi-Fi network.

••••••••

□ No Password

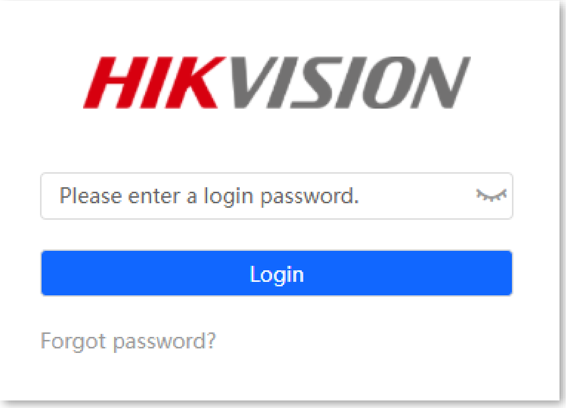
High

☑ Sync the login password with the Wi-Fi password.

6) Enter the login password you set, and click **Login**.

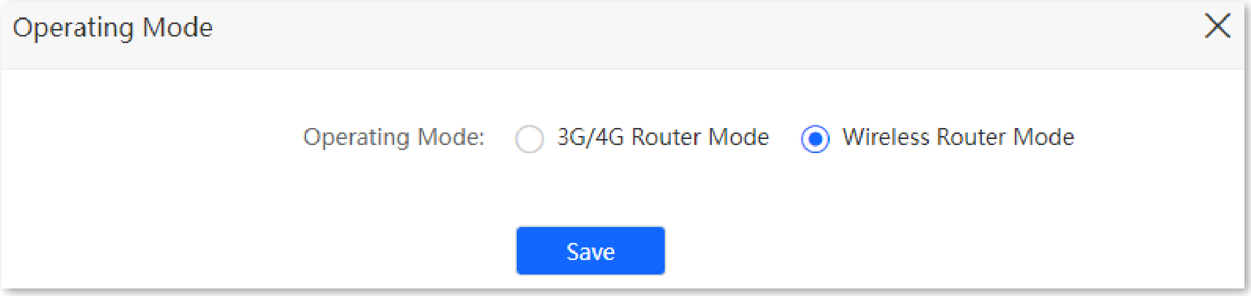
Note

You need to enter the Wi-Fi password of the wireless device to connect the Wi-Fi network of your router.



Step 2 Set the router to wireless router mode.

1) Choose **Advanced Settings** > **Operating Mode**.
2) Click **Wireless Router Mode**, and click **Save**.



Operating Mode: ○ 3G/4G Router Mode ● Wireless Router Mode

After rebooting, the router is set to wireless router mode.

10.2 SIM PIN (3G/4G router mode)

10.2.1 Overview

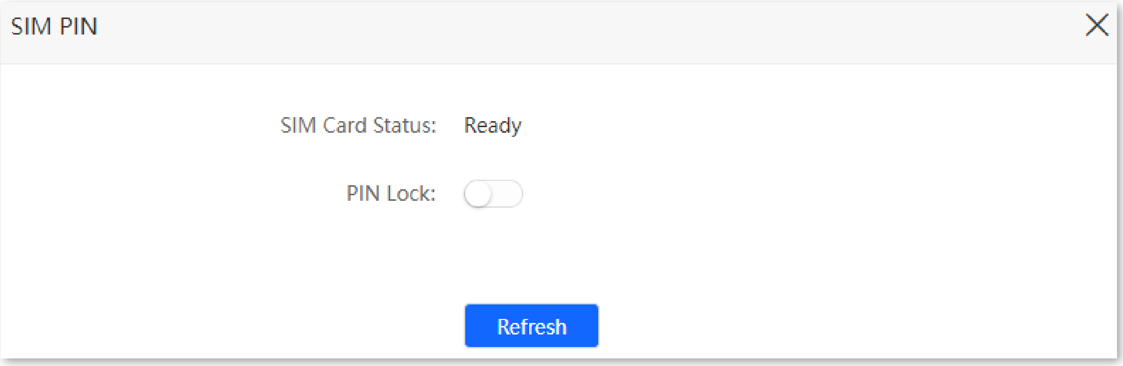
Note

This function is only available under the 3G/4G router mode. Refer to Operating mode to set the operating mode of the router.

SIM PIN is a protective measure to prevent your SIM card from misuse. If your SIM card is locked when you insert it into the router, you are required to unlock it for internet access. You can also enable the PIN lock for an unlocked SIM card.

To access the SIM PIN setting page, Log in to the web UI of the router and choose **Advanced Settings** > **SIM PIN**.

When the SIM card is not set with PIN Lock, the page is shown as below.



SIM Card Status: Ready

PIN Lock: ○

10.2.2 Unlock the SIM card

If you want to use a locked SIM card to access the internet, you need to unlock it first.

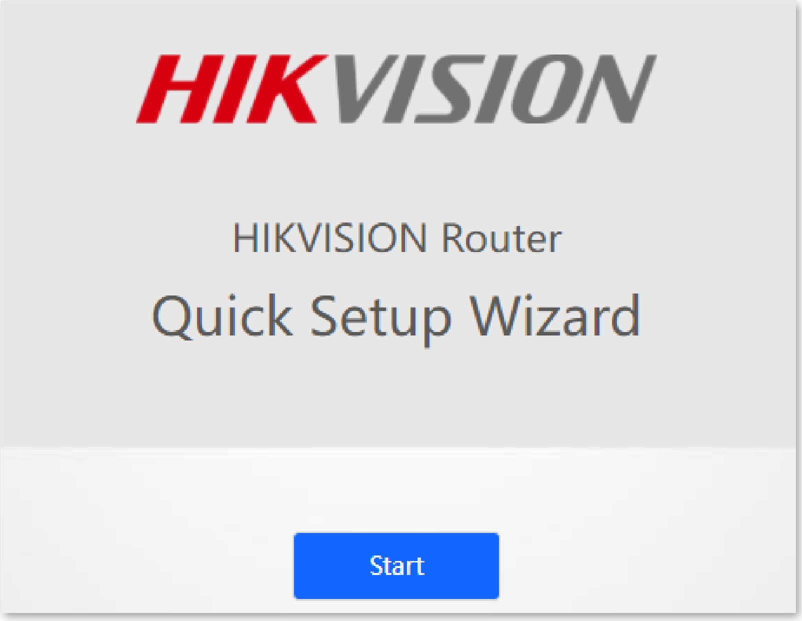
Unlock the SIM card in the quick setup wizard

When you use the router for the first time or the router is reset, you are required to unlock the SIM card in the quick setup wizard.

Configuring procedure:

Step 1 Start a web browser on the device connected to the router, and visit **https://hikvisionwifi.local**.

Step 2 Click **Start**.

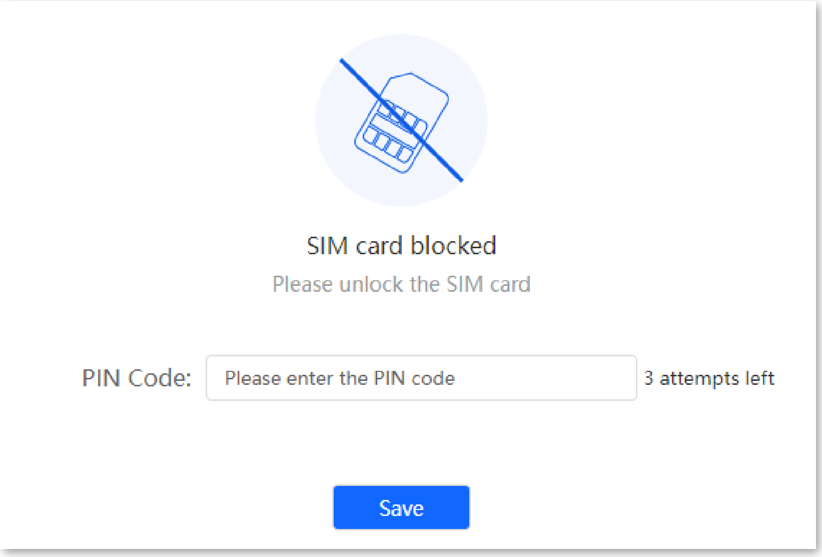


HIKVISION

HIKVISION Router

Quick Setup Wizard

Step 3 Enter the **PIN Code**, and click **OK**.



SIM card blocked

Please unlock the SIM card

PIN Code: Please enter the PIN code 3 attempts left

Note

You can only try the PIN code for 3 times. If you fail all, you must use PUK code to reset the PIN code. Contact your ISP for the PUK code. Otherwise, the SIM card may be locked permanently after entering the wrong PUK code for 10 times.

Step 4 Follow the steps to complete the setup process.

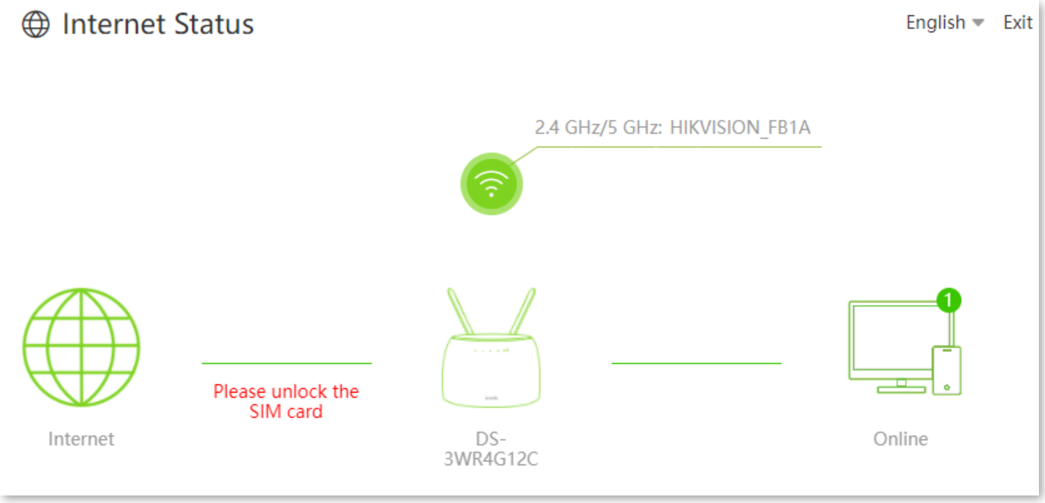
Unlock the SIM card in the web UI

You can also unlock the SIM card when you already can access the web UI of the router.

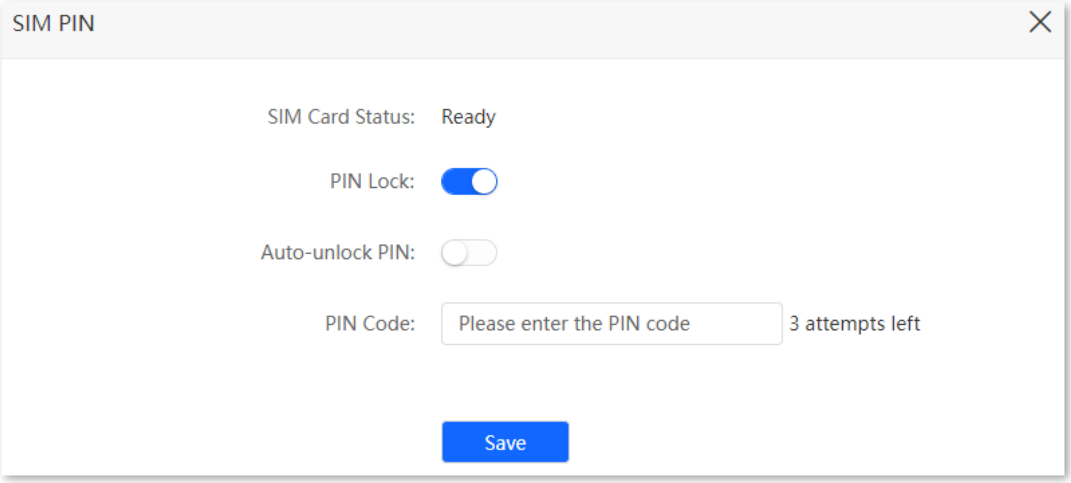
Configuring procedure:

Step 1 Log in to the web UI of the router.

Step 2 Click Please unlock the SIM card, or choose **Advanced Settings** > **SIM PIN**.



Step 3 Enter the **PIN Code**, and click **Save**.


SIM PIN

SIM Card Status: Ready

PIN Lock: ●

Auto-unlock PIN: ○

PIN Code: Please enter the PIN code 3 attempts left

Save

Note

- You can only try the PIN code for 3 times. If you fail all, you must use PUK code to reset the PIN code. Contact your ISP for the PUK code. Otherwise, the SIM card may be locked permanently after entering the wrong PUK code for 10 times.
- When **Auto-unlock PIN** is enabled, the router will unlock the SIM card automatically each time the router completes rebooting (the PIN code is still required after resetting).

10.2.3 Disable PIN lock for the SIM card

After disable PIN lock for the SIM card, your SIM card will not be protected by PIN lock.

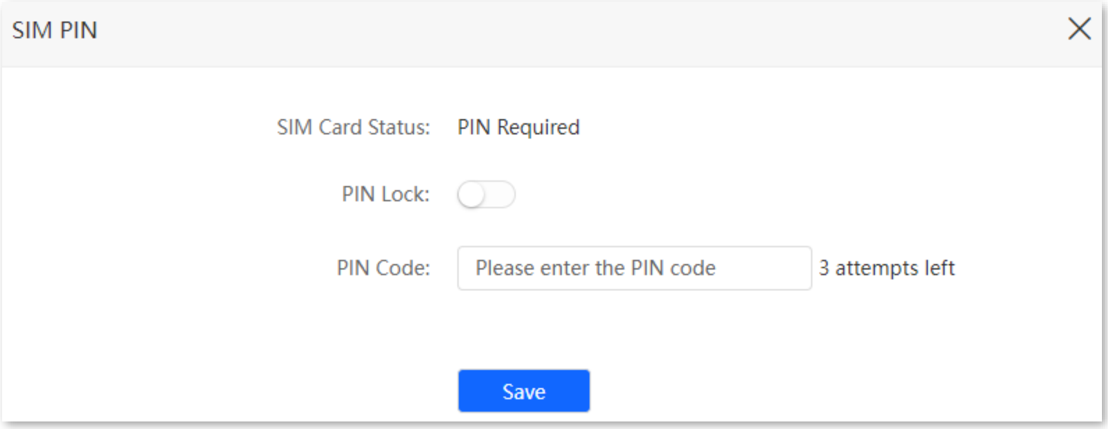
Configuring procedure:

Step 1 Log in to the web UI of the router.

Step 2 Choose **Advanced Settings** > **SIM PIN**.

Step 3 Disable **PIN Lock**.

Step 4 Enter the **PIN Code**, and click **Save**.



SIM PIN

SIM Card Status: PIN Required

PIN Lock: ○

PIN Code: Please enter the PIN code 3 attempts left

Note

You can only try the PIN code for 3 times. If you fail all, you must use PUK code to reset the PIN code. Contact your ISP for the PUK code. Otherwise, the SIM card may be locked permanently after entering the wrong PUK code for 10 times.

10.2.4 Enable PIN lock for the SIM card

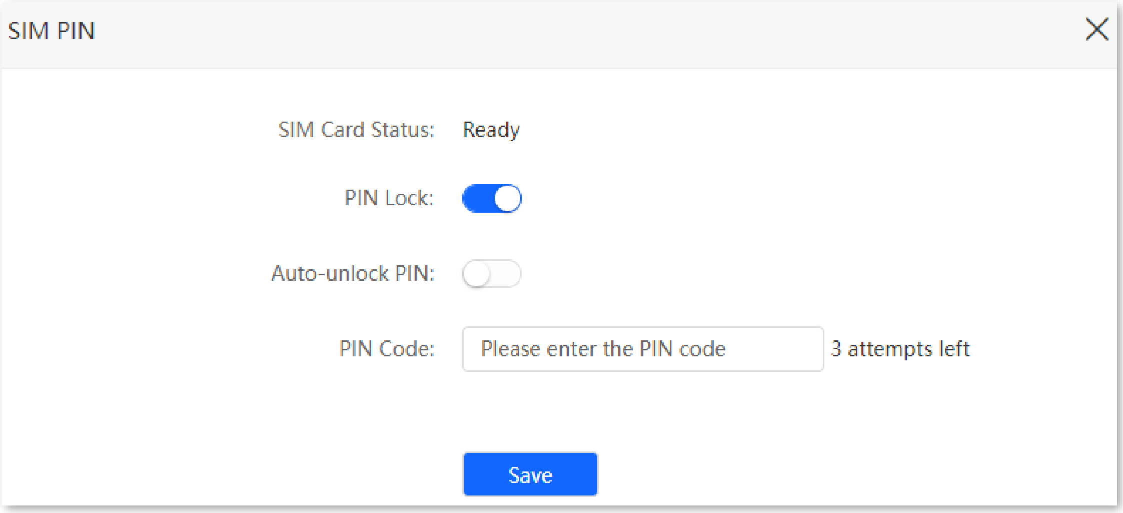
You can also set a PIN lock for a SIM card. SIM PIN is a protective measure to prevent your SIM card from misuse

Configuring procedure:

Step 1 Log in to the web UI of the router.

Step 2 Enable **PIN Lock**.

Step 3 Enter the **PIN Code**, and click **Save**.



SIM PIN

SIM Card Status: Ready

PIN Lock: ●

Auto-unlock PIN: ○

PIN Code: Please enter the PIN code 3 attempts left

Note

- You can only try the PIN code for 3 times. If you fail all, you must use PUK code to reset the PIN code. Contact your ISP for the PUK code. Otherwise, the SIM card may be locked permanently after entering the wrong PUK code for 10 times
- When **Auto-unlock PIN** is enabled, the router will unlock the SIM card automatically each time the router completes rebooting (the PIN code is still required after resetting).

10.3 Mobile data (3G/4G router mode)

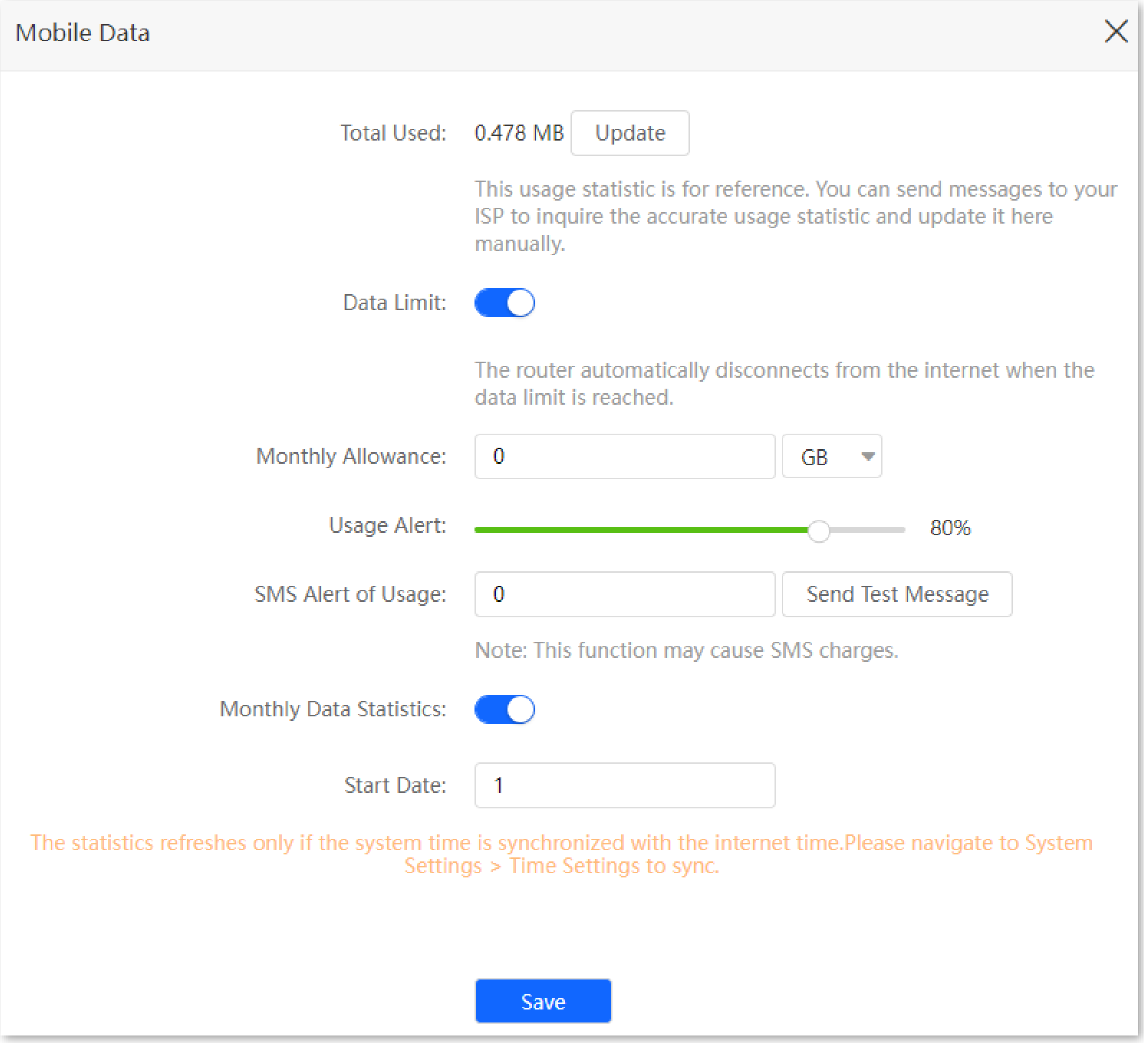
Note

This function is only available under the 3G/4G router mode. Refer to Operating mode to set the operating mode of the router.

10.3.1 Overview

You can view and update data usage statistics, and configure data usage settings, such as data usage limit and usage alert.

To access the configuration page, Log in to the web UI of the router and choose **Advanced Settings** > **Mobile Data**.



Mobile Data

Total Used: 0.478 MB Update

This usage statistic is for reference. You can send messages to your ISP to inquire the accurate usage statistic and update it here manually.

Data Limit: ●

The router automatically disconnects from the internet when the data limit is reached.

Monthly Allowance: 0 GB

Usage Alert: 80%

SMS Alert of Usage: 0 Send Test Message

Note: This function may cause SMS charges.

Monthly Data Statistics: ●

Start Date: 1

The statistics refreshes only if the system time is synchronized with the internet time.Please navigate to System Settings > Time Settings to sync.

Save

Table 10-1 Parameter description

Parameter	Description
Total Used	It specifies the total data traffic that has been used. You can correct it by consulting you ISP and clicking **Update** to change it manually. When the **Monthly Data Statistics** function is enabled, the router will clear the number at the date specified in **Start Date**.
Data Limit	It is used to enable or disable the data limit function. When the limit is reached, the router will disconnect from the internet automatically.
Monthly Allowance	It specifies the specific maximum data usage allowed for each month.
Usage Alert	When the percentage of data traffic used reaches the limit, the router will send an alert SMS message to a specified phone number.
SMS Alert of Usage	It specifies the phone number for receiving the alert SMS message. You can click **Send Test Message** to test the phone number you entered.
Monthly Data Statistics	It is used to enable or disable the Monthly Data Statistics. When it is enabled, the router will clear the number of **Total Used** at the date specified in **Start Date.**
Start Date	It specifies the date at which the router clears the data statistics of the last month and start to record in the following month.

10.3.2 An example of mobile data configurations

Scenario: You inserted a SIM card in the router to provide mobile internet access for your smartphone, iPad and laptop.

Goal: You want to receive SMS message alert on your smartphone and get prepared when the usage reaches a certain amount every month.

Solution: You can configure mobile data settings to reach the goal.

Assume that:

- Available data traffic: 10 GB
- Start date of data usage record: 1st each month
- Smartphone number: 188****1256
- Alert percentage: 80%

Configuring procedure:

Step 1 Log in to the web UI of the router.

Step 2 Choose **Advanced Settings** > **Mobile Data**.

Step 3 (Optional) Click **Update** to update the current usage data in **Total Used**.

Step 4 Enable **Data Limit**.

Step 5 Enter **10** in Monthly Allowance, and choose **GB** in the drop-down box.

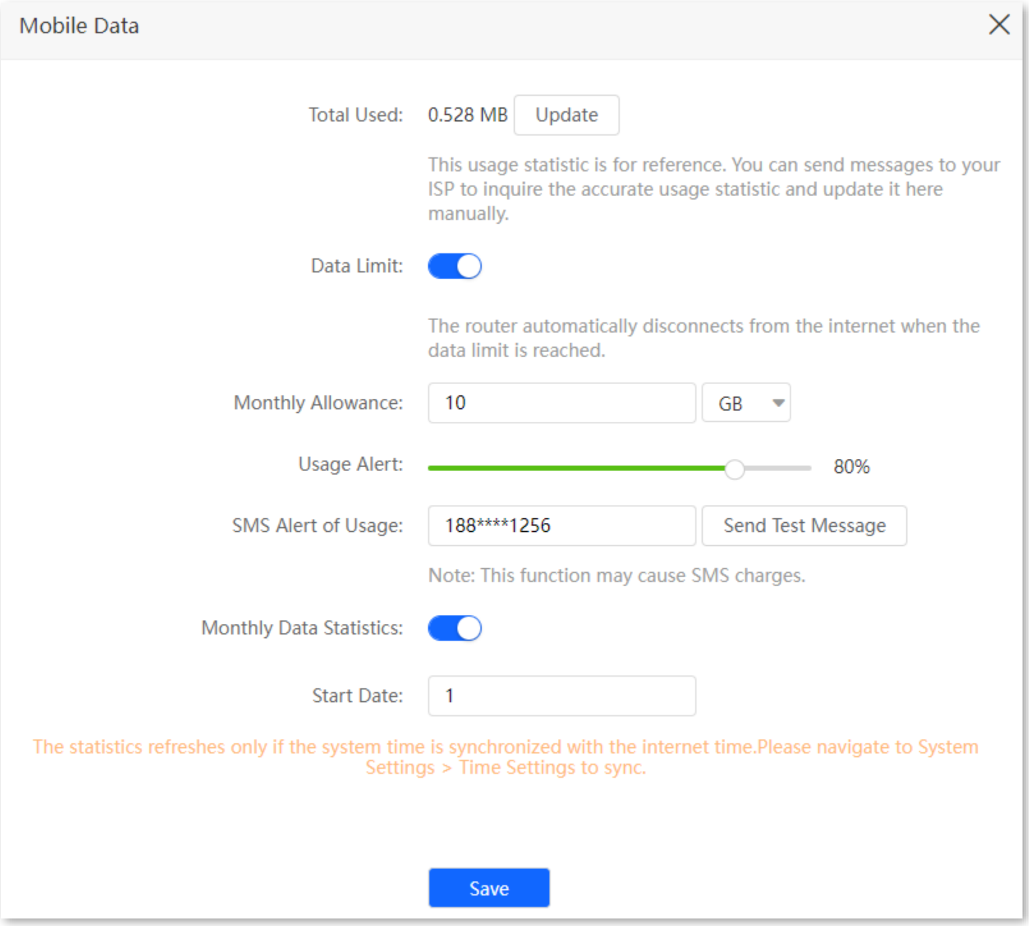
Step 6 Set **Usage Alert** to **80%**.

Step 7 Enter **188****1256** in **SMS Alert of Usage**.

Step 8 Enable **Monthly Data Statistics**.

Step 9 Enter **1** in **Start Date**.

Step 10 Click **Save**.


Mobile Data

Total Used: 0.528 MB

This usage statistic is for reference. You can send messages to your ISP to inquire the accurate usage statistic and update it here manually.

Data Limit: ●

The router automatically disconnects from the internet when the data limit is reached.

Monthly Allowance: 10 GB

Usage Alert: 80%

SMS Alert of Usage: 188****1256

Note: This function may cause SMS charges.

Monthly Data Statistics: ●

Start Date: 1

The statistics refreshes only if the system time is synchronized with the internet time.Please navigate to System Settings > Time Settings to sync.

After completing the configuration, you will receive a SMS message when the data traffic usage reached 8 GB and cannot access the internet through the router when the data traffic usage reached 10 GB.

Note

If you want to connect to the internet again after the data limit is reached, try the following methods:

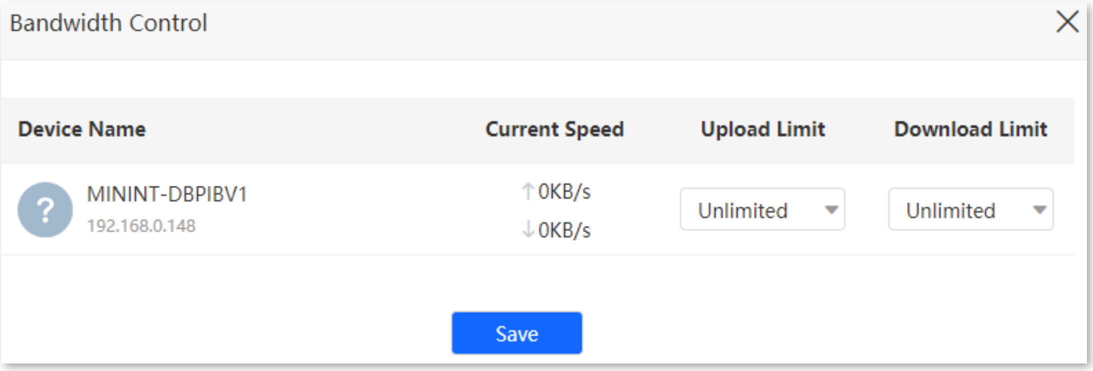
- Change the **Total Usage** by clicking **Update**.
- Disable **Data Limit**.
- Choose **Internet Settings**, and click **Connect** at the bottom of the page.

10.4 Bandwidth control

10.4.1 Overview

By configuring this function, you can limit the upload and download speed of devices connected to the router and allocate the bandwidth reasonably.

To access the configuration page, Log in to the web UI of the router and choose **Advanced Settings** > **Bandwidth Control**.


Bandwidth Control

Device Name	Current Speed	Upload Limit	Download Limit
MININT-DBPIBV1 192.168.0.148	↑0KB/s ↓0KB/s	Unlimited	Unlimited

Table 10-2 Parameter description

Parameter	Description
Device Name	It specifies the name and IP address of the device. You can click the name to change the name of the device.
Current Speed	It specifies the current upload and download speed of the device.
Upload Limit	They specify the upload and download speed limit for the device. You can click the drop-down box to choose a number or set it manually.
Download Limit	

10.4.2 Set the upload and download speed limit for users

Scenario: You want to allocate bandwidth equally among connected devices and enable all connected devices to enjoy smooth 720p videos.

Solution: Configure the bandwidth control function to meet the requirement.

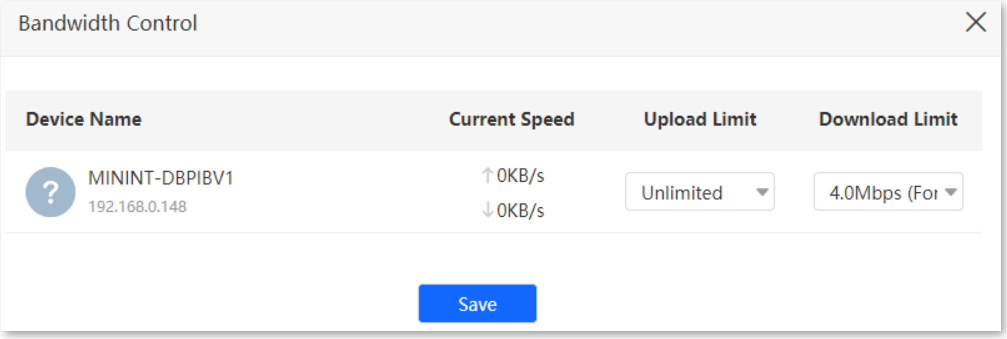
Configuring procedure:

Step 1 Log in to the web UI of the router.

Step 2 Choose **Advanced Settings** > **Bandwidth Control**.

Step 3 Target the devices to be controlled, and set the **Download Limit** to **4.0 Mbps (For HD Video).**

Step 4 Click **Save**.



Bandwidth Control

Device Name	Current Speed	Upload Limit	Download Limit
MININT-DBPIBV1 192.168.0.148	↑0KB/s ↓0KB/s	Unlimited	4.0Mbps (For

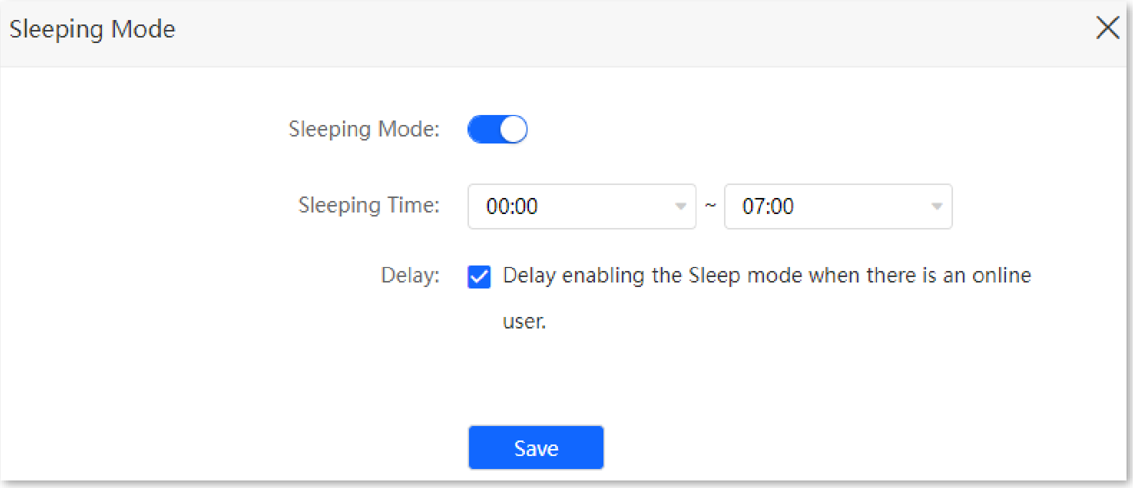
After the configuration, the highest speed for the device is 4 Mbps (512 KB/s) and the requirement of 720p videos can be satisfied.

10.5 Sleeping mode

When the sleeping mode function is enabled, the router turns off its LED indicators and disables the Wi-Fi network during the specified period.

To access the configuration page, Log in to the web UI of the router, and choose **Advanced Settings** > **Sleeping Mode**.

This function is disabled by default. When it is enabled, the page is shown as below.



Sleeping Mode

Sleeping Mode: ●

Sleeping Time: 00:00 ~ 07:00

Delay: ☑ Delay enabling the Sleep mode when there is an online user.

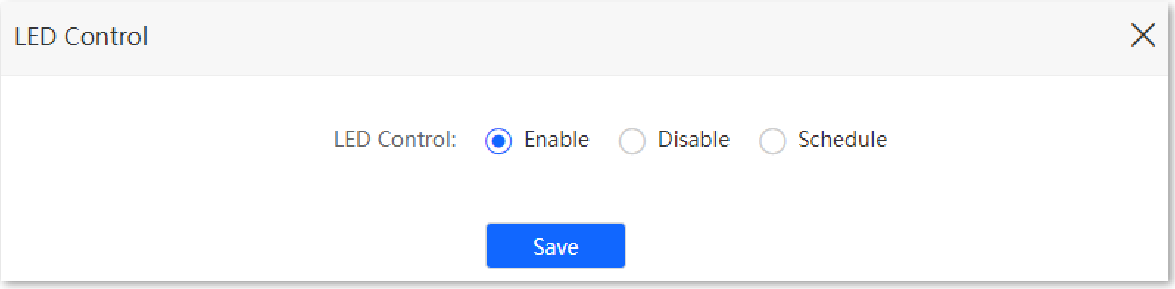
Table 10-3 Parameter description

Parameter	Description
Sleeping Mode	It is used to enable or disable the function. When the router is under sleeping mode and you want to use the Wi-Fi network, you can disable the function to wake up the router.
Sleeping Time	It specifies the period during which the router is under the sleeping mode.
Delay	It is used to enable or disable the Delay function. ● Ticked: The function is enabled. During the sleeping time, if there is any user connected to the router and the traffic over the router's WAN port exceeds 3 KB/s within 30 minutes, the router will delay entering the sleeping mode. If there is no user connected to the router and the traffic over the router's WAN port is slower than 3 KB/s within 3 minutes, the router will enter the sleeping mode. ● Unticked: The function is disabled. The router enters the sleeping mode during the sleeping time.

10.6 LED control

With the LED control function, you can control the status of the LED indicators.

To access the configuration page, Log in to the web UI of the router, and choose **Advanced Settings** > **LED Control**.



LED Control

LED Control: ● Enable ○ Disable ○ Schedule

Table 10-4 Parameter description

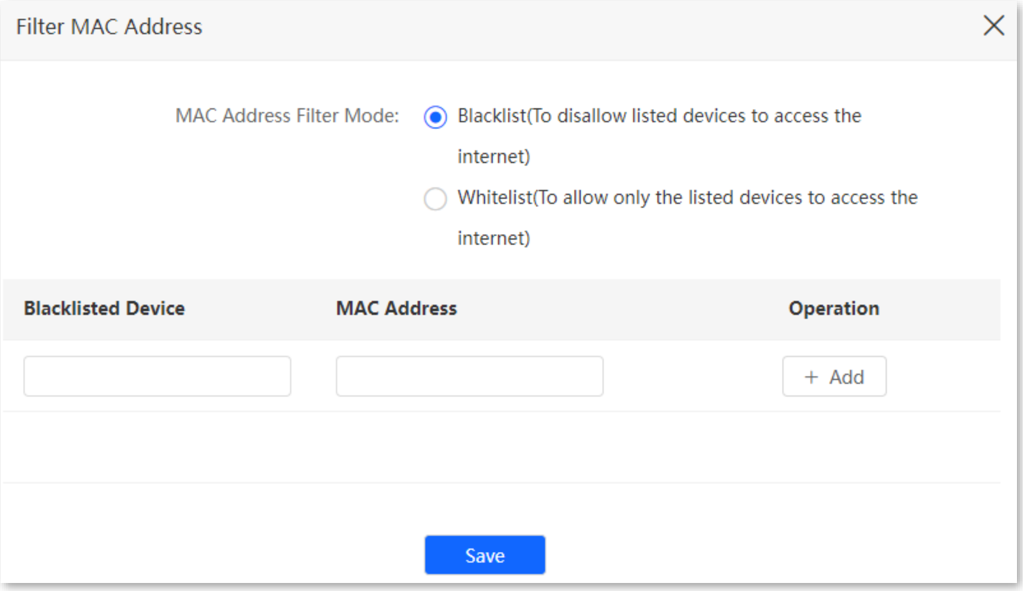
Parameter	Description
Enable	All LED indicators stay in their normal status.
Disable	All LED indicators are turned off.
Schedule	LED indicators are only turned off during the specified period.

10.7 Filter MAC address

10.7.1 Overview

This function enables you to add devices to the whitelist or blacklist to enable or disable specified users to access the internet through the router.

To access the configuration page, Log in to the web UI of the router, and choose **Advanced Settings** > **Filter MAC Address**.



Filter MAC Address ✕

MAC Address Filter Mode: ● Blacklist(To disallow listed devices to access the internet) ○ Whitelist(To allow only the listed devices to access the internet)

Blacklisted Device	MAC Address	Operation
		+ Add

Save

Table 10-5 Parameter description

Parameter	Description
MAC Address Filter Mode	It specifies the MAC address filter mode. ● **Blacklist**: Wireless devices listed are unable to connect to the Wi-Fi network of the router, and wired devices listed are unable to access the internet. ● **Whitelist**: Wireless devices listed can connect to the Wi-Fi network of the router, and wired devices listed are able to access the internet.
Blacklisted Device	They specify the name or remark for the device.
Whitelisted Device	
MAC Address	It specifies the MAC addresses of devices added to the list.
Operation	Available operations include: + Add: It is used to add new devices to the blacklist or whitelist. 🗑: It is used to remove devices from the blacklist or whitelist.
Add all online devices to the whitelist	It is only available when you set the whitelist for the first time. By clicking it, you can add all currently connected devices to the whitelist.

10.7.2 Only allow specified device to access the internet

Scenario: The Wi-Fi in your home is misused by unknown users sometimes.

Goal: Only allow certain devices of family members to access the internet.

Solution: You can configure the MAC address filter function to reach the goal.

Assume that:

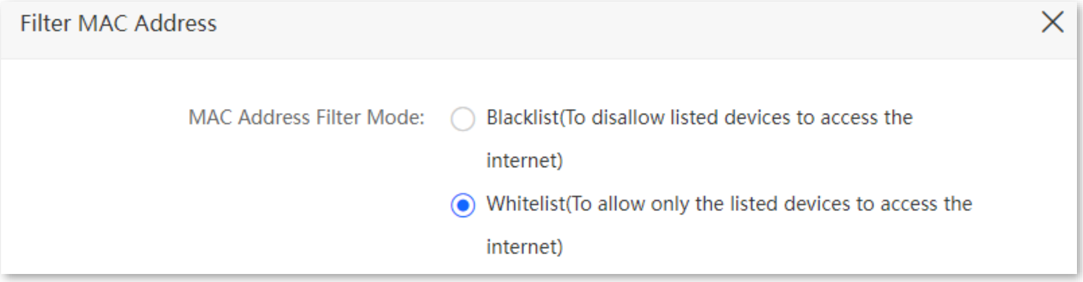
Device	MAC address	Status
Your own phone	8C:EC:4B:B3:04:92	Connected
Wife's phone	94:C6:91:29:C2:12	Disconnected
kid's phone	98:9C:57:19:D0:1B	Disconnected

Configuring procedure:

Step 1 Log in to the web UI of the router.

Step 2 Choose **Advanced Settings** > **Filter MAC Address**.

Step 3 Set the **MAC Address Filter Mode** to **Whitelist**.



Filter MAC Address

MAC Address Filter Mode: ○ Blacklist(To disallow listed devices to access the internet) ● Whitelist(To allow only the listed devices to access the internet)

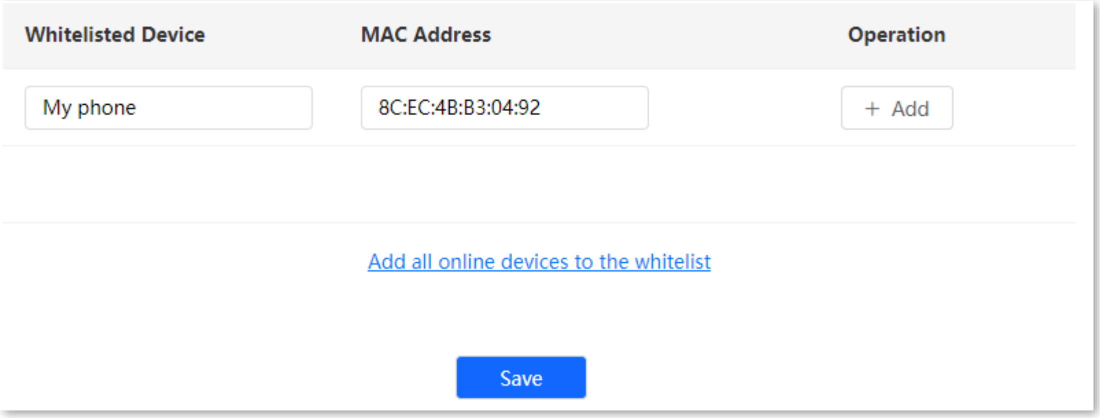
Step 4 (Optional) Enter the device name in the **Whitelisted Device** field, which is **My phone** in this example.

Step 5 Enter the **MAC Address** of the device, which is **8C:EC:4B:B3:04:92** in this example.

Step 6 Click **+Add**.

Note

Click Add all online devices to the whitelist, you will add all currently connected devices to the whitelist.



Whitelisted Device	MAC Address	Operation
My phone	8C:EC:4B:B3:04:92	+ Add

Step 7 Repeat **Step 4** to **Step 6** to add Wife’s phone (94:C6:91:29:C2:12) and kid’s phone (98:9C:57:19:D0:1B) to the whitelist.

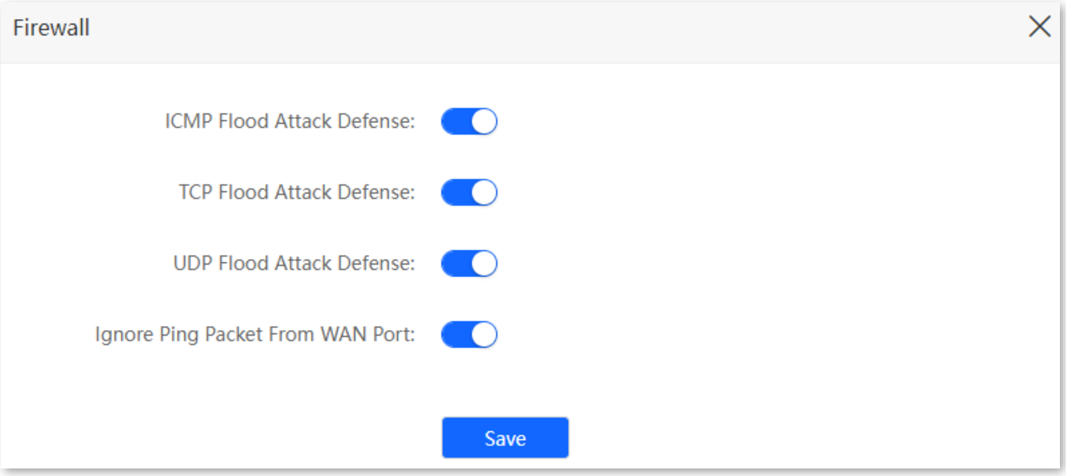
Step 8 Click **Save**.

When configuration is completed, only the three devices added can access the internet through the router.

10.8 Firewall

The firewall function helps the router detect and defend ICMP flood attack, TCP flood attack and UDP flood attack, and ignore Ping packet from WAN port. It is recommended to keep the default settings.

To access the configuration page, Log in to the web UI of the router, and choose **Advanced Settings** > **Firewall**.


Firewall

ICMP Flood Attack Defense: ●

TCP Flood Attack Defense: ●

UDP Flood Attack Defense: ●

Ignore Ping Packet From WAN Port: ●

Table 10-6 Parameter description

Parameter	Description
ICMP Flood Attack protection	It is used to enable or disable the ICMP flood attack protection. The ICMP flood attack means that, to implement attacks on the target host, the attacker sends a large number of ICMP Echo messages to the target host, which causes the target host to spend a lot of time and resources on processing ICMP Echo messages, but cannot process normal requests or responses.
TCP Flood Attack protection	It is used to enable or disable the TCP flood attack protection. The TCP flood attack means that, to implement attacks on the target host, the attacker quickly initiates a large number of TCP connection requests in a short period of time, and then suspends in a semi-connected state, thereby occupying a large amount of server resources until the server denies any services.
UDP Flood Attack protection	It is used to enable or disable the UDP flood attack protection. The UDP flood attack is implemented in a similar way with ICMP flood attack, during which the attacker sends many UDP packets to the target host, causing the target host to be busy processing these UDP packets, but unable to process normal packet requests or responses.
Ignore Ping Packet From WAN Port	It is used to enable or disable the Ignore Ping packet from WAN Port function. When it is enabled, the router automatically ignores the ping to its WAN from hosts from the internet and prevents itself from being exposed, while preventing external ping attacks.

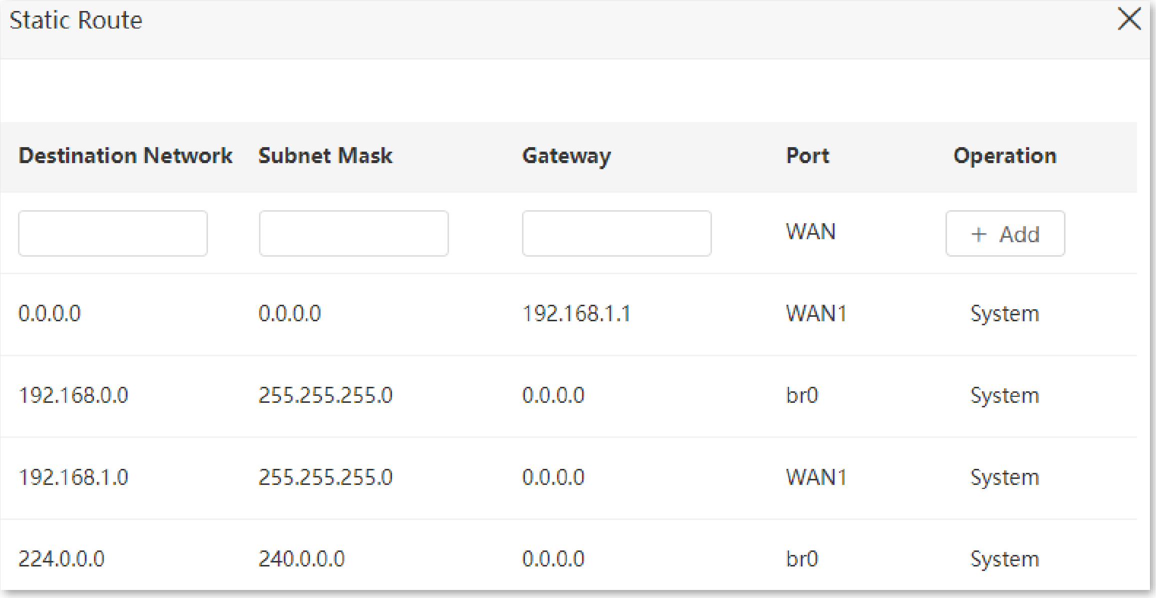
10.9 Static route

10.9.1 Overview

Routing is the act of choosing an optimal path to transfer data from a source address to a destination address. A static route is a special route that is manually configured and has the advantages of simplicity, efficiency, and reliability. Proper static routing can reduce routing problems and overload of routing data flow, and improve the forwarding speed of data packets.

A static route is set by specifying the target network, subnet mask, default gateway, and interface. The target network and subnet mask are used to determine a target network or host. After the static route is established, all data whose destination address is the destination network of the static route are directly forwarded to the gateway address through the static route interface.

To access the configuration page, Log in to the web UI of the router, and choose **Advanced Settings** > **Static Route**.


Static Route

Destination Network	Subnet Mask	Gateway	Port	Operation
			WAN	+ Add
0.0.0.0	0.0.0.0	192.168.1.1	WAN1	System
192.168.0.0	255.255.255.0	0.0.0.0	br0	System
192.168.1.0	255.255.255.0	0.0.0.0	WAN1	System
224.0.0.0	240.0.0.0	0.0.0.0	br0	System

Table 10-7 Parameter description

Parameter	Description
Destination Network	It specifies the IP address of the destination network. When the Destination Network and Subnet Mask are both 0.0.0.0, it indicates that this is the default route. **Note** When the route of packets cannot be found in the routing table, the router will forward the packets using the default route.
Subnet Mask	It specifies the subnet mask of the destination network.

Parameter	Description
Gateway	It specifies the ingress IP address of the next hop route after the data packet exits from the interface of the router. 0.0.0.0 indicates that the destination network is directly connected to the router.
Port	It specifies the interface that the packet exits from.
Operation	Available operations include: + Add: It is used to add new devices to the blacklist or whitelist. 🗑: It is used to remove devices from the blacklist or whitelist.

10.9.2 Add a static route rule

Scenario: You have a DS-3WR4G12C and another two routers. Router1 is connected to the internet and its DHCP server is enabled. Router2 is connected to an intranet and its DHCP server is disabled.

Goal: You can access both the internet and intranet at the same time.

Solution: You can configure the static route function to reach the goal.

Note

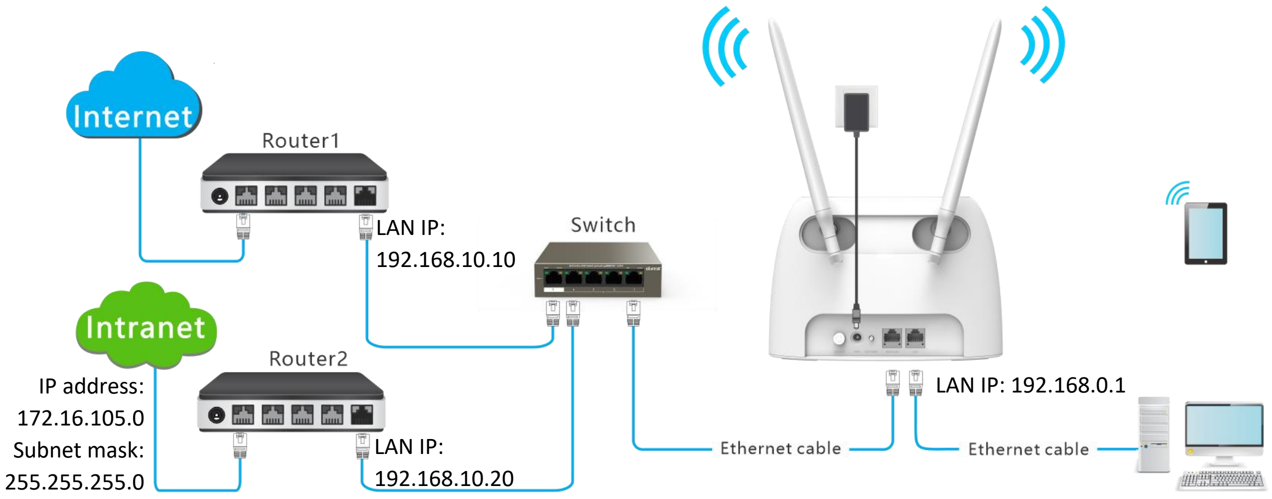
This solution is only applicable when the router is under wireless router mode.

Assume the LAN IP addresses of these devices are:

- DS-3WR4G12C: 192.168.0.1
- Router1: 192.168.10.10
- Router2: 192.168.10.20

The information about the intranet:

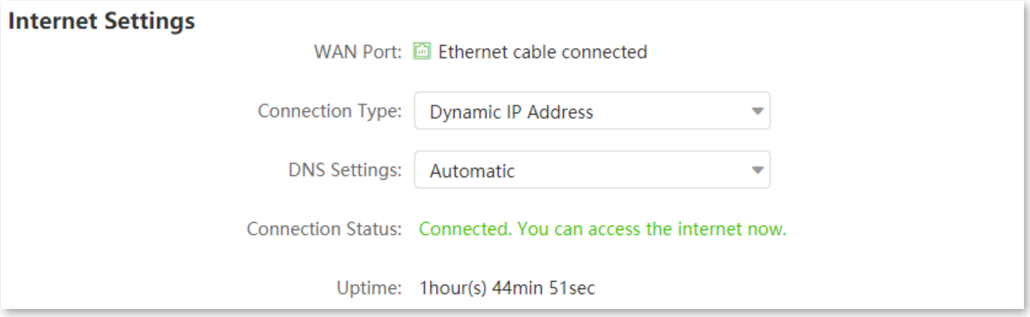
- IP address: 172.16.105.0
- Subnet mask: 255.255.255.0



Configuring procedure:

Step 1 Log in to the web UI of the router.

Step 2 Refer to Access the internet with a dynamic IP address to configure the internet access for the router.



Internet Settings

WAN Port: Ethernet cable connected

Connection Type: Dynamic IP Address

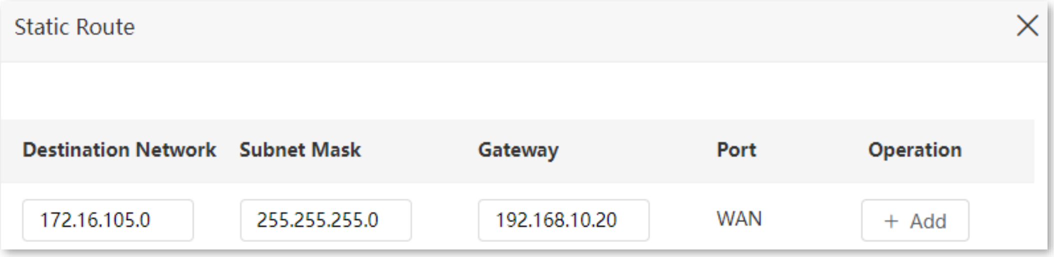
DNS Settings: Automatic

Connection Status: Connected. You can access the internet now.

Uptime: 1hour(s) 44min 51sec

Step 3 Add a static route rule.

1) Choose **Advanced Settings** > **Static Route**.
2) Enter the IP address of the destination network, which is **172.16.105.0** in this example.
3) Enter the subnet mask of the destination network, which is **255.255.255.0** in this example.
4) Enter the ingress IP address of the next hop route, which is **192.168.10.20** in this example.
5) Click +Add.



Static Route

Destination Network	Subnet Mask	Gateway	Port	Operation
172.16.105.0	255.255.255.0	192.168.10.20	WAN	+ Add

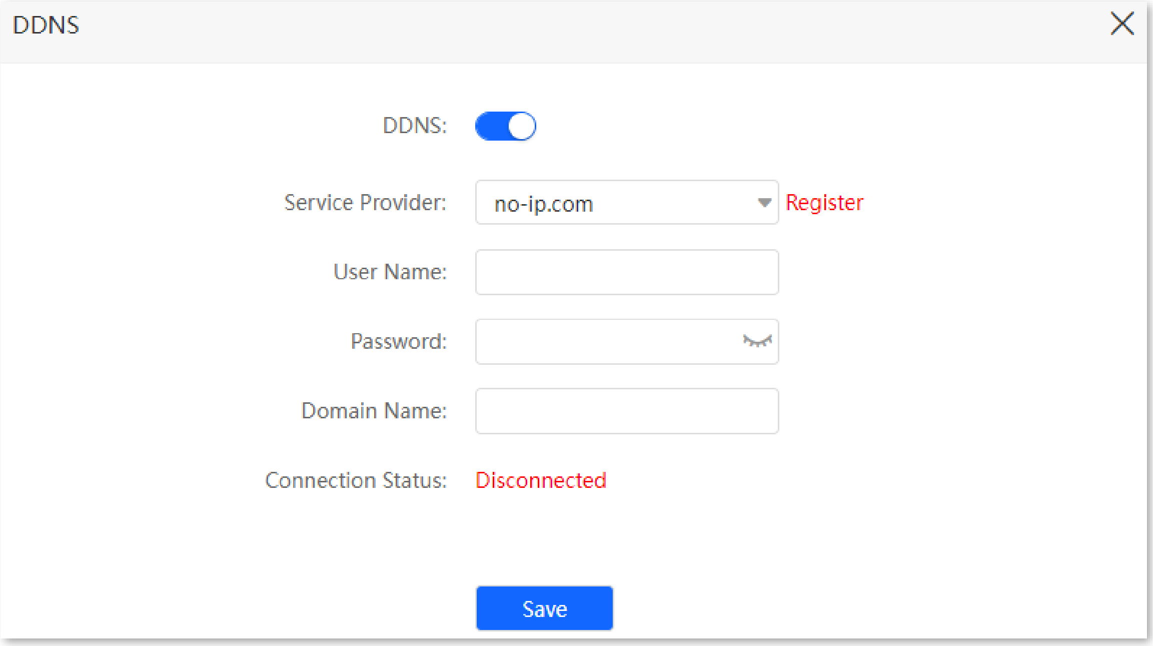
When completing the configurations, you can access both the internet and intranet through DS-3WR4G12C at the same time.

10.10 DDNS

10.10.1 Overview

DDNS normally interworks with virtual server, DMZ host and remote management, so that the internet users can be free from the influence of dynamic WAN IP address and access the internal server or the router's web UI with a fixed domain name.

To access the configuration page, Log in to the web UI of the router, and choose **Advanced Settings** > **DDNS**. This function is disabled by default. When it is enabled, the page is shown as below.



DDNS

DDNS: ●

Service Provider: no-ip.com

User Name:

Password:

Domain Name:

Connection Status: Disconnected

Table 10-8 Parameter description

Parameter	Description
DDNS	It is used to enable or disable the DDNS function.
Service Provider	It specifies the DDNS service provider.
User Name	They specify the user name and password registered on a DDNS service provider's website for logging in to the DDNS service.
Password	
Domain Name	It specifies the domain name registered on the DDNS service provider's website. If this field is invisible after the service provider is chosen, it is not required.
Connection Status	It specifies the current connection status of the DDNS service.

10.10.2 Enable internet users to access LAN resources using a domain name

Scenario: You have set up an FTP server within your LAN.

Goal: Open the FTP server to internet users and enable family members who are not at home to access the resources of the FTP server from the internet using a domain name.

Solution: You can configure the DDNS plus virtual server functions to reach the goal.

Assume that the information of the FTP server includes:

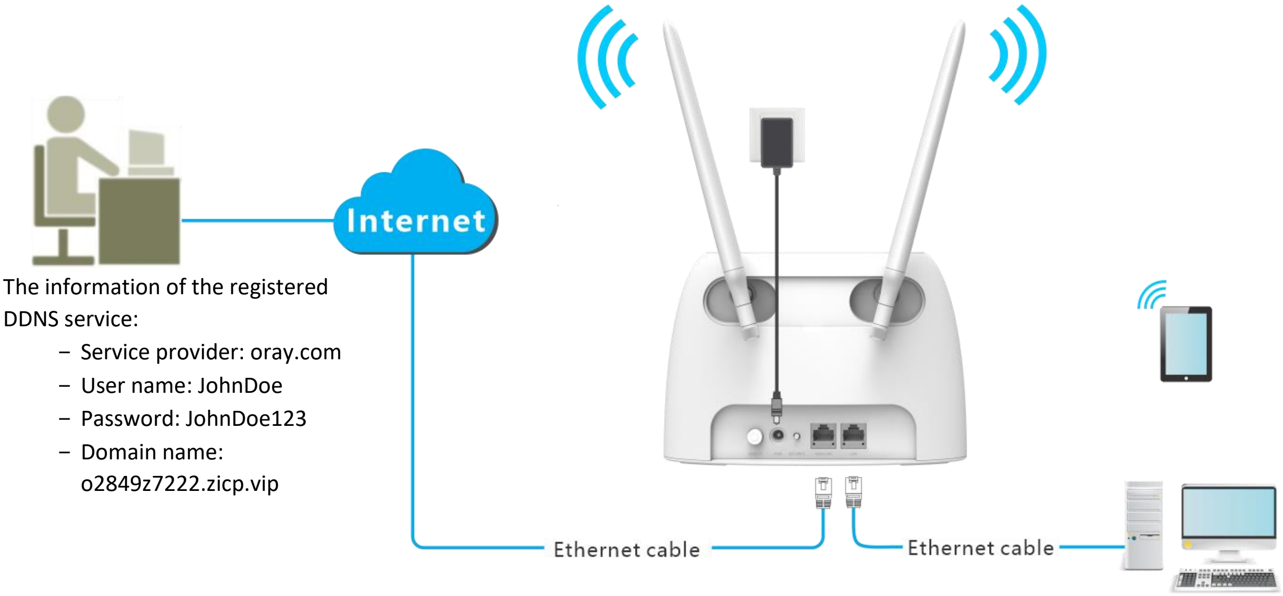
- IP address: 192.168.0.136
- MAC address of the host: D4:61:DA:1B:CD:89
- Service port: 21

The information of the registered DDNS service:

- Service provider: oray.com
- User name: JohnDoe
- Password: JohnDoe123
- Domain name: o2849z7222.zicp.vip

Note

Please ensure that router obtains an IP address from the public network. This function may not work on a host with an IP address of a private network or an intranet IP address assigned by ISPs that starts with 100. Common IPv4 addresses are classified into class A, class B and class C. Private IP addresses of class A range from 10.0.0.0 to 10.255.255.255. Private IP addresses of class B range from 172.16.0.0-172.31.255.255. Private IP addresses of class C range from 192.168.0.0-192.168.255.255.



The information of the registered DDNS service:

- Service provider: oray.com
- User name: JohnDoe
- Password: JohnDoe123
- Domain name: o2849z7222.zicp.vip

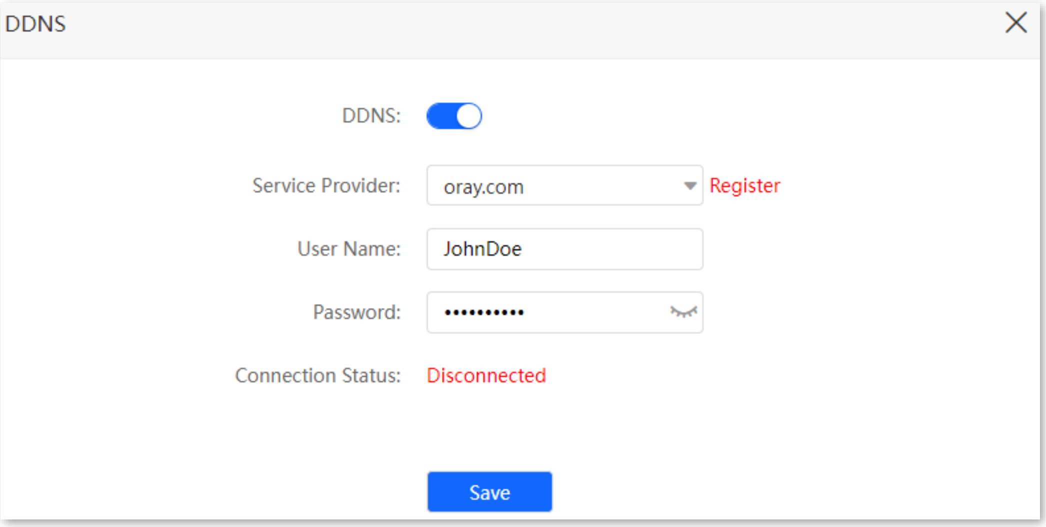
IP address: 192.168.0.136
MAC address: D4:61:DA:1B:CD:89
Service port: 21

Configuration procedure:

Step 1 Log in to the web UI of the router.

Step 2 Configure the DDNS function.

1) Choose **Advanced Settings** > **DDNS**.
2) Enabled the **DDNS** function.
3) Choose a service provider, which is **oray.com** in this example.
4) Enter the user name and password, which are **JohnDoe** and **JohnDoe123** in this example.
5) Click **Save**.



DDNS

DDNS: ●

Service Provider: oray.com ▾ Register

User Name: JohnDoe

Password: ••••••••••

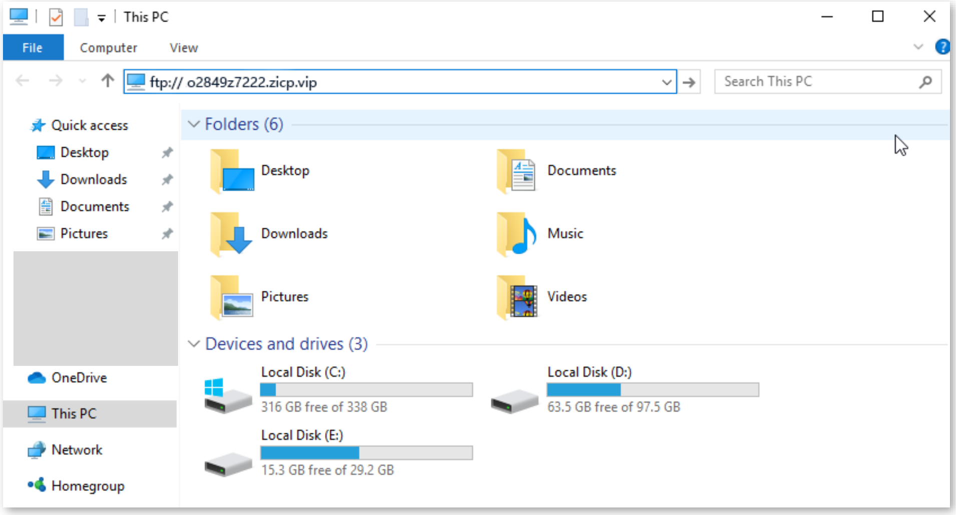
Connection Status: Disconnected

Save

Wait a moment, when the Connection Status turns Connected, the configurations succeed.

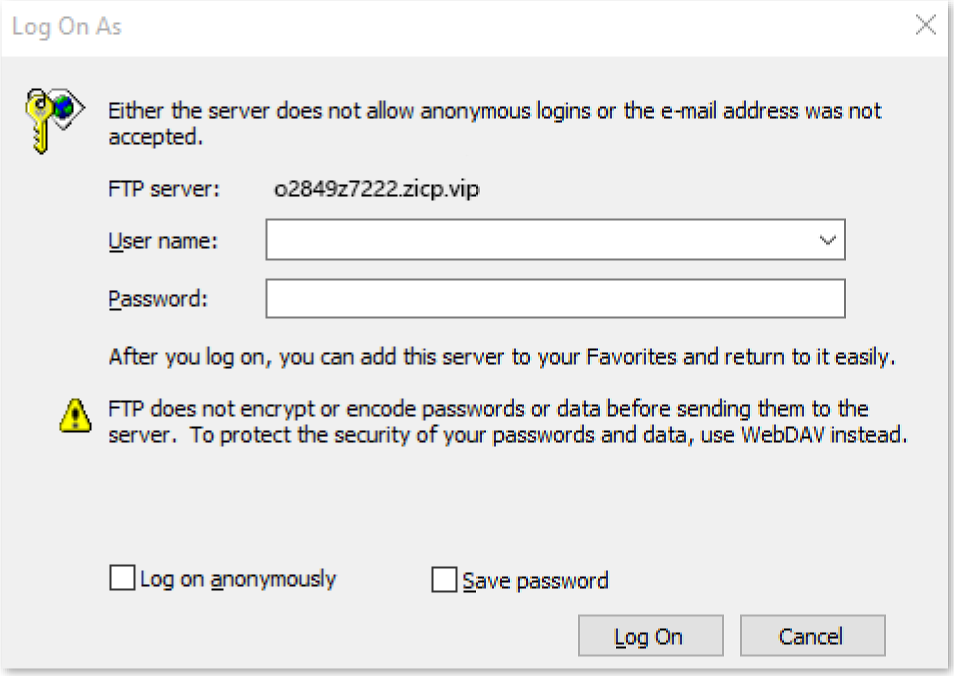
Step 3 Configure the virtual server function (refer to Virtual server)

When completing the configurations, users from the internet can access the FTP server by visiting "*Intranet service application layer protocol name*://*the domain name*". If the WAN port number is not the same as the default intranet service port number, the visiting address should be: "*Intranet service application layer protocol name*://*the domain name*:*WAN port number*". In this example, the address is **ftp://o2849z7222.zicp.vip**



ftp:// o2849z7222.zicp.vip

Enter the user name and password to access the resources on the FTP server.



Either the server does not allow anonymous logins or the e-mail address was not accepted.

FTP server: o2849z7222.zicp.vip

User name:

Password:

After you log on, you can add this server to your Favorites and return to it easily.

FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use WebDAV instead.

□ Log on anonymously □ Save password

Note

After the configurations, if internet users still cannot access the FTP server, try the following methods:

- Ensure that the LAN port number configured in the virtual server function is the same as the service port number set on the server.
- Close the firewall, antivirus software and security guards on the host of the FTP server and try again.

10.11 Virtual server

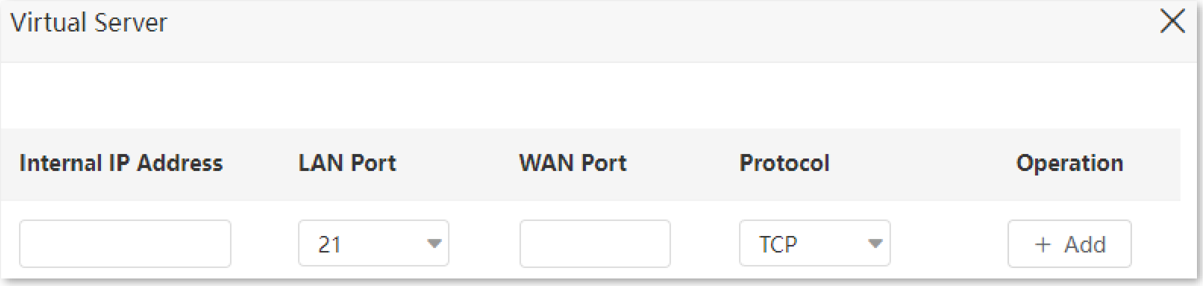
10.11.1 Overview

By default, internet users cannot actively access the LAN of the router.

The virtual server function opens a port of the router, and binds the LAN server to the port using the server's IP address and intranet service port. All access requests to the WAN port of the router will be directed to the server. Therefore, the server within the LAN can be accessed by internet users and the LAN can be free from attacks from the internet.

For example, the virtual server function enables internet users to access web servers or FTP servers within the LAN.

To access the configuration page, Log in to the web UI of the router, and choose **Advanced Settings** > **Virtual Server**.



Virtual Server

Internal IP Address	LAN Port	WAN Port	Protocol	Operation
	21		TCP	+ Add

Table 10-9 Parameter description

Parameter	Description
Internal IP Address	It specifies the IP address of the server within the LAN of the router.
LAN Port	It specifies the service port number of the server under the LAN of the router. You can either choose a service port number in the drop-down box, or enter a service port number manually.
WAN Port	It specifies the port of the router which is opened and accessible to internet users.
Protocol	It specifies the transport layer protocol of the service. If you are not sure about this parameter, **TCP&UDP** is recommended.
Operation	Available operations include: + Add : It is used to add a new virtual server rule. 🗑: It is used to delete existing virtual server rules.

10.11.2 Enable internet users to access LAN resources

Scenario: You have set up an FTP server within your LAN.

Goal: Open the FTP server to internet users and enable family members who are not at home to access the resources of the FTP server from the internet.

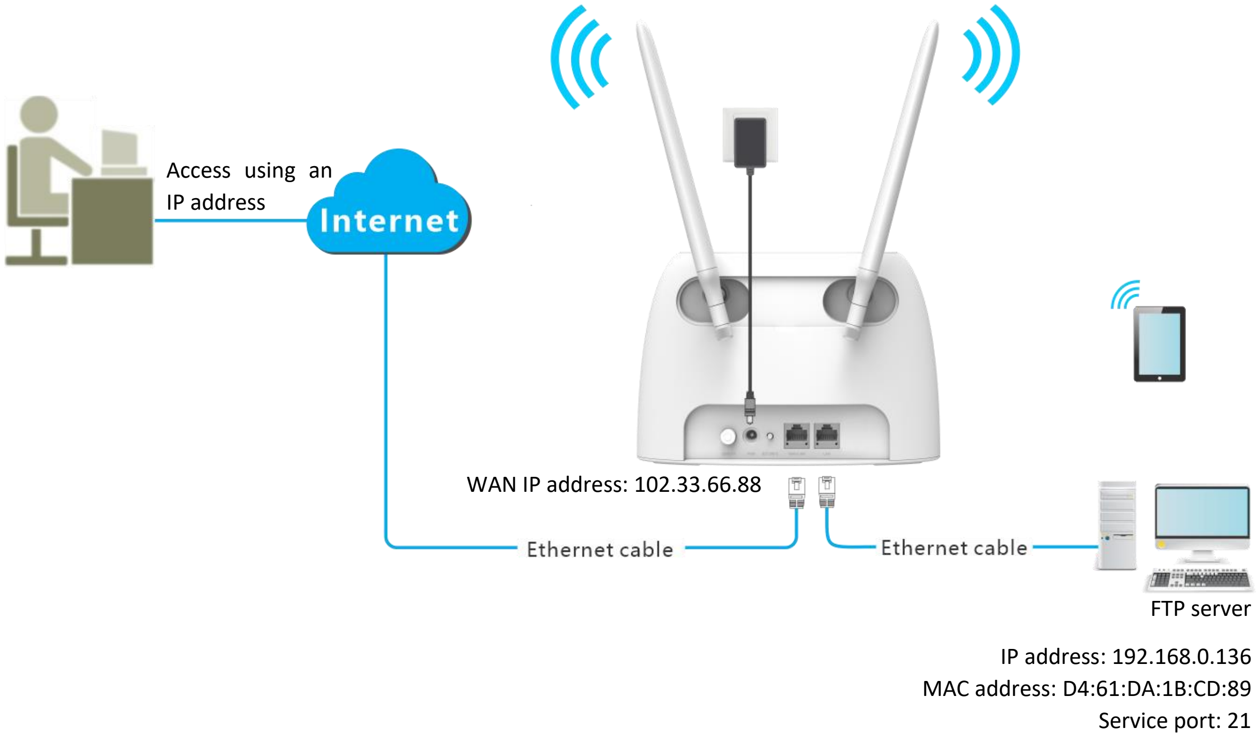
Solution: You can configure the virtual server function to reach the goal.

Assume that the information of the FTP server includes:

- IP address: 192.168.0.136
- MAC address: D4:61:DA:1B:CD:89
- Service port: 21
- The WAN IP address of the router: 102.33.66.88.

Note

- Please ensure that router obtains an IP address from the public network. This function may not work on a host with an IP address of a private network or an intranet IP address assigned by ISPs that start with 100. Common IPv4 addresses are classified into class A, class B and class C. Private IP addresses of class A range from 10.0.0.0 to 10.255.255.255; Private IP addresses of class B range from 172.16.0.0-172.31.255.255; Private IP addresses of class C range from 192.168.0.0-192.168.255.255.
- ISPs may block unreported web services to be accessed with the default port number 80. Therefore, when the default LAN port number is 80, please change it to an uncommon port number (1024-65535) manually, such as 9999.
- The LAN port number can be different from the WAN port number.


Access using an IP address
Internet
WAN IP address: 102.33.66.88
Ethernet cable
Ethernet cable
FTP server
IP address: 192.168.0.136
MAC address: D4:61:DA:1B:CD:89
Service port: 21

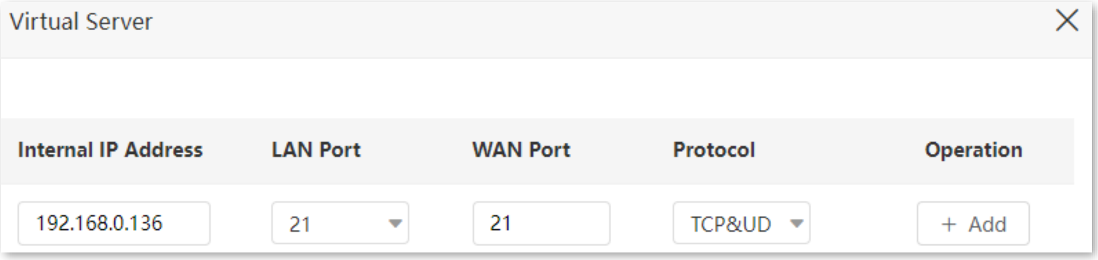
Configuration procedure:

Step 1 Log in to the web UI of the router.

Step 2 Add a virtual server rule.

1) Choose **Advanced Settings** > **Virtual Server**.

2) Enter the **Internal IP Address**, which is **192.168.0.136** in this example.
3) Choose a **LAN Port** in the drop-down box, which is **21** in this example.
4) Enter a **WAN Port**, which is **21** in this example.
5) Choose a protocol, which is **TCP&UDP** in this example.
6) Click **+Add**.

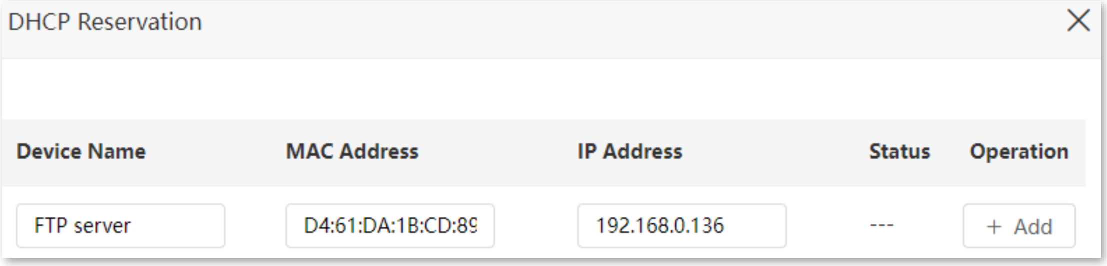


Virtual Server

Internal IP Address	LAN Port	WAN Port	Protocol	Operation
192.168.0.136	21	21	TCP&UD	+ Add

Step 3 Assign a fixed IP address to the host where the server locates.

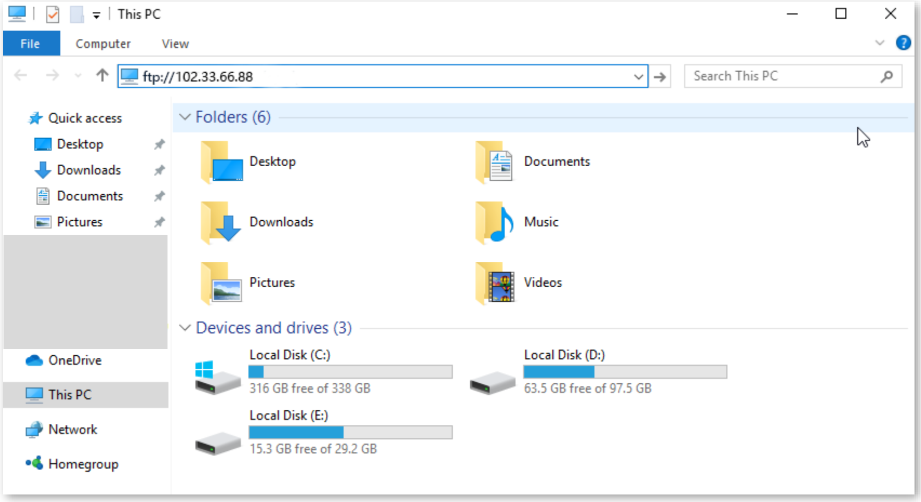
1) Choose **System Settings** > **DHCP Reservation**.
2) Specifies a **Device Name** for the host of the server, which is **FTP server** in this example.
3) Enter the **MAC Address** of the host of the server, which is **D4:61:DA:1B:CD:89** in this example.
4) Enter the **IP Address** of host of the server, which is **192.168.0.136** in this example.
5) Click **+Add**.



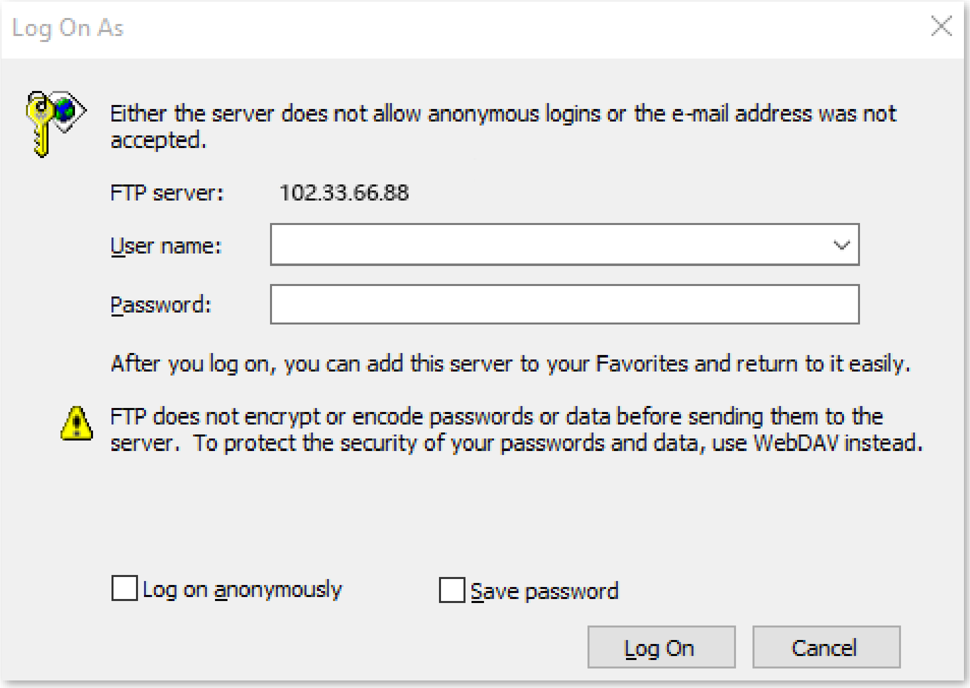
DHCP Reservation

Device Name	MAC Address	IP Address	Status	Operation
FTP server	D4:61:DA:1B:CD:89	192.168.0.136	---	+ Add

When completing the configurations, users from the internet can access the FTP server by visiting "*Intranet service application layer protocol name*://*WAN IP address of the router*". If the WAN port number is not the same as the default intranet service port number, the visiting address should be: "*Intranet service application layer protocol name*://*WAN IP address of the router:WAN port number*". In this example, the address is "**ftp://102.33.66.88**". You can find the WAN IP address of the router in View system information.



Enter the user name and password to access the resources on the FTP server.



Log On As

Either the server does not allow anonymous logins or the e-mail address was not accepted.

FTP server: 102.33.66.88

User name:

Password:

After you log on, you can add this server to your Favorites and return to it easily.

FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use WebDAV instead.

□ Log on anonymously □ Save password

If you want to access the server within a LAN using a domain name, refer to the solution DDNS + Virtual server.

Note

After the configurations, if internet users still cannot access the FTP server, try the following methods:

- Ensure that the LAN port number configured in the virtual server function is the same as the service port number set on the server.
- Close the firewall, antivirus software and security guards on the host of the FTP server and try again.

10.12 DMZ host

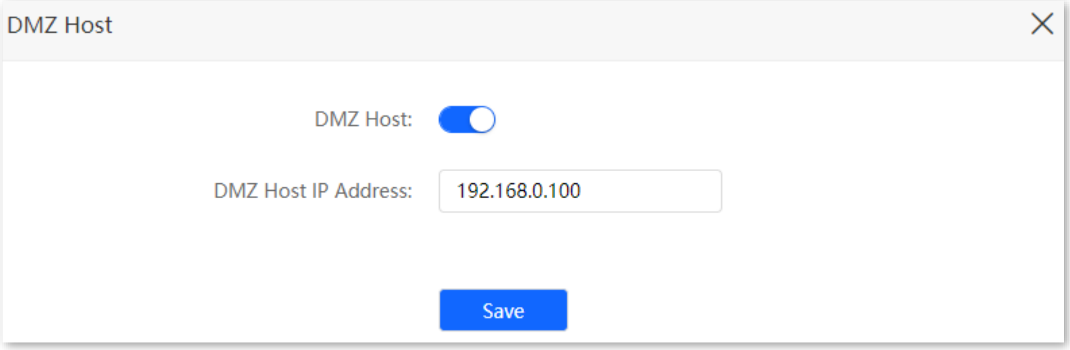
10.12.1 Overview

A DMZ host on a LAN is free from restrictions in communicating with the internet. It is useful for getting better and smoother experience in video conferences and online games. You can also set the host of a server within the LAN as a DMZ host when in need of accessing the server from the internet.

Caution

- A DMZ host is not protected by the firewall of the router. A hacker may leverage the DMZ host to attack your LAN. Therefore, enable the DMZ function only when necessary.
- Hackers may leverage the DMZ host to attack the local network. Do not use the DMZ host function randomly.
- Security software, antivirus software, and the built-in OS firewall of the computer may cause DMZ function failures. Disable them when using the DMZ function. If the DMZ function is not required, you are recommended to disable it and enable your firewall, security, and antivirus software.

To access the configuration page, Log in to the web UI of the router, and choose **Advanced Settings** > **DMZ Host**. This function is disabled by default. When it is enabled, the page is shown as below.



DMZ Host: ●

DMZ Host IP Address: 192.168.0.100

Table 10-10 Parameter description

Parameter	Description
DMZ Host	It is used to enable or disable the DMZ host function.
DMZ Host IP Address	It specifies the IP address of the host that is to be set as the DMZ host.

10.12.2 Enable internet users to access LAN resources

Scenario: You have set up an FTP server within your LAN.

Goal: Open the FTP server to internet users and enable family members who are not at home to access the resources of the FTP server from the internet.

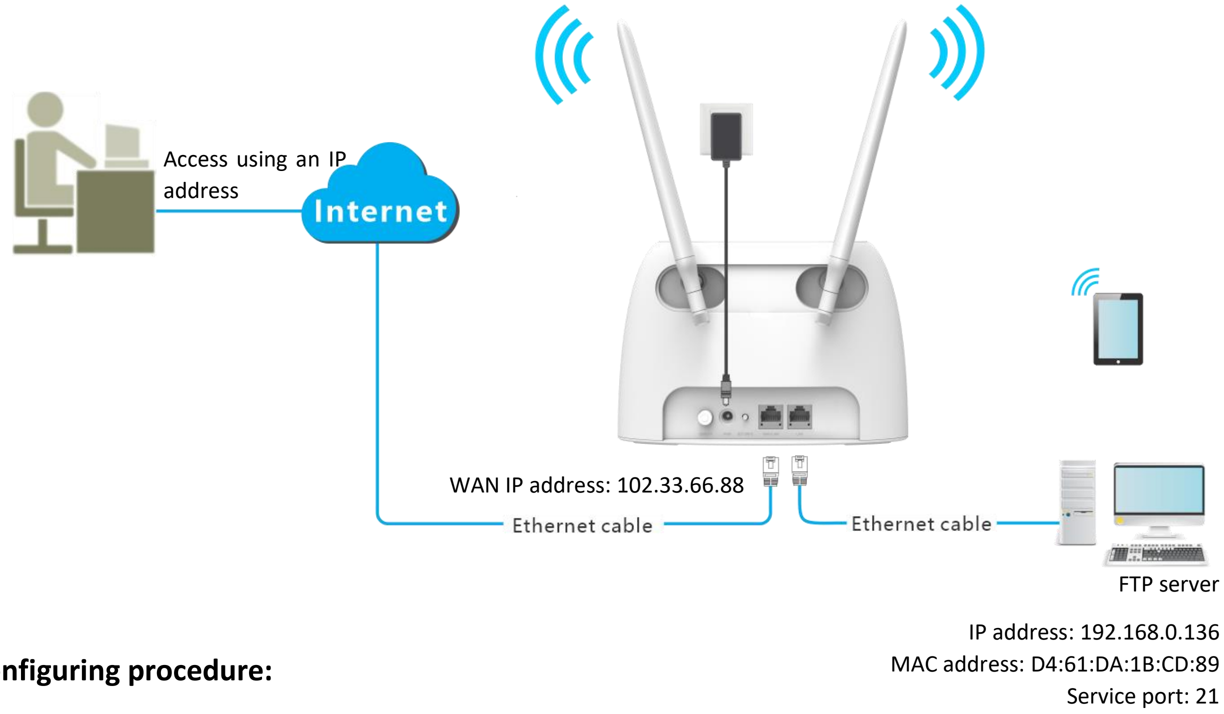
Solution: You can configure the DMZ host function to reach the goal.

Assume that the information of the FTP server includes:

- IP address: 192.168.0.136
- MAC address: D4:61:DA:1B:CD:89
- Service port: 21
- The WAN IP address of the router: 102.33.66.88.

Note

Please ensure that router obtains an IP address from the public network. This function may not work on a host with an IP address of a private network or an intranet IP address assigned by ISPs that start with 100. Common IPv4 addresses are classified into class A, class B and class C. Private IP addresses of class A range from 10.0.0.0 to 10.255.255.255. Private IP addresses of class B range from 172.16.0.0-172.31.255.255. Private IP addresses of class C range from 192.168.0.0-192.168.255.255.

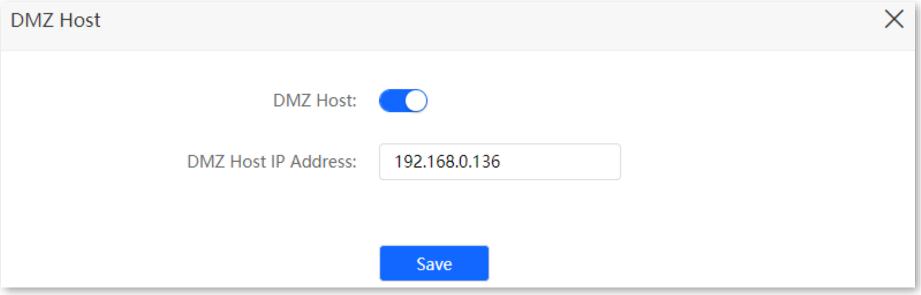

Access using an IP address
Internet
WAN IP address: 102.33.66.88
Ethernet cable
Ethernet cable
FTP server
IP address: 192.168.0.136
MAC address: D4:61:DA:1B:CD:89
Service port: 21

Configuring procedure:

Step 1 Log in to the web UI of the router.

Step 2 Set the server host as the DMZ host.

1) Choose **Advanced Settings** > **DMZ Host**.
2) Enable **DMZ Host**.
3) Enter the IP address of the host, which is **192.168.0.136** in this example.
4) Click **Save**.



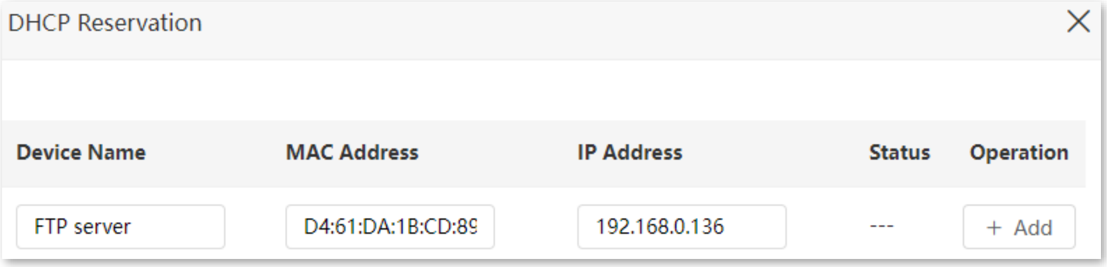
DMZ Host

DMZ Host: ●

DMZ Host IP Address: 192.168.0.136

Step 3 Assign a fixed IP address to the host where the server locates.

1) Choose **System Settings** > **DHCP Reservation**.
2) Specify a **Device Name** for the server host, which is **FTP server** in this example.
3) Enter the **MAC Address** of the host of the server, which is **D4:61:DA:1B:CD:89** in this example.
4) Enter the reserved **IP Address** for the server host, which is **192.168.0.136** in this example.
5) Click **+Add**.



DHCP Reservation

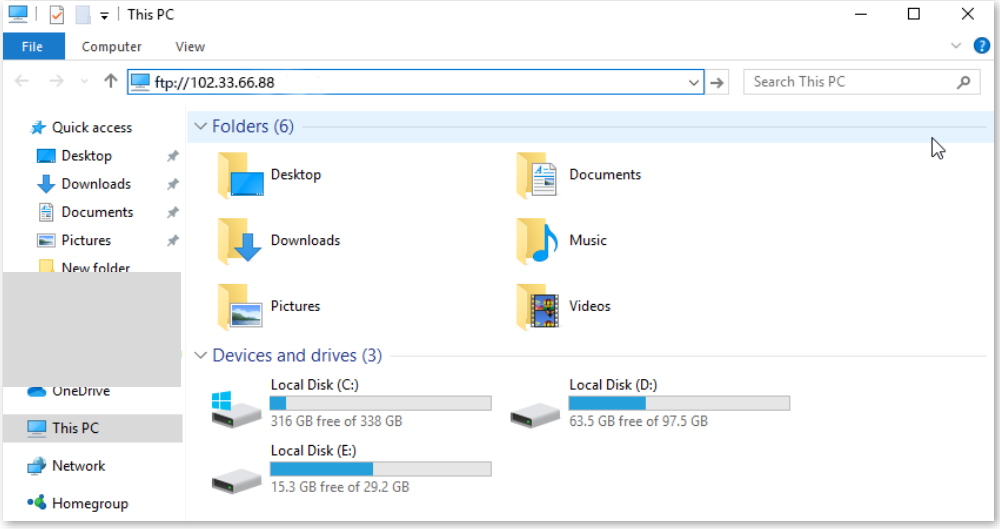
Device Name	MAC Address	IP Address	Status	Operation
FTP server	D4:61:DA:1B:CD:89	192.168.0.136	---	+ Add

When the configurations are completed, users from the internet can access the DMZ host by visiting "*Intranet service application layer protocol name://WAN IP address of the router*". If the intranet service port number is not the default number, the visiting address should be: "*Intranet service application layer protocol name://WAN IP address of the router:intranet service port number*".

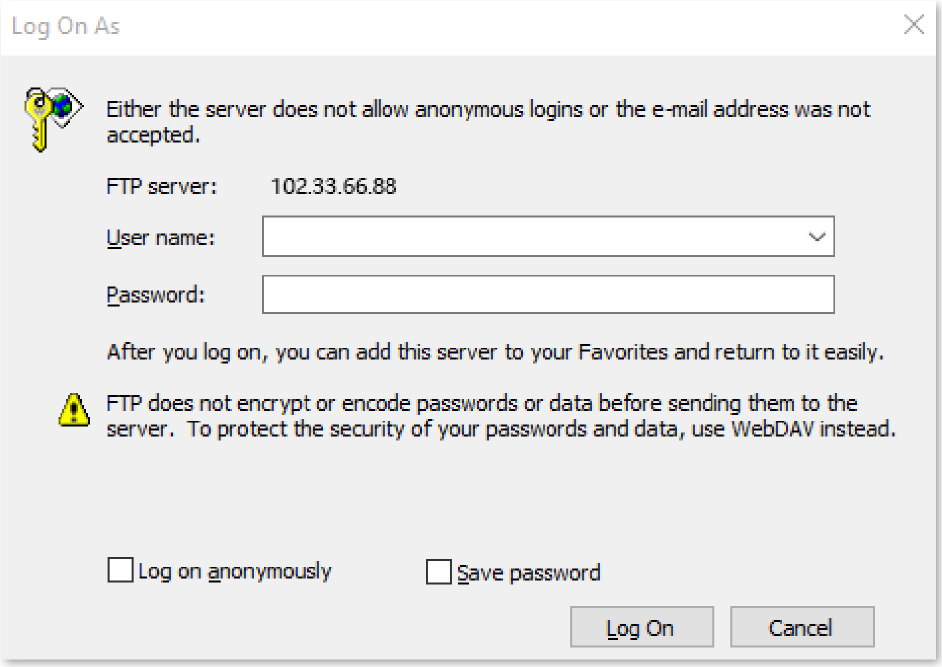
In this example, the address is "**ftp://102.33.66.88**". You can find the WAN IP address of the router in View system information.

Note

When the default intranet service port number is 80, please change the service port number to an uncommon one (1024-65535), such as 9999.



Enter the user name and password to access the resources on the FTP server.



Log On As

Either the server does not allow anonymous logins or the e-mail address was not accepted.

FTP server: 102.33.66.88

User name:

Password:

After you log on, you can add this server to your Favorites and return to it easily.

FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use WebDAV instead.

□ Log on anonymously □ Save password

If you want to access the server within a LAN using a domain name, you can configure DMZ + DDNS to reach the goal. Refer to the solution Virtual server + DDNS for specific steps.

Note

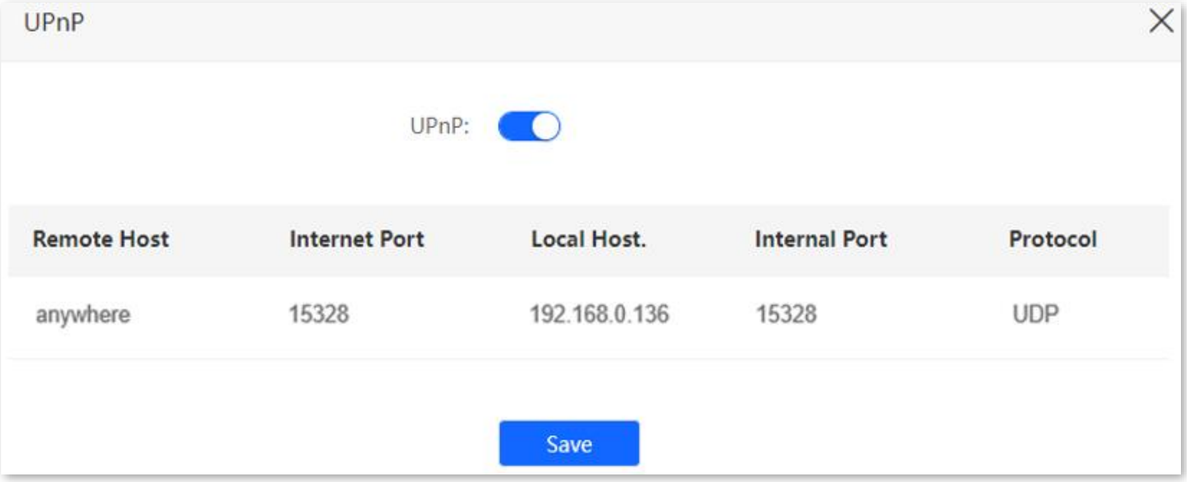
After the configurations, if internet users still cannot access the FTP server, close the firewall, antivirus software and security guards on the host of the FTP server and try again.

10.13 UPnP

UPnP is short for Universal Plug and Play. This function enables the router to open port automatically for UPnP-based programs. It is generally used for P2P programs, such as BitComet and AnyChat, and helps increase the download speed.

To access the configuration page, Log in to the web UI of the router, and choose **Advanced Settings** > **UPnP**.

This function is disabled by default. When it is enabled, and any program that supports the UPnP function is launched, you can find the port conversion information on this page when the program sends any requests.

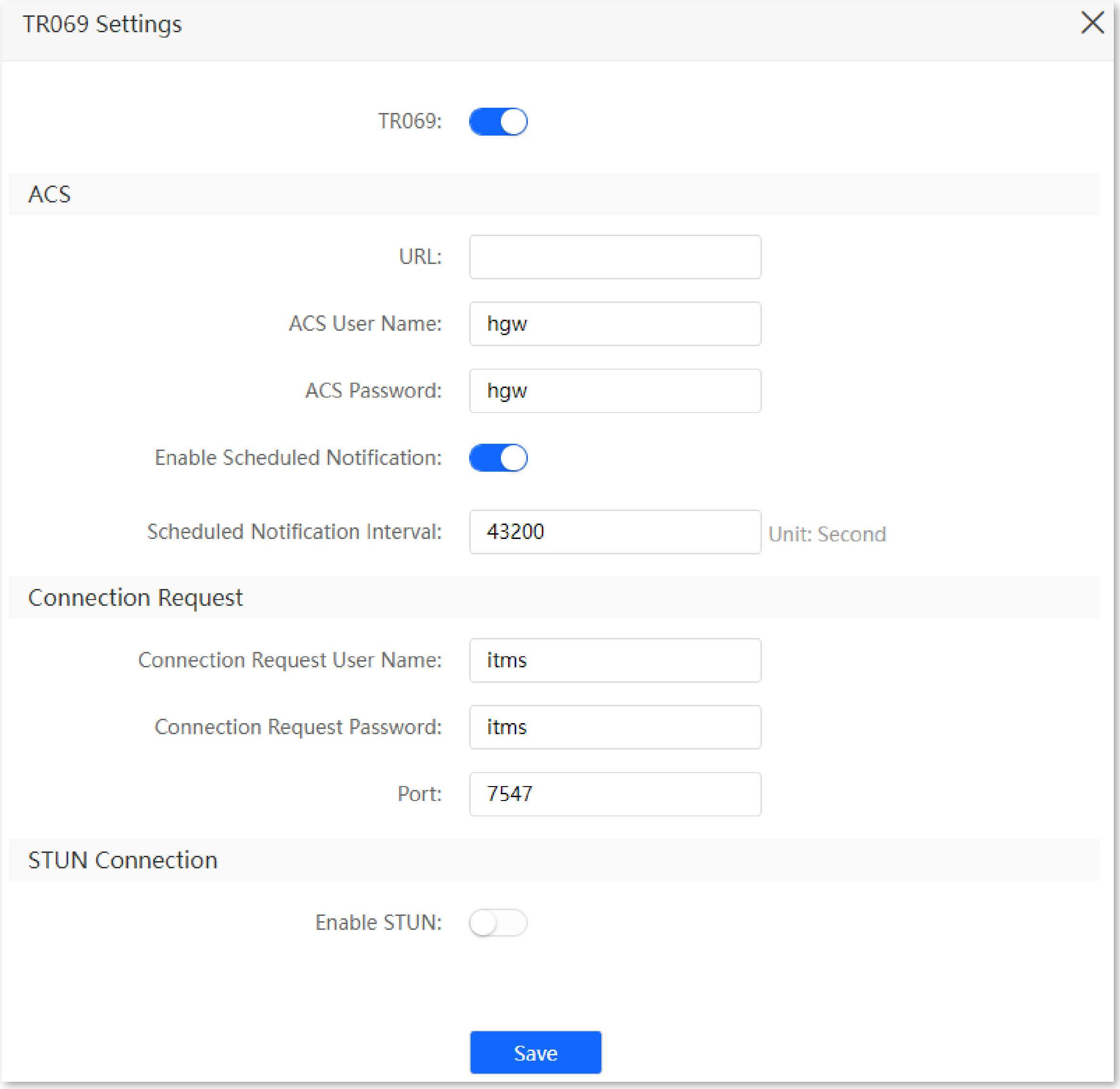


Remote Host	Internet Port	Local Host.	Internal Port	Protocol
anywhere	15328	192.168.0.136	15328	UDP

10.14 TR069

The TR069 (Technical Report - 069) protocol allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to the router from the internet. Generally, it is used by the ISP to manage the router and is disabled by default. Contact your ISP for these parameters.

To access the configuration page, Log in to the web UI of the router and choose **Advanced Settings** > **TR069**. This function is disabled by default. When it is enabled, the page is shown as below.



TR069 Settings

TR069: ●

ACS

URL:

ACS User Name: hgw

ACS Password: hgw

Enable Scheduled Notification: ●

Scheduled Notification Interval: 43200 Unit: Second

Connection Request

Connection Request User Name: itms

Connection Request Password: itms

Port: 7547

STUN Connection

Enable STUN: ○

Table 10-11 Parameter description

Parameter	Description
TR069	It is used to enable or disable the TR069 function.
URL	It specifies the domain name of the ACS.
ACS User Name	It specifies the user name used to authenticate the router when the router connects to the ACS using the TR069 protocol.
ACS Password	It specifies the password used to authenticate the router when the router connects to the ACS using the TR069 protocol.
Enable Scheduled Notification	It is used to enable or disable the scheduled notification function, which enables the router to send messages to the ACS at interval.
Scheduled Notification Interval	It specifies the interval at which the router sent messages to the ACS.
Connection Request User Name	It specifies the user name used to authenticate the ACS when it sends the connection request to the router.
Connection Request Password	It specifies the password used to authenticate the ACS when it sends the connection request to the router.
Port	It specifies the port used to receive the connection request sent by the ACS.
Enable STUN	It is used to enable or disable the STUN function, which facilitates the communication between the router and the public network when the router is under a LAN.
STUN Server Address	It specifies the IP address of the STUN server.
STUN Server Port	It specifies the port of the STUN server.

Chapter 11 System settings

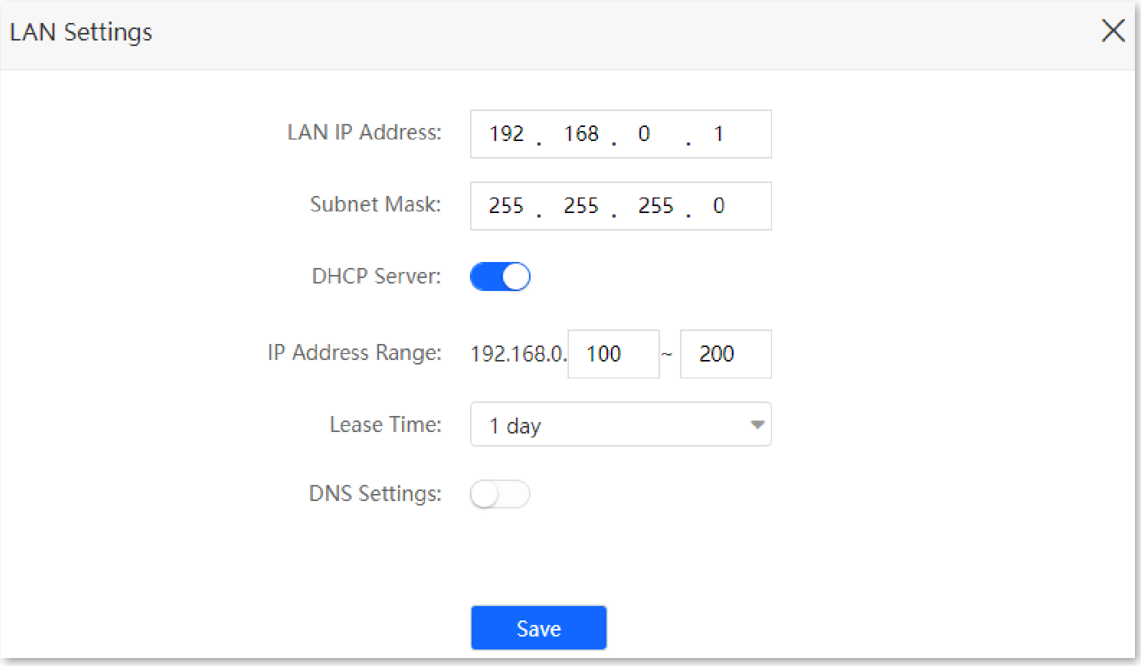
11.1 LAN settings

To access the configuration page, Log in to the web UI of the router, and choose **System Settings** > **LAN Settings**.

On this page, you can:

- Change the LAN IP address and subnet mask of the router.
- Change the DHCP server parameters of the router.

  The DHCP server can automatically assign IP address, subnet mask, gateway and other information to clients within the LAN. If you disable this function, you need to manually configure the IP address information on the client to access the internet. Do not disable the DHCP server function unless necessary.
- Configure the DNS information assigned to clients.


LAN Settings

LAN IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255 . 255 . 255 . 0

DHCP Server: ●

IP Address Range: 192.168.0. 100 ~ 200

Lease Time: 1 day

DNS Settings: ○

Table 11-1 Parameter description

Parameter	Description
LAN IP Address	It specifies the LAN IP address of the router, which is also the management IP address for logging in to the web UI of the router.
Subnet Mask	It specifies the subnet mask of the LAN port, used to identify the IP address range of the local area network.

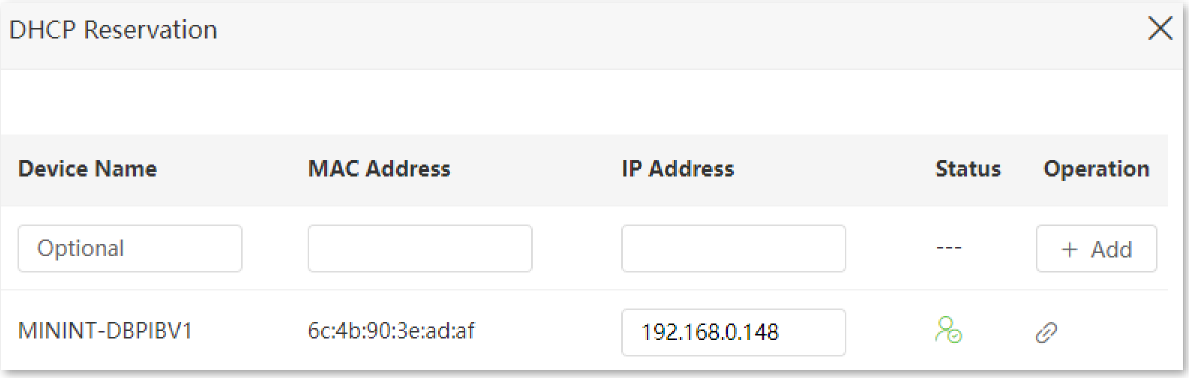
Parameter		Description
DHCP Server	IP Address Range	It specifies the range of IP addresses that can be assigned to devices connected to the router. The default range is 192.168.0.100 to 192.168.0.200.
	Lease Time	It specifies the valid duration of the IP address that is assigned to a client. When the lease time reaches half, the client will send a DHCP Request to the DHCP server for renewal. If the renewal succeeds, the lease is renewed based on the time of the renewal application; if the renewal fails, the renewal process is repeated at 7/8 of the lease period. If it succeeds, the lease is renewed based on the time of the renewal application. If it still fails, the client needs to reapply for IP address information after the lease expires. It is recommended to keep the default value.
DNS Settings	Primary DNS Server	It specifies the primary DNS address of the router, which is assigned to the clients. You can change it if necessary. **Note** Make sure that the primary DNS server is the IP address of the correct DNS server or DNS proxy. Otherwise, you may fail to access the internet.
	Secondary DNS Server	It specifies the secondary DNS address of the router used to assign to the clients. It is an optional field and is left blank.

11.2 DHCP reservation

11.2.1 Overview

Through the DHCP reservation function, specified clients can always obtain the same IP address when connecting to the router, ensuring that the router's "Virtual server", "DDNS", "DMZ host" and other functions can function normally. This function takes effect only when the DHCP server function of the router is enabled.

To access the configuration page, Log in to the web UI of the router, and choose **System Settings** > **DHCP Reservation**.



DHCP Reservation ×

Device Name	MAC Address	IP Address	Status	Operation
Optional			---	+ Add
MININT-DBPIBV1	6c:4b:90:3e:ad:af	192.168.0.148	👤	🔗

Table 11-2 Parameter description

Parameter	Description
Device Name	It specifies the device name of the client.
MAC Address	It specifies the MAC address of the client.
IP Address	It specifies the IP address reserved for the client.
Status	It specifies whether the client is online or not.
Operation	Available options include: + Add : It is used to add a new DHCP reservation rule. 🔗: It is used to bind the MAC address to the reserved IP address. ⛓: It is used to unbind the MAC address from the reserved IP address. 🗑: It is used to delete the DHCP reservation rule.

11.2.2 Assign static IP addresses to LAN clients

Scenario: You have set up an FTP server within your LAN.

Goal: Assign a fixed IP address to the host of the FTP server and prevent the failure of access to the FTP server owing to the change of IP address.

Solution: You can configure the DHCP reservation function to reach the goal.

Assume that the information of the FTP server includes:

- The fixed IP address for the server: 192.168.0.136
- MAC address of the FTP server host: D4:61:DA:1B:CD:89

Configuring procedure:

Step 1 Log in to the web UI of the router.

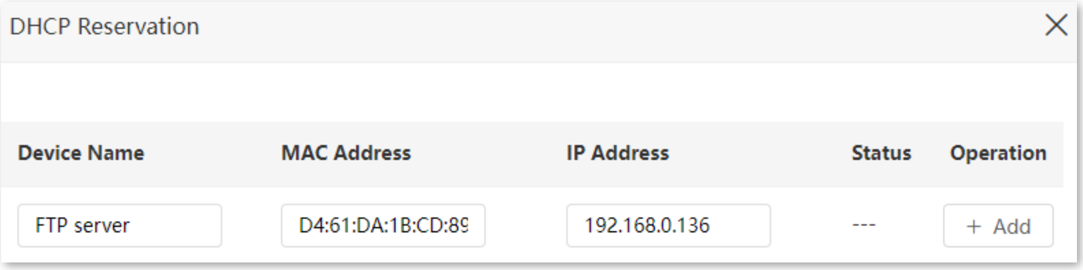
Step 2 Choose **System Settings** > **DHCP Reservation**.

Step 3 (Optional) Enter the device name for the host. which is **FTP server** in this example.

Step 4 Enter the MAC address of the host, which is **D4:61:DA:1B:CD:89** in this example.

Step 5 Enter the IP address reserved for the host, which is **192.168.0.136** in this example.

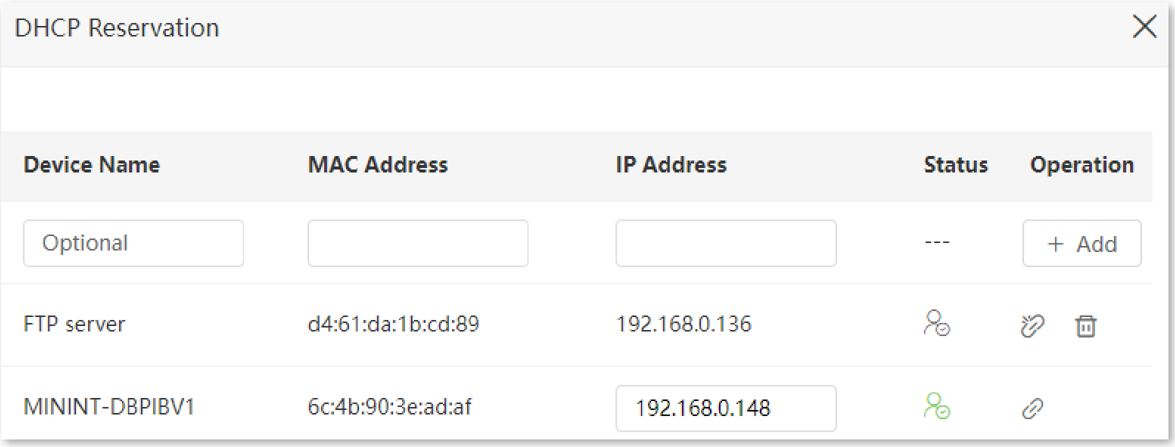
Step 6 Click **+Add**.



DHCP Reservation

Device Name	MAC Address	IP Address	Status	Operation
FTP server	D4:61:DA:1B:CD:89	192.168.0.136	---	+ Add

When the configuration is completed, the page is shown as below and the FTP server host always gets the same IP address when connecting to the router, which is 192.168.0.136 in this example.



DHCP Reservation

Device Name	MAC Address	IP Address	Status	Operation
Optional			---	+ Add
FTP server	d4:61:da:1b:cd:89	192.168.0.136		
MININT-DBPIBV1	6c:4b:90:3e:ad:af	192.168.0.148		

11.3 WAN settings (wireless router mode)

Note

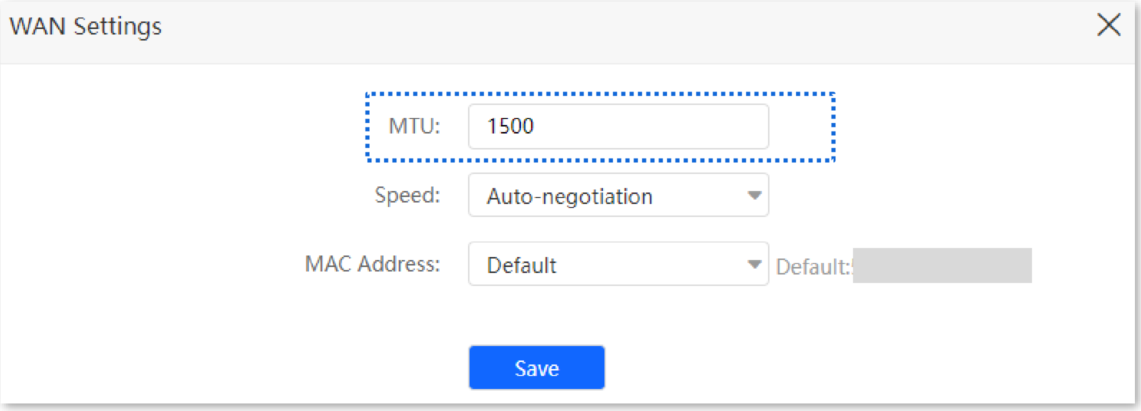
This function is only available under the wireless router mode. Refer to Operating mode to set the operating mode of the router.

In the **WAN Parameters** module, you can check and modify MTU value, WAN speed, duplex mode, MAC address.

11.3.1 Change MTU value

Maximum Transmission Unit (MTU) is the largest data packet transmitted by a network device. When the connection type is PPPoE, the default MTU value is 1480. When the connection type is dynamic IP address or static IP address, the default MTU value is 1500. Do not change the value unless necessary. If you need to, please refer to the following instructions.

To access the configuration page, Log in to the web UI of the router, and choose **System Settings** > **WAN Settings**.



WAN Settings

MTU: 1500

Speed: Auto-negotiation

MAC Address: Default Default:[redacted]

Generally, the default value is recommended. Try to change the MTU value when:

- You cannot access some specific websites or encrypted websites (such as E-banking or Paypal websites).
- You cannot receive or send Emails or access an FTP or POP server.

You can try reducing the value of MTU gradually from 1500 until the problem is resolved (The recommended range is 1400 to 1500).

Table 11-3 MTU application description

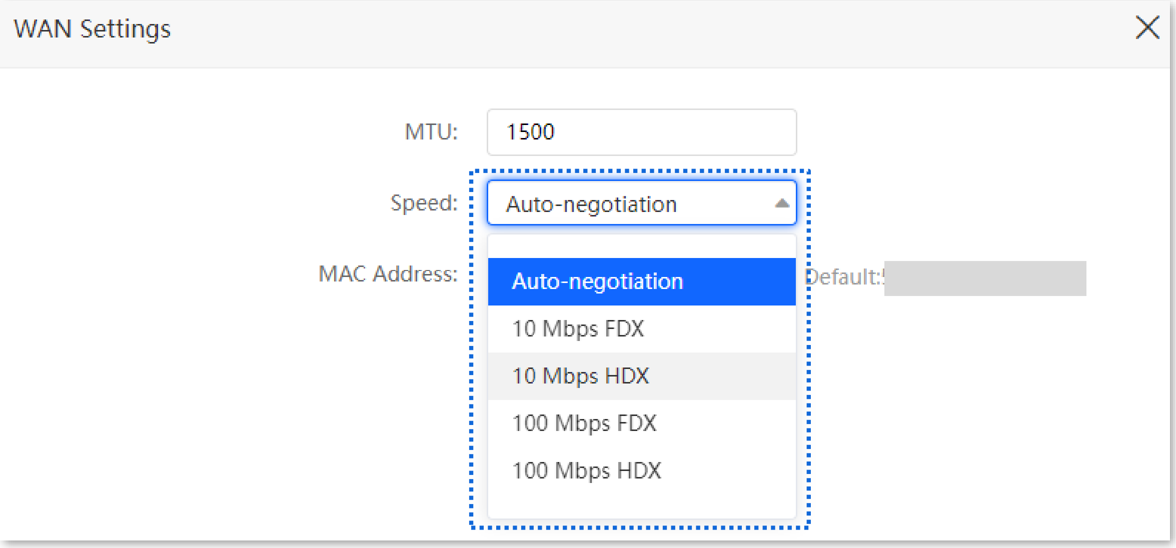
MTU	Application
1500	It is commonly used for non-ADSL and non-VPN dial-up connections.
1492, 1480	It is used for ADSL dial-up connections.
1472	It is the maximum value for the ping command. A packet with a larger size is fragmented.
1468	It is used for DHCP connections.

1436	It is used for VPN or PPTP connections.

11.3.2 Change the WAN speed and duplex mode

To access the configuration page, Log in to the web UI of the router, and choose **System Settings** > **WAN Settings**.

When the Ethernet cable is intact and connected to the WAN port properly, but **Ethernet cable disconnected** is still shown on the **Internet Settings** page, you can try to change the **Speed** to **10 Mbps FDX** or **10 Mbps HDX** to solve the problem. Otherwise, keep the default settings.



WAN Settings

MTU: 1500

Speed: Auto-negotiation

MAC Address: Default:[redacted]

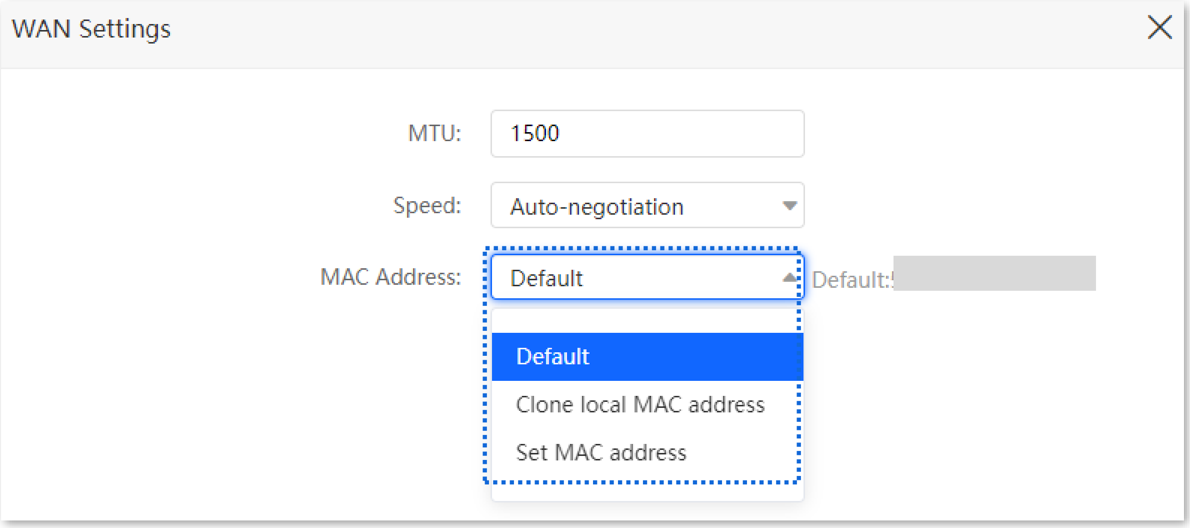
Table 11-4 Speed application description

Speed	Application
10 Mbps FDX	10 Mbps Full Duplex. It indicates that the WAN port is working at the speed of 10 Mbps, and the port can receive and send data packets at the same time.
10 Mbps HDX	10 Mbps Half Duplex. It indicates that the WAN port is working at the speed of 10 Mbps, but the port can only receive or send data packets alternately.
100 Mbps FDX	100 Mbps Full Duplex. It indicates that the WAN port is working at the speed of 100 Mbps, and the port can receive and send data packets at the same time.
100 Mbps HDX	100 Mbps Half Duplex. It indicates that the WAN port is working at the speed of 100 Mbps, but the port can only receive or send data packets alternately.

11.3.3 Change the MAC address of the WAN port

If you still cannot access the internet after completing Access the internet throuth the WAN port, it could be the result of the ISP's configuration to bind the internet account information with a fixed MAC address. In this case, you can clone and change the MAC address of the router to solve the problem.

To access the configuration page, Log in to the web UI of the router, and choose **System Settings** > **WAN Settings.**



WAN Settings

MTU: 1500

Speed: Auto-negotiation

MAC Address: Default

Default: [redacted]

- **Default**: Keep the factory setting of MAC address.
- **Clone local MAC address**: Set the MAC address of the router to the same as that of the device which is configuring the router.
- **Set MAC address**: Manually set a MAC address.

Note

Please ensure the cloned MAC address is that of the computer or the router which is already able to access the internet.

Configuration procedure:

Step 1 Log in to the web UI of the router.

Step 2 Choose **System Settings** > **WAN Settings**.

Step 3 Click the drop-down box of **MAC Address**, choose **Clone local MAC address**, or **Set MAC address** and enter the desired MAC address.

Step 4 Click **Save**.

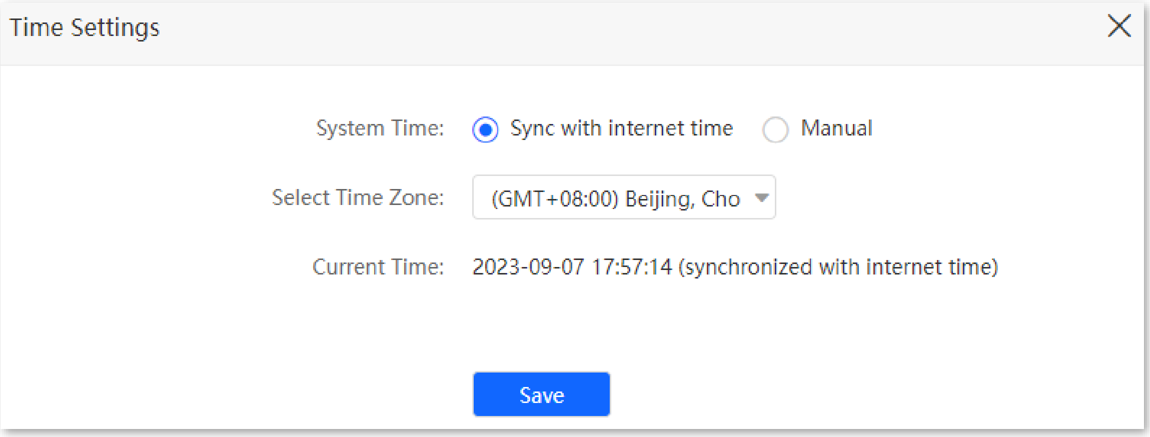
11.4 Time settings

To access the configuration page, Log in to the web UI of the router, and choose **System Settings** > **Time Settings.**

You can change the time settings on this page. The functioning of functions based on time requires an accurate system time. The system time of the router can be synchronized with the internet or set manually. By default, it is synchronized with the internet.

11.4.1 Sync system time with the internet time

Under this mode, the router will automatically sync its time with the internet time when it is connected to the internet. You can also choose the time zone to be synchronized.



Time Settings

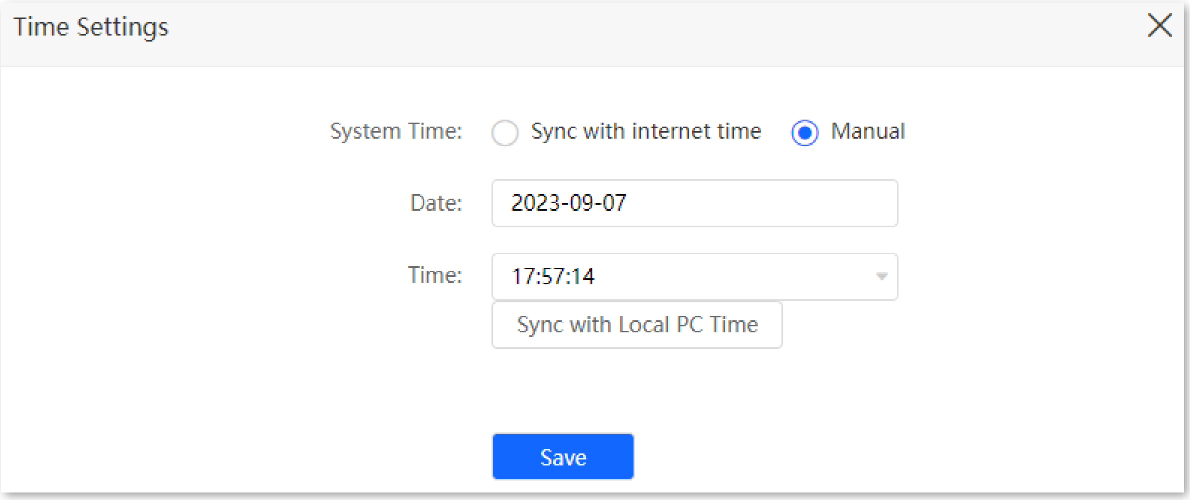
System Time: ● Sync with internet time ○ Manual

Select Time Zone: (GMT+08:00) Beijing, Cho

Current Time: 2023-09-07 17:57:14 (synchronized with internet time)

11.4.2 Set system time manually

When the system time is set to **Manual**, you can enter a desired time or sync the system time of the router with the device that is configuring the router. Besides, you need to correct it every time after you reboot the router to ensure the accuracy of system time.



Time Settings

System Time: ○ Sync with internet time ● Manual

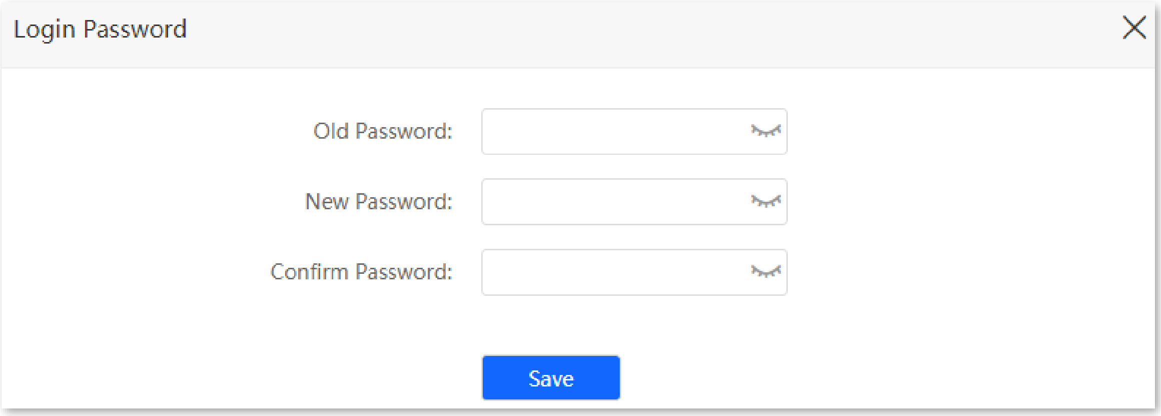
Date: 2023-09-07

Time: 17:57:14

11.5 Login password

To ensure network security, a login password is recommended. A login password consisting of more types of characters, such as uppercase letters and lowercase letters, brings higher security.

To access the configuration page, log in to the web UI and choose **System Settings** > **Login Password**. You can change the password on this page and the old password is required.



Login Password

Old Password:

New Password:

Confirm Password:

Note

If you forget your login password and cannot Log in to the web UI of the router, refer to reset the router to restore the router to factory settings and perform settings again.

11.6 Reboot and reset

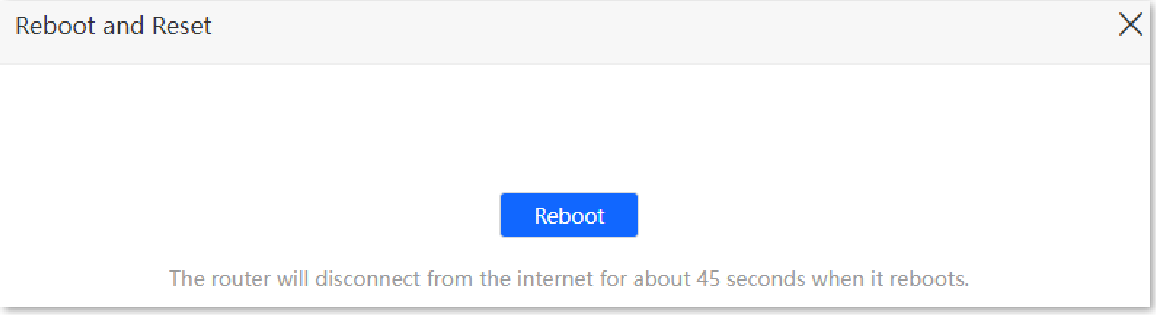
11.6.1 Reboot the router

If any parameter fails to take effect or the router does not work properly, you can try rebooting the router.

Note

Rebooting the router will disconnect all connections to the router. Reboot the router in spare times.

To reboot the router, Log in to the web UI of the router and choose **System Settings** > **Reboot and Reset**. Click **Reboot** to reboot the router.



The router will disconnect from the internet for about 45 seconds when it reboots.

Wait for a moment until the ongoing process finishes.

11.6.2 Reset the router

If you are uncertain about why the internet is inaccessible through the router or you forget the login password of the router, you can reset the router.

⚠ **Caution**

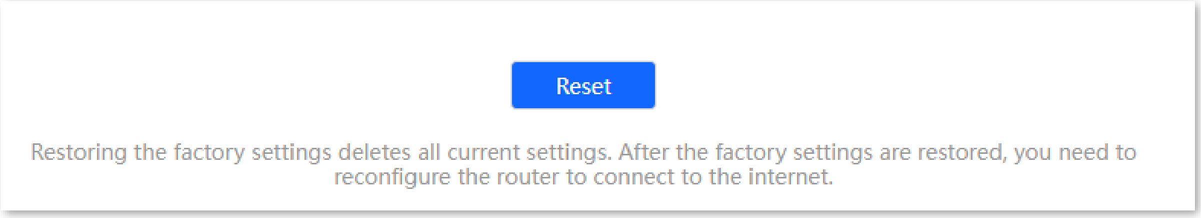
- Resetting the router is not recommended unless you cannot find a solution for the current problem anyway. You need to reconfigure the router after it is reset.
- Ensure that the power supply of the router is normal when the router is reset. Otherwise, the router could be damaged.
- The default login IP address is 192.168.0.1 after resetting.

Reset the router using the reset button

Hold down the **RST/WPS** button on the rear panel of the router for about 8 seconds and release it when all LED indicators blink once. The router is reset and restored to factory settings.

Reset the router on the web UI

Start a web browser and Log in to the web UI of the router. Choose **System Settings** > **Reboot and Reset**, and click **Reset**.



Restoring the factory settings deletes all current settings. After the factory settings are restored, you need to reconfigure the router to connect to the internet.

Wait for a moment until the ongoing process finishes.

11.7 Firmware upgrade

This function enables the router to obtain the latest functions and more stable performance.

When the router is connected to the internet, it auto-detects whether there is a new firmware and displays the detected information on the page. You can choose whether to upgrade to the latest firmware.

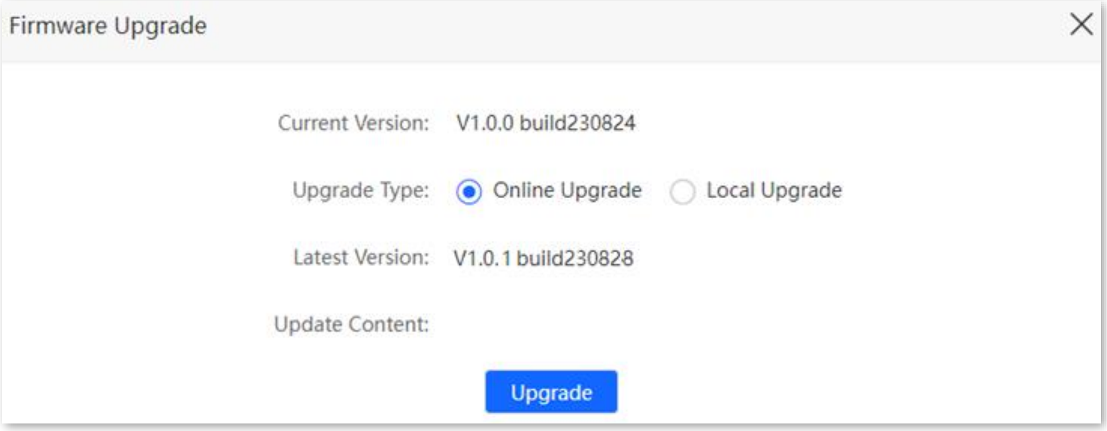
Configuration procedure:

Step 1 Log in to the web UI of the router.

Step 2 Choose **System Settings** > **Firmware Upgrade**.

Step 3 Wait until a new firmware version is detected.

Step 4 Click **Update**.



Firmware Upgrade

Current Version: V1.0.0 build230824

Upgrade Type: ● Online Upgrade ○ Local Upgrade

Latest Version: V1.0.1 build230828

Update Content:

Wait for a moment until the ongoing process finishes. Log in to the web UI of the router again. Choose **System Settings** > **System Status** and check whether the upgrade is successful based on the **Firmware Version**.

Note

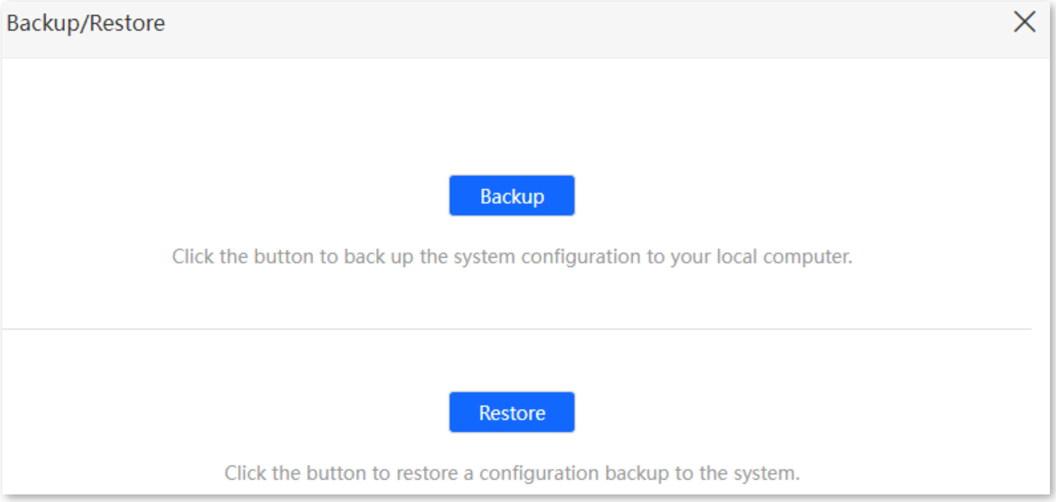
For better performance of the new firmware of the router, you are recommended to reset the router to factory default settings and re-configure the router when the upgrading is completed.

11.8 Backup/Restore

In this module, you can back up the current configurations of the router to your computer. You are recommended to back up the configuration after the settings of the router are significantly changed, or the router works in a good condition.

After you restore the router to factory settings or upgrade it, you can use this function to restore the configurations that have been backed up.

To access the configuration page, Log in to the web UI of the router, and choose **System Settings** > **Backup/Restore.**



Backup/Restore

Click the button to back up the system configuration to your local computer.

Click the button to restore a configuration backup to the system.

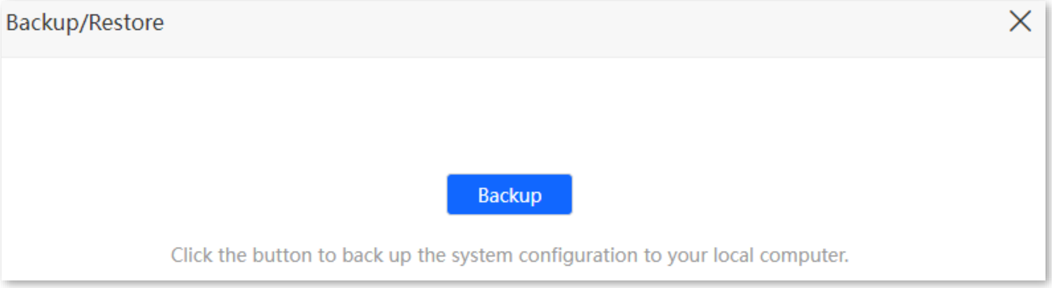
11.8.1 Back up the configurations of the router

To back up the configurations of the router:

Step 1 Log in to the web UI of the router.

Step 2 Choose **System Settings** > **Backup/Restore**.

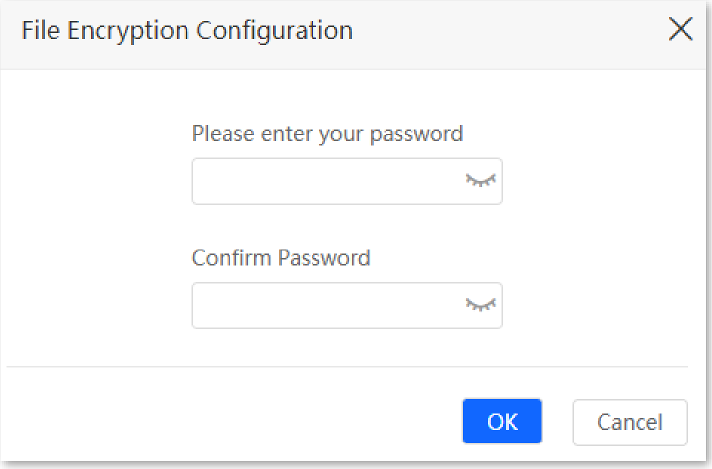
Step 3 Click **Backup**.



Backup/Restore

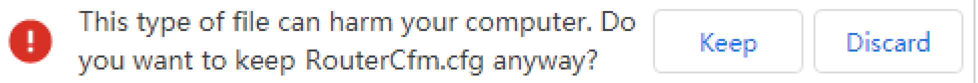
Click the button to back up the system configuration to your local computer.

Step 4 Enter the login password, and click **OK** in the pop-up window.



Note

- Some browsers may not give such tips.
- Your browser may notice you the safety of the file as follows. Please click **Keep** to save the file.


This type of file can harm your computer. Do you want to keep RouterCfm.cfg anyway?

A file named **RouterCfm.cfg** will be downloaded to your local host.

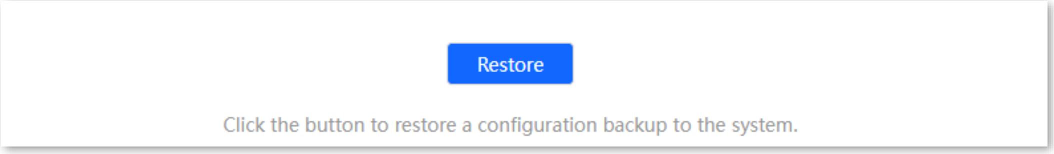
11.8.2 Restore previous configurations of the router

To restore the previous configurations of the router:

Step 1 Log in to the web UI of the router.

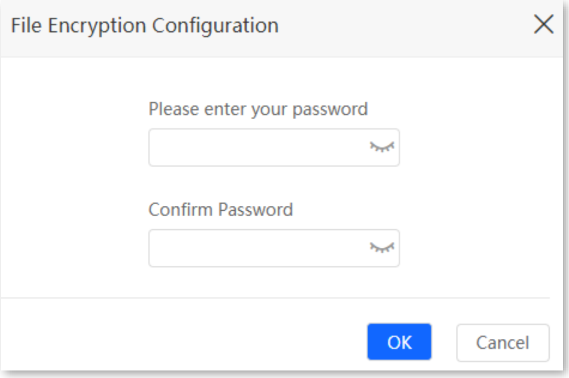
Step 2 Choose **System Settings** > **Backup/Restore**.

Step 3 Click **Restore**.

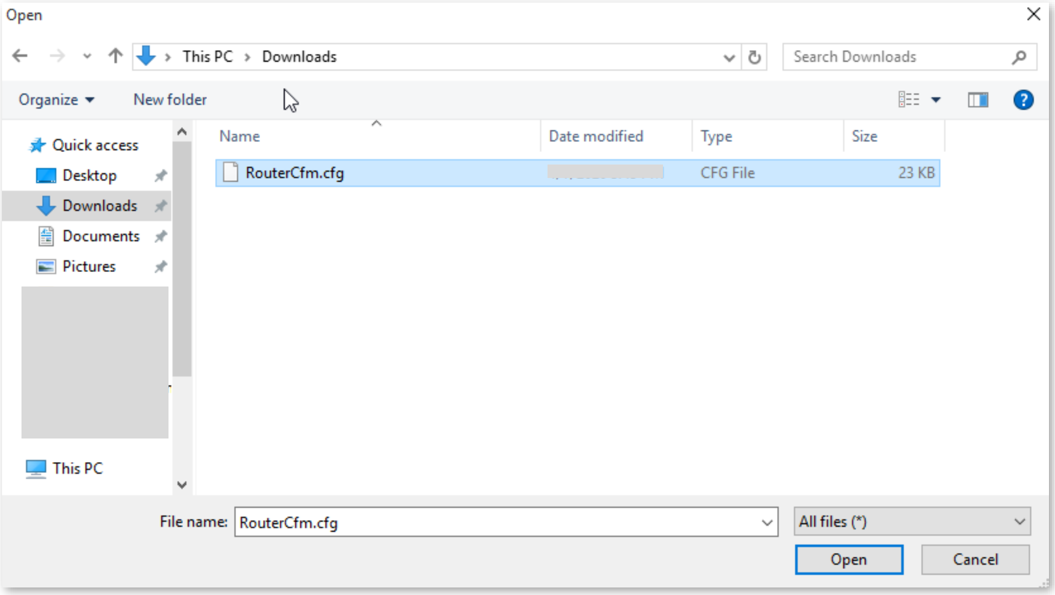


Click the button to restore a configuration backup to the system.

Step 4 Enter the login password, and click **OK** in the pop-up window.



Step 5 Choose the configuration file (extension: cfg) to be restored, and click **Open**.



Name	Date modified	Type	Size
RouterCfm.cfg	[redacted]	CFG File	23 KB

File name: RouterCfm.cfg

Wait for a moment until the ongoing process finishes, and previous settings are restored to the router.

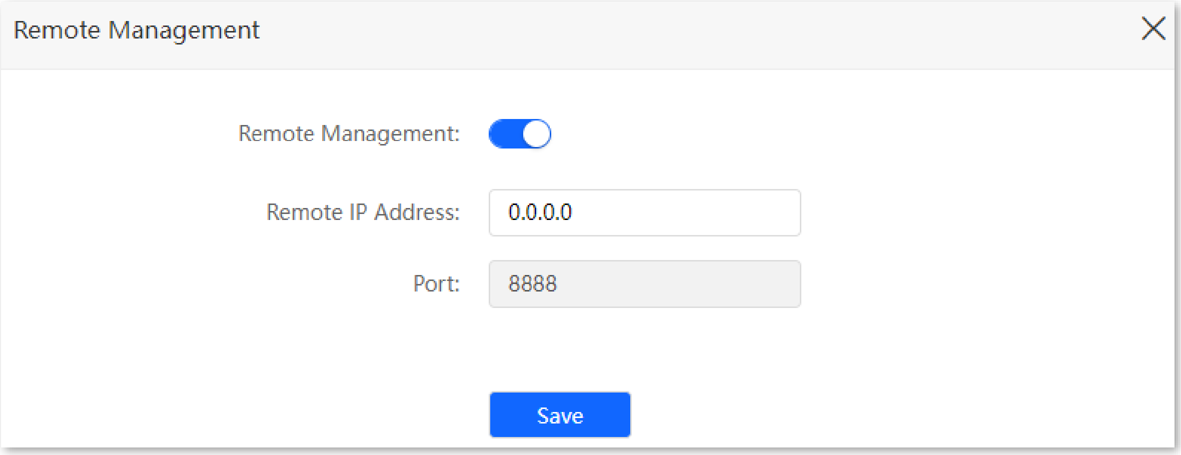
11.9 Remote management

11.9.1 Overview

Generally, the web UI of the router can only be accessed on devices that are connected to the router by a LAN port or wireless connection. When you encounter a network fault, you can ask for remote technical assistance, which improves efficiency and reduces costs and efforts.

To access the configuration page, Log in to the web UI of the router, and choose **System Settings** > **Remote Management.**

By default, this function is disabled. When this function is enabled, the page is shown as below.



Remote Management

Remote Management: ●

Remote IP Address: 0.0.0.0

Port: 8888

Table 11-5 Parameter description

Parameter	**Description**
Remote Management	It is used to enable or disable the remote management function of the router.
Remote IP Address	It specifies the IP address of the host which can access the web UI of the router remotely. ● 0.0.0.0: It indicates that hosts with any IP address from the internet can access the web UI of the router. It is not recommended for security. ● Other specified IP address: Only the host with the specified IP address can access the web UI of the router remotely. If the host is under a LAN, ensure that the IP address is the IP address of the gateway of the host (a public IP address).

Parameter	Description
Port	It specifies the port number of the router which is opened for remote management. Change it as required. **Note** ● The port number from 1 to 1024 has been occupied by familiar services. It is strongly recommended to enter a port number from 1025 to 65535 to prevent conflict. ● Remote management can be achieved by visiting "https://the WAN IP address of the router:port number". If the DDNS host function is enabled, the web UI can also be accessed through "https://the domain name of the router's WAN port:port number".

11.9.2 Enable Hikvision techical support to acces and manage the web UI

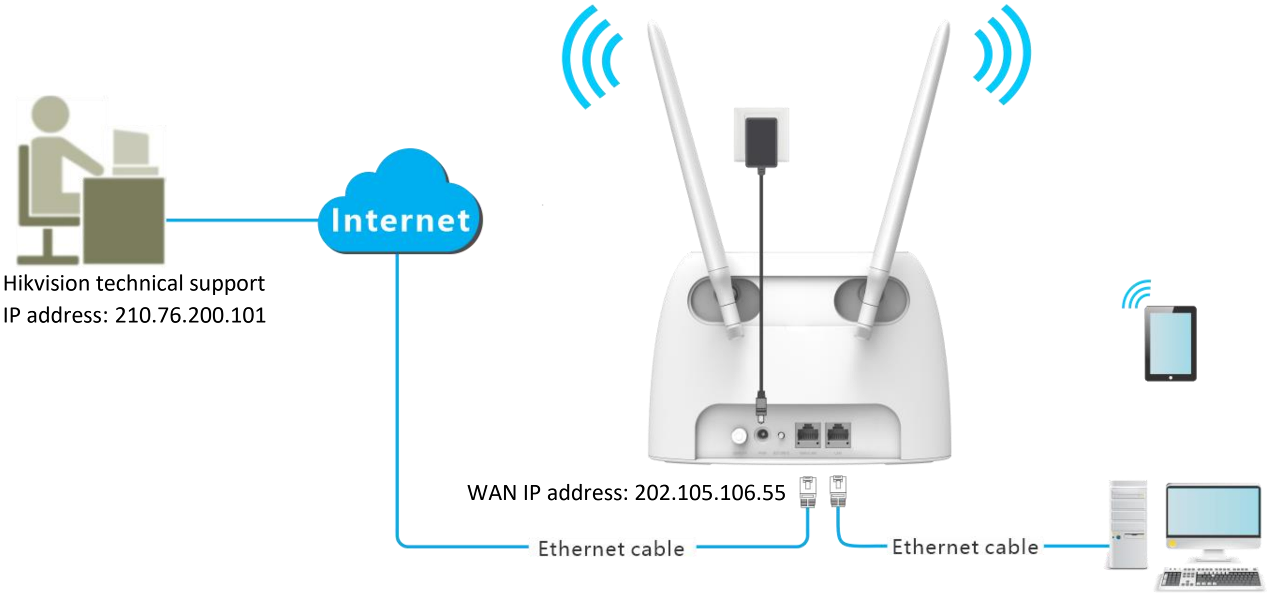
Scenario: You encounter a problem in configuring the router, and the router can access internet access.

Goal: Ask the Hikvision technical support to help you configure the router remotely.

Solution: You can configure the remote management function to reach the goal.

Assume that:

- The IP address of Hikvision technical support: 210.76.200.101
- The WAN port IP address of the router: 202.105.106.55


Internet
Hikvision technical support
IP address: 210.76.200.101
WAN IP address: 202.105.106.55
Ethernet cable
Ethernet cable

Configuring procedure:

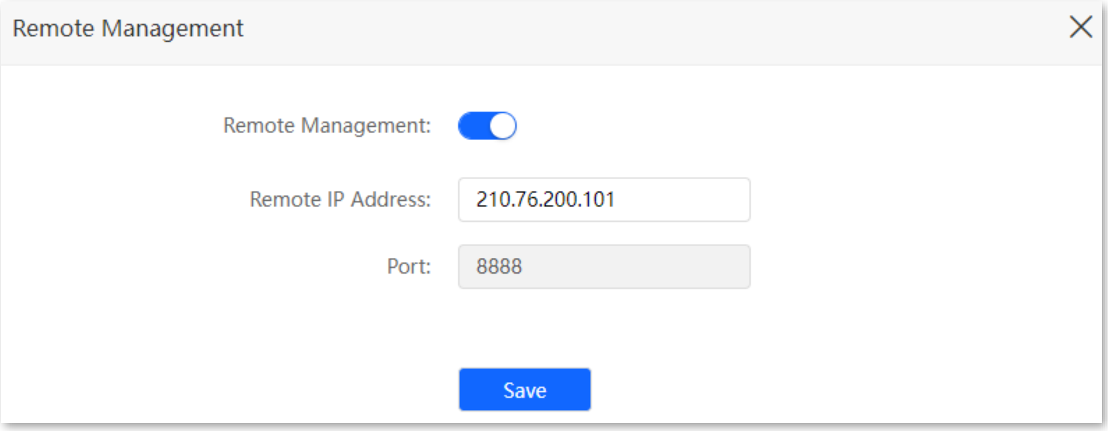
Step 1 Log in to the web UI of the router.

Step 2 Choose **System Settings** > **Remote Management**.

Step 3 Enable the **Remote Management**.

Step 4 Enter the IP address that can access the web UI remotely, which is **210.76.200.101** in this example.

Step 5 Click **Save**.



Remote Management

Remote Management: ●

Remote IP Address: 210.76.200.101

Port: 8888

When the configurations are completed, the Hikvision technical support can access and manage the web UI of the router by visiting “https://202.105.106.55:8888” on the computer.

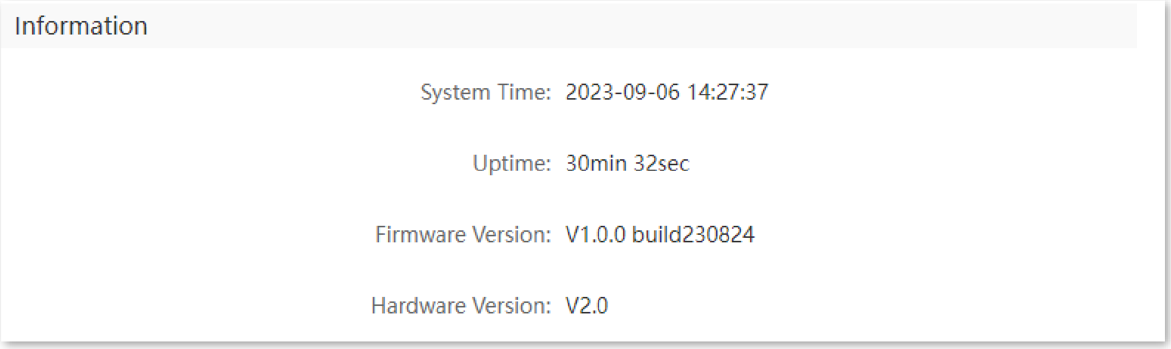
11.10 System status

On this page, you can find the basic information of the router, WAN status, LAN status, Wi-Fi status and IPv6 status.

To access the page, Log in to the web UI of the router, and choose **System Settings** > **System Status.**

11.10.1 Basic information

In this part, you can view the basic information of the router, such as system time, uptime and firmware version and hardware version.



Information

System Time: 2023-09-06 14:27:37

Uptime: 30min 32sec

Firmware Version: V1.0.0 build230824

Hardware Version: V2.0

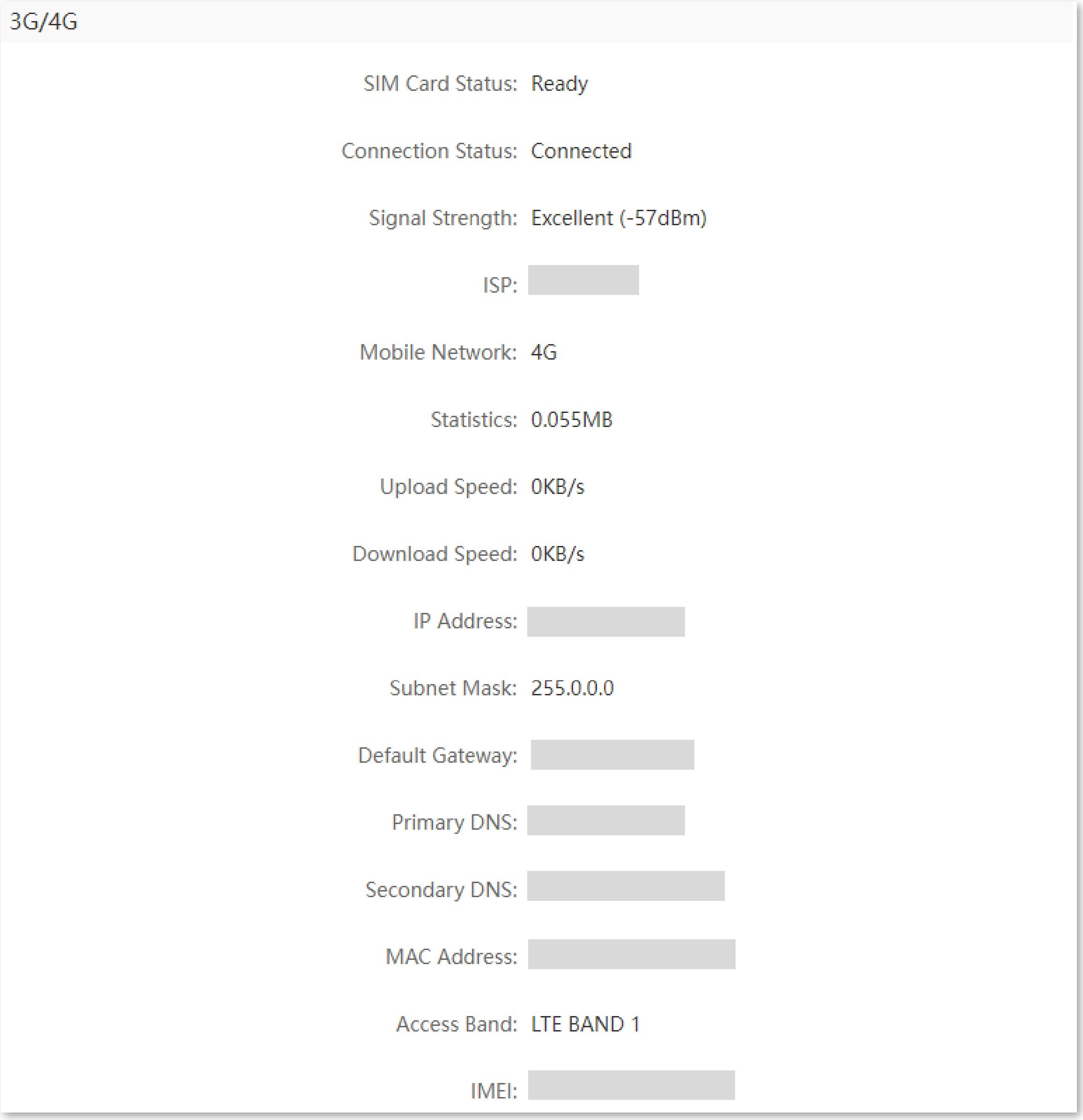
Table 11-6 Parameter description

Parameter	**Description**
System Time	It specifies the system time of the router.
Uptime	It specifies operating time of the router since it is powered on.
Firmware Version	It specifies the firmware version of the router.
Hardware Version	It specifies the hardware version of the router.

11.10.2 Connection status

3G/4G

Under the 3G/4G router mode, you can view the information of the SIM card and 3G/4G network in this part.



3G/4G

SIM Card Status: Ready

Connection Status: Connected

Signal Strength: Excellent (-57dBm)

ISP: [redacted]

Mobile Network: 4G

Statistics: 0.055MB

Upload Speed: 0KB/s

Download Speed: 0KB/s

IP Address: [redacted]

Subnet Mask: 255.0.0.0

Default Gateway: [redacted]

Primary DNS: [redacted]

Secondary DNS: [redacted]

MAC Address: [redacted]

Access Band: LTE BAND 1

IMEI: [redacted]

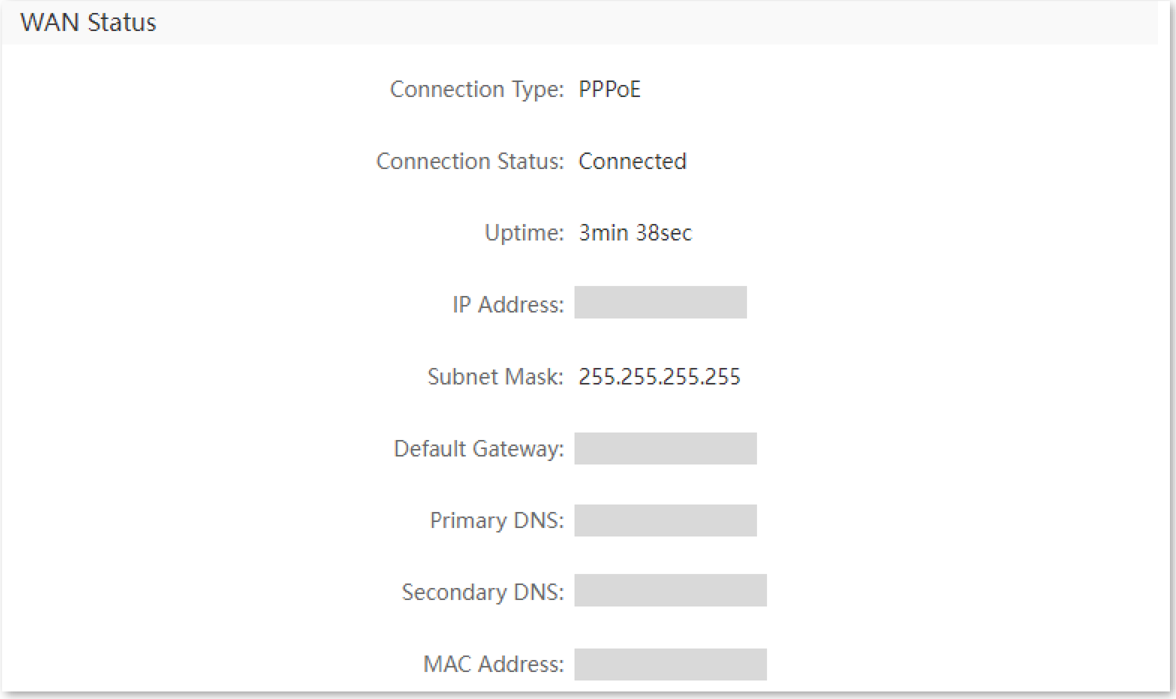
Table 11-7 Parameter description

Parameter	Description
SIM Card Status	It specifies the SIM card status inserted in the router.
Connection Status	It specifies internet connection status of 3G/4G mobile network.
Signal Strength	It specifies the signal strength of 3G/4G mobile network, including Excellent, Good and Fair.

Parameter	Description
ISP	It specifies the ISP (Internet Service Provider) name of the SIM card.
Mobile Network	It specifies the current network type for internet access.
Statistics	It specifies the data traffic of the SIM card that has been used.
Upload Speed	It specifies the upload speed of the mobile network of the router.
Download Speed	It specifies the download speed of the mobile network of the router.
IP address	It specifies the IP address of the router obtained from the ISP.
Subnet Mask	It specifies the subnet mask of mobile network.
Default Gateway	It specifies the gateway IP address of the router.
Primary DNS	It specifies the IP address of primary and secondary DNS servers of the router.
Secondary DNS	
MAC Address	It specifies the 3G/4G MAC address of the router.
Access Band	It specifies the 3G/4G band that the router is working in.
IMEI	It specifies International Mobile Equipment Identity (IMEI) of the router.

Wireless router mode

Under the wireless router mode, you can view the information of the WAN port, including connection type, connection status and connection duration.



WAN Status

Connection Type: PPPoE

Connection Status: Connected

Uptime: 3min 38sec

IP Address:

Subnet Mask: 255.255.255.255

Default Gateway:

Primary DNS:

Secondary DNS:

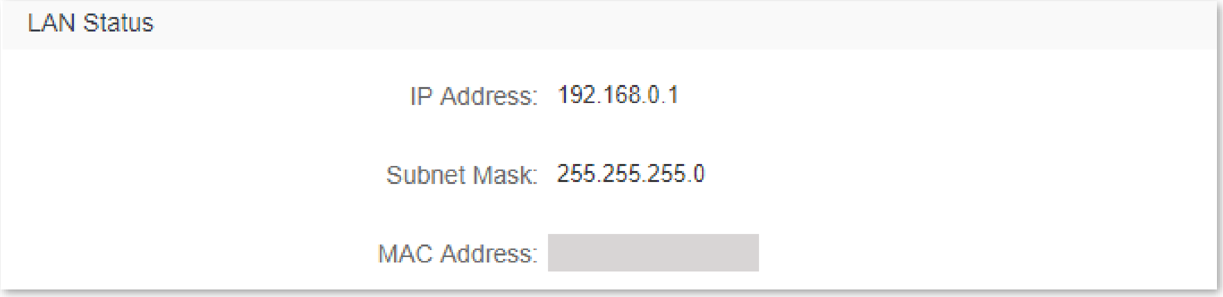
MAC Address:

Table 11-8 Parameter description

Parameter	Description
Connection Type	It specifies the IPv4 connection type of the WAN port.
Connection Status	It specifies internet connection status of the WAN port.
Uptime	It specifies the duration since the router is connected to the internet.
IP address	It specifies the WAN IP address of the router.
Subnet Mask	It specifies the WAN subnet mask of the router.
Default Gateway	It specifies the gateway IP address of the router.
Primary DNS	They specify the IP address of primary and secondary DNS servers of the router.
Secondary DNS	
MAC Address	It specifies the WAN MAC address of the router.

11.10.3 LAN status

In this part, you can view the information, such as LAN IPv4 address, subnet mask and MAC address.



LAN Status

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

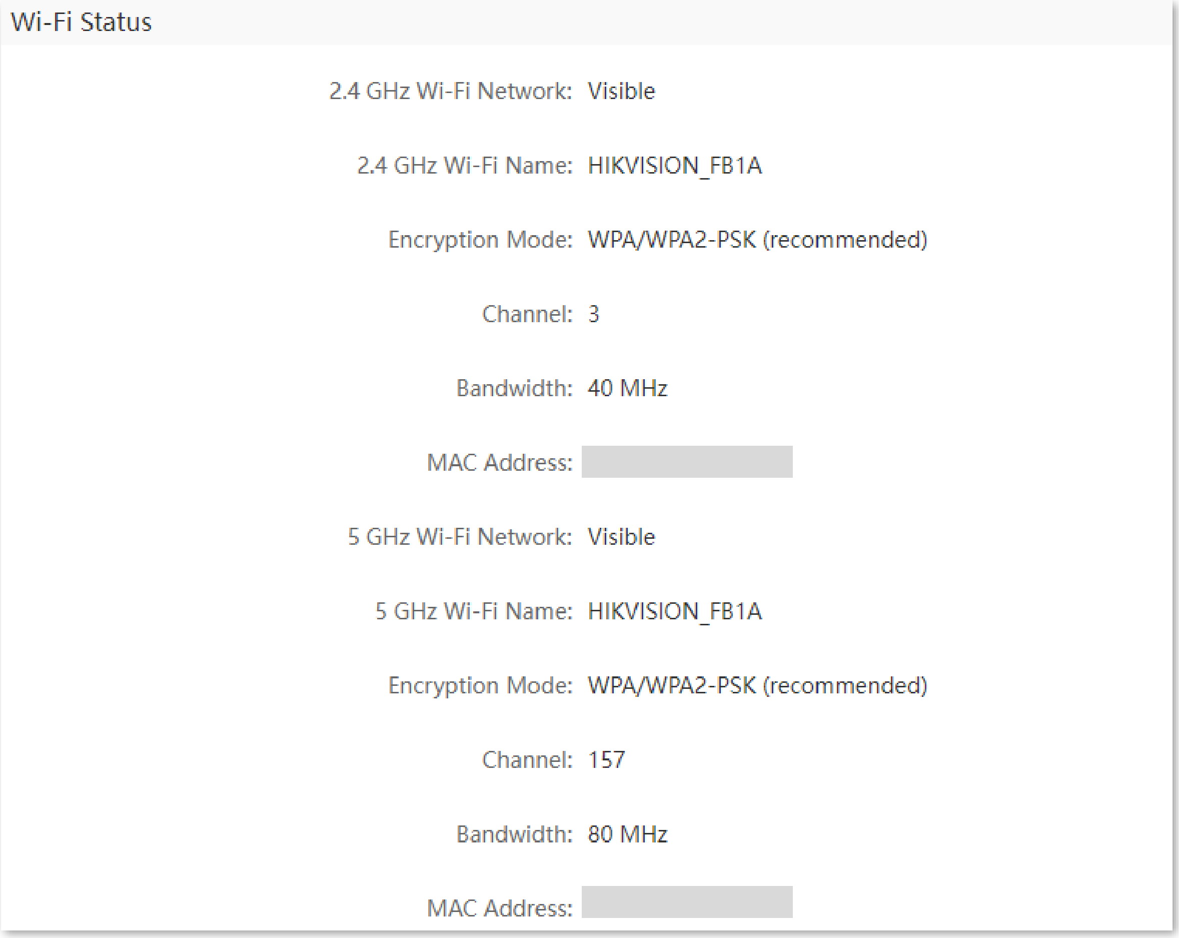
MAC Address: [redacted]

Table 11-9 Parameter description

Parameter	Description
IP Address	It specifies the LAN IP address of the router, and the IP address for logging in to the web UI of the router.
Subnet Mask	It specifies the LAN subnet mask of the router.
MAC Address	It specifies the LAN MAC address of the router.

11.10.4 Wi-Fi status

In this part, you can view the information of 2.4 GHz and 5 GHz Wi-Fi network, including the connection status, visibility, hotspot name and encryption mode.



Wi-Fi Status

2.4 GHz Wi-Fi Network: Visible

2.4 GHz Wi-Fi Name: HIKVISION_FB1A

Encryption Mode: WPA/WPA2-PSK (recommended)

Channel: 3

Bandwidth: 40 MHz

MAC Address: [redacted]

5 GHz Wi-Fi Network: Visible

5 GHz Wi-Fi Name: HIKVISION_FB1A

Encryption Mode: WPA/WPA2-PSK (recommended)

Channel: 157

Bandwidth: 80 MHz

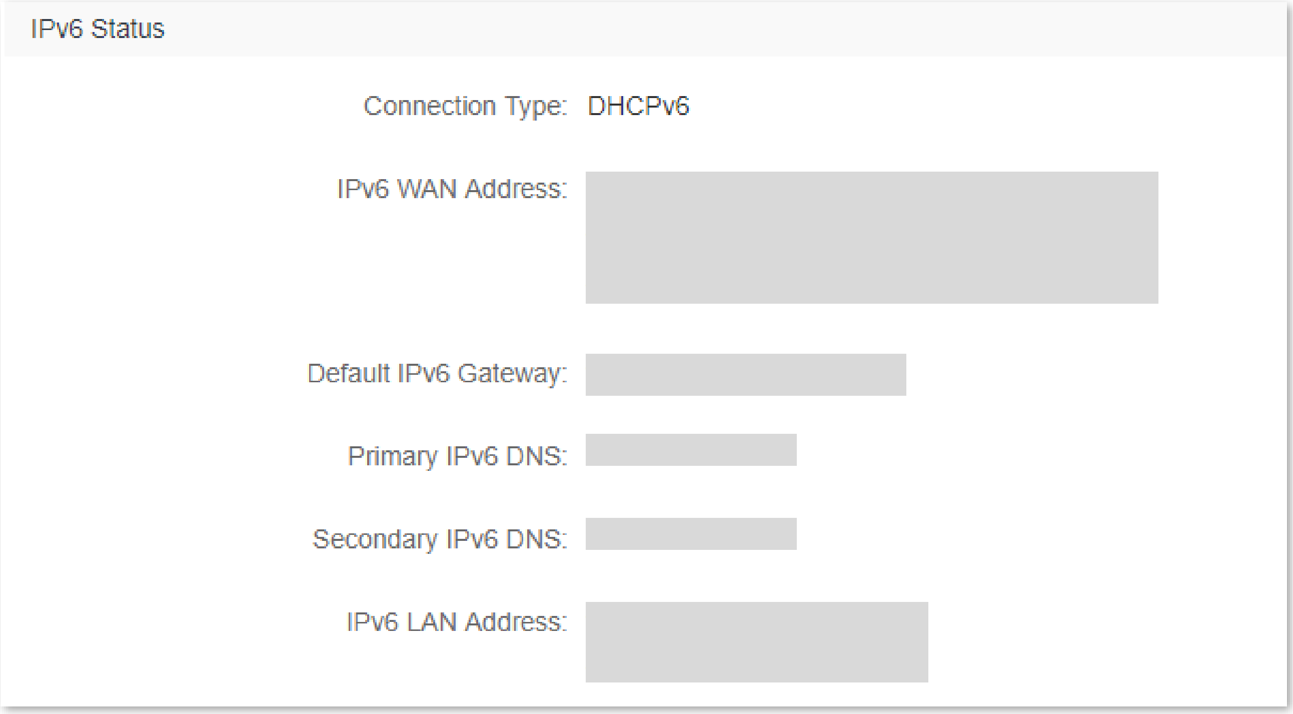
MAC Address: [redacted]

Table 11-10 Parameter description

Parameter	Description
2.4 GHz Wi-Fi Network	They specify whether the corresponding Wi-Fi network is enabled or disabled, and the visibility of the Wi-Fi network.
5 GHz Wi-Fi Network	
2.4 GHz Wi-Fi Name	They specify the 2.4 GHz Wi-Fi and 5 GHz Wi-Fi name of the router.
5 GHz Wi-Fi Name	
Encryption Mode	It specifies the encryption mode of the respective Wi-Fi network.
Channel	It specifies the channel that the respective Wi-Fi network works in.
Bandwidth	It specifies the bandwidth of the respective Wi-Fi network.
MAC Address	It specifies the MAC address of the respective Wi-Fi network.

11.10.5 IPv6 status

This part is only displayed when the IPv6 function is enabled. You can view the information of IPv6 connection, including connection type, IPv6 WAN address and IPv6 LAN address.



IPv6 Status

Connection Type: DHCPv6

IPv6 WAN Address:

Default IPv6 Gateway:

Primary IPv6 DNS:

Secondary IPv6 DNS:

IPv6 LAN Address:

Table 11-11 Parameter description

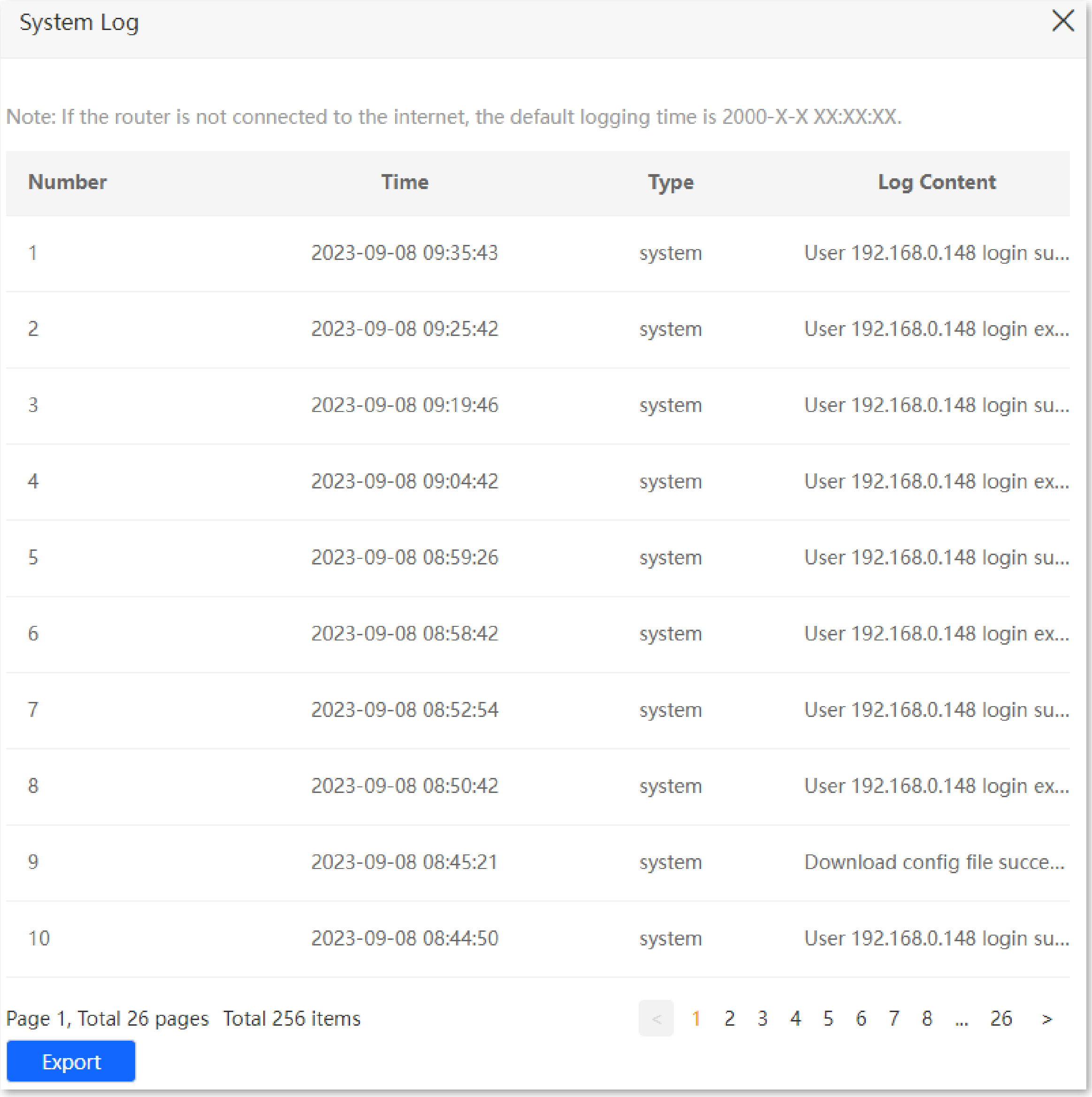
Parameter	Description
Connection Type	It specifies the IPv6 connection type of the router.
IPv6 WAN Address	It specifies the WAN IPv6 address of the router. After the IPv6 function is configured, the WAN port of the router obtains a global unicast IPv6 address or a tunnel address.
Default IPv6 Gateway	It specifies the primary DNS server address of IPv6 network.
Primary IPv6 DNS	They specify the primary and secondary DNS server address of IPv6 network.
Secondary IPv6 DNS	
IPv6 LAN Address	It specifies the LAN IPv6 address of the router. After the IPv6 function is configured, the LAN port of the router obtains a global unicast IPv6 address or a tunnel address, and a link local address.

11.11 System log

To access the configuration page, Log in to the web UI of the router, and choose **System Settings** > **System Log.**

This function logs all key events that occur after the router is started. If you encounter a network fault, you can turn to system logs for fault rectification.

If necessary, you can also export the system logs to your local computer by clicking **Export**.



System Log

Note: If the router is not connected to the internet, the default logging time is 2000-X-X XX:XX:XX.

Number	Time	Type	Log Content
1	2023-09-08 09:35:43	system	User 192.168.0.148 login su...
2	2023-09-08 09:25:42	system	User 192.168.0.148 login ex...
3	2023-09-08 09:19:46	system	User 192.168.0.148 login su...
4	2023-09-08 09:04:42	system	User 192.168.0.148 login ex...
5	2023-09-08 08:59:26	system	User 192.168.0.148 login su...
6	2023-09-08 08:58:42	system	User 192.168.0.148 login ex...
7	2023-09-08 08:52:54	system	User 192.168.0.148 login su...
8	2023-09-08 08:50:42	system	User 192.168.0.148 login ex...
9	2023-09-08 08:45:21	system	Download config file succe...
10	2023-09-08 08:44:50	system	User 192.168.0.148 login su...

Page 1, Total 26 pages Total 256 items

Note

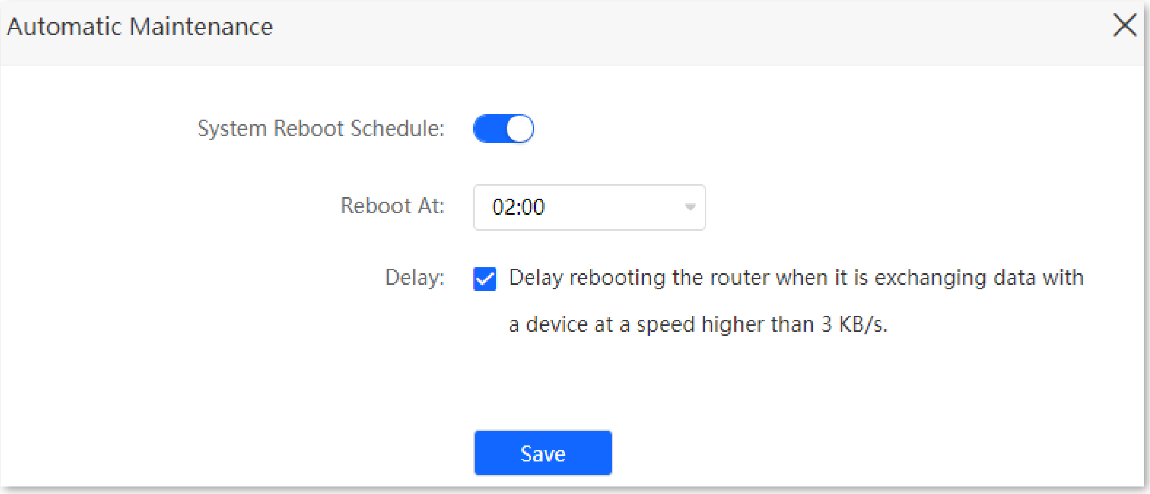
Rebooting the router will clear all previous system logs.

11.12 Automatic maintenance

Automatic maintenance enables you to make the router restart regularly. It helps improve the stability and service life of the router.

To access the configuration page, Log in to the web UI of the router, and choose **System Settings** > **Automatic Maintenance.**

This function is enabled by default.



Automatic Maintenance

System Reboot Schedule: ●

Reboot At: 02:00

Delay: ☑ Delay rebooting the router when it is exchanging data with a device at a speed higher than 3 KB/s.

Table 11-12 Parameter description

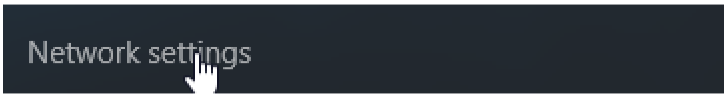
Parameter	Description
System Reboot Schedule	It is used to enable or disable the automatic reboot function.
Reboot At	It specifies the time when the router reboots automatically every day.
Delay	It is used to enable or disable the delay function. ● **Ticked**: The function is enabled. When the time for rebooting approaches, if there is any user connected to the router and the traffic over the router's WAN port exceeds 3 KB/s within 30 minutes, the router will delay rebooting. If there is any user connected to the router and the traffic over the WAN port does not exceed 3 KB/s within 30 minutes, or there is no user connected to the router and the traffic over the router's WAN port is slower than 3 KB/s within 3 minutes, the router will reboot automatically. ● **Unticked**: The function is disabled. The router reboots immediately when the specified time for rebooting approaches. **Note** When the system reboot schedule function is enabled, the router detects the traffic over the WAN port continuously within 2 hours after the specified reboot time and reboot when the traffic requirement for rebooting is met.

Appendix

Configuring the computer to obtain an IPv4/IPv6 address automatically

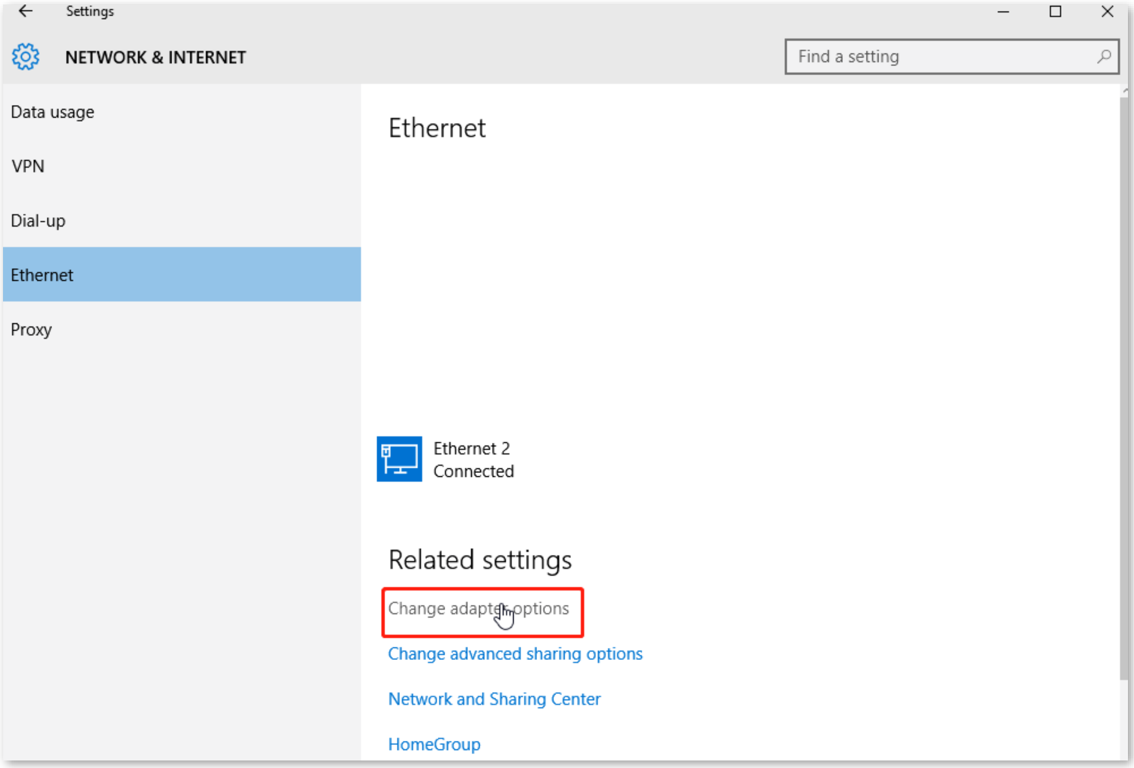
Windows 10 is used for illustration here.

Step 1 Click in the bottom right corner of the desktop and choose **Network settings**.



Network settings

Step 2 Click **Change adapter options**.



Settings

NETWORK & INTERNET

Find a setting

Data usage

VPN

Dial-up

Ethernet

Proxy

Ethernet

Ethernet 2
Connected

Related settings

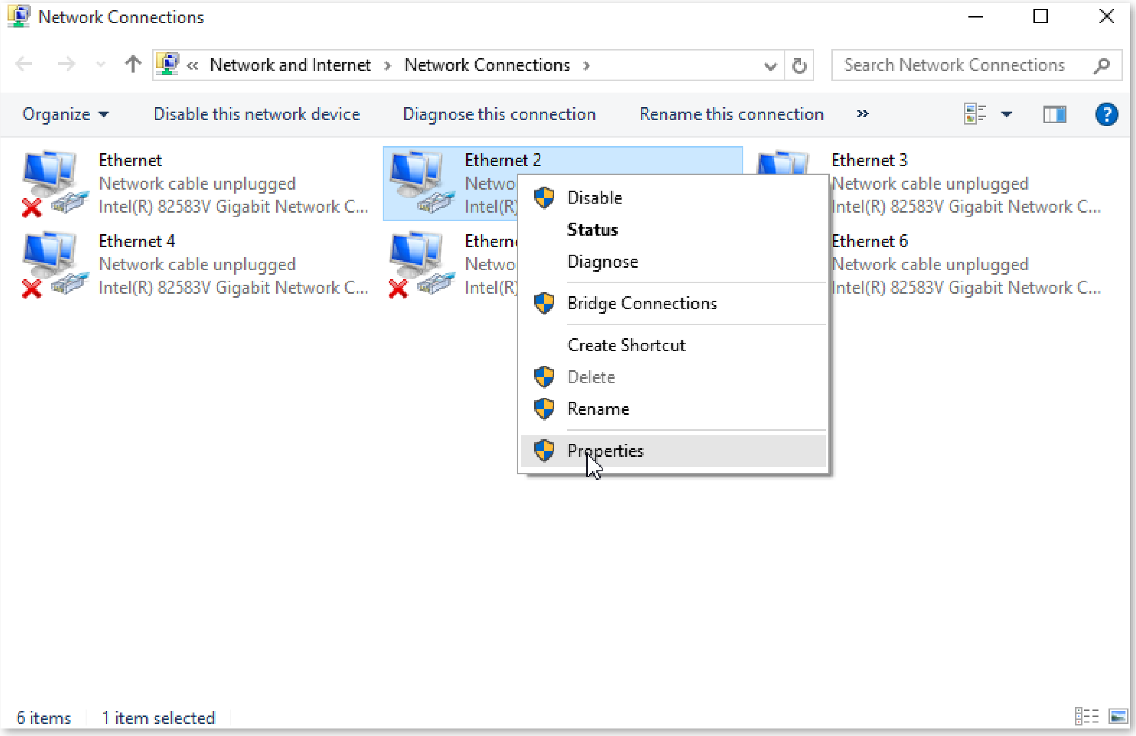
Change adapter options

Change advanced sharing options

Network and Sharing Center

HomeGroup

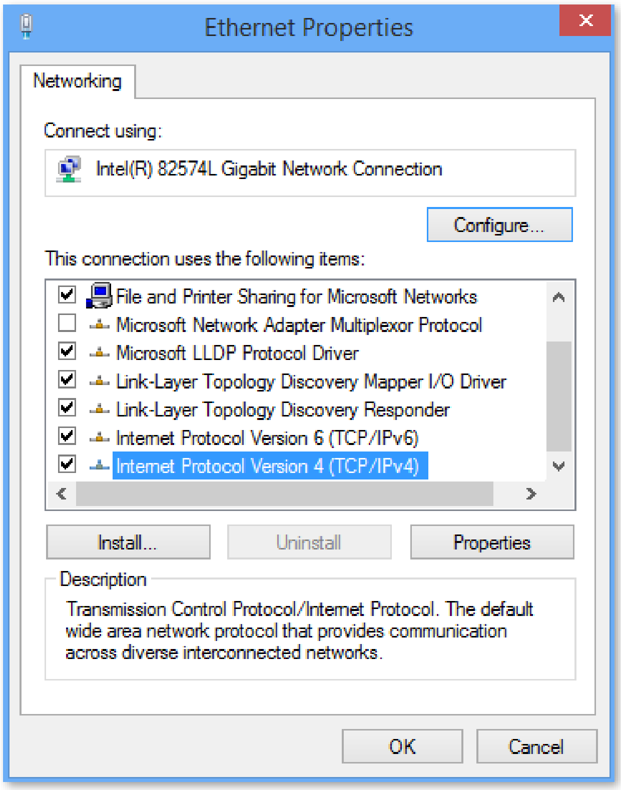
Step 3 Right click on the connection which is being connected, and then click **Properties**.



Step 4 Double-click **Internet Protocol Version 4 (TCP/IPv4)**.

Note

If you want to configure the computer to allow it obtain an IPv6 address automatically, choose **Internet Protocol Version 6 (TCP/IPv6)**.



Connect using:

Intel(R) 82574L Gigabit Network Connection

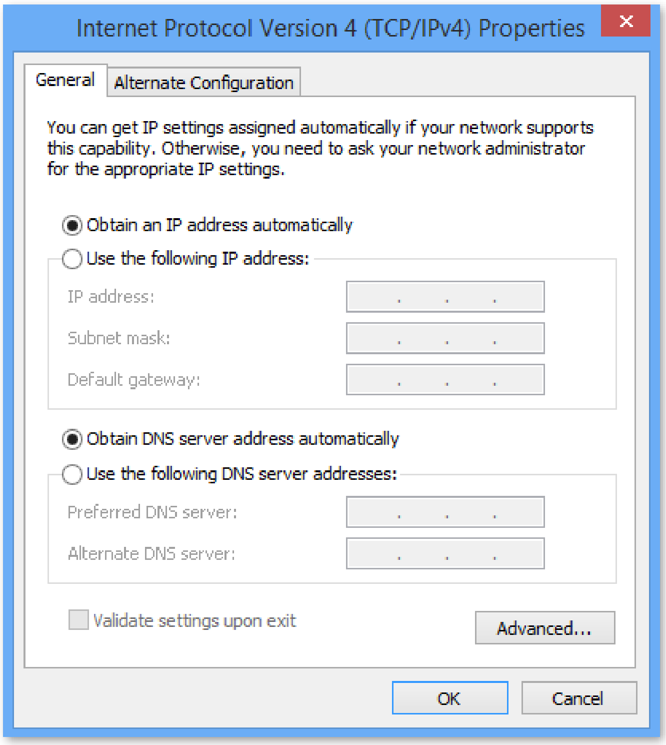
This connection uses the following items:

☑ File and Printer Sharing for Microsoft Networks
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Step 5 Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**, and click **OK**.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Step 6 Click **Close** in the Ethernet Properties window.

Acronyms and abbreviations

Acronym or Abbreviation	**Full Spelling**
AES	Advanced Encryption Standard
AP	Access Point
CE	Customer Edge
DDNS	Dynamic Domain Name System
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol Version 6
DMZ	Demilitarized Zone
DNS	Domain Name System
GMT	Greenwich Mean Time
IP	Internet Protocol
IPTV	Internet Protocol Television
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
MAC	Medium Access Control
MTU	Maximum Transmission Unit
PIN	Personal Identification Number
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point to Point Tunneling Protocol
PUK	Personal Identification Number Unlock Key
SIM	Subscriber Identity Module
SMS	Short Message Service
SSID	Service Set Identifier
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play

Acronym or Abbreviation	**Full Spelling**
USSD	Unstructured Supplementary Service Data
WAN	Wide Area Network
WISP	Wireless Internet Service Provider
WPA-PSK	WPA-Pre-shared Key

See Far, Go Further