4G N300 Wi-Fi LTE Router

User Manual

Legal Information

About this Document

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

About this Product

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

Acknowledgment of Intellectual Property Rights

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

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Applicable Models

This guide is applicable to the model: DS-3WR4G3N

Symbol Conventions

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

Item	Presentation	Example
Cascading Menus	>	Navigate to **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
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 Quick setup

This chapter describes how to connect the devices and enable Internet access through the quick setup wizard. You can complete quick setup for Internet access by following the instructions on the web UI wizard. This wizard only occurs upon your first setup.

Procedure:

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

Note

By default, the WAN/LAN and LAN ports are both LAN ports. When the Failover function is enabled, the WAN/LAN port only serves as a WAN port.

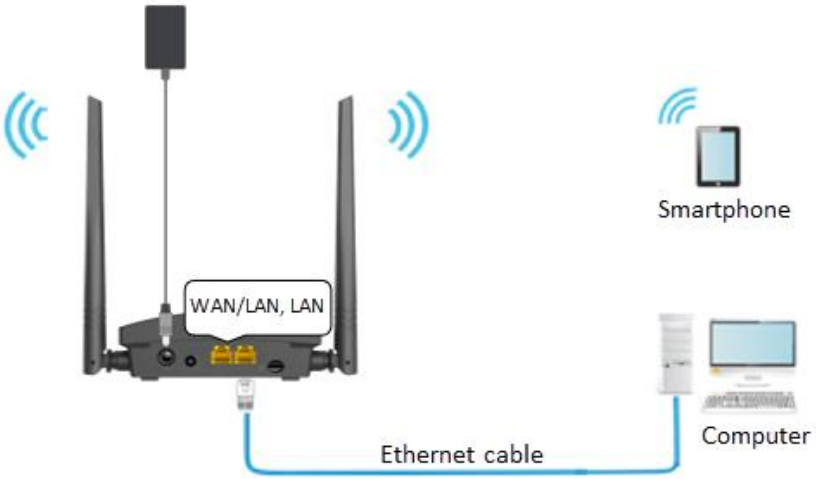


Figure 1-1 Physical connection

Step 2 Start a web browser on the device connected to the router, and visit **https://hikvisionwifi.local** (computer used as an example).

Note

When logging in to the web UI page, the browser may prompt that the address is not secure. Navigate to **Advanced** > **Proceed to hikvisionwifi.local (unsafe)** to continue to visit.

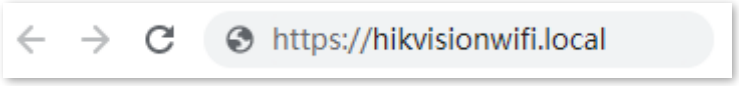


Figure 1-2 Log in to the web UI of the router

Step 3 Click **Start**.

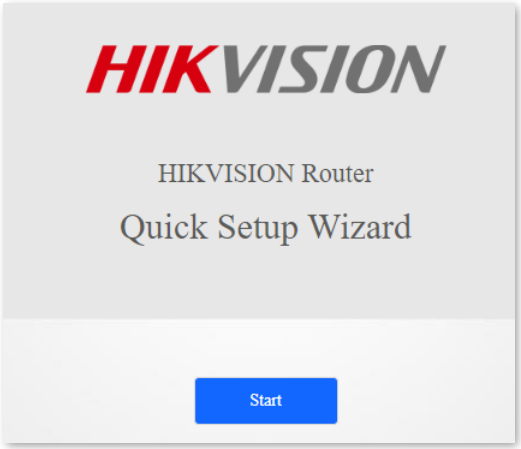


Figure 1-3 Quick setup wizard

Note

- If the SIM card is inserted properly and the Internet connection is normal, you can continue to set up.
- If **No SIM Card** is shown on the page, ensure the SIM card is inserted properly.
- If **SIM card blocked** is shown on the page, refer to Unlock the SIM card in the quick setup wizard.
- 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.
  - Try to log in to the web UI of the router with the LAN IP address. It is **192.168.0.1** by default. If the LAN IP address has been changed, use the new LAN IP address to log in.
  - Restore the router to factory settings and try again.

Step 4 Set parameters as required, and click **Next**.

Note

- If you do not want to use a password, tick **No Password**. In this case, any client can access the Internet without a password. **No Password** is not recommended as it leads to low network security.
- To use the same password for Wi-Fi connection and web UI login, tick **Sync the login password with the Wi-Fi password**.
- To use different passwords for Wi-Fi connection and web UI login, set Wi-Fi name and Wi-Fi password for Wi-Fi connection and login password for web UI login.
- For initial setup or after a reset, set new login and Wi-Fi passwords for privacy and security (The longer the password, the stronger the protection). The character limit and composition rules for passwords are subject to software user interface prompts.

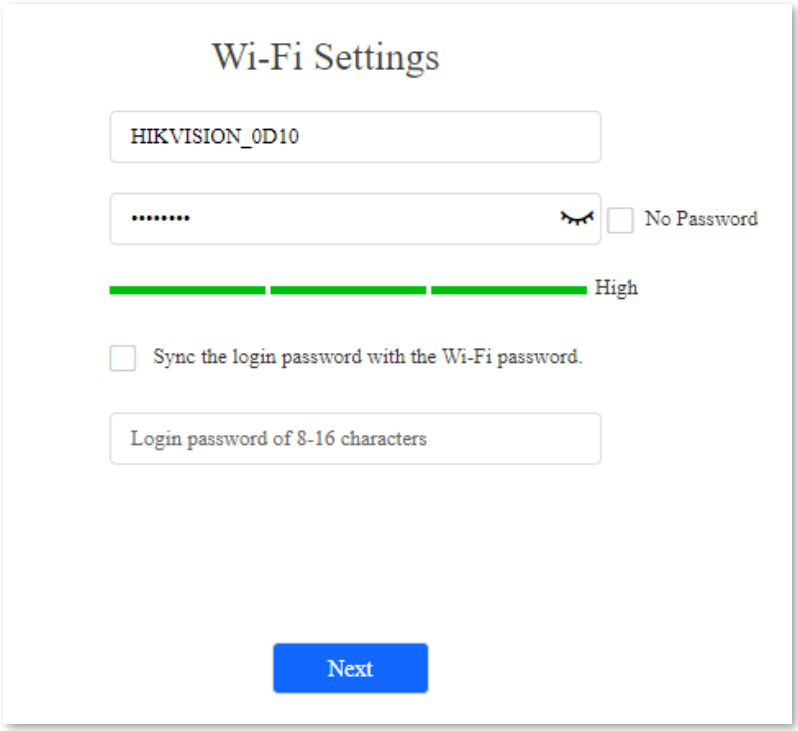


Figure 1-4 Configure Wi-Fi settings

If the following information is displayed, the quick setup for Internet access is finished.

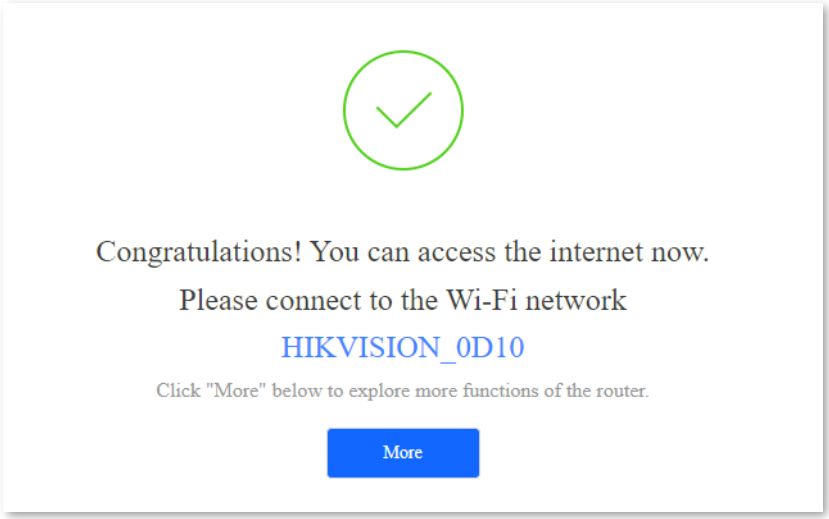


Figure 1-5 Configuration completed

Now you can access the Internet with:

- Wired devices: Connect to the LAN port of your router
- Wireless devices: Connect to your Wi-Fi network using the Wi-Fi name and password you set

Chapter 2 Web UI

2.1 Log in to the web UI

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

Note

By default, the WAN/LAN and LAN ports are both LAN ports. When the Failover function is enabled, the WAN/LAN port only serves as a WAN port.

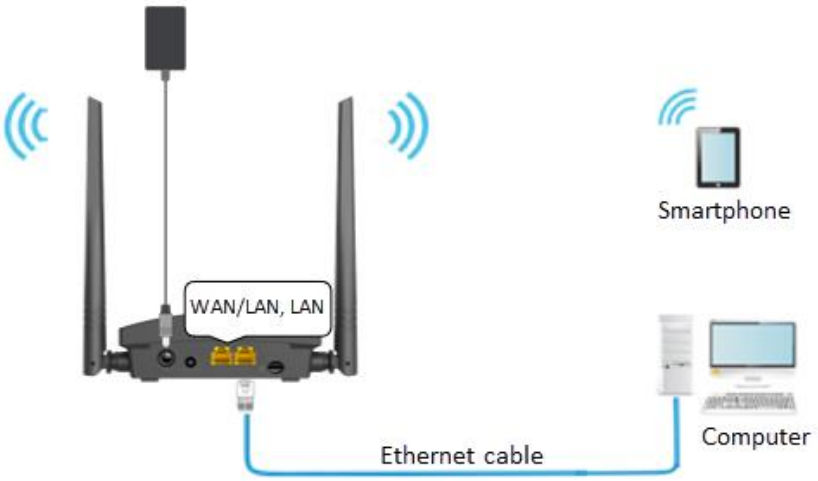


Figure 2-1 Physical connection

Step 2 Start a web browser on the device connected to the router, and visit **https://hikvisionwifi.local** (computer used as an example).

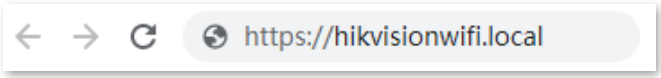


Figure 2-2 Log in to the web UI of the router

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

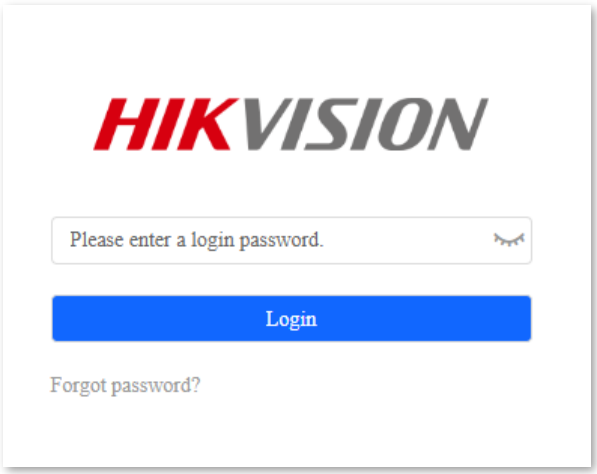


Figure 2-3 Enter login password

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.
- Try to log in to the web UI of the router with the LAN IP address. It is **192.168.0.1** by default. If the LAN IP address has been changed, use the new LAN IP address to log in.
- Restore the router to factory settings and try again.

The following page appears.

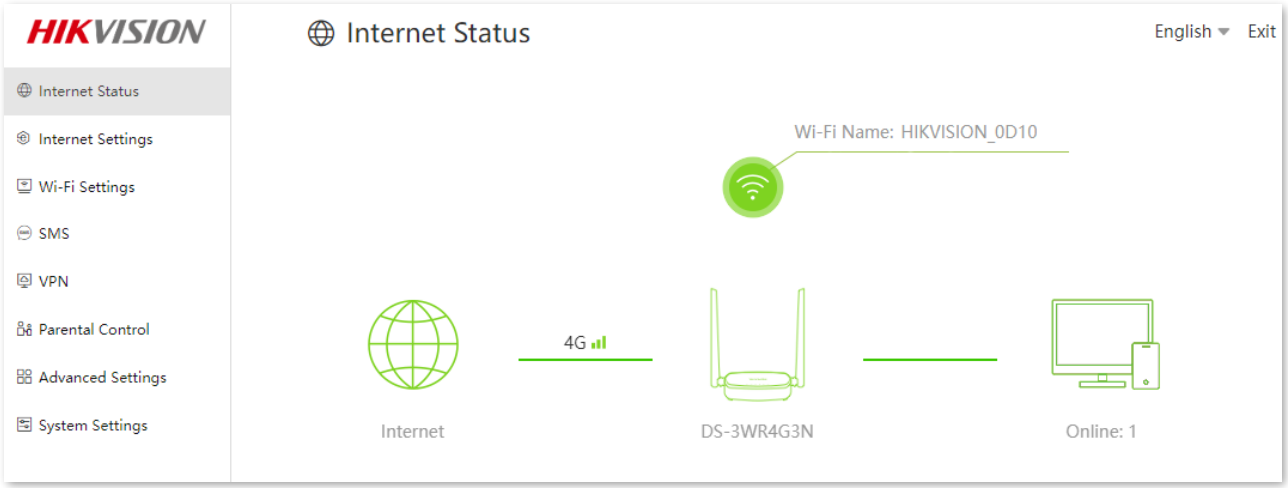


Figure 2-4 Web UI of the router

2.2 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** in the upper right corner of the web UI.

2.3 Change the language

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

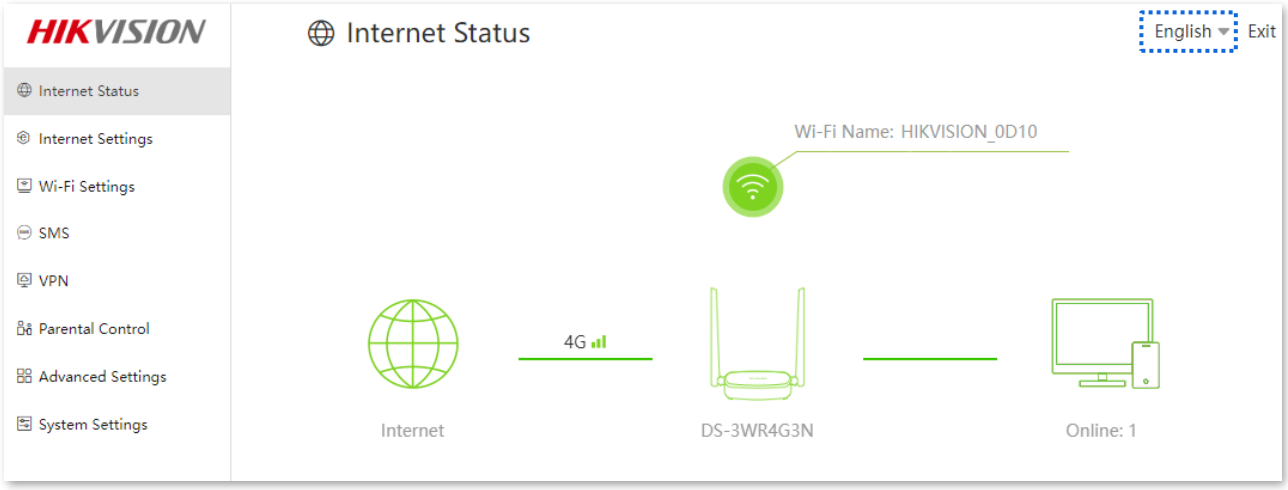


Figure 2-5 Change the language

2.4 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.

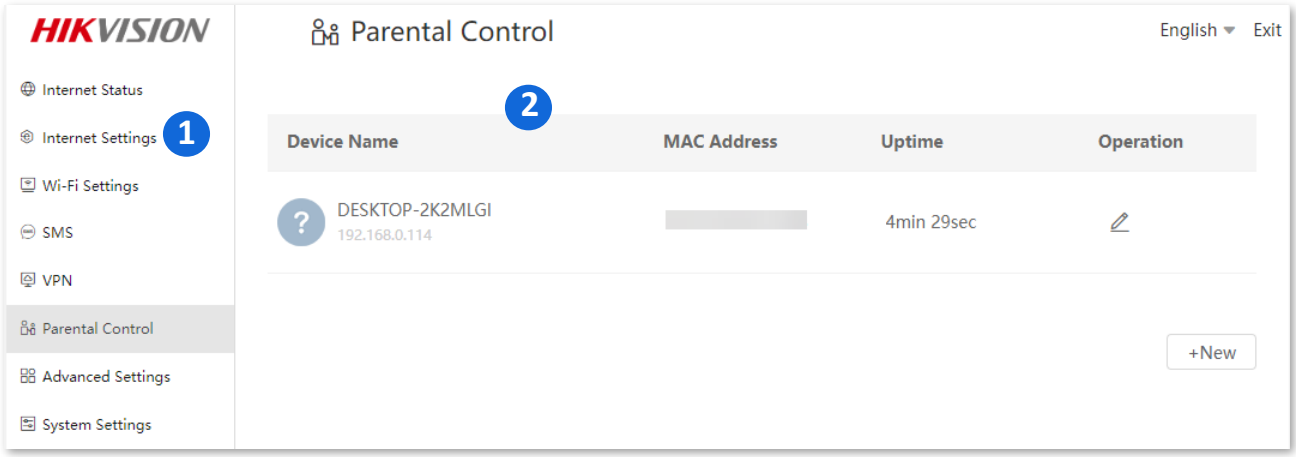


Figure 2-6 Web UI layout

Table 2-1 Parameter description

No.	Name	Description
1	Navigation bar	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	Used to modify or view your configurations.

Chapter 3 Internet status

To enter the page, log in to the web UI of the router and navigate to **Internet Status**. You can:

- View the Internet status
- View wireless information
- View WAN status
- View system information
- View online or blacklist devices

3.1 View internet status

3.1.1 Through a SIM card

To enter the page, log in to the web UI of the router, and you can perform troubleshooting as prompted on the page when you access the Internet through a SIM card.

No SIM card inserted

When "No SIM card Inserted" is shown on the page, ensure the SIM card is inserted properly.

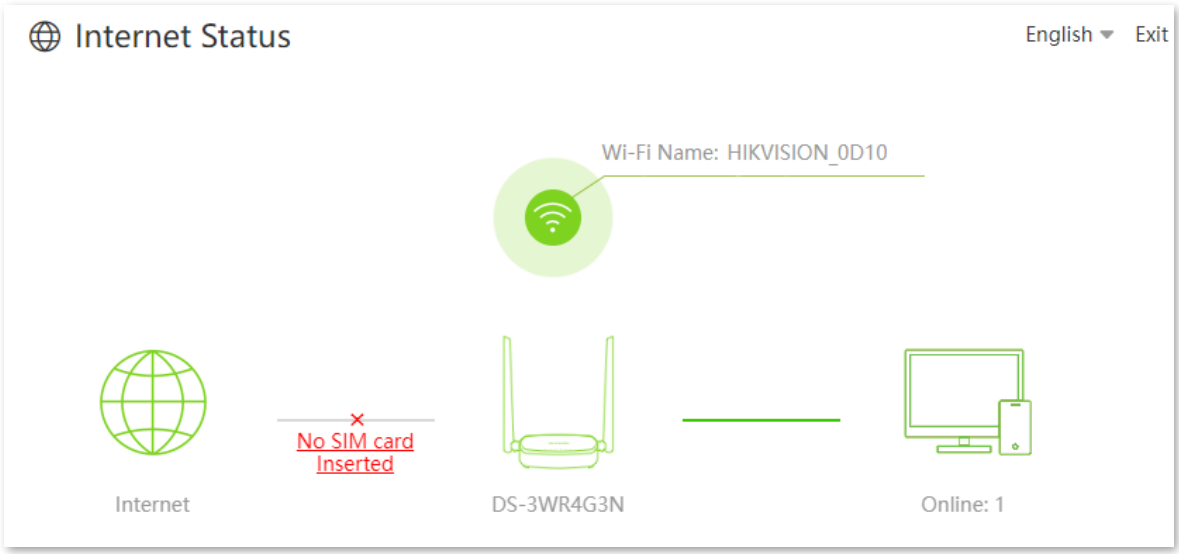


Figure 3-1 No SIM card inserted

SIM card blocked

When "**SIM card blocked**" or "Please unlock the SIM card" is shown on the page, refer to Unlock the SIM card.

Automatically matching APN failed

On the **SIM Settings** page, automatic matching of APN parameters is available. Manually selecting Profile name or creating Profile will suspend the matching. When "Matching failed, please set Profile manually." is shown on the page, you need to manually configure the correct APN parameters according to the page prompts.

APN not correctly identified

When "APN not correctly identified" is shown on the page, it indicates that you need to configure the correct APN parameters. Click **APN not correctly identified** to navigate to the **Internet Settings** page and modify APN parameters.

Data traffic disabled

When "The data traffic has been manually disabled. Please enable it." is shown on the page, ensure that the **Mobile Data** function is enabled on the **Internet Settings** page.

Network connection disabled

When "The network connection has been manually disabled. Please enable it." is shown on the page, you can click **Connect** to connect to the Internet again on the **Internet Settings** page.

Monthly data limit reached

When "The monthly data limit is reached." is shown on the page, it indicates that the router will disconnect from the Internet automatically when the limit is reached. Refer to Mobile Data to modify the related parameters.

Connection failed

When "Connection failed." is shown on the page, it indicates that the connection is abnormal.

Try the following solutions:

- Navigate to **Internet Settings**, and ensure that the **Mobile Data** and **Data Roaming** functions are enabled.
- Navigate to **Internet Settings**, and ensure that the dial-up settings parameters are identified by the router automatically. If not, ensure that 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. Ensure that you have an active plan.
- If the SIM card balance is sufficient, it is recommended that contact our technical support for help.

3.1.2 Through the WAN port (Example: PPPoE)

To enter the page, log in to the web UI of the router, and you can perform troubleshooting as prompted on the page when you access the Internet through the WAN port.

Note

Before checking the Internet status, you should connect the WAN/LAN port to the Internet using an Ethernet cable, enable the Failover function and configure Internet parameters on the **Internet Settings** page.

Ethernet cable disconnected

When "No Ethernet cable is connected to the WAN port" is shown on the page, ensure that the Ethernet cable is connected to the WAN port properly.

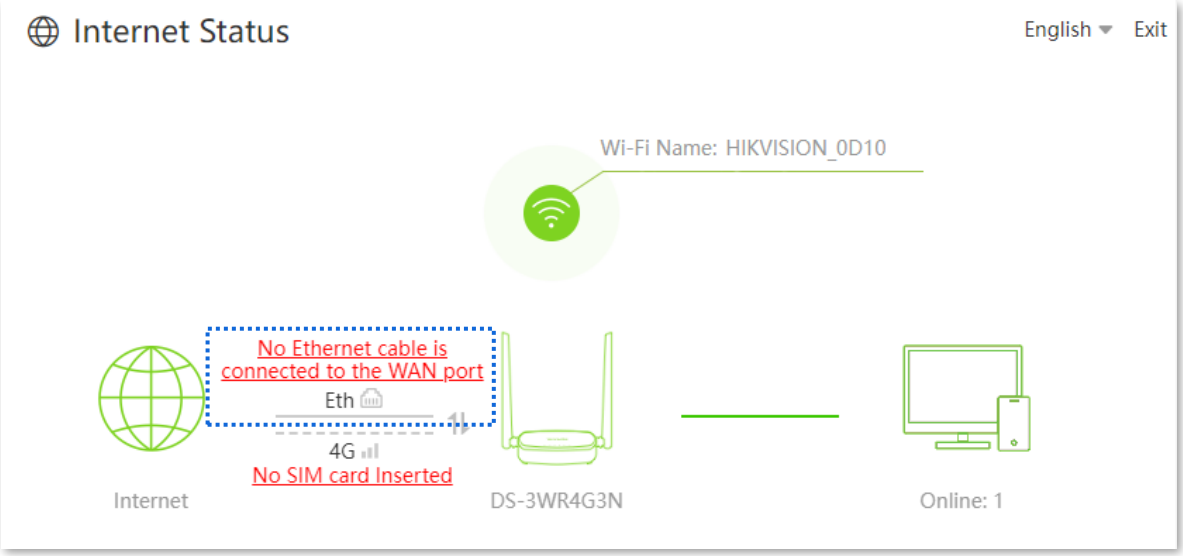


Figure 3-2 Ethernet cable disconnected

Incorrect user name and password

When "The user name and password are incorrect." is shown on the page, ensure that the PPPoE user name and password are entered correctly.

Note

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

- Pay attention to case sensitivity, such as "Z" and "z".
- Pay attention to similar letters and numbers, such as "I" and "1".
- Ensure the completeness of account parameters, such as "0755000513@163.gd", rather than "0755000513".

If the problem persists, contact your ISP for help.

No response from the remote server

When "No response from the remote server." is shown on the page, it indicates that the upstream server network may be abnormal. Contact your ISP for help.

Connection disconnected

- When “Disconnected” is shown on the page, you can click **Connect** to connect to the Internet again on the **Internet Settings** page.
- When “Disconnected. Please contact your ISP for help.” is shown on the page, it indicates that the connection is abnormal. Contact your ISP for help.

3.1.3 Through SIM card and WAN port

When you access the Internet through the SIM card and WAN port, the WAN port is prioritized for Internet access by default. You can click ⇅ to manually switch the current Internet connection mode on the **Internet Status** page as required.

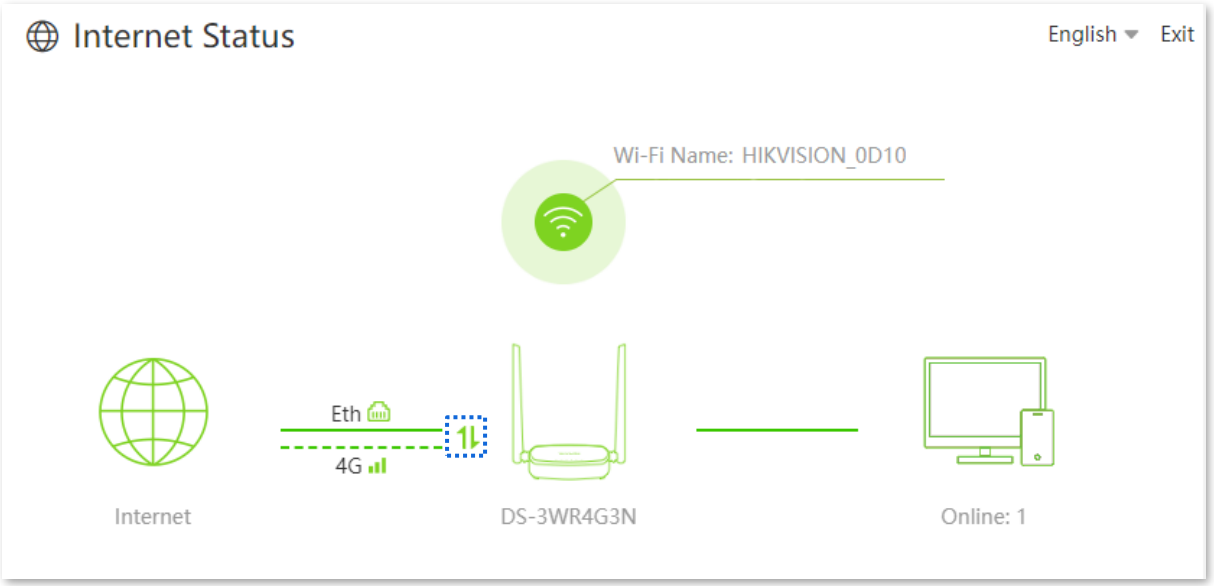


Figure 3-3 Manually switch the Internet connection mode

Note

- If there is a network failure, the router will automatically switch to an available Internet connection mode.
- If the other abnormal information is shown between the Internet and the router, refer to Through a SIM card or Through the WAN port (Example: PPPoE) to find a solution.

3.2 View wireless information

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

Step 2 Navigate to **Internet Status**.

Step 3 Click .

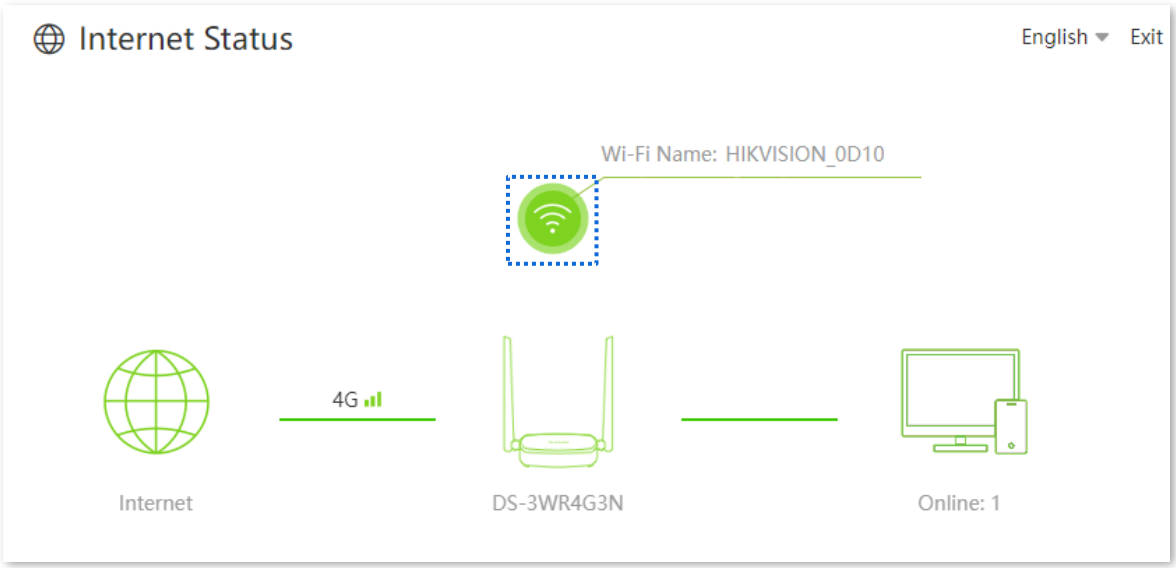


Figure 3-4 View wireless information

You can change wireless parameters as required.

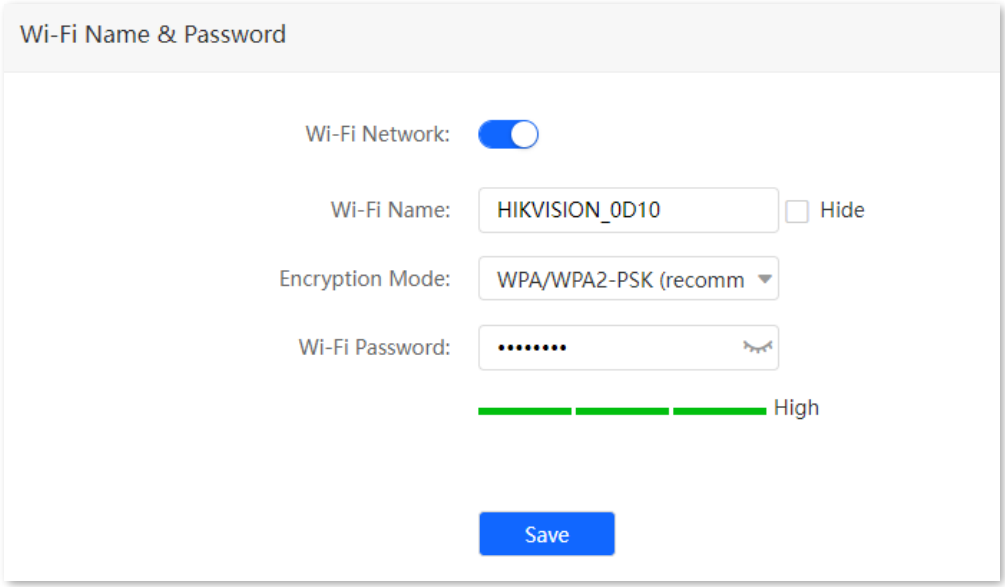


Figure 3-5 Change wireless parameters

3.3 View WAN status

You can view the WAN status, including 3G/4G and Ethernet WAN status.

Note

Before checking the WAN status, you should connect the WAN/LAN port to the Internet using an Ethernet cable, enable the Failover function and configure Internet parameters on the **Internet Settings** page.

Procedure:

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

Step 2 Navigate to **Internet Status**.

Step 3 Click .

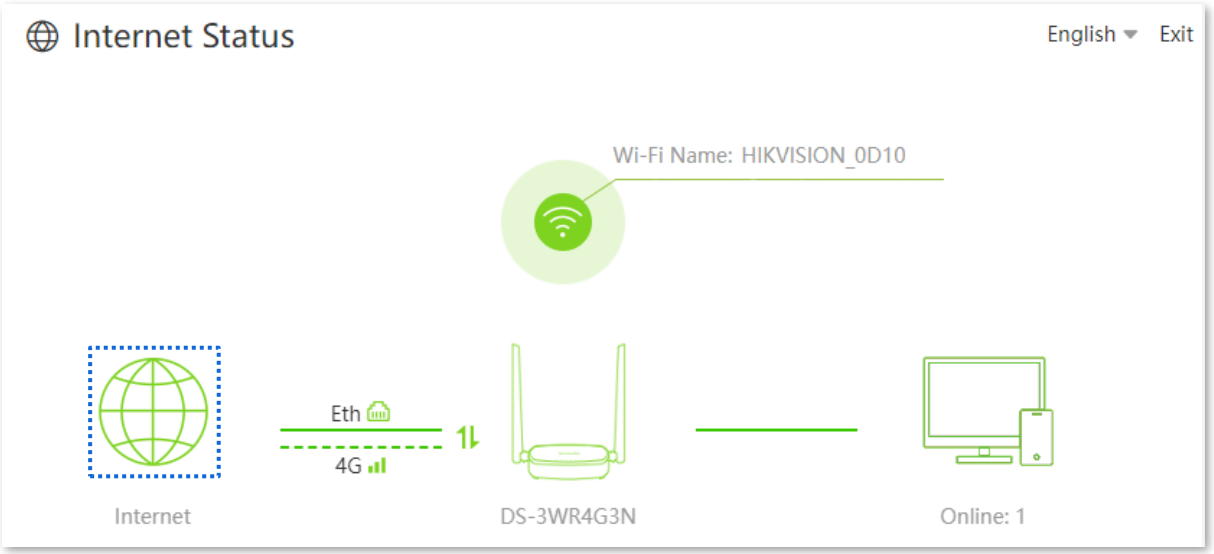


Figure 3-6 View WAN status

3.3.1 3G/4G WAN status

In this part, you can view the information of the SIM card and 3G/4G network.

To enter the page, log in to the web UI of the router, navigate to **Internet Status** and click .

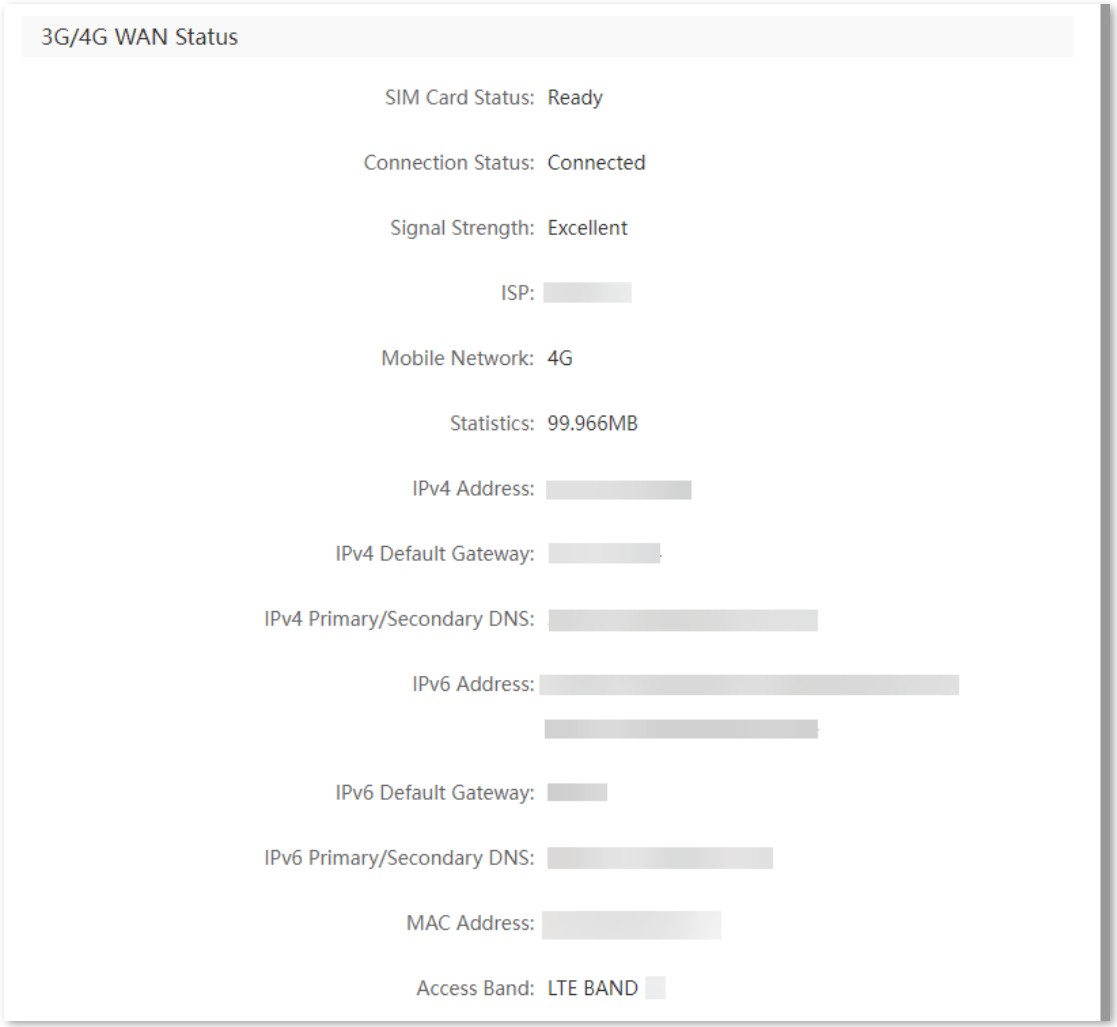


Figure 3-7 View 3G/4G WAN status

Table 3-1 Parameter description

Parameter	**Description**
SIM Card Status	Specifies the SIM card status inserted in the router.
Connection Status	Specifies Internet connection status of 3G/4G mobile network.
Signal Strength	Specifies the signal strength of 3G/4G mobile network, including **Excellent**, **Good** and **Fair**.
ISP	Specifies the ISP name of the SIM card.
Mobile Network	Specifies the current network type for Internet access.
Statistics	Specifies the data traffic of the SIM card that has been used.
IPv4/IPv6 Address	Specifies the IP address of the router obtained from the ISP.
IPv4/IPv6 Default Gateway	Specifies the gateway IP address of the router.
IPv4/IPv6 Primary/Secondary DNS	Specifies the primary and secondary DNS server address of the router.

Parameter	Description
MAC Address	Specifies the 3G/4G MAC address of the router.
Access Band	Specifies the access band of the mobile network of the router.

3.3.2 Ethernet WAN status

In this part, you can view the information of the WAN/LAN port connected to the Ethernet cable.

To enter the page, log in to the web UI of the router, navigate to **Internet Status** and click .

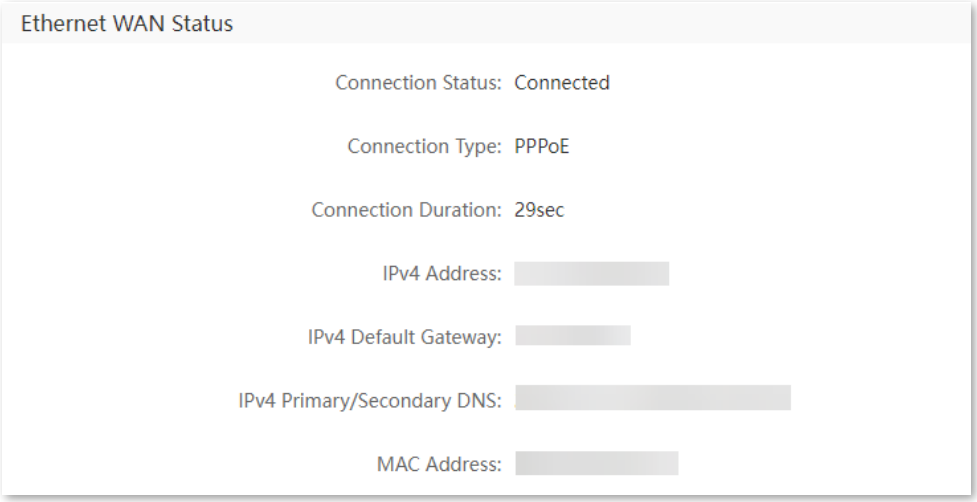


Figure 3-8 View Ethernet WAN status

Table 3-2 Parameter description

Parameter	Description
Connection Status	Specifies Internet connection status of the WAN port.
Connection Type	Specifies how your router connects to the Internet, including: ● **PPPoE**: Select this type if you access the Internet using the PPPoE username and PPPoE password. ● **Dynamic IP Address**: Select this type if you can access the Internet by simply plugging in an Ethernet cable. ● **Static IP Address**: Select this type if you want to access the Internet using fixed IP information.
Connection Duration	Specifies the duration since the router is connected to the Internet through the WAN port.
IPv4 Address	Specifies the IP address of the router obtained from the ISP.
IPv4 Default Gateway	Specifies the gateway IP address of the router.
IPv4 Primary/Secondary DNS	Specifies the IP address of primary and secondary DNS servers of the router.

Parameter	Description
MAC Address	Specifies the Ethernet MAC address of the router.

3.4 View system information

You can view the system information of the router, such as basic information, LAN status and Wi-Fi status.

To enter the page, log in to the web UI of the router, navigate to **Internet Status** and click .

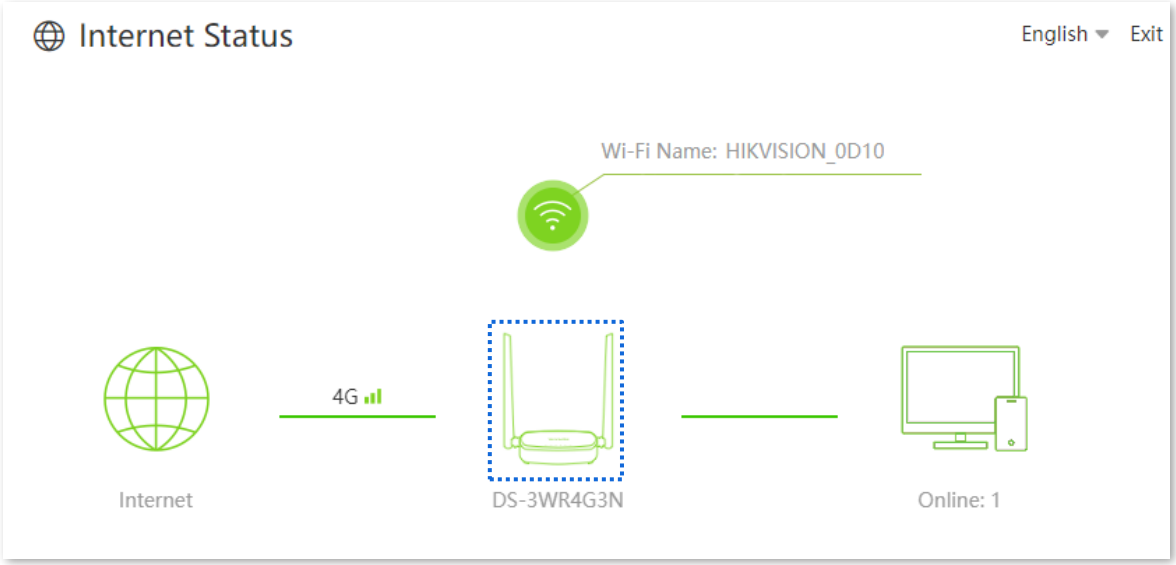


Figure 3-9 View system information

3.4.1 Basic information

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

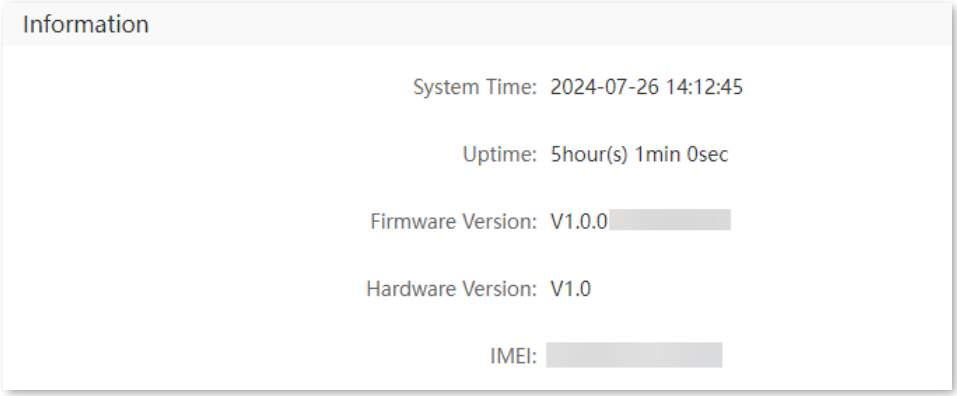


Figure 3-10 View basic information

Table 3-3 Parameter description

Parameter	Description
System Time	Specifies the system time of the router.
Uptime	Specifies the operating time of the router since it is powered on.
Firmware Version	Specifies the firmware version of the router.
Hardware Version	Specifies the hardware version of the router.
IMEI	Specifies the International Mobile Equipment Identity (IMEI) of the mobile device.

3.4.2 LAN status

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

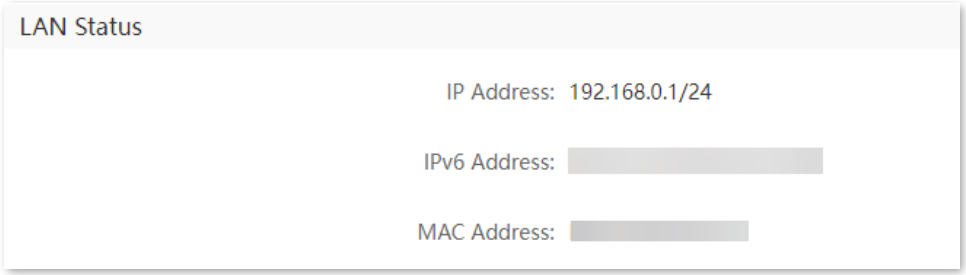


Figure 3-11 View LAN status

Table 3-4 Parameter description

Parameter	Description
IP Address	Specifies the LAN IP address of the router which is the IP address for logging in to the web UI of the router.
IPv6 Address	Specifies the LAN IPv6 address of the router.
MAC Address	Specifies the LAN MAC address of the router.

3.4.3 Wi-Fi status

In this part, you can view the information of Wi-Fi network, including the visibility, Wi-Fi name, bandwidth, channel and MAC address.

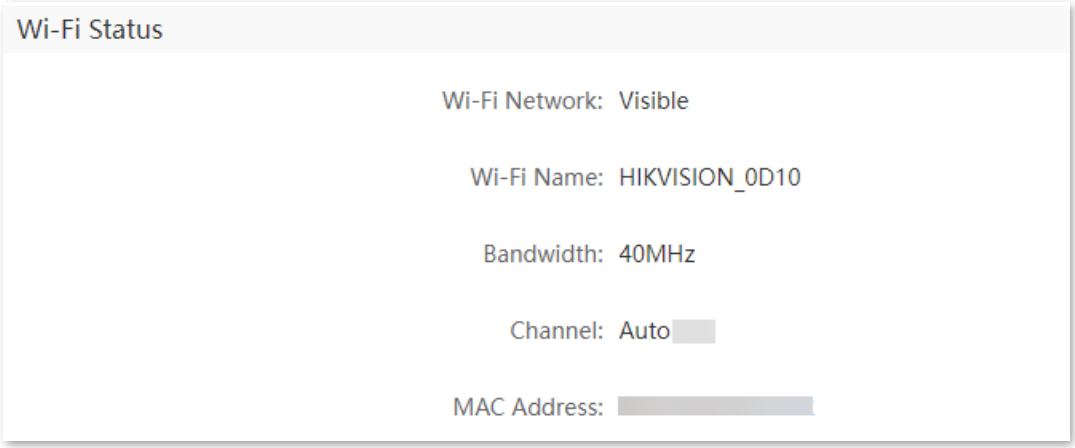


Figure 3-12 View Wi-Fi status

Table 3-5 Parameter description

Parameter	Description
Wi-Fi Network	Specifies whether the Wi-Fi network is hidden.
Wi-Fi Name	Specifies the Wi-Fi name of the router.
Bandwidth	Specifies the bandwidth of the Wi-Fi network.
Channel	Specifies the channel that the Wi-Fi network works in.
MAC Address	Specifies the MAC address of the Wi-Fi network.

3.5 View online or blacklisted devices

You can view the information of devices connected to the router, including the current speed and access type. You can also view and add devices to the blacklist.

To enter the page, log in to the web UI of the router, navigate to **Internet Status** and click .

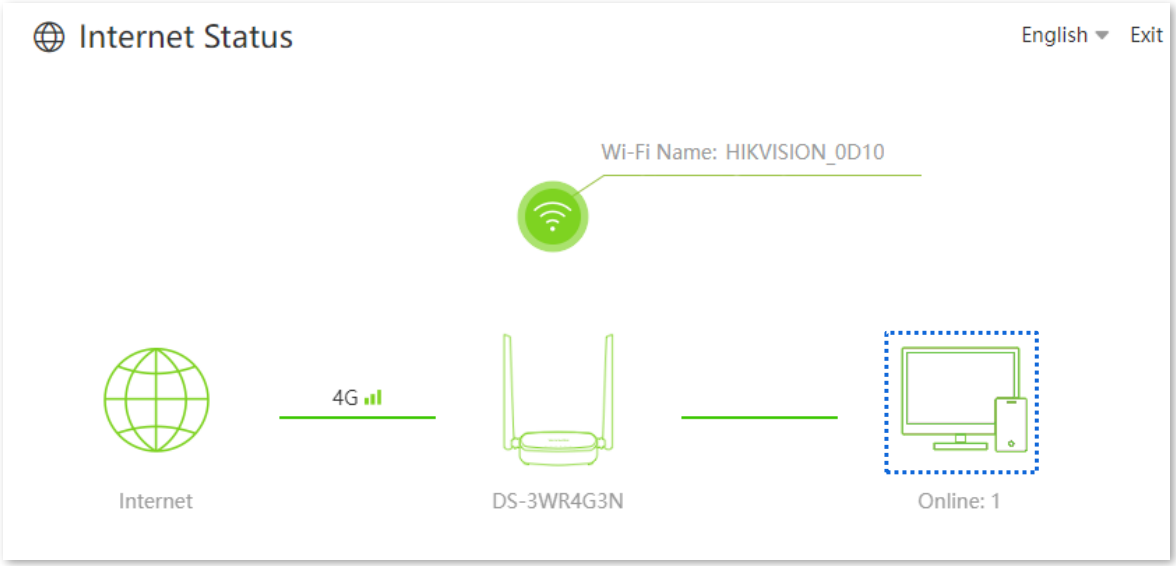


Figure 3-13 View online or blacklisted devices

3.5.1 Add devices to the blacklist

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

Step 2 Navigate to **Internet Status**.

Step 3 Click .

Step 4 Locate the device to be added, and click **Add**.

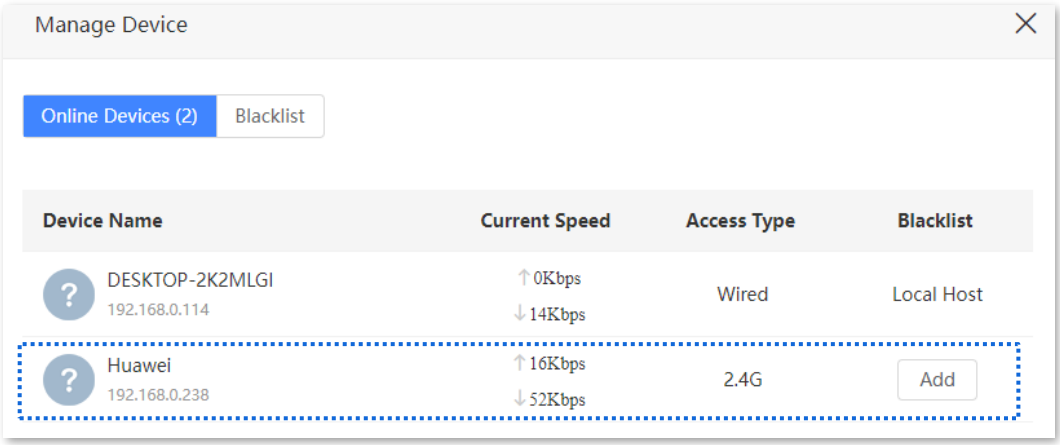


Figure 3-14 Add devices to the blacklist

After the configuration is completed, you can click **Blacklist** to view the blacklisted devices.

Table 3-6 Parameter description

Parameter	Description
Device Name	Specifies the name of online device connected to the router.
Current Speed	Specifies the upload speed and download speed of the device.
Access Type	Specifies the access type of online device connected to the router.
Blacklist	Specifies Whether to add other online devices to the blacklist.

3.5.2 Remove devices from the blacklist

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

Step 2 Navigate to **Internet Status**.

Step 3 Click .

Step 4 Choose **Blacklist**, and locate the device to be removed from the blacklist.

Step 5 Click **Remove**.

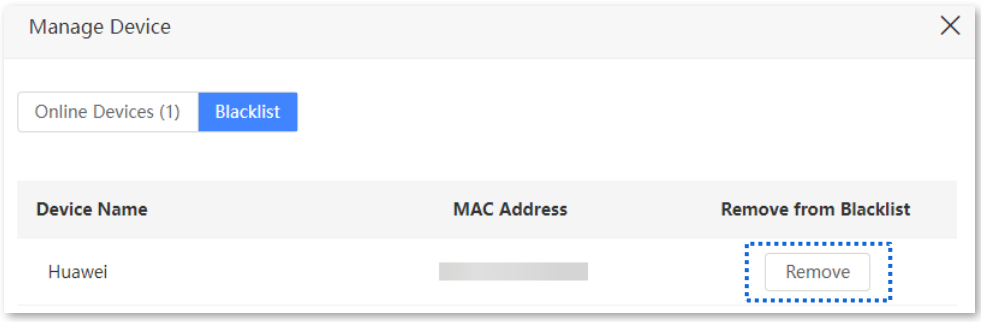


Figure 3-15 Remove devices from the blacklist

After the configuration is completed, the device is removed from the blacklist and can be connected to the router again.

Table 3-7 Parameter description

Parameter	Description
Device Name	Specifies the name of the blacklist device.
MAC Address	Specifies the MAC address of the blacklist device.
Remove from Blacklist	Specifies Whether to remove the device from the blacklist.

Chapter 4 Internet settings

By configuring the Internet settings, you can achieve the shared Internet access (IPv4) for multiple users within the LAN.

4.1 Access the Internet with a SIM card

You can change the Internet settings when you access the Internet with a SIM card.

To enter the page, log in to the web UI of the router, and navigate to **Internet Settings**.

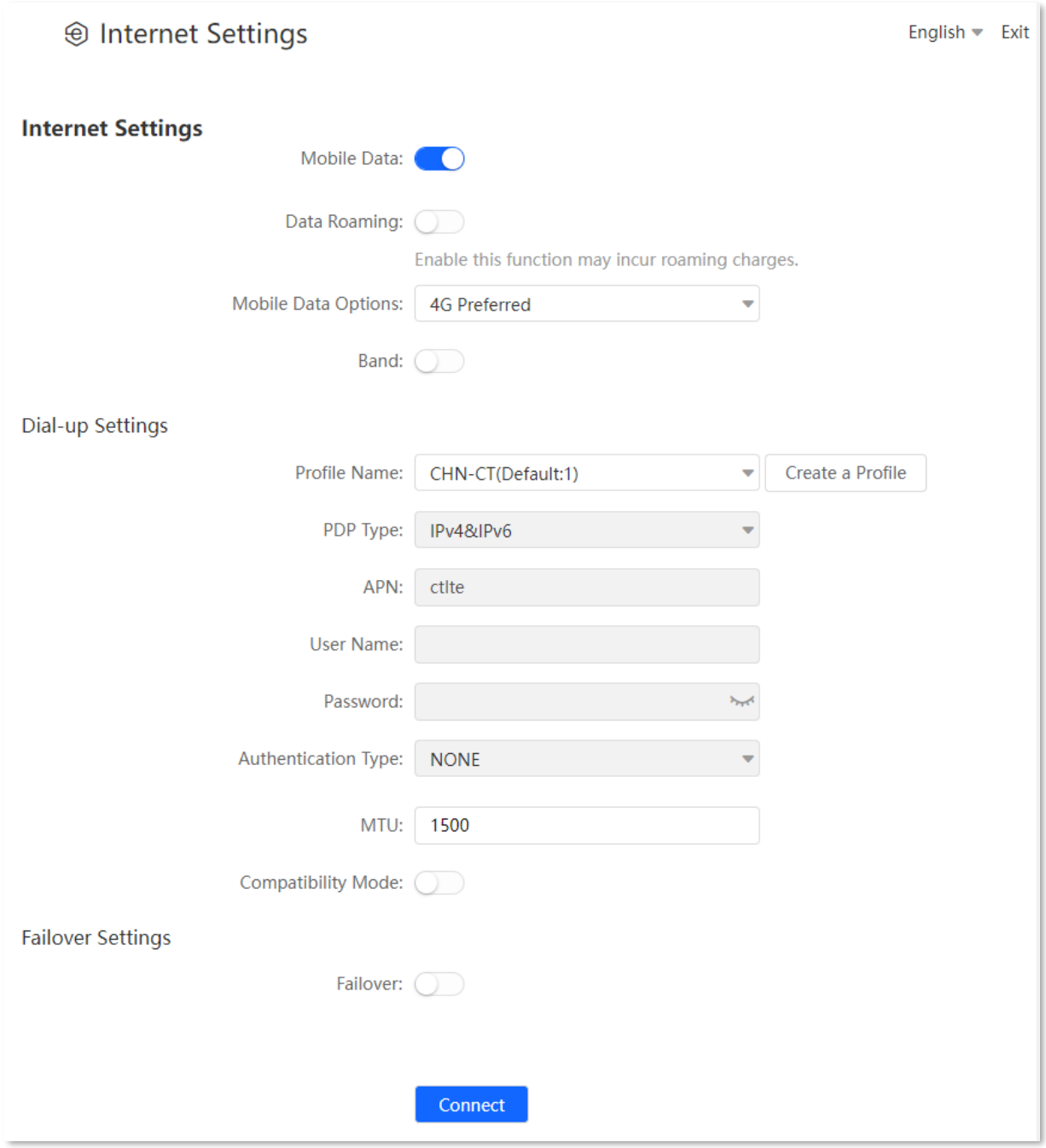


Figure 4-1 Configure Internet settings

Table 4-1 Parameter description

Parameter	Description
Mobile Data	Used to enable or disable the mobile data traffic. When it is disabled, you cannot access the Internet through the router.
Data Roaming	Used to enable or disable data roaming for the SIM card inserted in the router.
Mobile Data Options	Specifies the mobile network type for Internet access. ● **4G Preferred:** Priority to sign up for the 4G Wi-Fi network to access the Internet. ● **4G Only:** Only access the Internet by signing up for the 4G Wi-Fi network. ● **3G Only:** Only access the Internet by signing up for the 3G Wi-Fi network.
Band	Specifies whether to enable the Lock Band function to improve the Internet experience. With the function enabled, it will scan and match the band supported by the SIM card and ISP according to the surrounding network environment.
Band List	Used to select single or multiple bands as required. Selecting a single band can only register the specified band to improve the Internet experience. Selecting multiple bands will use a band from the selected options according to the actual network conditions (signal strength, signal quality and so on).
Profile Name PDP Type APN User Name Password Authentication Type	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 help.
Create a Profile	Used to create an APN dial-up profile when the router fails to identify these parameters automatically.
MTU	Maximum Transmission Unit (MTU) is the largest data packet transmitted by a network device. The default MTU value is 1460. Do not change the value unless necessary.

Parameter	Description
Compatibility Mode	Used to share the hotspot and traffic of the SIM card for Internet access, which can solve the problem of ISP traffic restrictions. The SIM card package includes traffic and hotspot. If the traffic can only be used for mobile devices (such as smartphones) and the hotspot can only be used for the router, you can enable the compatibility mode on the web UI to modify the Time to Live (TTL) and Hop Limit (HL) values to share the hotspot and traffic for Internet access. **Note** It is applicable to some ISPs limited plans. The TTL and HL values can be modified for packet capture analysis according to your needs.

4.1.1 Change mobile network preference

When you use a SIM card to access the Internet, 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.

Procedure:

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

Step 2 Navigate to **Internet Settings**.

Step 3 Enable **Mobile Data** and **Data Roaming**.

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

Step 5 Click **Connect**.

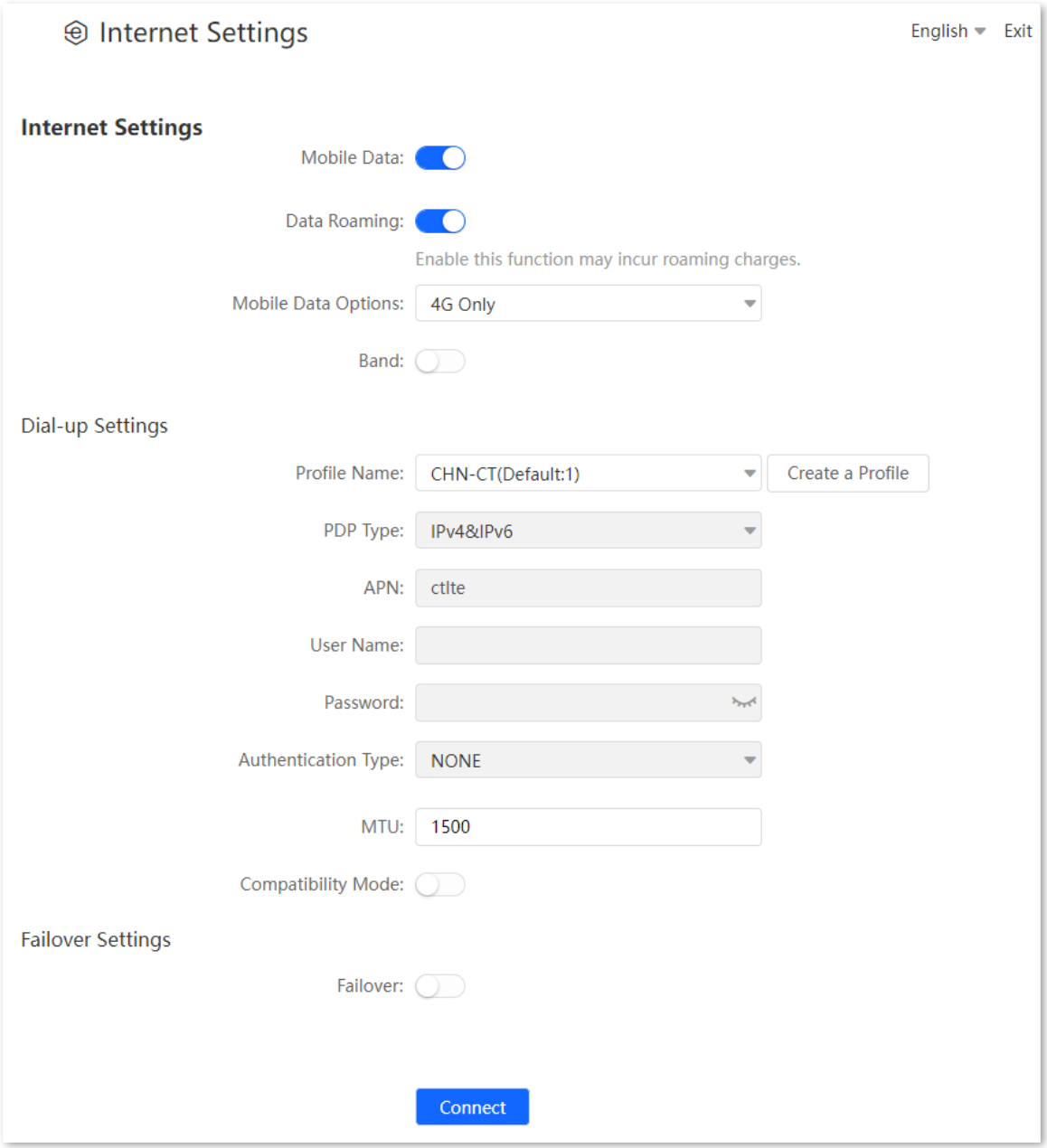


Figure 4-2 Change mobile network preference

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

4.1.2 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.

Procedure:

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

Step 2 Navigate to **Internet Settings**.

Step 3 Click Create a Profile.

Step 4 Enter required parameters inquired from your ISP.

Step 5 Click **Save**.

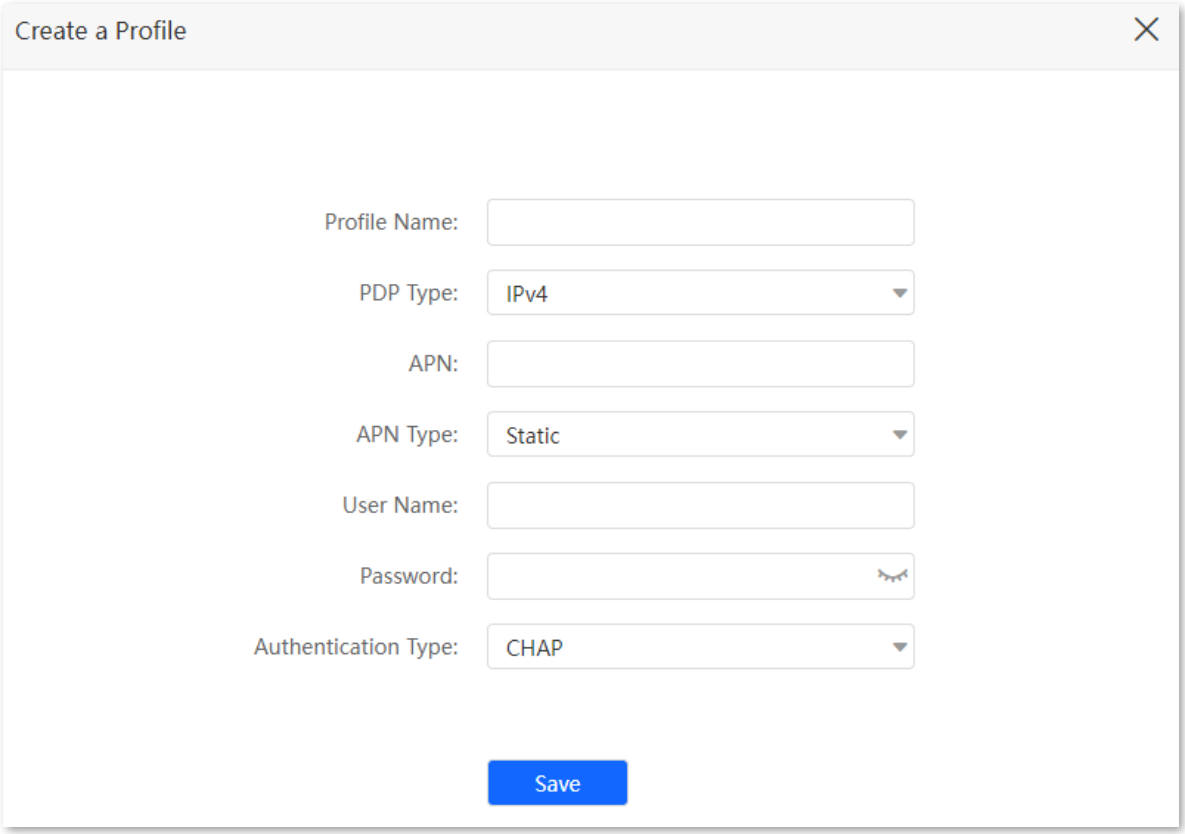


Figure 4-3 Create an APN profile

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.

4.2 Access the Internet through the WAN port

If you want to connect your broadband to the router to access the Internet, you can access the Internet through the WAN port.

Note

Parameters for accessing the Internet are provided by your ISP. Contact your ISP for help.

4.2.1 Use 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.

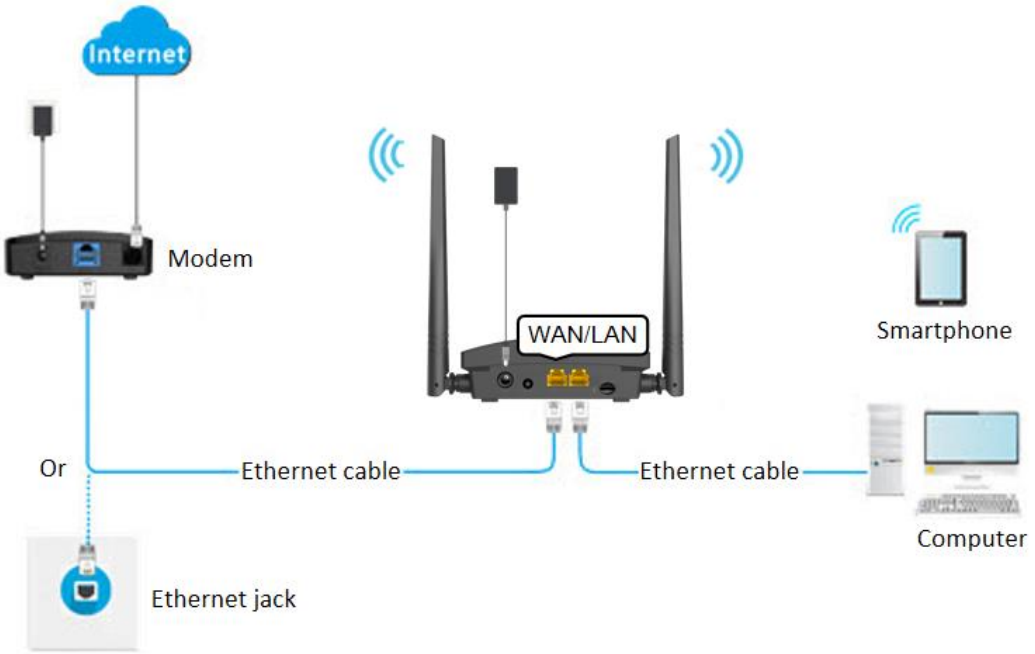


Figure 4-4 Physical connection

Procedure:

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

Step 2 Navigate to **Internet Settings**.

Step 3 Enable the **Failover** function.

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

Step 5 Enter the **PPPoE Username** and **PPPoE Password**.

Step 6 Click **Connect**.

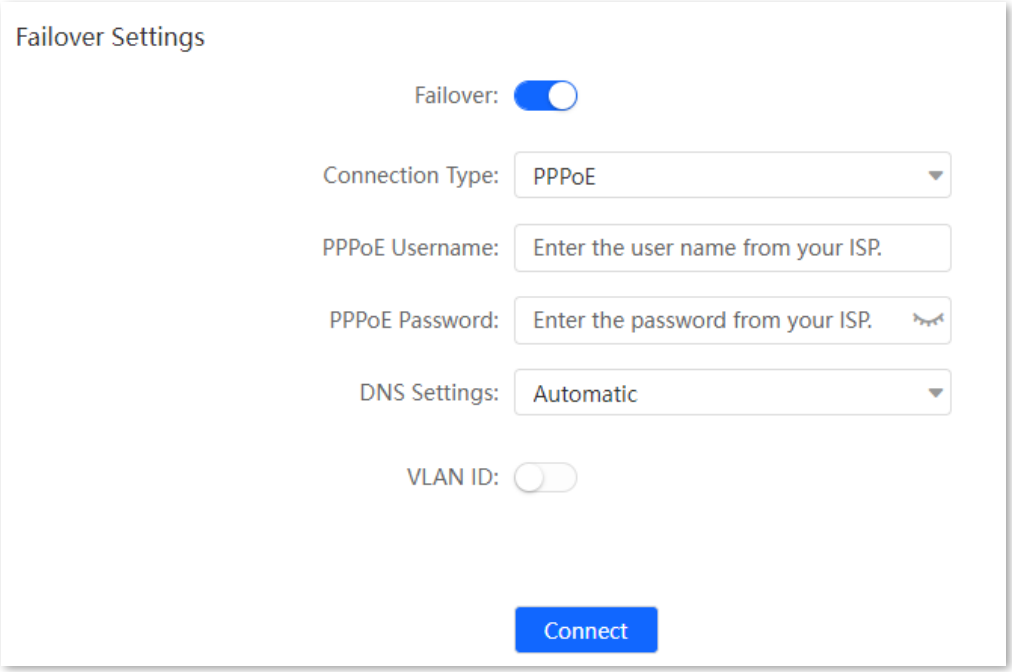


Figure 4-5 Configure PPPoE connection

Wait a moment. When "Eth" is shown on the **Internet Status** page, you can access the Internet.

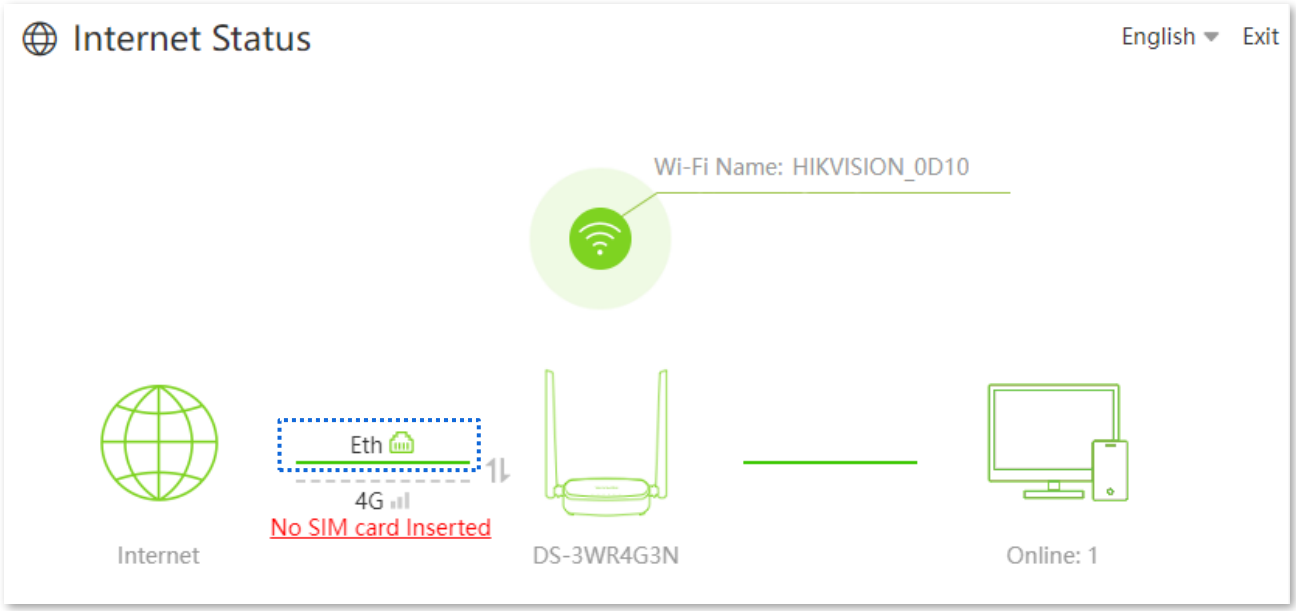


Figure 4-6 PPPoE connection succeeded

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

Table 4-2 Parameter description

Parameter	Description
Failover	Used to enable or disable the Failover function.
Connection Type	Specifies how your router connects to the Internet, including: ● **PPPoE**: Select this type if you access the Internet using the PPPoE user name and PPPoE password. ● **Dynamic IP**: Select this type if you can access the Internet by simply plugging in an Ethernet cable. ● **Static IP**: Select this type if you want to access the Internet using fixed IP information.
PPPoE Username	When PPPoE is chosen as Connection Type, you need to enter the user name and password provided by your ISP to access the Internet.
PPPoE Password	
DNS Settings	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.
VLAN ID	Used to enable or disable the VLAN ID according to the actual network environments. When the function is enabled, the VLAN ID is required to enter. Consult your ISP for this parameter. The value range is 1 to 4094.

4.2.2 Use a 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-3WR4G3N as the other one.

The application scenario is shown below.

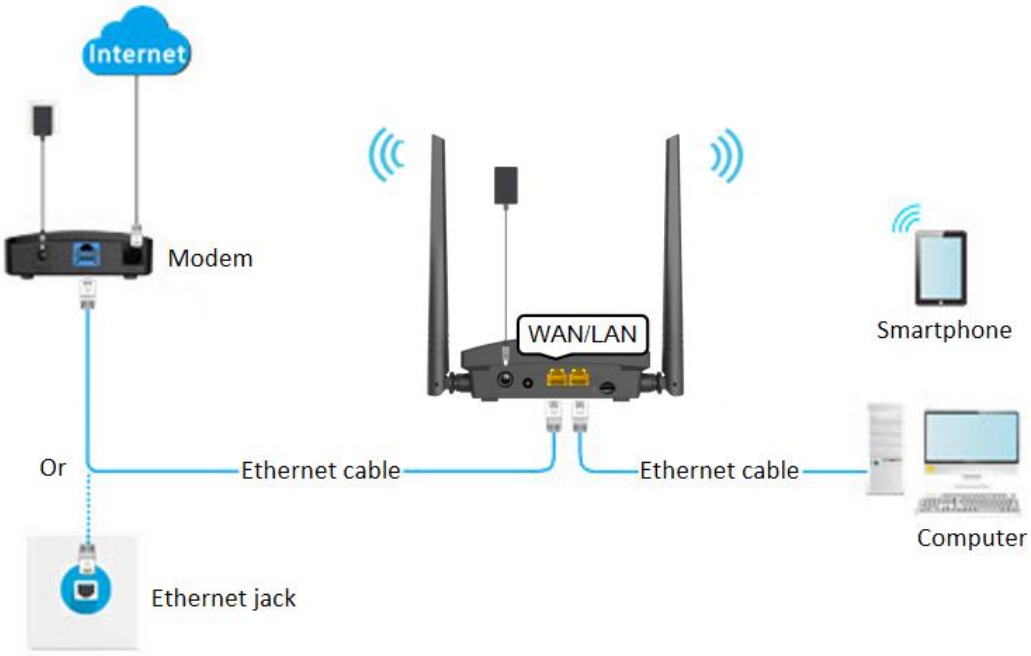


Figure 4-7 Physical connection

Procedure:

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

Step 2 Navigate to **Internet Settings**.

Step 3 Enable the **Failover** function.

Step 4 Set **Connection Type** to **Dynamic IP Address**.

Step 5 Click **Connect**.

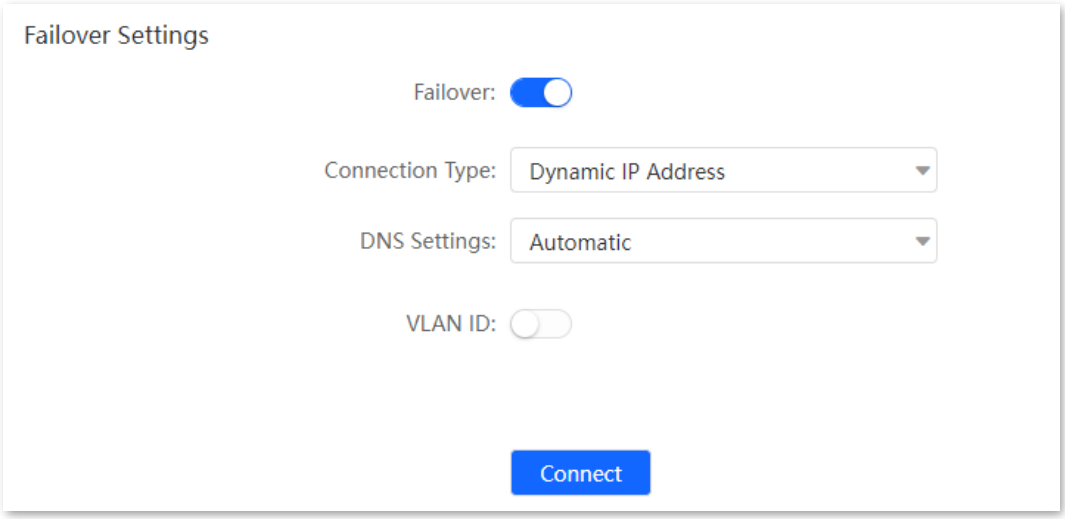


Figure 4-8 Configure dynamic IP address

Wait a moment. When "Eth" is shown on the **Internet Status** page, you can access the Internet.

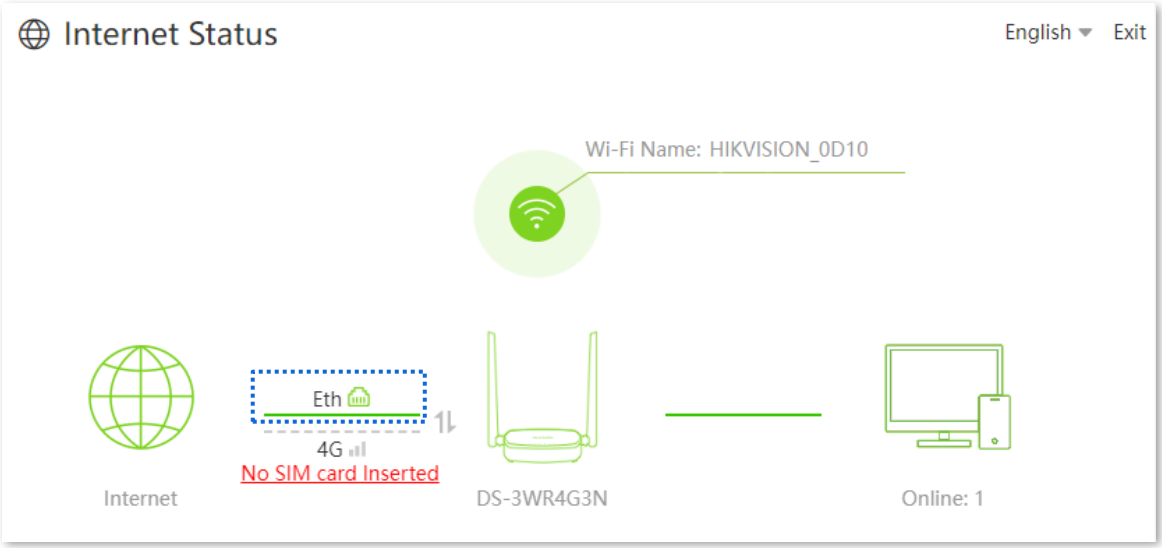


Figure 4-9 Dynamic IP connection succeeded

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

Table 4-3 Parameter description

Parameter	Description
Failover	Used to enable or disable the Failover function.
Connection Type	Specifies how your router connects to the Internet, including: ● **PPPoE**: Select this type if you access the Internet using the PPPoE user name and PPPoE password. ● **Dynamic IP**: Select this type if you can access the Internet by simply plugging in an Ethernet cable. ● **Static IP**: Select this type if you want to access the Internet using fixed IP information.

Parameter	Description
DNS Settings	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.
VLAN ID	Used to enable or disable the VLAN ID according to the actual network environments. When the function is enabled, the VLAN ID is required to enter. Consult your ISP for this parameter. The value range is 1 to 4094.

4.2.3 Use 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.

Procedure:

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

Step 2 Navigate to **Internet Settings**.

Step 3 Enable the **Failover** function.

Step 4 Set **Connection Type** to **Static IP Address**.

Step 5 Enter **IP Address**, **Subnet Mask**, **Default Gateway** and **Primary/Secondary DNS Server**.

Step 6 Click **Connect**.

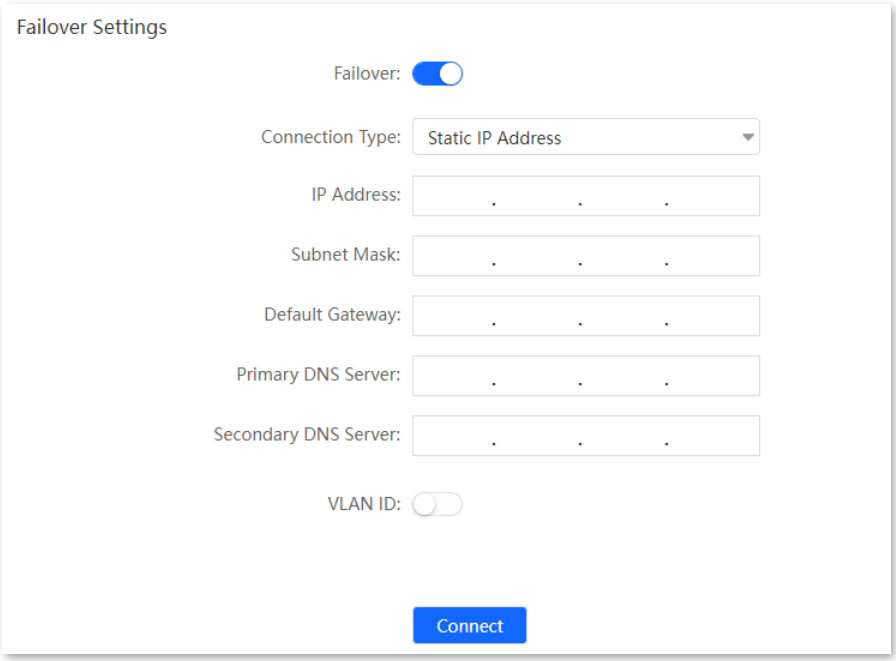


Figure 4-10 Configure static IP address information

Wait a moment. When “Eth ” is shown on the **Internet Status** page, you can access the Internet.

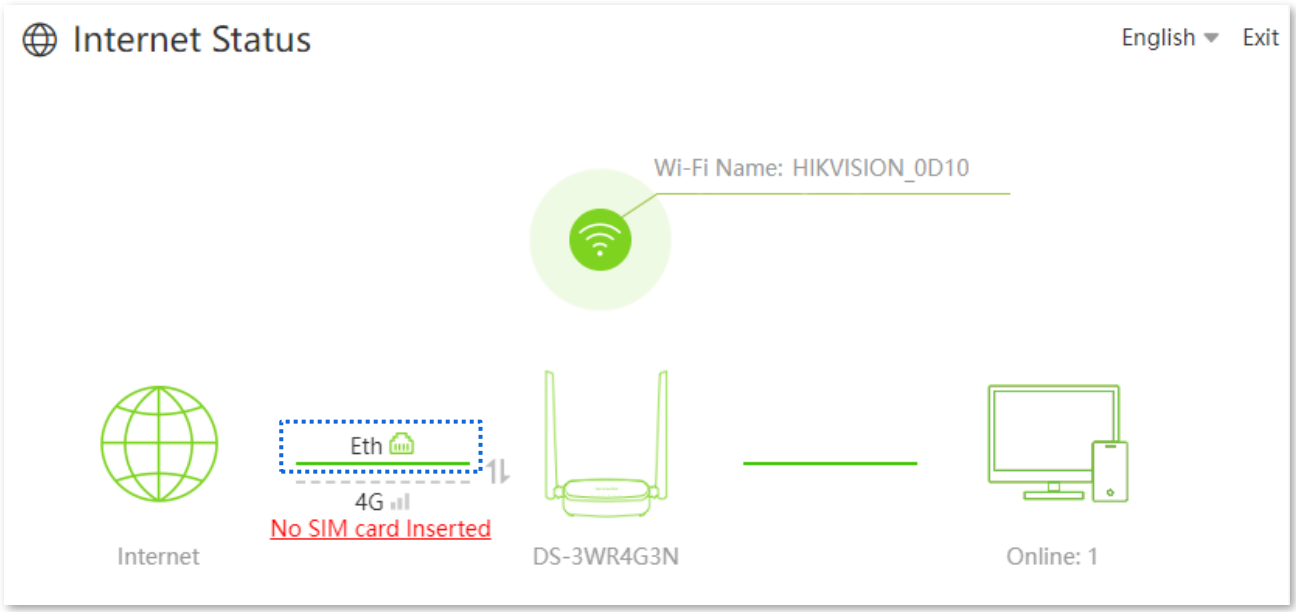


Figure 4-11 Static IP connection succeeded

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

Table 4-4 Parameter description

Parameter	Description
Failover	Used to enable or disable the Failover function.
Connection Type	Specifies how your router connects to the Internet, including: ● **PPPoE**: Select this type if you access the Internet using the PPPoE user name and PPPoE password. ● **Dynamic IP**: Select this type if you can access the Internet by simply plugging in an Ethernet cable. ● **Static IP**: Select this type if you want to access the Internet using fixed IP information.
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	
VLAN ID	Used to enable or disable the VLAN ID according to the actual network environments. When the function is enabled, the VLAN ID is required to enter. Consult your ISP for this parameter. The value range is 1 to 4094.

4.3 Set Failover connection

4.3.1 Overview

By configuring the Failover function, you can set parameters of the Internet connection mode other than the current one. If there is a network failure, the router will automatically switch to an available Internet connection mode, 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 enter the page, log in to the web UI of the router, navigate to **Internet Settings**, and locate the **Failover Settings** part. This function is disabled by default.

When the Failover function is enabled, the page is shown as below. You can configure the Failover connection by referring to Access the Internet through the WAN port.

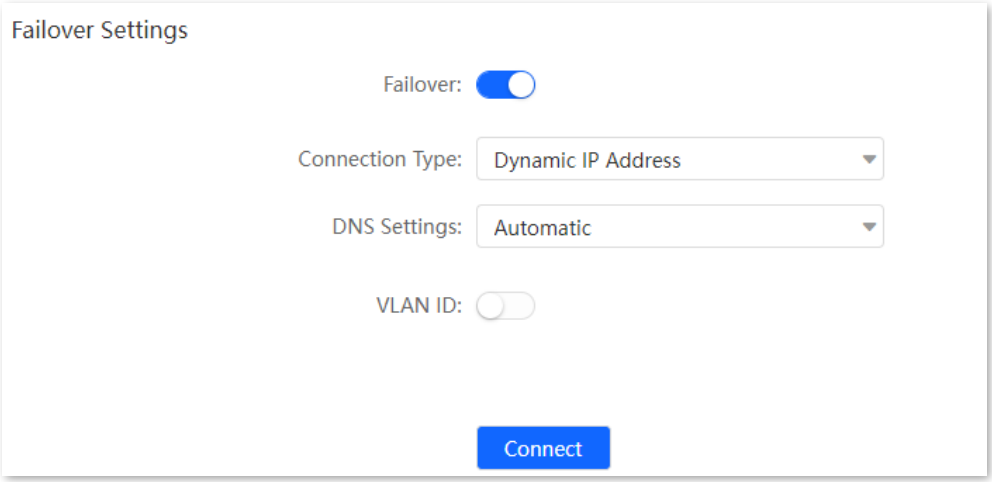


Figure 4-12 Failover settings

4.3.2 Example of setting 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.

Requirements: 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.

Procedures:

Step 1 Connect the WAN/LAN port of the router to the LAN port of your smart home gateway.

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

Step 3 Navigate to **Internet Settings**.

Step 4 Enable the **Failover** function.

Step 5 Set **Connection Type** to **PPPoE**, and enter the **PPPoE Username** and **PPPoE Password** provided by your ISP.

Step 6 Click **Connect**.

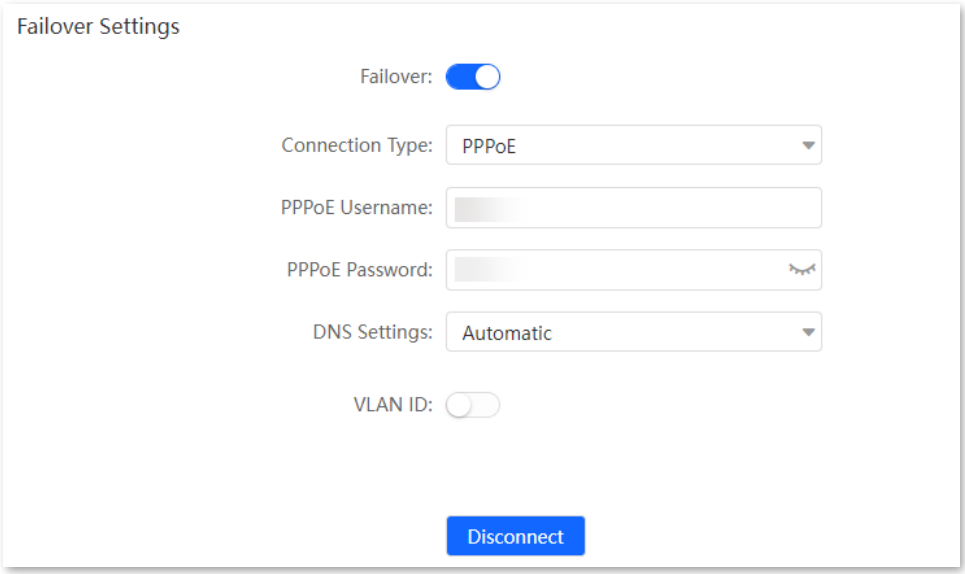


Figure 4-13 Configure Failover settings

When the figure is shown below on the **Internet Status** page, the router is connected to the Internet successfully and you can enjoy uninterrupted Internet access guaranteed by both the broadband and SIM card.

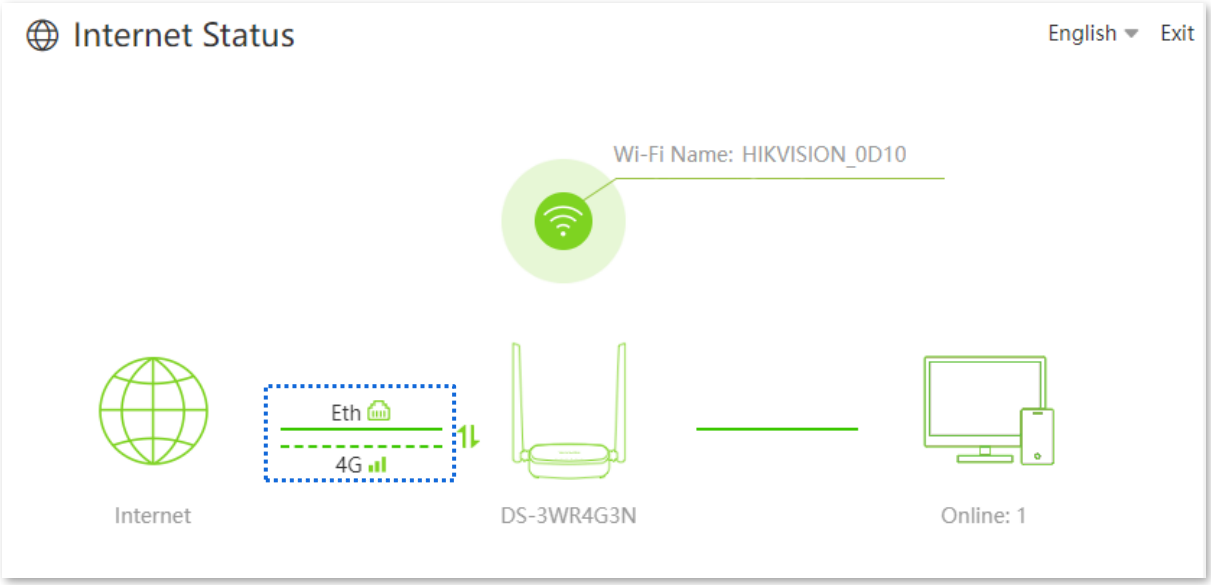


Figure 4-14 Access the Internet through the broadband and SIM card

Chapter 5 Wi-Fi settings

5.1 Wi-Fi name & password

5.1.1 Overview

To enter the page, log in to the web UI of the router, and navigate to **Wi-Fi Settings** > **Wi-Fi Name & Password**.

You can configure basic Wi-Fi parameters, such as the Wi-Fi name and password.

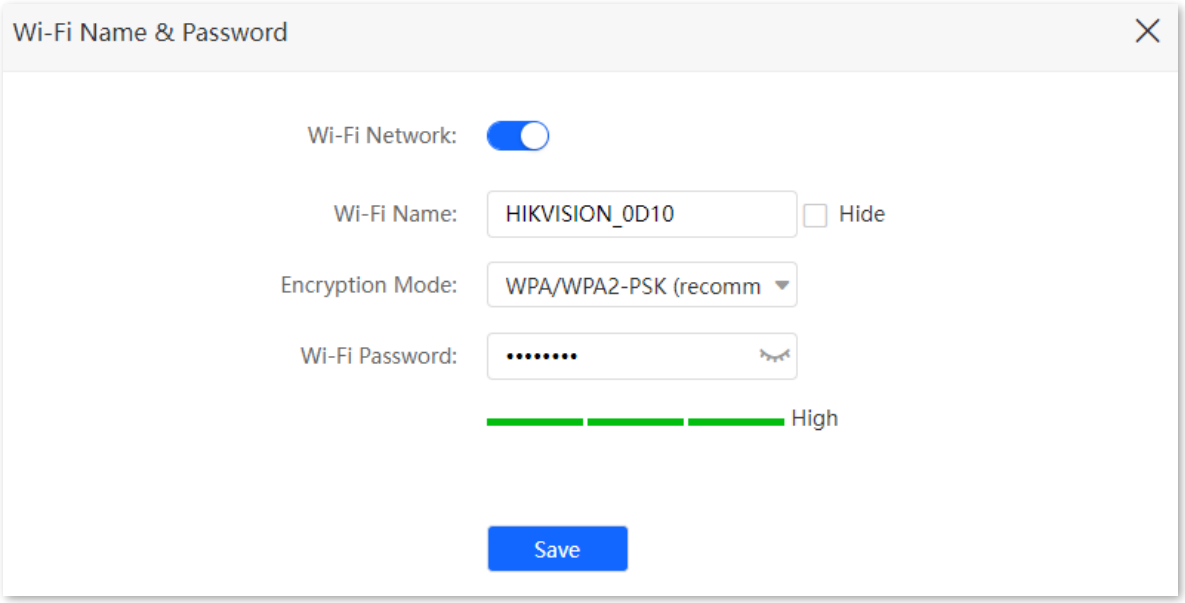


Figure 5-1 Wi-Fi name & password

Table 5-1 Parameter description

Parameter	Description
Wi-Fi network	Used to enable or disable the Wi-Fi network of the router.
Wi-Fi Name	Specifies the Wi-Fi network name (SSID) of the Wi-Fi network.
Hide	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.

Parameter	Description
Encryption Mode	Specifies the encryption modes supported by the router, including: • **None**: 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)**: WPA-PSK and WPA2-PSK are adopted to encrypt the network, providing both security and compatibility.
Wi-Fi Password	Specifies the password for connecting to the Wi-Fi network. You are strongly recommended to set a Wi-Fi password for security. **Note** For initial setup or after a reset, set new Wi-Fi password for privacy and security (The longer the password, the stronger the protection). The character limit and composition rules for passwords are subject to software user interface prompts.

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

Assume that you want to change the 2.4 GHz Wi-Fi name and password to **John_Doe_2.4GHz** and **Hikvision+WiFi24**. And **WPA/WPA2-PSK (recommended)** is set to the encryption mode.

Procedure:

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

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

Step 3 Change the parameters of the Wi-Fi network.

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

Step 4 Click **Save**.

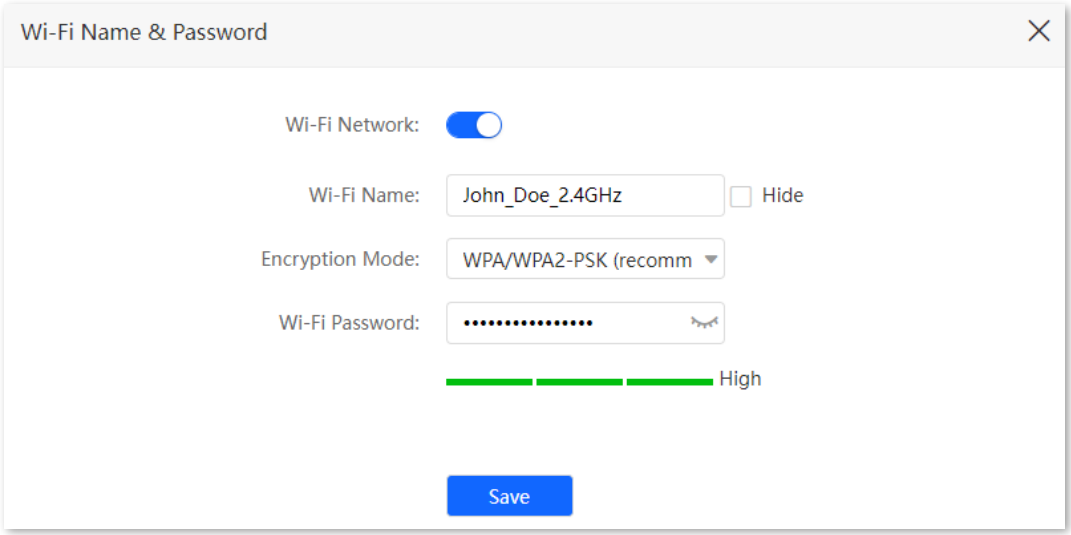


Figure 5-2 Change Wi-Fi name and password

After the configuration is completed, you can connect your wireless devices to the Wi-Fi network of the router to access the Internet.

5.1.3 Hide the Wi-Fi network

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

Procedure:

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

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

Step 3 Tick **Hide**.

Step 4 Click **Save**.

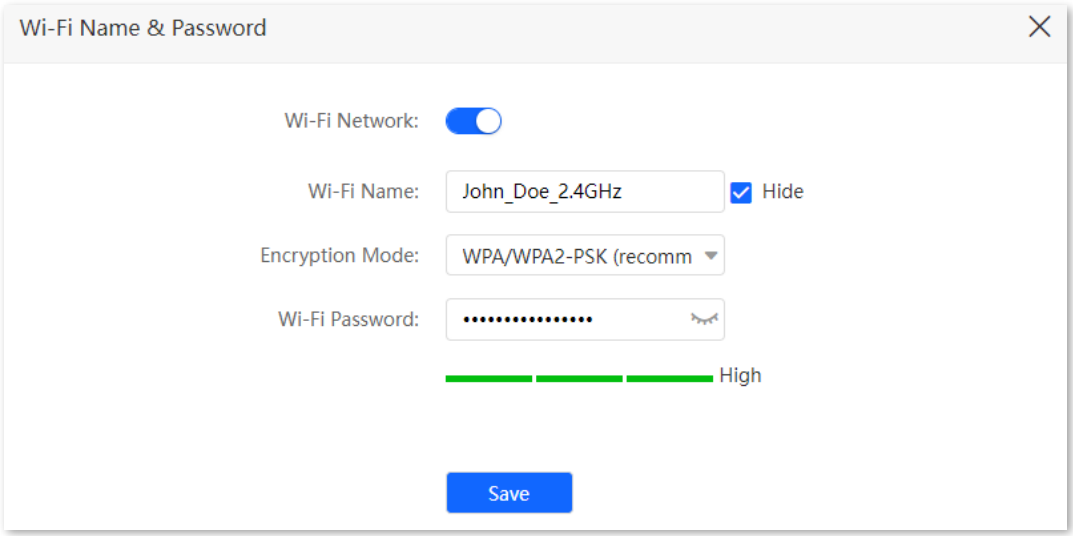


Figure 5-3 Hide the Wi-Fi network

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

5.1.4 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 parameters are:

- Wi-Fi name: Jone_Doe
- Encryption type: WPA/WPA2-PSK (recommended)
- Wi-Fi password: Hikvision+WiFi24

Note

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

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

Step 1 Tap **Settings** on your phone, and tap **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+WiFi24** in this example.

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

Step 6 Tap **Join**.

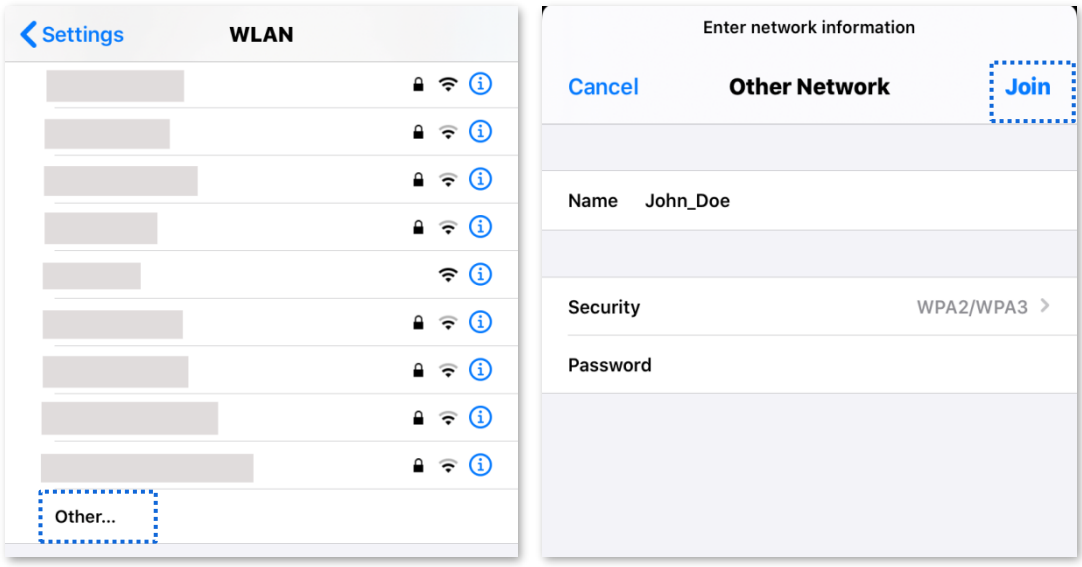


Figure 5-4 Connect to a hidden Wi-Fi network

After the configuration is completed, you can connect to the hidden Wi-Fi network to access the Internet.

5.2 Channel & bandwidth

In this section, you can change the wireless channel and wireless bandwidth of the Wi-Fi network.

To enter the page, log in to the web UI of the router, and navigate to **Wi-Fi Settings** > **Channel & Bandwidth**.

Note

To ensure the wireless performance, it is recommended to maintain the default settings without professional instructions.

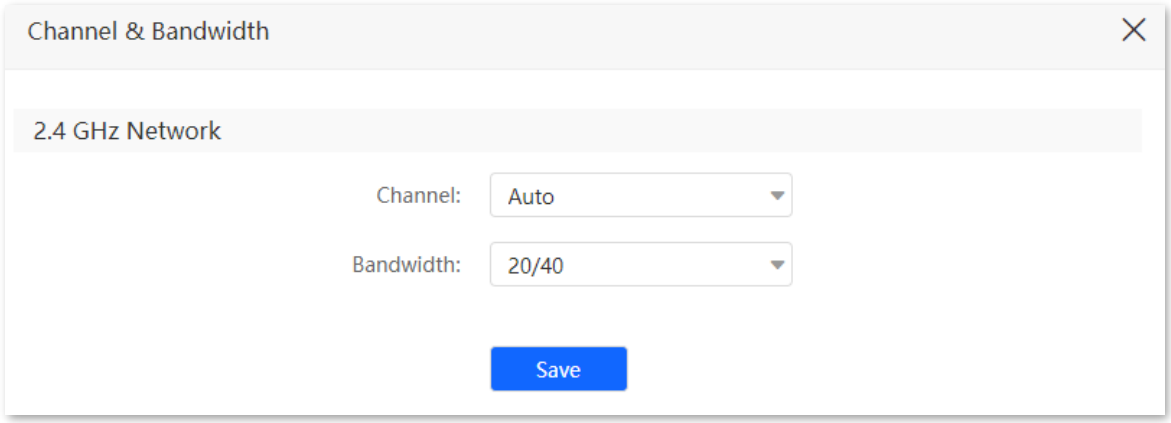


Figure 5-5 Configure channel & bandwidth

Table 5-2 Parameter description

Parameter	Description
Channel	Specifies the channel of the Wi-Fi network. 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	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.

5.3 WPS

5.3.1 Overview

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

To enter the page, log in to the web UI of the router, and navigate to **Wi-Fi Settings** > **WPS**.

Note

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

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

Step 1 Find the **WPS/RST** 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 smartphone.
2) Tap **WLAN**.
3) Tap ⋮, and choose **WLAN settings**.

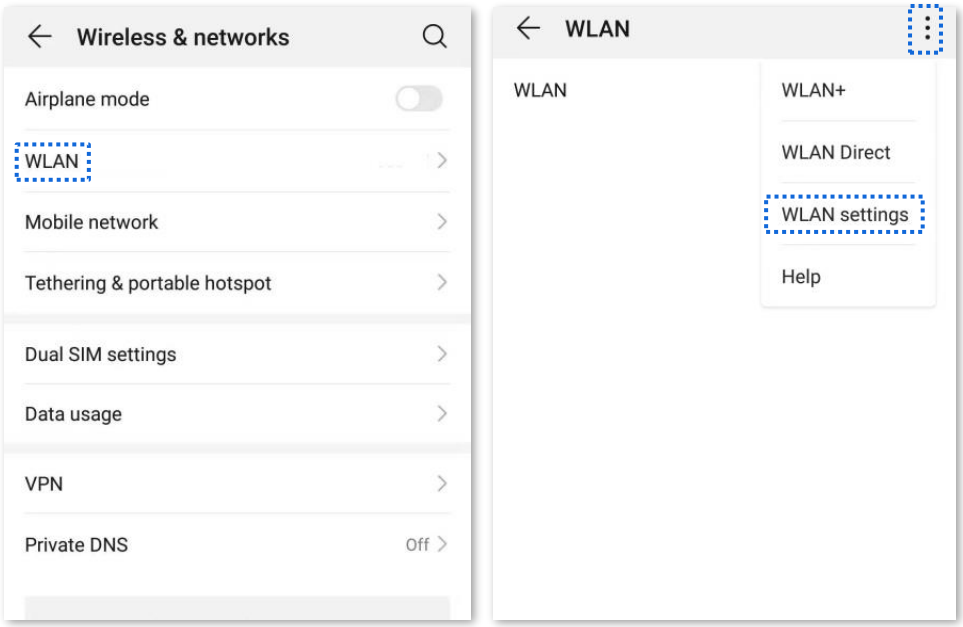


Figure 5-6 Configure WLAN settings

4) Tap **WPS connection**.

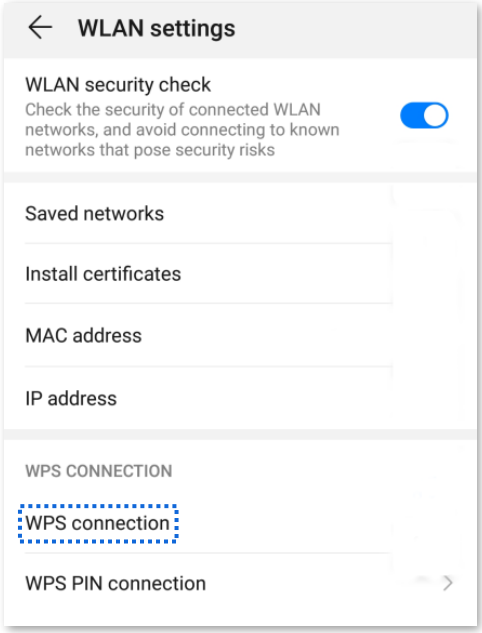


Figure 5-7 Tap WPS connection

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

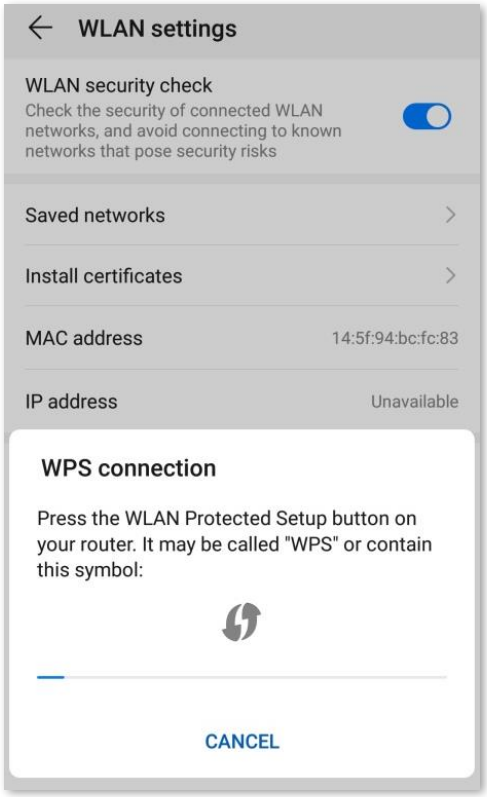


Figure 5-8 Perform WPS negotiation

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

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

Step 2 Navigate to **Wi-Fi Settings** > **WPS**.

Step 3 Enable **WPS**.

Step 4 Click Click Here.

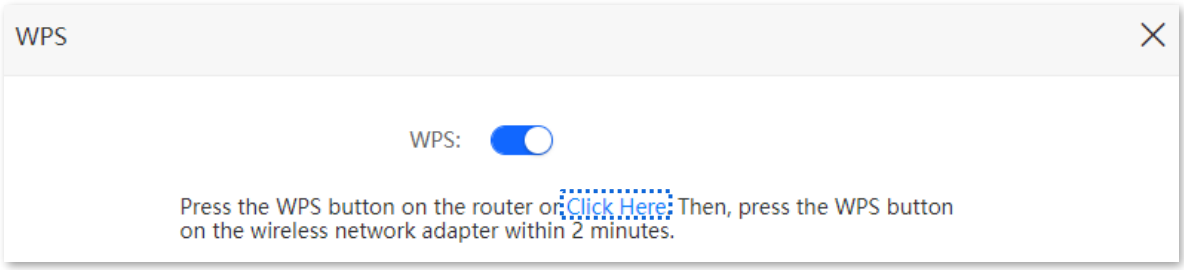


Figure 5-9 Enable WPS

Step 5 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 smartphone.
2) Tap **WLAN**.
3) Tap ⋮, and choose **WLAN settings**.

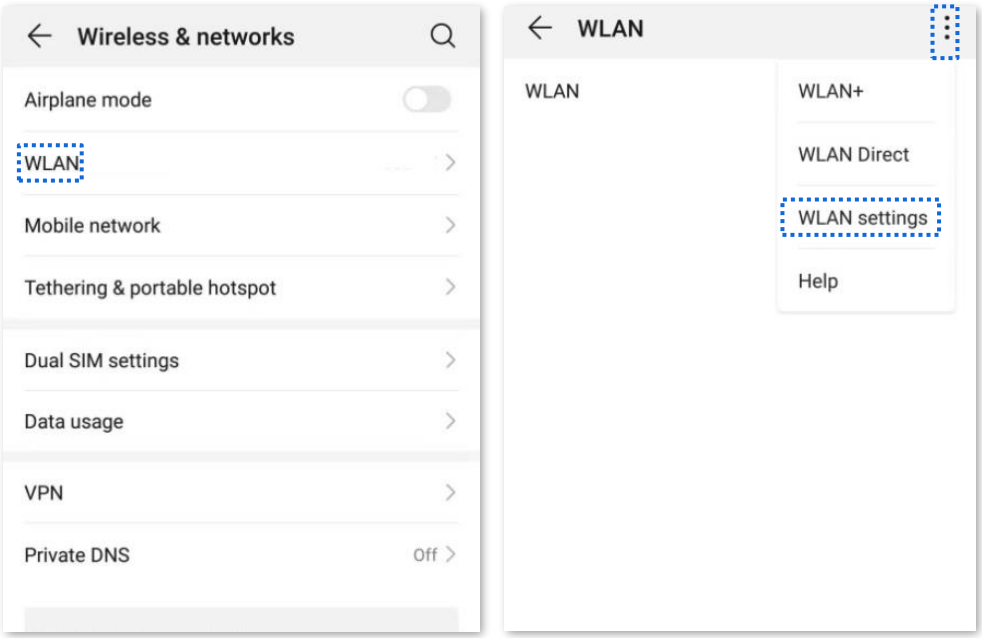


Figure 5-10 Configure WLAN settings

4) Tap **WPS connection**.

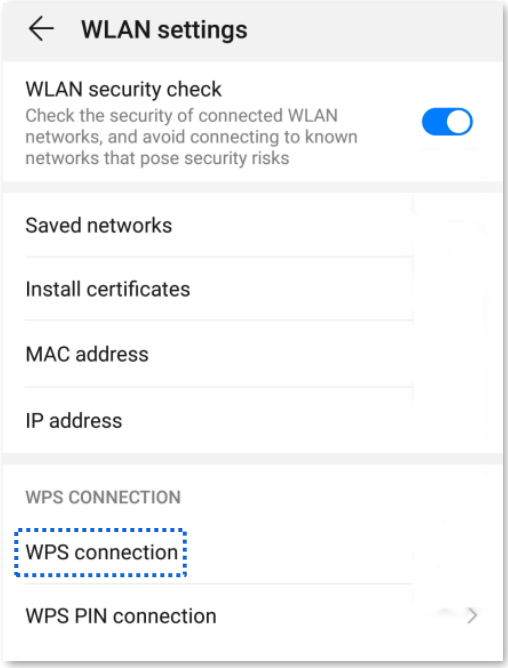


Figure 5-11 Tap WPS connection

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

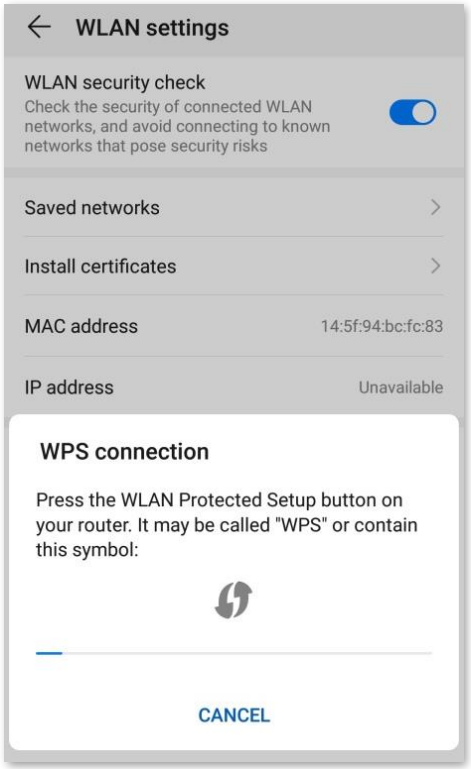


Figure 5-12 Perform WPS negotiation

Chapter 6 SMS

6.1 Manage SMS messages

This router can send, receive, delete and export SMS messages on the web UI of the router.

To enter the page, log in to the web UI of the router, and navigate to **SMS** > **Messages**.

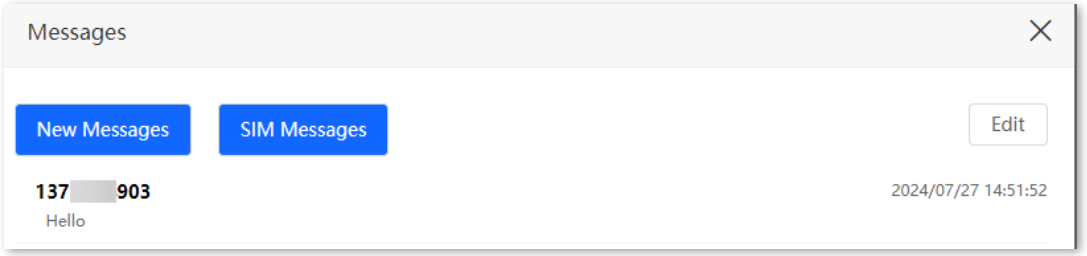


Figure 6-1 Manage SMS messages

6.1.1 Send SMS messages

Send messages to a new smartphone number

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

Step 2 Navigate to **SMS** > **Messages**.

Step 3 Click **New Messages**.

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

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

Step 6 Click **Send** in the lower right corner.

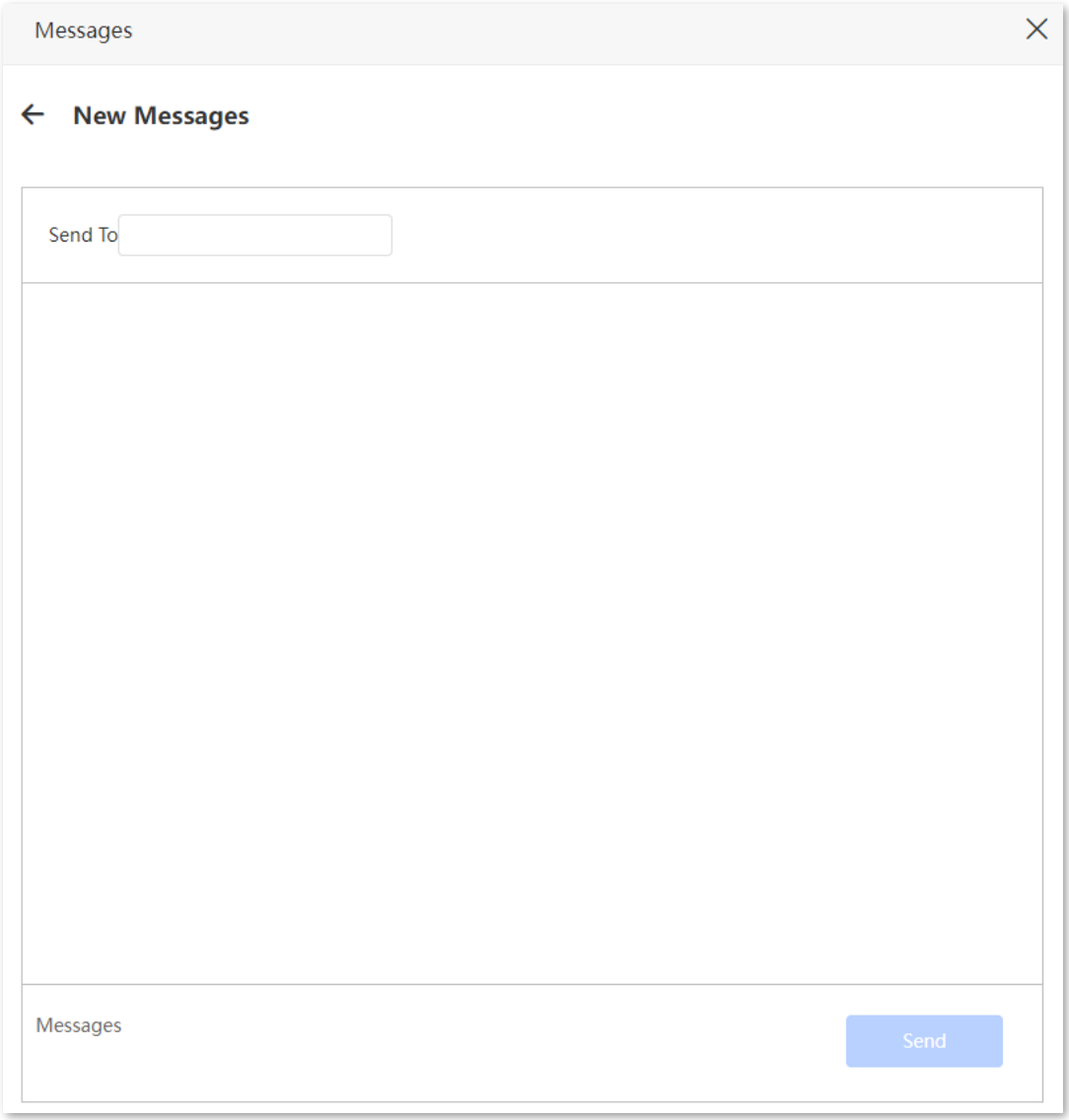


Figure 6-2 Send messages to a new smartphone number

Send messages to an existing smartphone number

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

Step 2 Navigate to **SMS** > **Messages**.

Step 3 Click the targeted smartphone number.

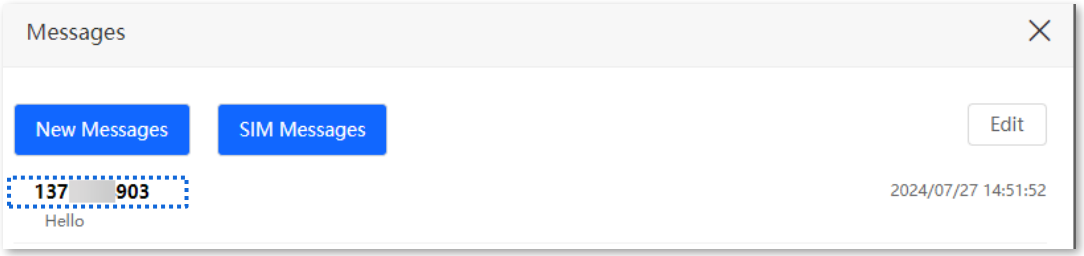


Figure 6-3 Locate the smartphone number to send messages

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

Step 5 Click **Send**.

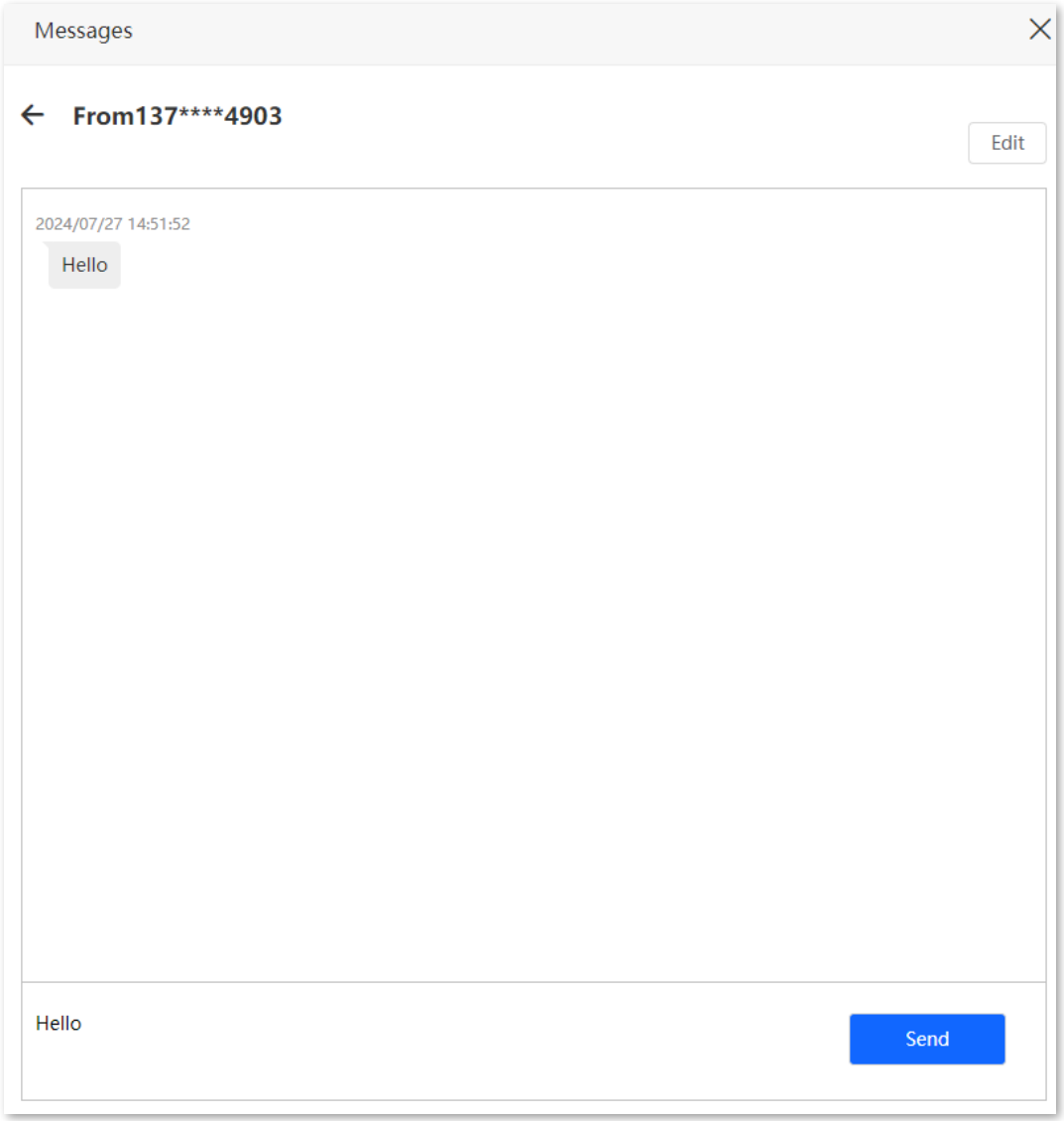


Figure 6-4 Enter the message content

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

6.1.2 Delete SMS messages

Delete all messages of the same smartphone number

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

Step 2 Navigate to **SMS** > **Messages**.

Step 3 Click **Edit** in the upper right corner.

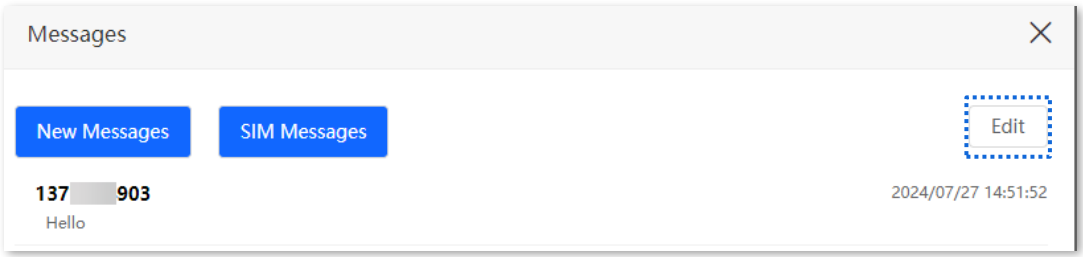


Figure 6-5 Manage messages

Step 4 Select the smartphone number to be deleted.

Step 5 Click .

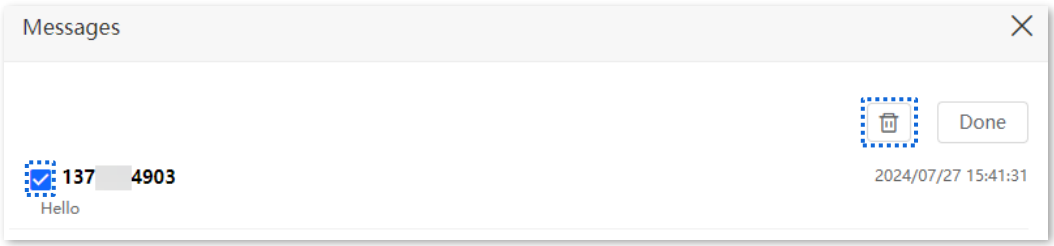


Figure 6-6 Select the smartphone number to delete messages

Delete certain messages of the same smartphone number

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

Step 2 Navigate to **SMS** > **Messages**.

Step 3 Click the targeted smartphone number.

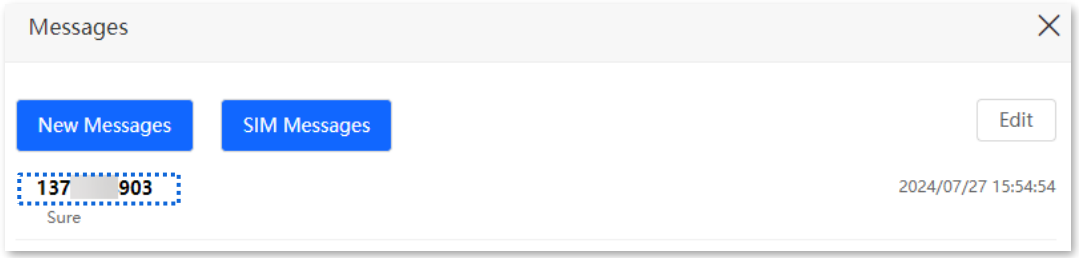


Figure 6-7 Locate the smartphone number to delete messages

Step 4 Click **Edit**.

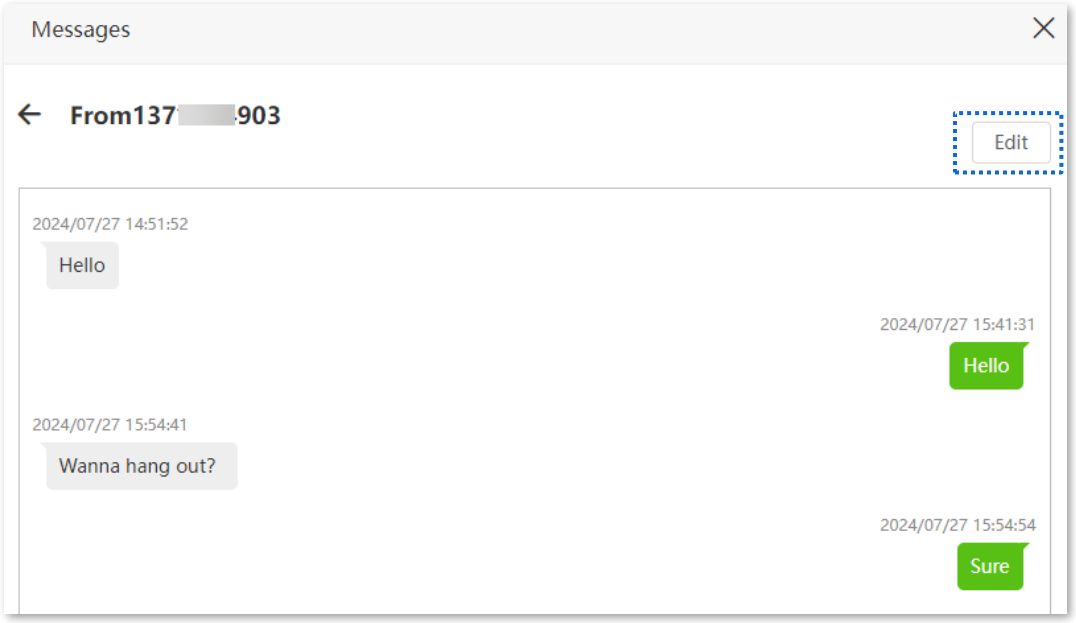


Figure 6-8 Manage messages

Step 5 Select the messages to be deleted.

Step 6 Click .

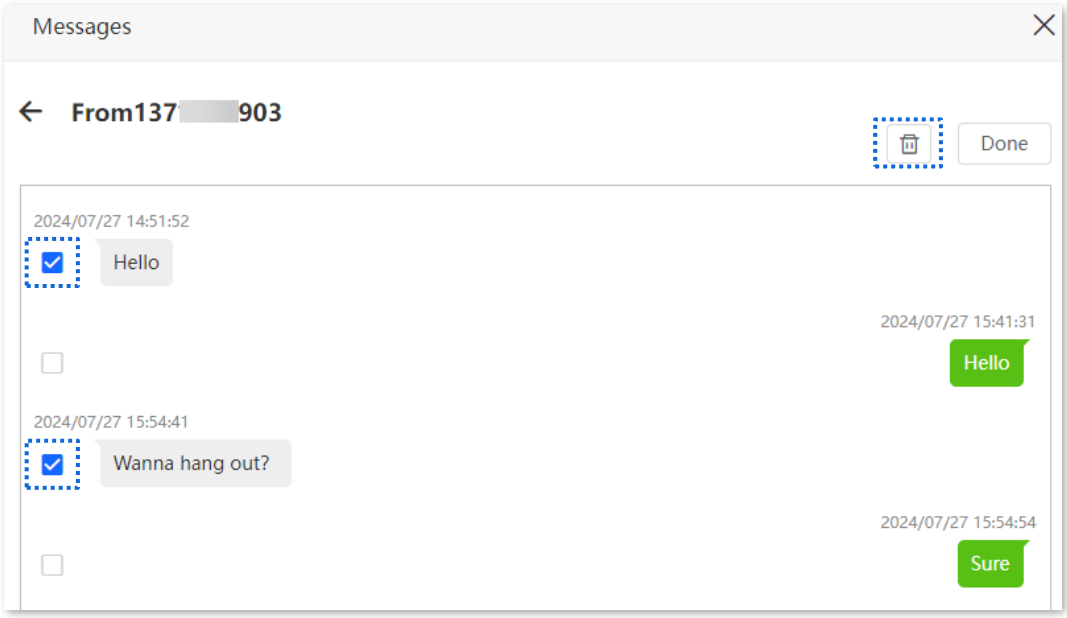


Figure 6-9 Delete messages to be selected

Delete certain messages of the SIM card

Note

This function is available only when SIM messages are stored in the SIM card.

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

Step 2 Navigate to **SMS** > **Messages**.

Step 3 Click **SIM Messages**.

Step 4 Click **Edit** in the upper right corner.

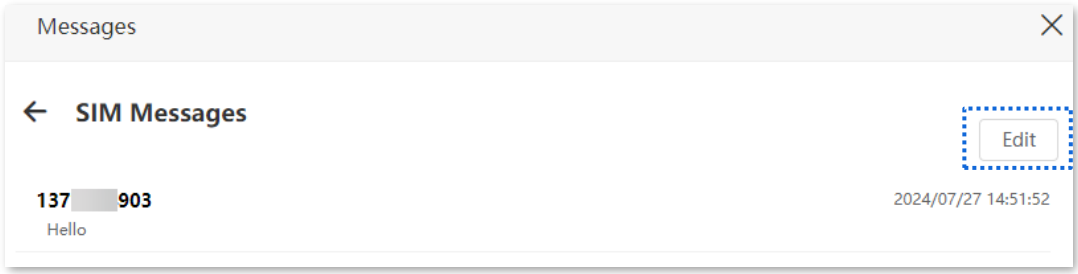


Figure 6-10 Manage messages

Step 5 Select the smartphone number to be deleted.

Step 6 Click .

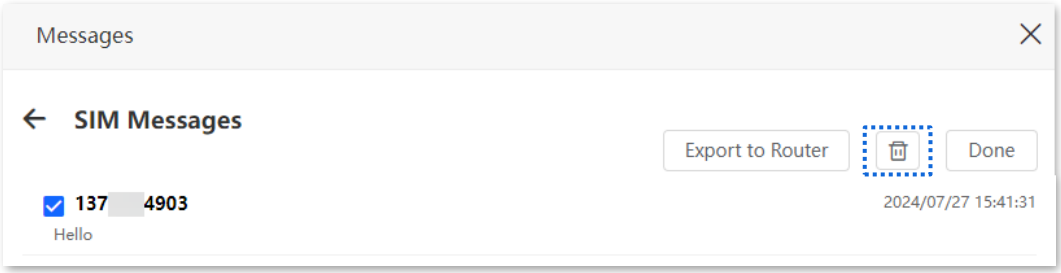


Figure 6-11 Delete messages of the SIM card

Export SMS messages

For wireless devices (such as smartphones), SMS messages can be stored on the SIM card. When the SIM card is inserted into the router, you can export messages in the SIM card to the router to view them on the web UI of the router.

Procedure:

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

Step 2 Navigate to **SMS** > **Messages**.

Step 3 Click **SIM Messages**.

Step 4 Click **Edit** in the upper right corner.

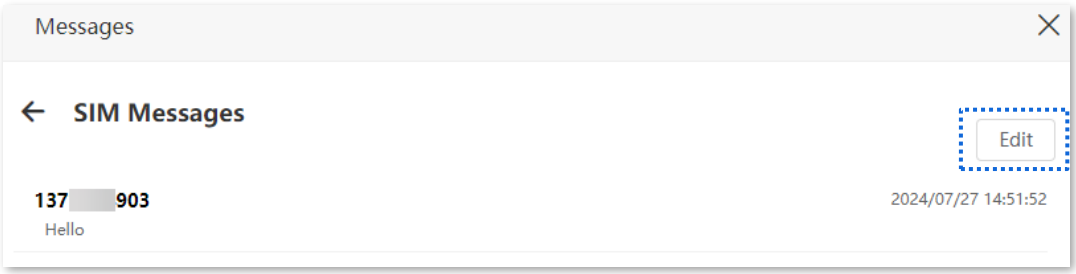


Figure 6-12 Manage messages

Step 5 Select the smartphone number to export messages.

Step 6 Click **Export to Router**.

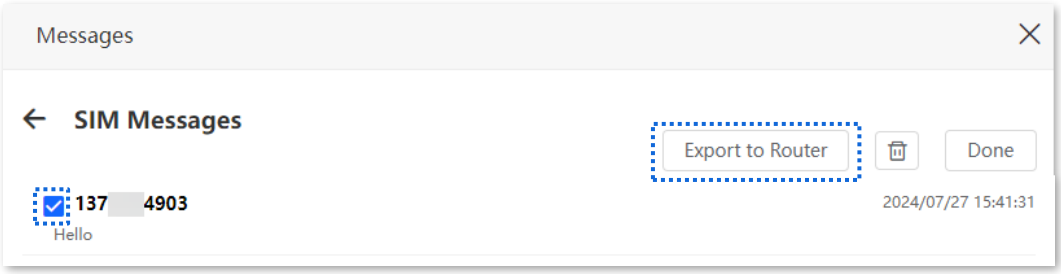


Figure 6-13 Export messages to the router

After the messages are exported, you can view them on the **Messages** page.

6.2 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 on the web UI of the router if it is wrong.

Procedure:

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

Step 2 Navigate to **SMS** > **Messages Settings**.

Step 3 Enable **Messages Settings**.

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

Step 5 Click **Save**.

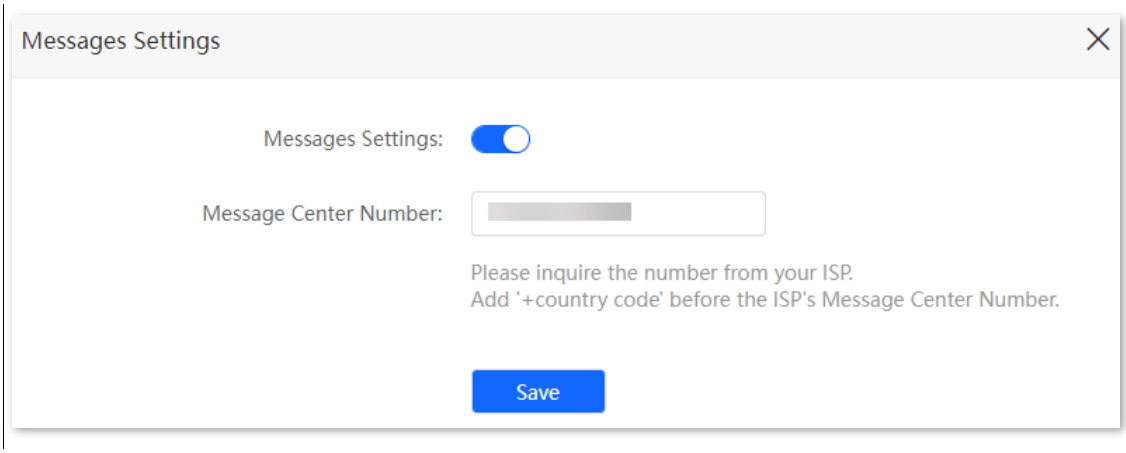


Figure 6-14 Set the message center number

After the configuration is completed, you can send SMS messages with a correct message center number.

6.3 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.

Procedure:

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

Step 2 Navigate to **SMS** > **USSD**.

Step 3 Set the **USSD CMD**, which is ***108#** in this example.

Step 4 Click **Send**.

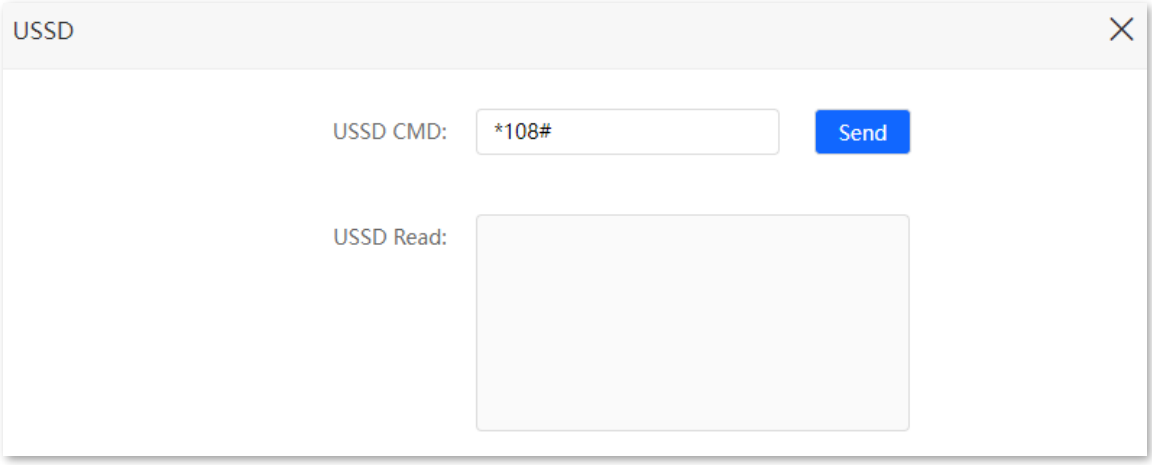


Figure 6-15 Inquire information by sending USSD commands

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

Chapter 7 VPN

A Virtual Private Network (VPN) 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.

Figure 7-1 VPN network typology

7.1 PPTP server

7.1.1 Overview

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

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

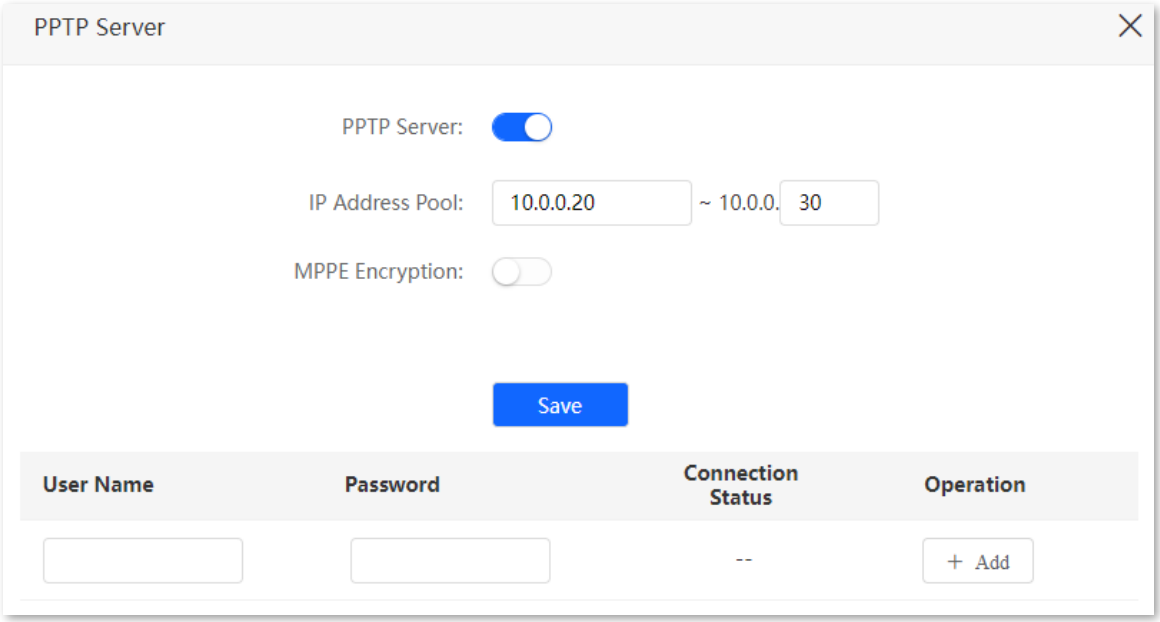


Figure 7-2 Enable PPTP server

Table 7-1 Parameter description

Parameter	Description
PPTP Server	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.
IP Address Pool	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	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	Specify the VPN user name and password, which the VPN user needs to enter when making PPTP dial-ups (VPN connections).
Password	
Connection Status	Specifies the connection status of the VPN connection.
Operation	Available operations include: + Add : Used to add new PPTP user accounts. : Used to disable the PPTP user account. : Used to enable the PPTP user account. : Used to delete the PPTP user account.

7.1.2 Enable Internet users to access resources of the LAN

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

Requirements: 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 requirements. 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

Ensure that the 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. 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.

Procedure:

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

Step 2 Enable the PPTP server function.

1) Navigate to **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**.

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**.

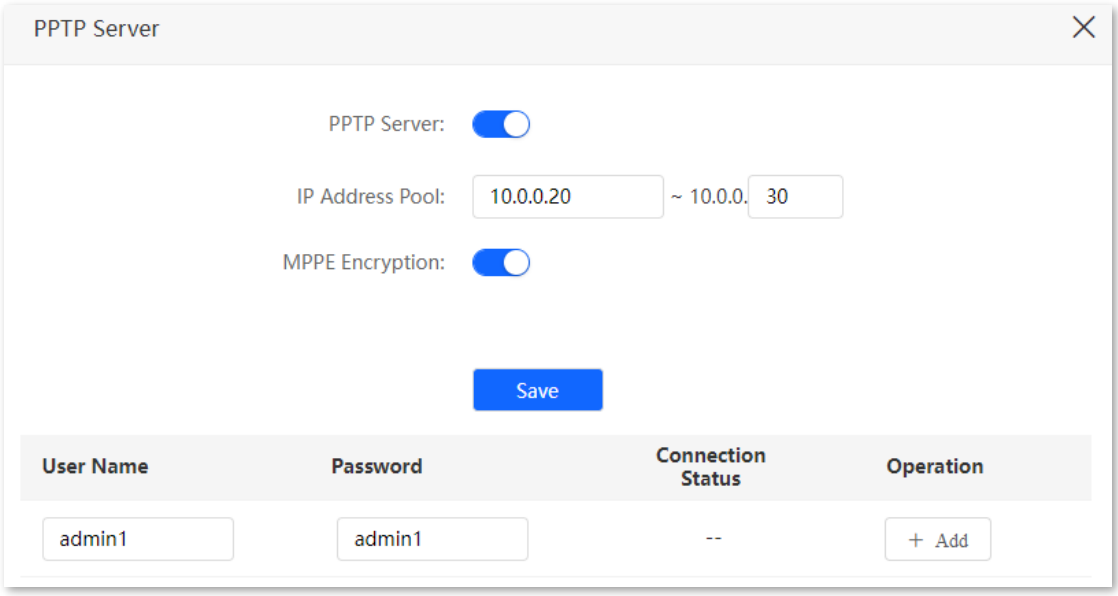


Figure 7-3 Configure PPTP server

After the configuration is completed, Internet users can access the FTP server by following these steps (Example: Windows 10).

Step 1 Click in the lower right corner of the desktop and choose **Network & Internet settings**.

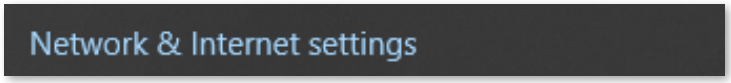


Figure 7-4 Choose Network & Internet settings

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

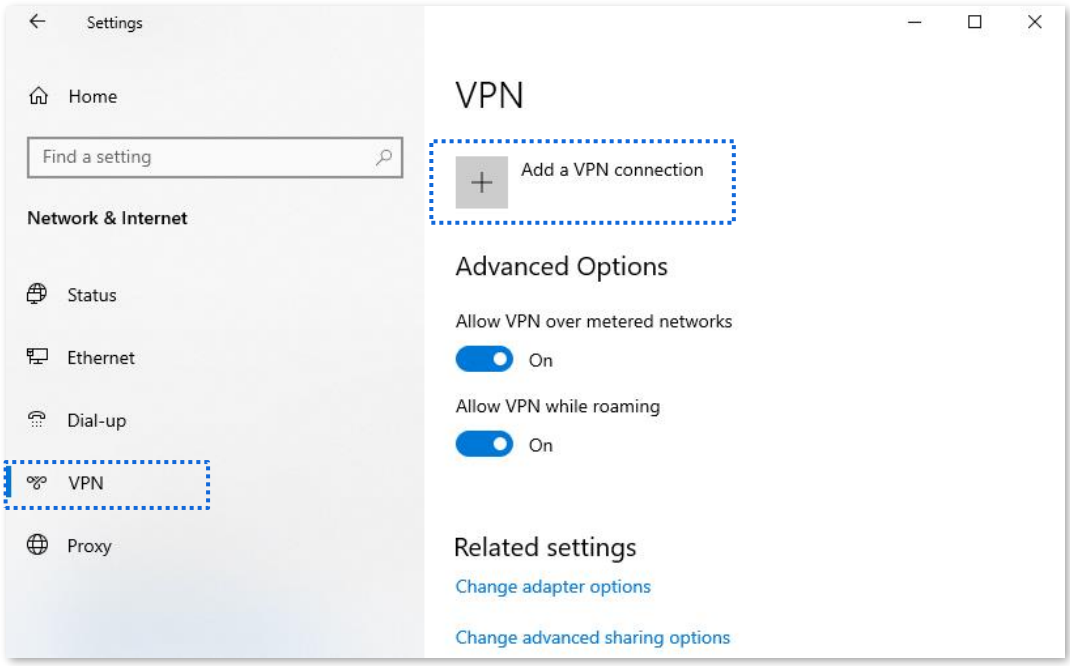


Figure 7-5 Add VPN connection

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**.

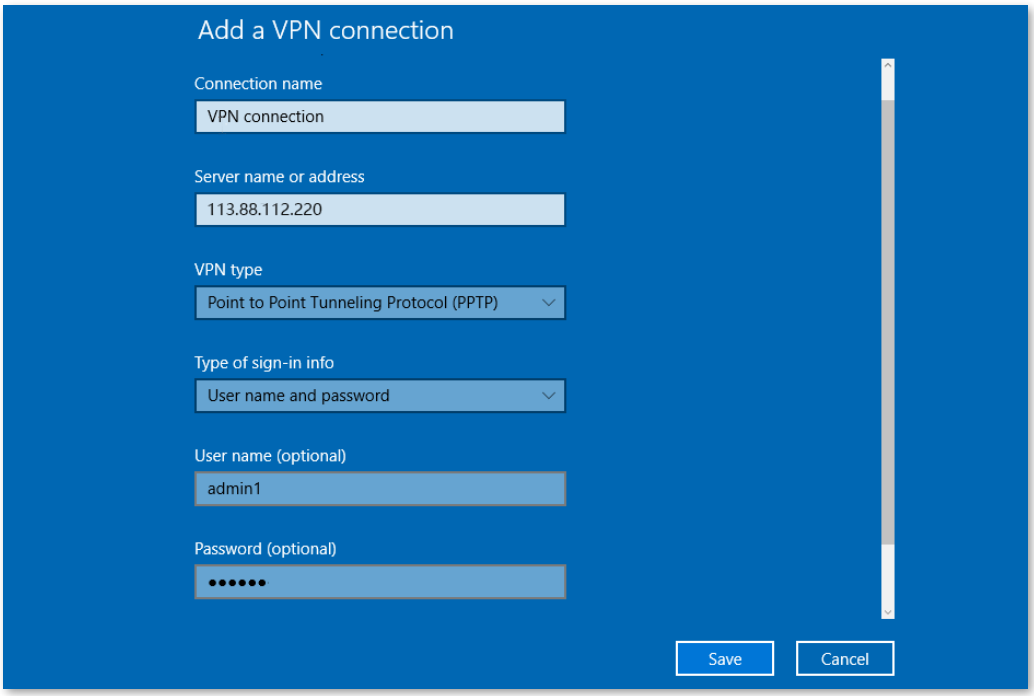


Figure 7-6 Configure VPN parameters

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

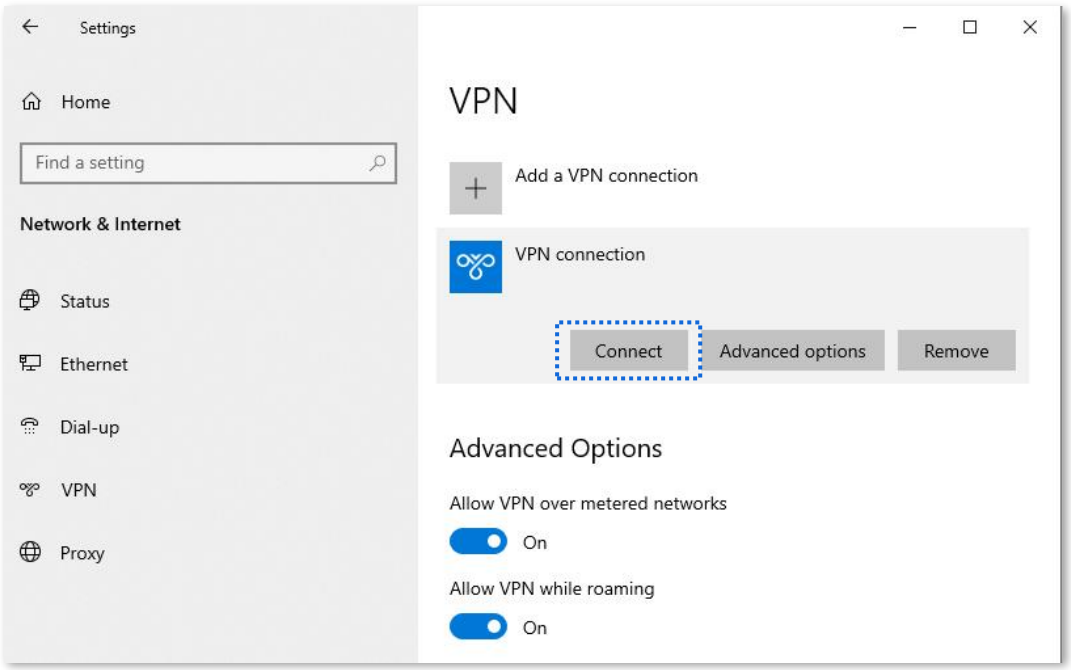


Figure 7-7 Connect the VPN connection

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.

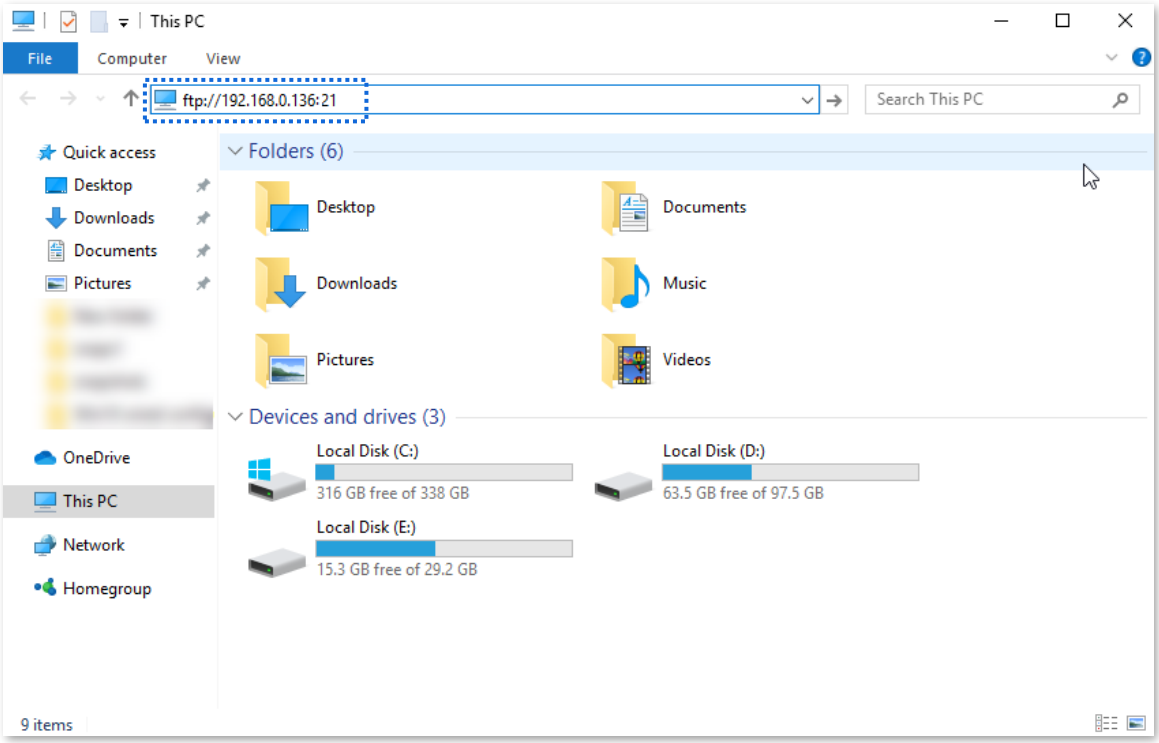


Figure 7-8 Access the FTP server

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**.

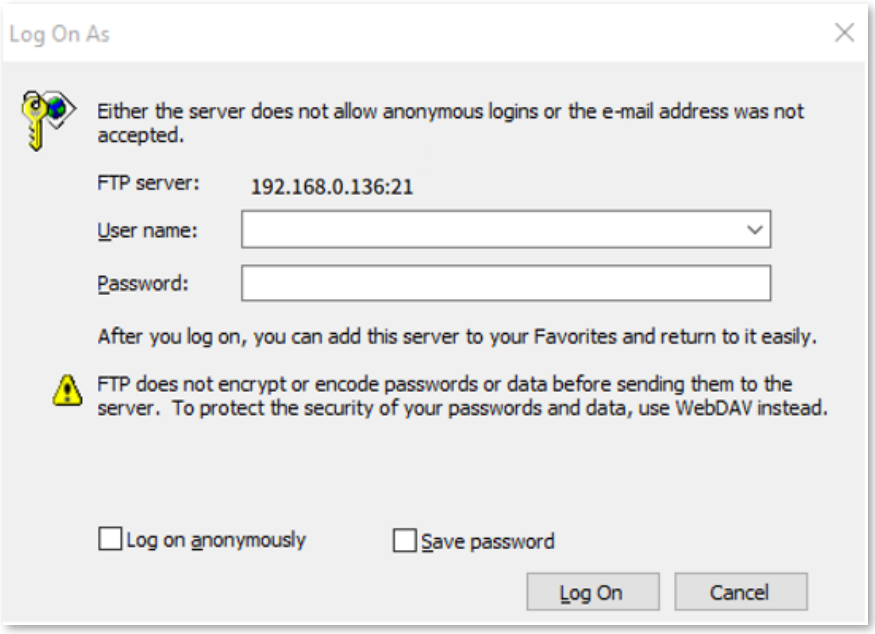


Figure 7-9 Enter the user name and password

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

7.2 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 enter the page, log in to the web UI of the router, and navigate to **VPN** > **Online PPTP Users**.

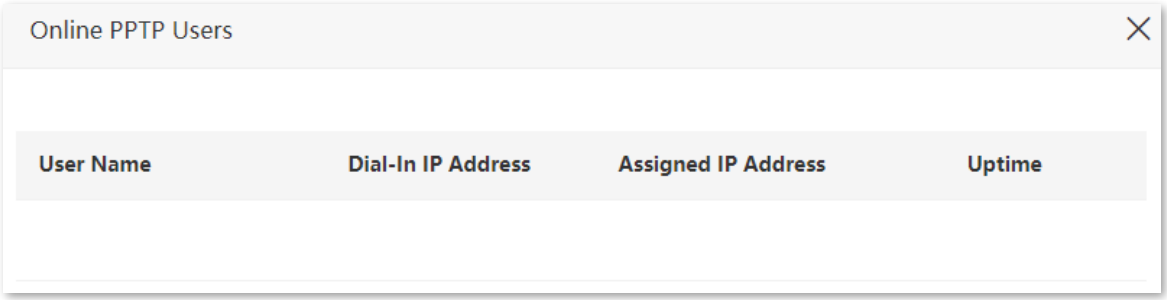


Figure 7-10 View VPN clients

Table 7-2 Parameter description

Parameter	Description
User Name	Specifies the VPN user name, which the VPN user uses when making PPTP dial-ups (VPN connection).
Dial-In IP Address	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	Specifies the IP address that the PPTP server assigns to the client.
Uptime	Specifies the online time since the VPN connection succeeds.

7.3 PPTP/L2TP client

7.3.1 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.

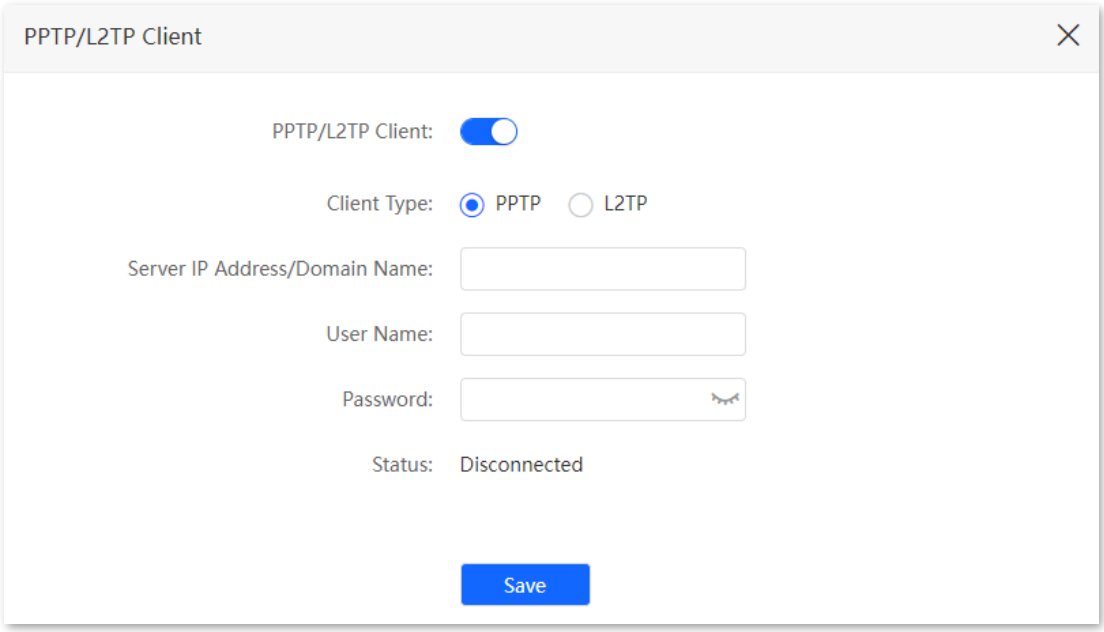


Figure 7-11 Enable PPTP/L2TP client

Table 7-3 Parameter description

Parameter	Description
PPTP/L2TP Client	Used to enable or disable the PPTP/L2TP client function.
Client Type	Specifies the client type that the router serves as. ● **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	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	Specify the user name and password that the PPTP/L2TP server assigns to the PPTP/L2TP clients.
Password	
Status	Specifies the connection status of the VPN connection.

7.3.2 Access VPN resources with the router

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

Requirements: Access the VPN resources of your ISP.

Solution: You can configure the PPTP/L2TP client function to reach the requirements. 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.

Procedure:

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

Step 2 Navigate to **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**.

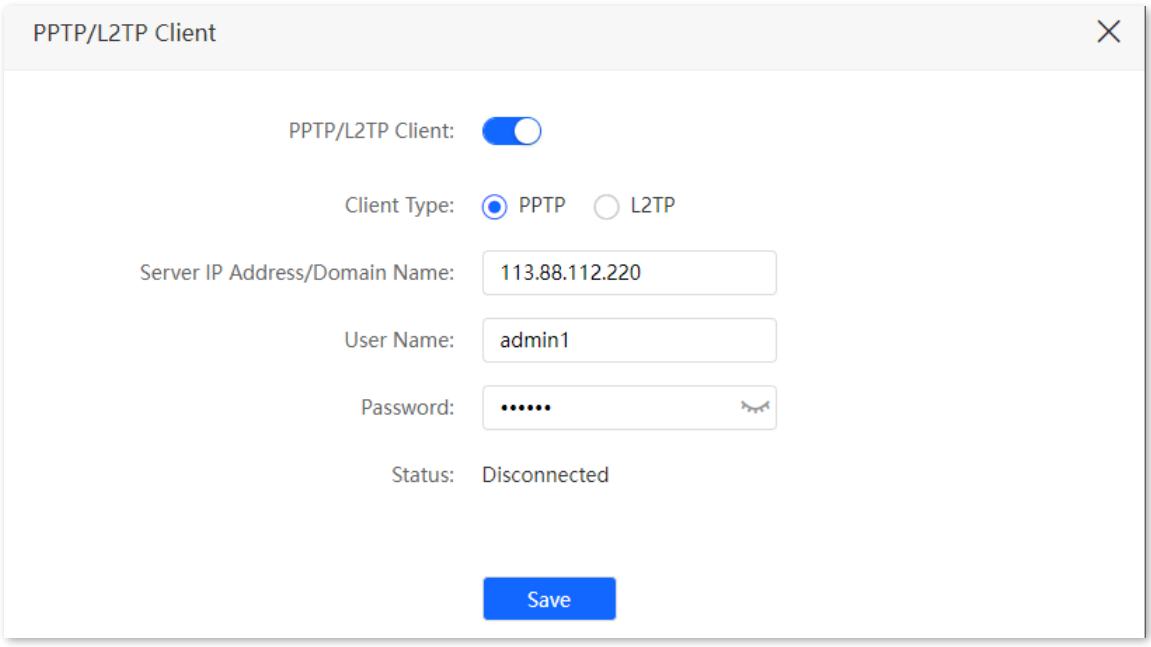


Figure 7-12 Configure PPTP/L2TP client

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

Chapter 8 Parental control

8.1 Overview

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

To enter the page, log in to the web UI of the router, and navigate to **Parental Control**.

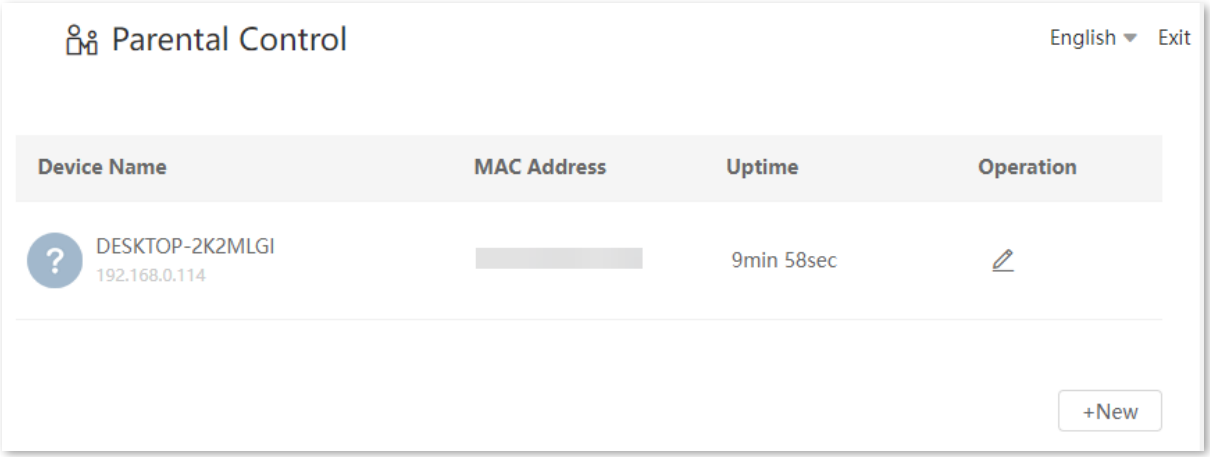


Figure 8-1 Parental control

Table 8-1 Parameter description

Parameter	Description
Device Name	Specifies the name of the online device.
MAC Address	Specifies the MAC address of the online device.
Uptime	Specifies the online duration of the device.
Operation	Available operations include: : Used to configure a parental control rule for the device. : Used to enable the configured rule. : Used 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.

8.2 Configure the parental control rule

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

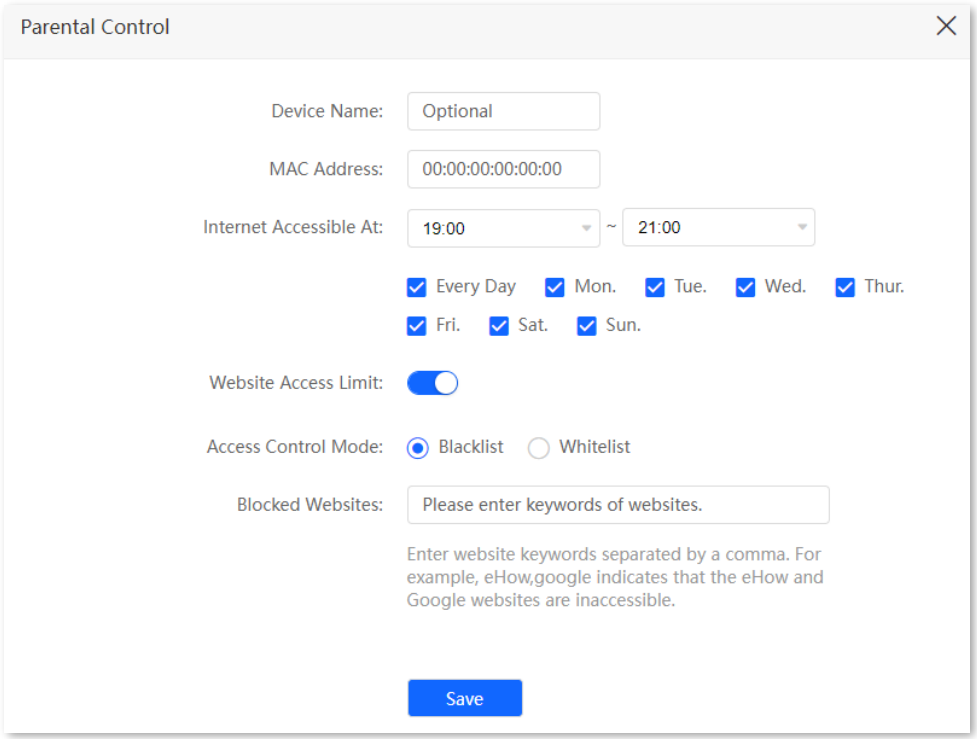


Figure 8-2 Add a parental control rule

Table 8-2 Parameter description

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

Parameter	Description
Blocked Websites	Specify the websites that the device is blocked from accessing or allowed to access during the specified period.
Unblocked Websites	

8.3 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.

Requirements: You want to allow Internet access during 8:00 to 22:00 on weekends for your kid's PC, while blocking Facebook, Twitter, YouTube and Instagram websites.

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

Procedure:

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

Step 2 Navigate to **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.

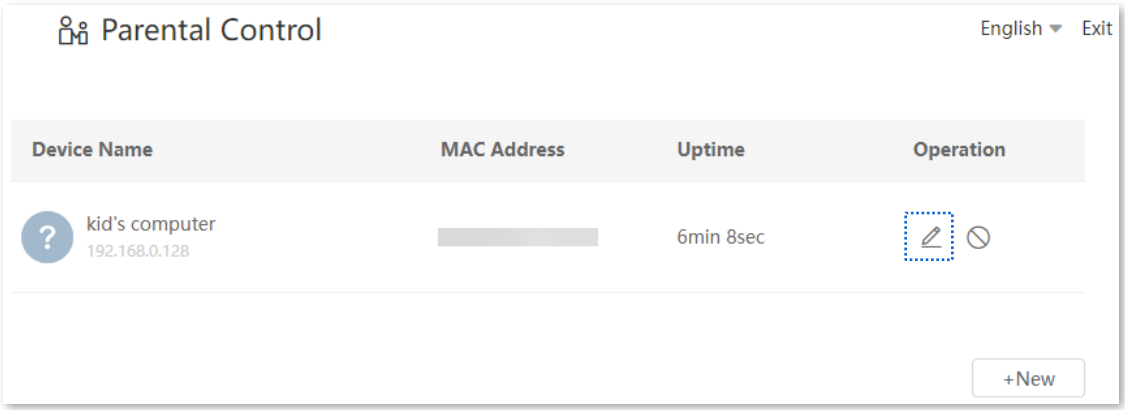


Figure 8-3 Edit the parental control rule

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 select **Blacklist**.
5) Set **Blocked Websites**, which is **Facebook,Twitter,YouTube,Instagram** in this example.
6) Click **Save**.

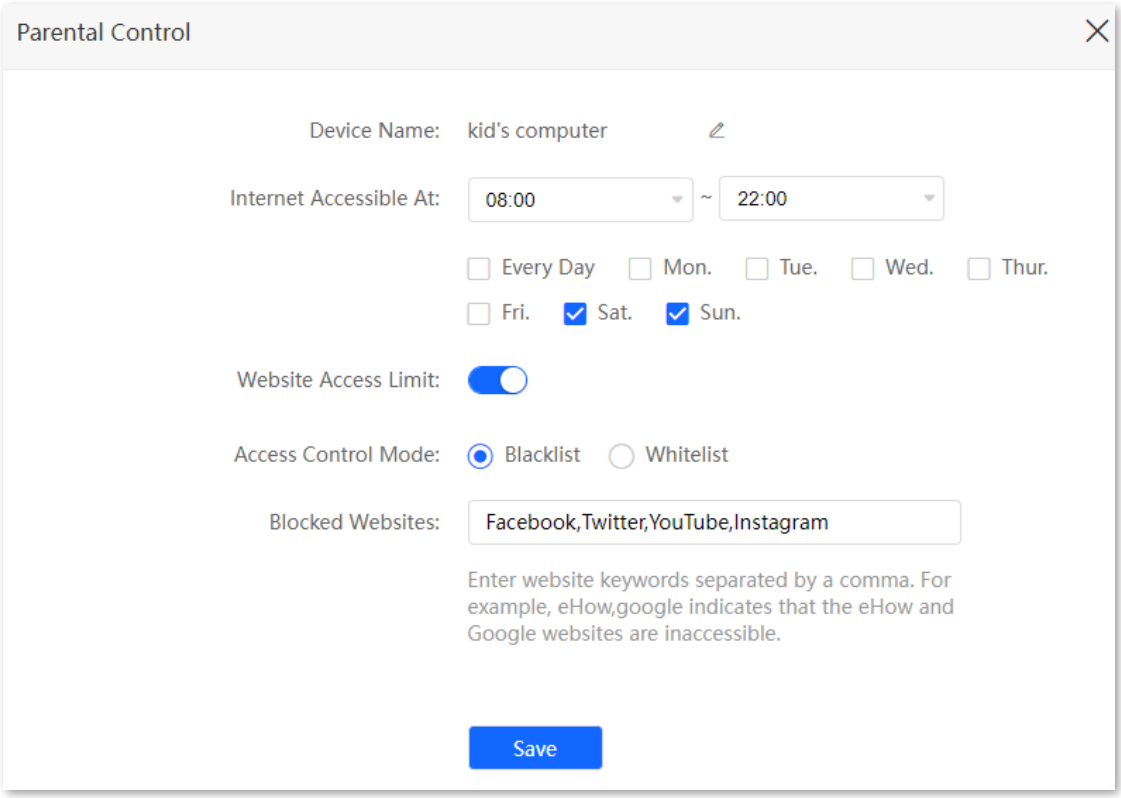


Figure 8-4 Configure parental control parameters

After the configuration is completed, your kid is allowed to access any websites except for Facebook, Twitter, YouTube and Instagram from 8:00 to 22:00 on weekends.

Chapter 9 Advanced settings

9.1 SIM PIN

9.1.1 Overview

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 enter the page, log in to the web UI of the router, and navigate to **Advanced Settings** > **SIM PIN**.

When the SIM card without enabling the PIN Lock function, the page is shown as below.

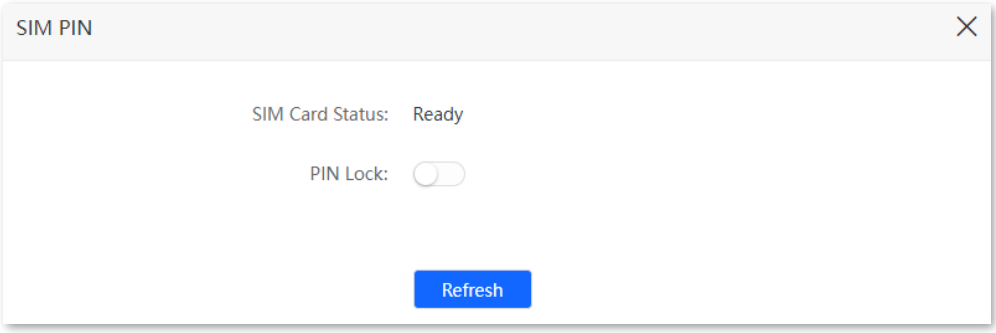


Figure 9-1 Disable PIN lock

9.1.2 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.

Procedure:

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

Step 2 Click **Start**.

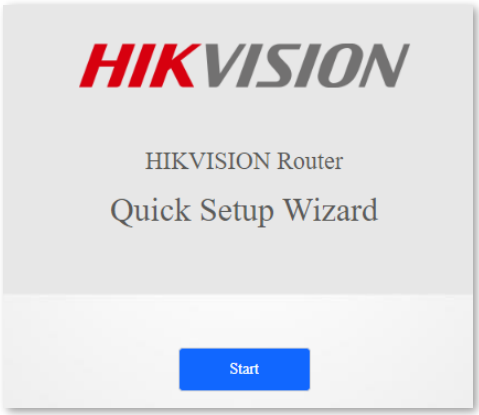


Figure 9-2 Quick setup wizard

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

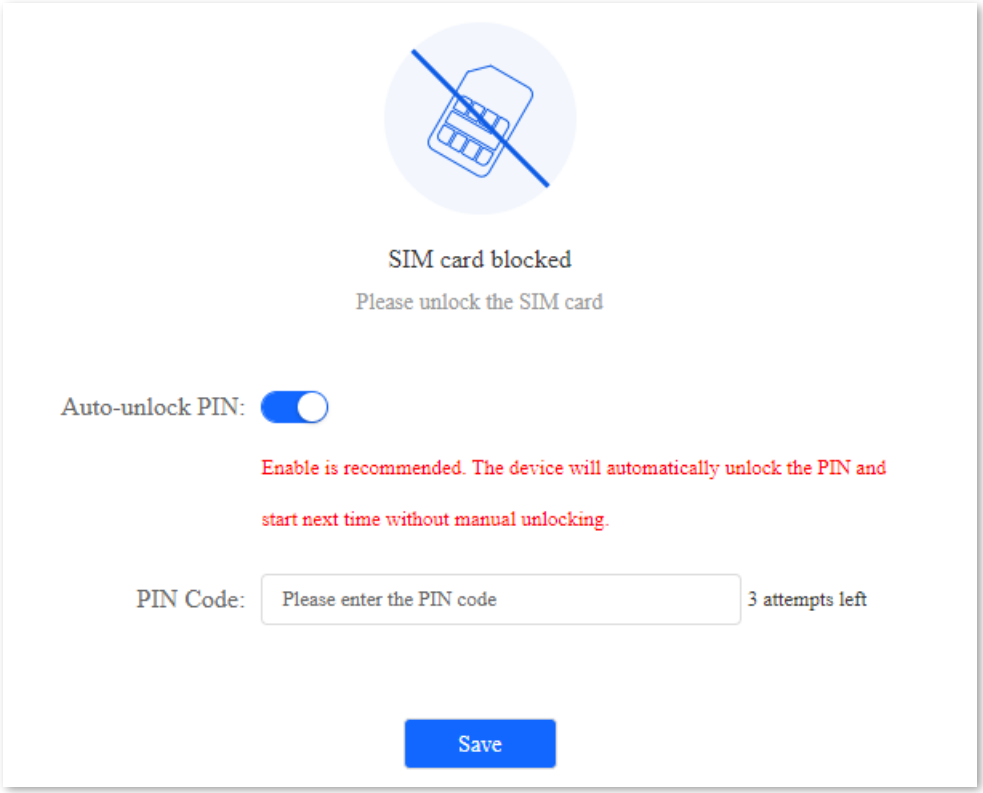


Figure 9-3 Unlock the SIM card

Note

- It is recommended to enable the Auto-unlock PIN function.
- Contact your ISP for the original PIN code.
- 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 Perform operations as prompted to complete the setup process.

Unlock the SIM card on the web UI

You can also unlock the SIM card when you have already logged in to the web UI of the router.

Procedure:

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

Step 2 Click Please unlock the SIM card, and navigate to **Advanced Settings** > **SIM PIN**.

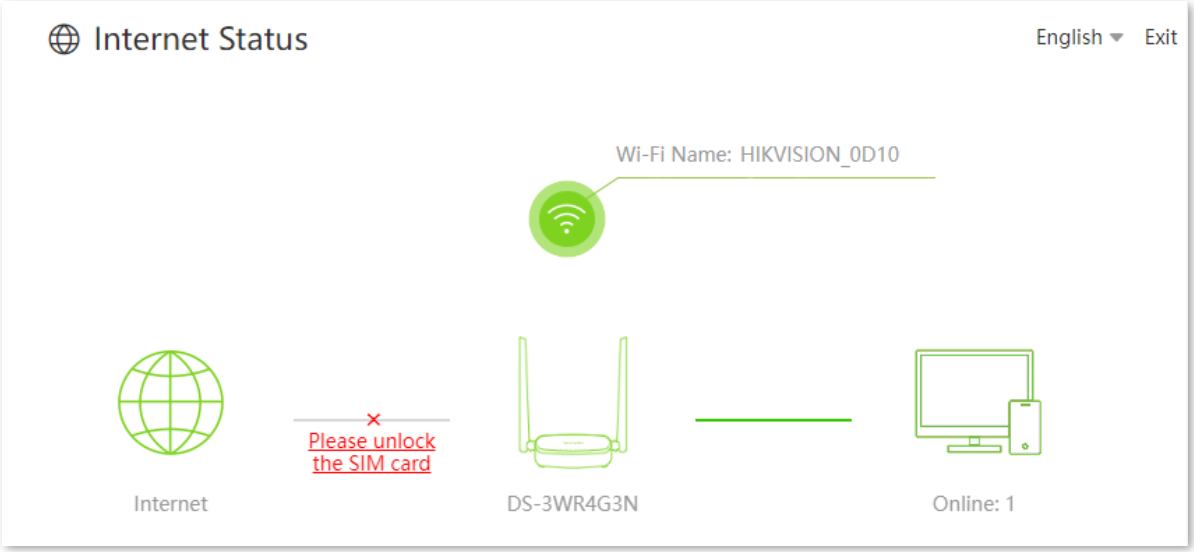


Figure 9-4 PIN blocked

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

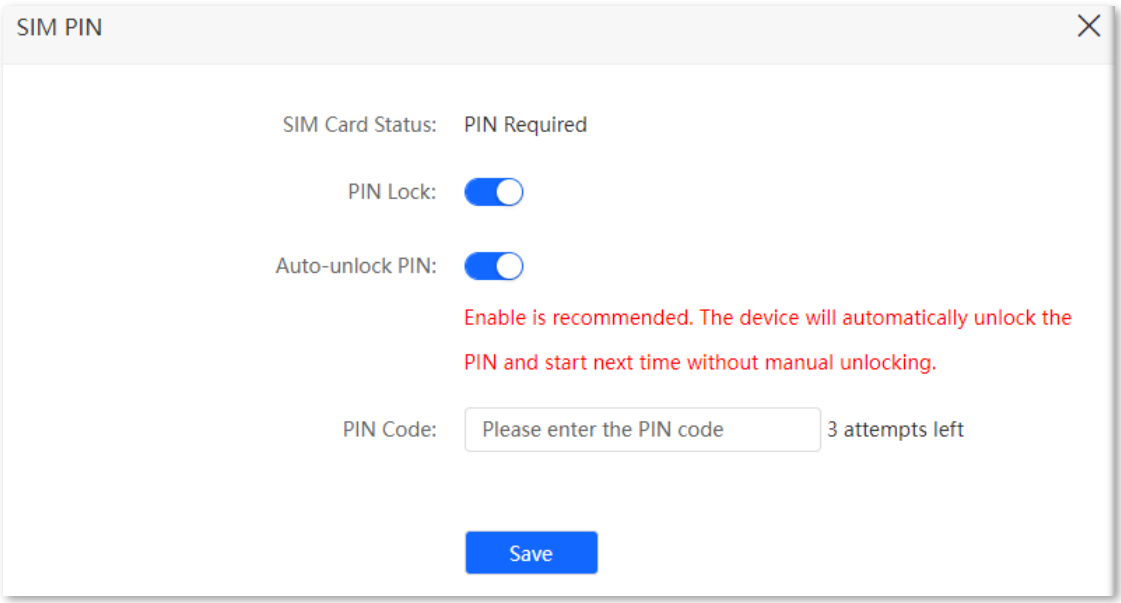


Figure 9-5 Unlock the SIM card

Note

- It is recommended to enable the Auto-unlock PIN function.
- Contact your ISP for the original PIN code.
- 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.

9.1.3 Disable PIN lock for the SIM card

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

Procedure:

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

Step 2 Navigate to **Advanced Settings** > **SIM PIN**.

Step 3 Disable **PIN Lock**.

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

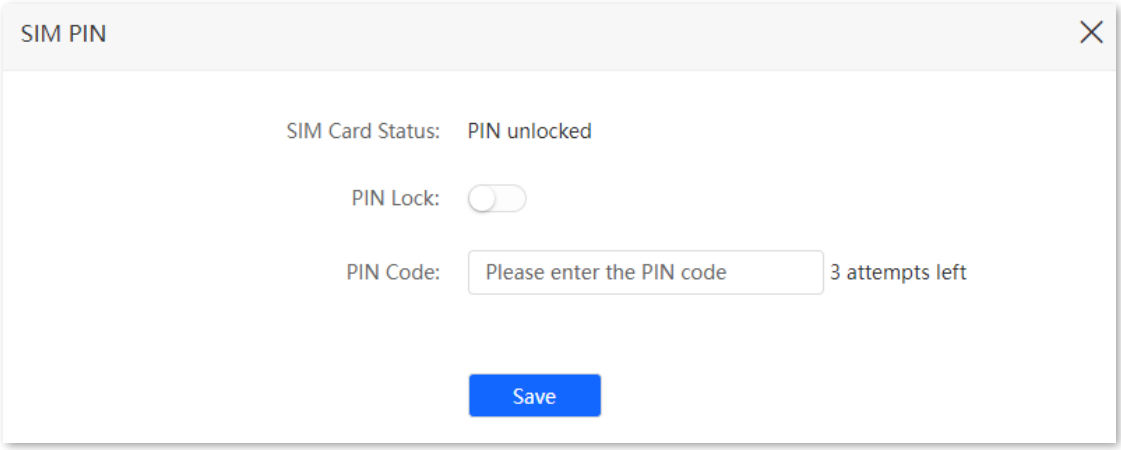


Figure 9-6 Disable PIN lock for the SIM card

Note

- Contact your ISP for the original PIN code.
- 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.

9.1.4 Enable PIN lock for the SIM card

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

Procedure:

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

Step 2 Navigate to **Advanced Settings** > **SIM PIN**.

Step 3 Enable **PIN Lock**.

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

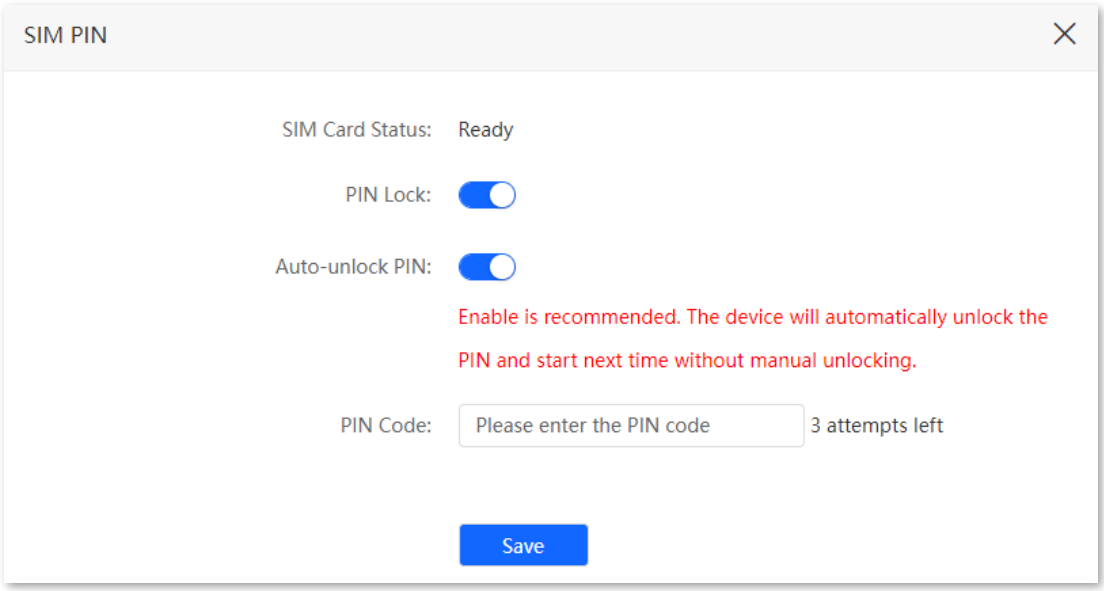


Figure 9-7 Enable PIN lock for the SIM card

Note

- It is recommended to enable the Auto-unlock PIN function.
- Contact your ISP for the original PIN code.
- 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

9.1.5 Use PUK code to reset PIN code

If you fail to enter PIN code for three times, you must use PUK code to reset the PIN code. Contact your ISP for the PUK code. Otherwise, the SIM card will be locked permanently after you enter the wrong PUK code for 10 times. And then set a new PIN code for the SIM card.

To enter the page, log in to the web UI of the router, and navigate to **Advanced Settings** > **SIM PIN.**

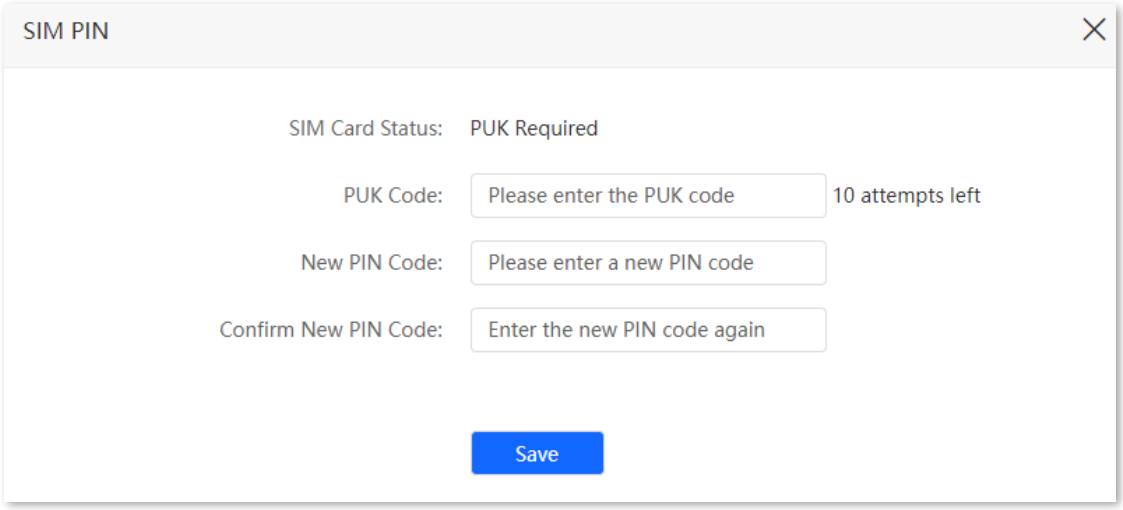


Figure 9-8 Use PUK code to reset PIN code

9.2 Mobile data

9.2.1 Overview

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

To enter the page, log in to the web UI of the router, and navigate to **Advanced Settings** > **Mobile Data**.

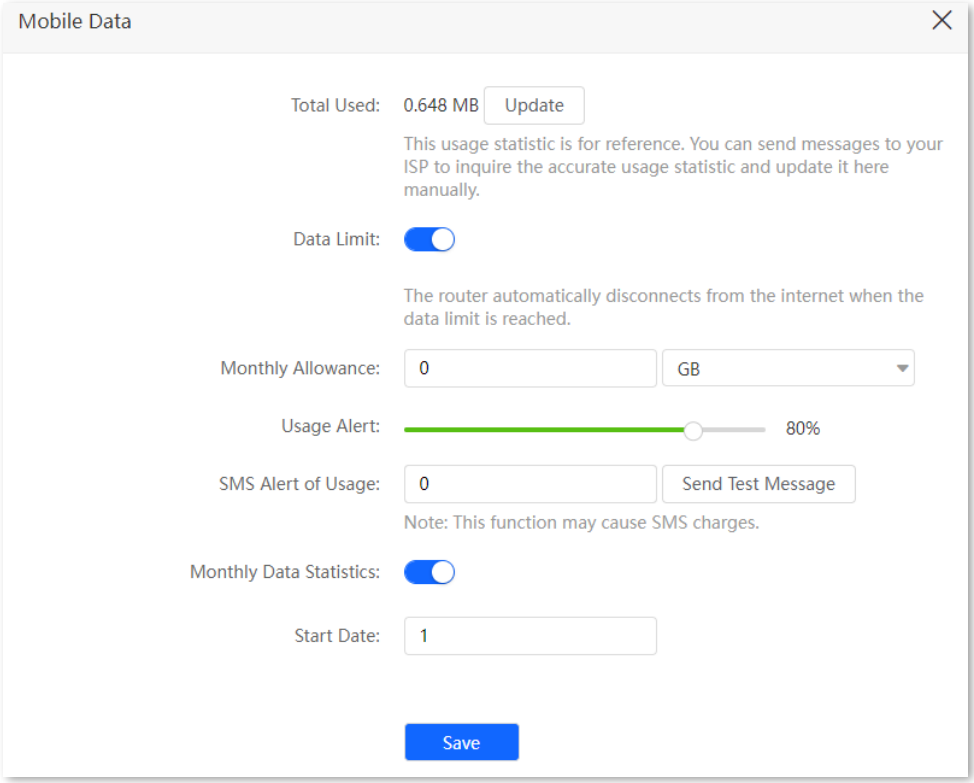


Figure 9-9 Mobile data

Table 9-1 Parameter description

Parameter	Description
Total Used	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	Used to enable or disable the data limit function. When the limit is reached, the router will disconnect from the Internet automatically.
Monthly Allowance	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 smartphone number.

Parameter	Description
SMS Alert of Usage	Specifies the smartphone number for receiving the alert SMS message. You can click **Send Test Message** to test the smartphone number you entered.
Monthly Data Statistics	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	Specifies the date at which the router clears the data statistics of the last month and start to record in the following month.

9.2.2 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.

Requirements: 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 requirements. Assume that:

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

Procedure:

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

Step 2 Navigate to **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**, and click **Save**.

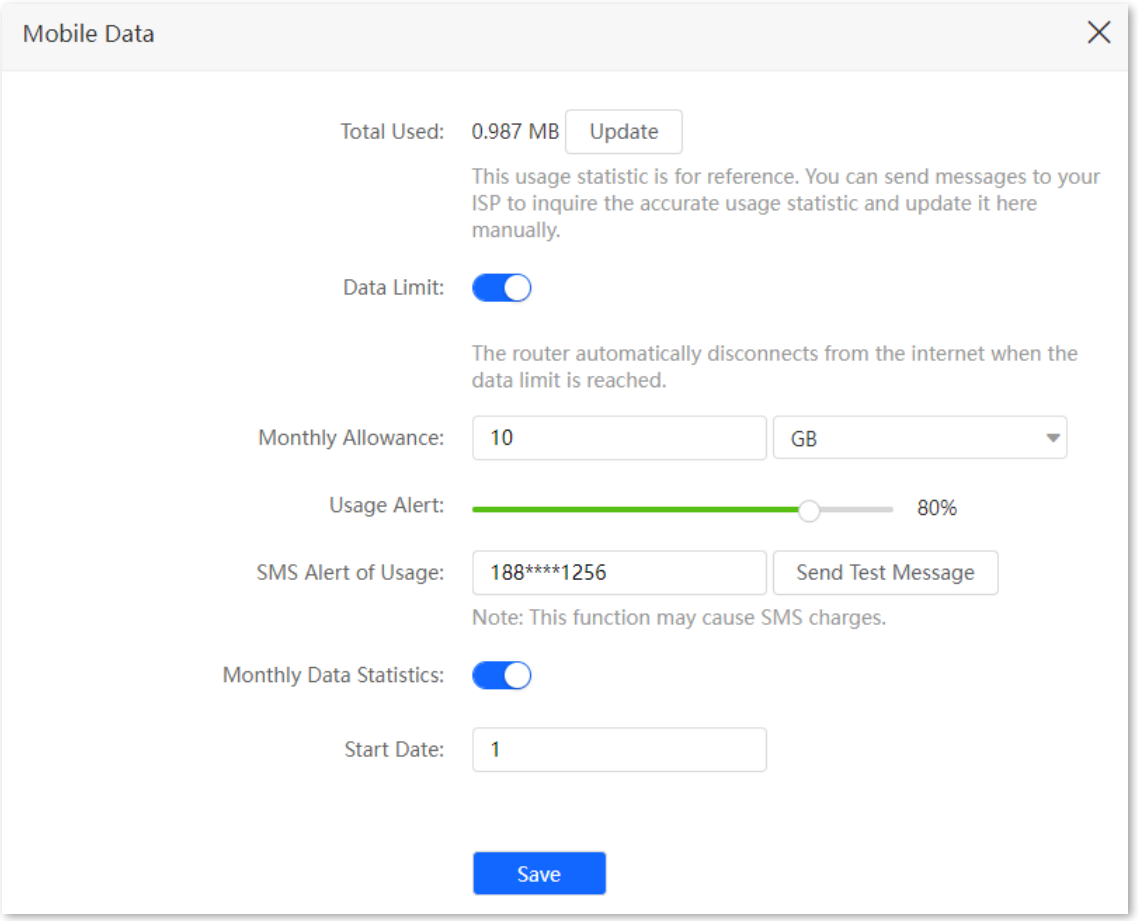


Figure 9-10 Configure mobile data parameters

After the configuration is completed, you will receive an 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**.
- Navigate to **Internet Settings**, and click **Connect** at the bottom of the page.

9.3 Bandwidth control

9.3.1 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 enter the page, log in to the web UI of the router, and navigate to **Advanced Settings** > **Bandwidth Control**.

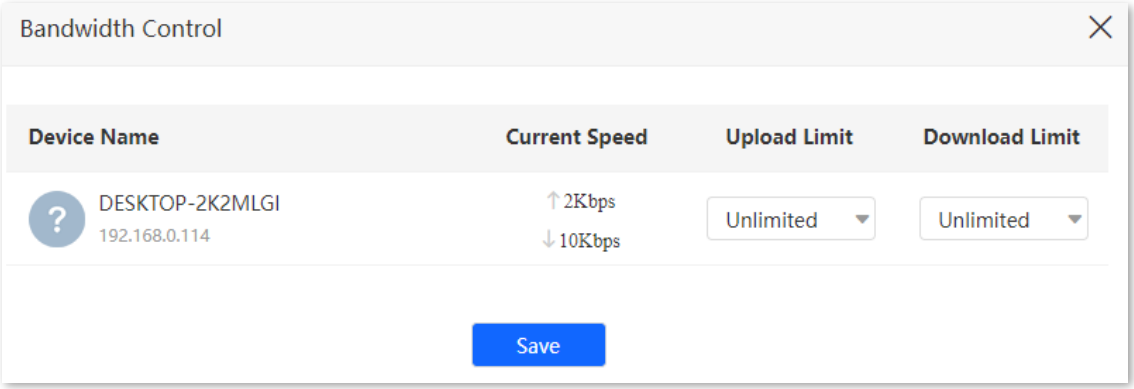


Figure 9-11 Bandwidth Control

Table 9-2 Parameter description

Parameter	Description
Device Name	Specifies the name and IP address of the device. You can click the device name to change it.
Current Speed	Specifies the current upload and download speed of the device.
Upload Limit	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	

9.3.2 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 requirements.

Procedure:

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

Step 2 Navigate to **Advanced Settings** > **Bandwidth Control**.

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

Step 4 Click **Save**.

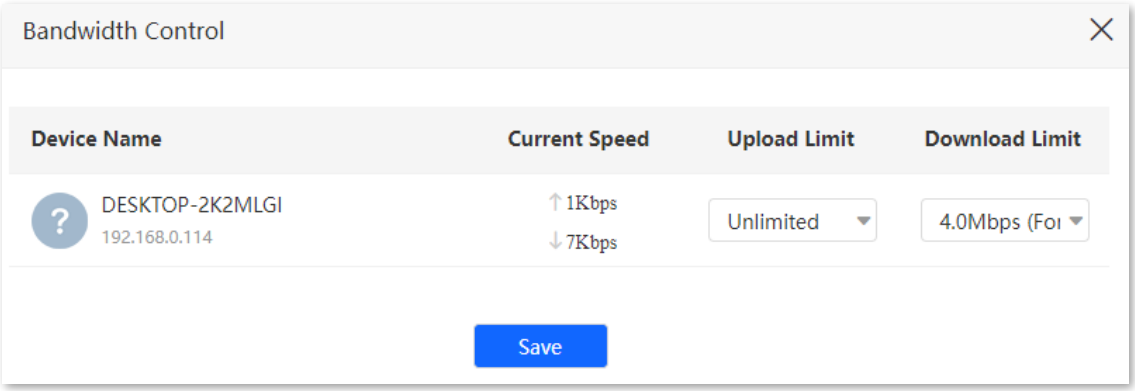


Figure 9-12 Set the download limit

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

9.4 Filter MAC address

9.4.1 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 enter the page, log in to the web UI of the router, and navigate to **Advanced Settings** > **Filter MAC Address**.

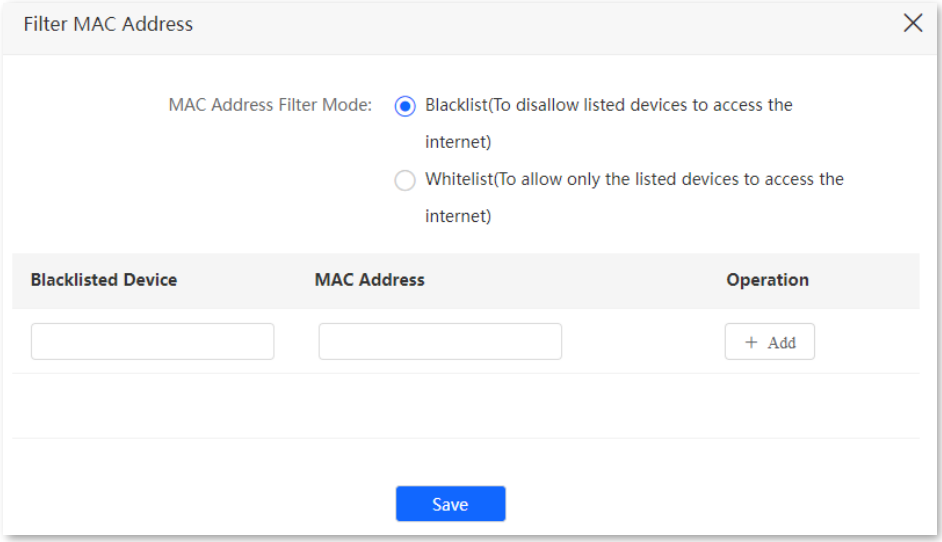


Figure 9-13 Filter MAC Address

Table 9-3 Parameter description

Parameter	Description
MAC Address Filter Mode	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	Specify the name or remark for the device.
Whitelisted Device	
MAC Address	Specifies the MAC addresses of devices added to the list.
Operation	Available operations include: + Add : Used to add new devices to the blacklist or whitelist. : 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.

9.4.2 Only allow specified device to access the Internet

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

Requirements: Only allow certain devices of family members to access the Internet.

Solution: You can configure the MAC address filter function to reach the requirements. Assume that:

Table 9-4 Device MAC address and status

Device	MAC address	Status
Your own smartphone	8C:EC:4B:B3:04:92	Connected
Kid 1's smartphone	94:C6:91:29:C2:12	Disconnected
Kid 2's smartphone	98:9C:57:19:D0:1B	Disconnected

Procedure:

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

Step 2 Navigate to **Advanced Settings** > **Filter MAC Address**.

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

Step 4 (Optional) Enter the device name in the **Whitelisted Device** field, which is **Kid 1's smartphone** in this example.

Step 5 Enter the **MAC Address** of the device, which is **94:C6:91:29:C2:12** 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. **My phone** is used for illustration here.

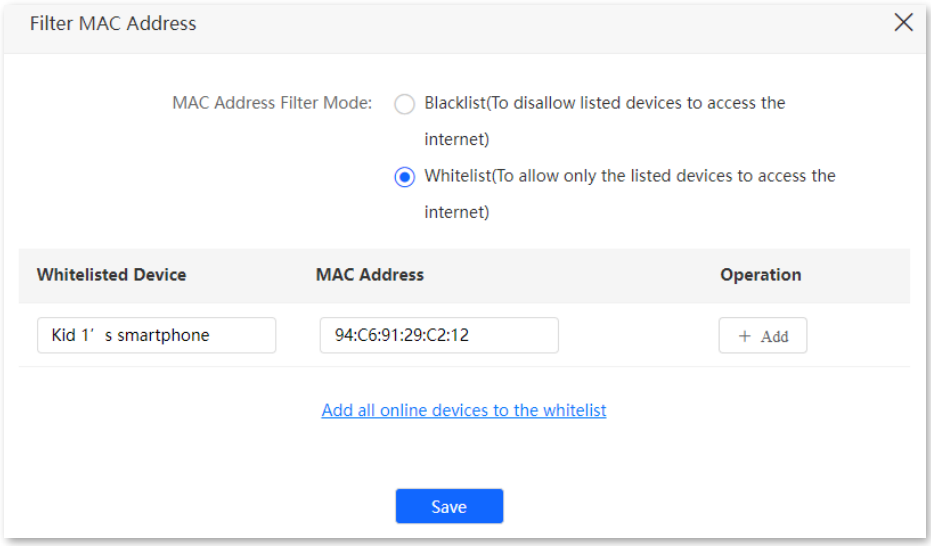


Figure 9-14 Add whitelisted devices

Step 7 Repeat **Step 4** to **Step 6** to add **Kid 2's smartphone** (**98:9C:57:19:D0:1B**) to the whitelist.

Step 8 Click **Save**.

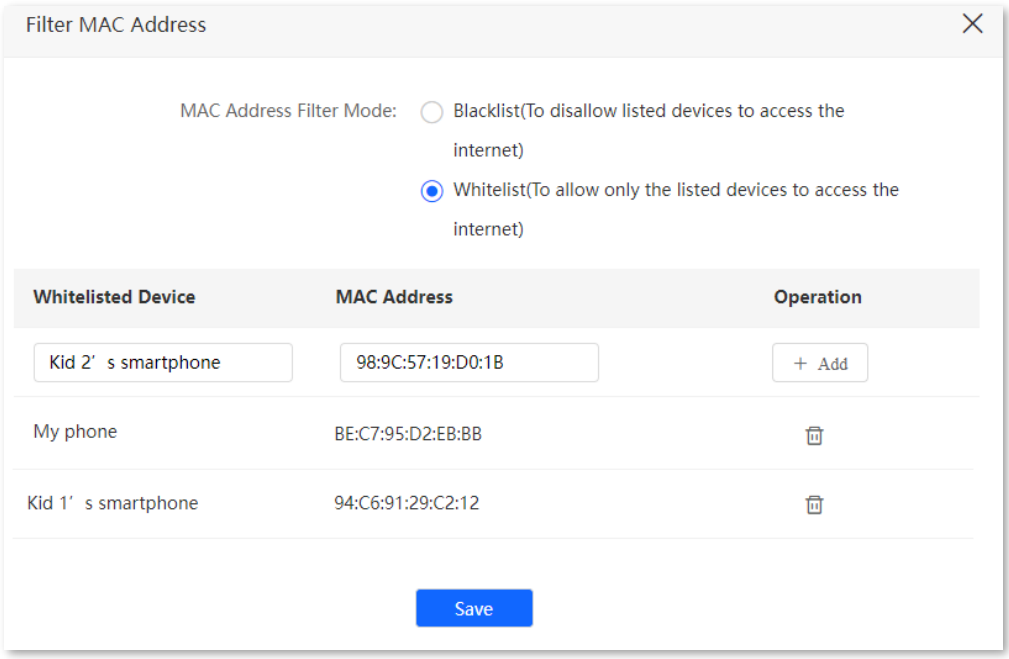


Figure 9-15 Add whitelisted devices

After the configuration is completed, only the three devices added can access the Internet through the router.

9.4.3 Disallow specified device to access the Internet

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

Requirements: Disallow the certain device of family member to access the Internet.

Solution: You can configure the MAC address filter function to reach the requirements. Assume that:

Table 9-5 Device MAC address and status

Device	MAC address	Status
Kid's smartphone	94:C6:91:29:C2:12	Disconnected

Procedure:

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

Step 2 Navigate to **Advanced Settings** > **Filter MAC Address**.

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

Step 4 Enter the device name in the **Blacklisted Device** field, which is **Kid's smartphone** in this example.

Step 5 Enter the **MAC Address** of the device, which is **94:C6:91:29:C2:12** in this example.

Step 6 Click **+Add**, and click **Save**.

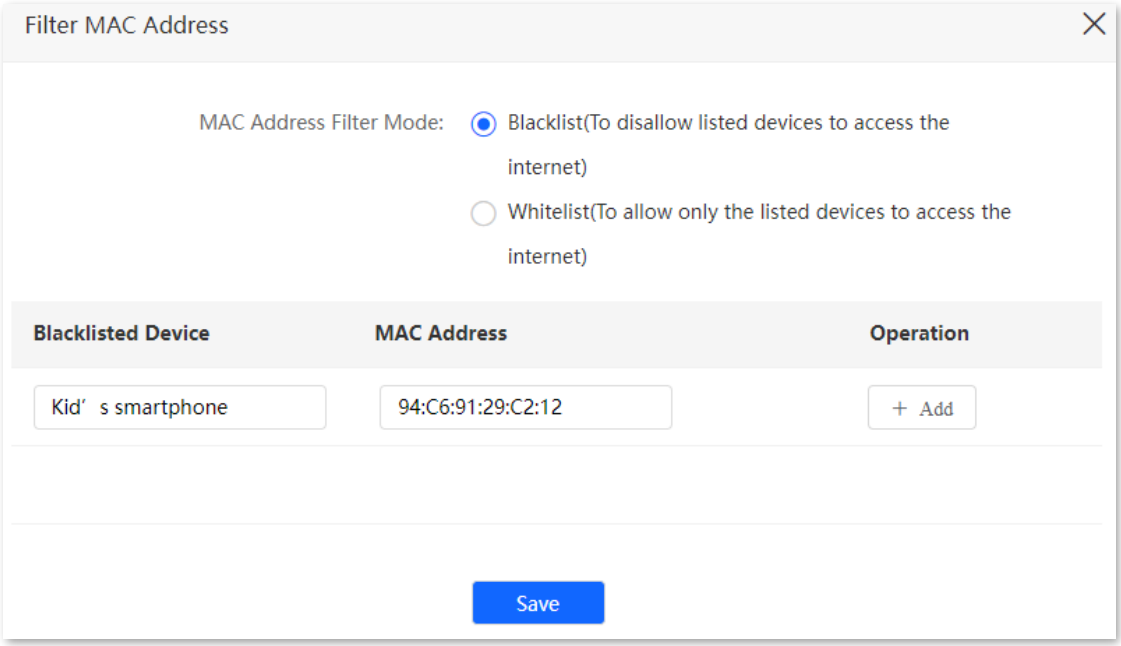


Figure 9-16 Add blacklisted device

After the configuration is completed, the device added cannot access the Internet through the router.

9.5 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 enter the page, log in to the web UI of the router, and navigate to **Advanced Settings** > **UPnP**.

This function is enabled by default.

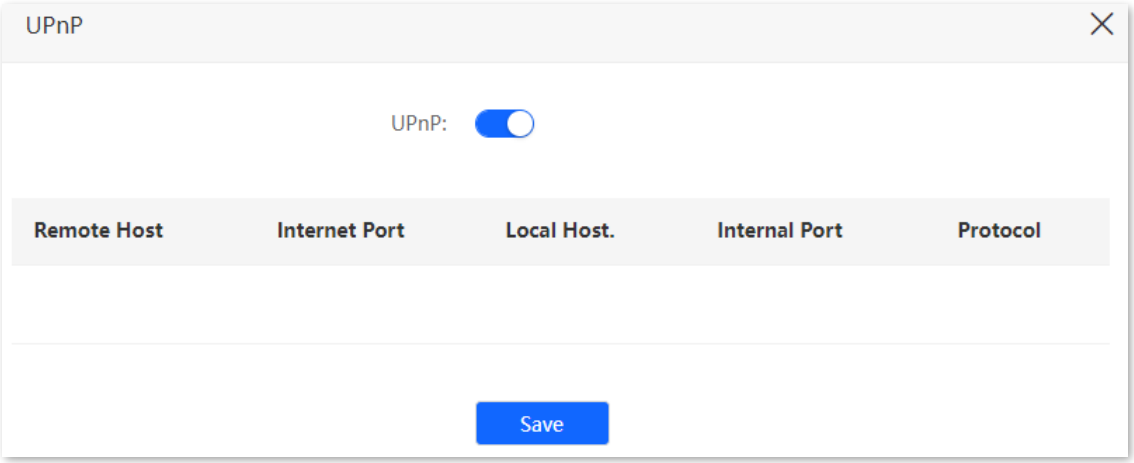


Figure 9-17 Enable UPnP

With the function enabled, any program that supports the UPnP function is launched, and you can find the port conversion information when the program sends any requests. The following figure is for reference only.

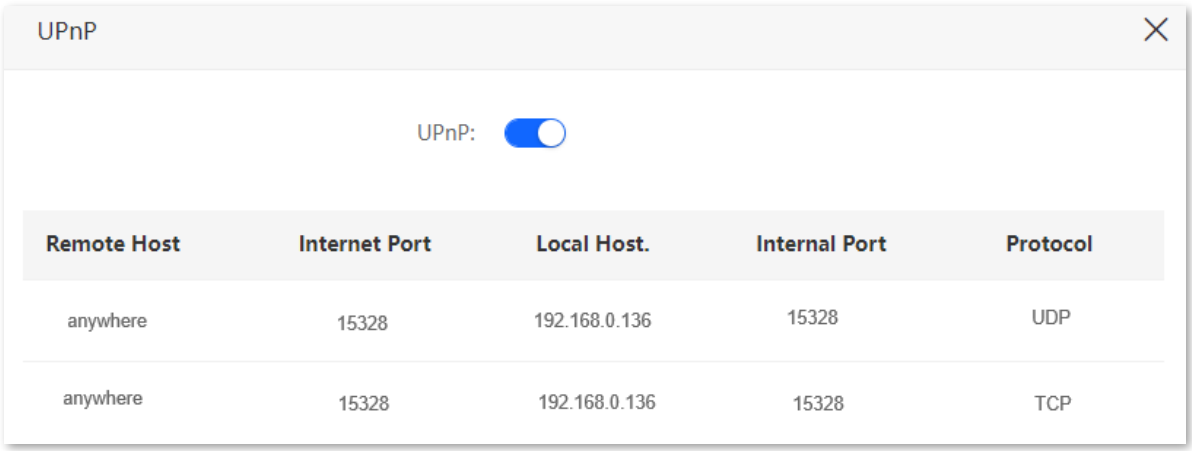


Figure 9-18 View port conversion information

9.6 Port forwarding

9.6.1 Overview

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

The port forwarding 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 port forwarding function enables Internet users to access web servers or FTP servers within the LAN.

To enter the page, log in to the web UI of the router, and navigate to **Advanced Settings** > **Port Forwarding**.

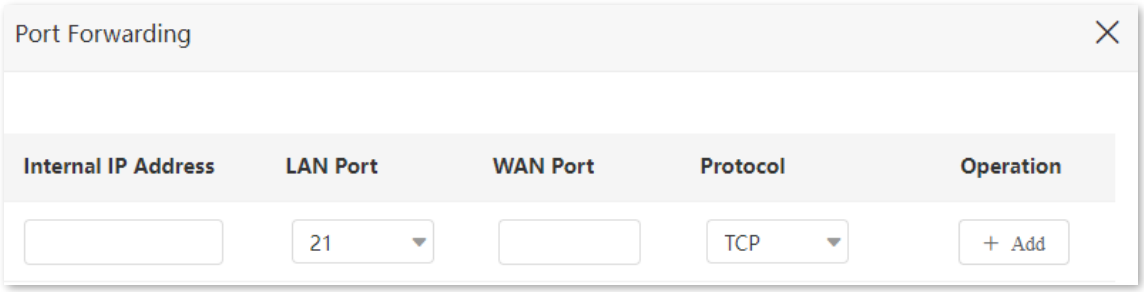


Figure 9-19 Port forwarding

Table 9-6 Parameter description

Parameter	Description
Internal IP Address	Specifies the IP address of the server within the LAN of the router.
LAN Port	Specifies the service port number of the server under the LAN of the router.
WAN Port	Specifies the port of the router which is opened and accessible to Internet users.
Protocol	Specifies the transport layer protocol of the service. If you are not sure about the protocol type of the service, you are recommended to select **TCP&UDP**, which indicates that both **TCP** and **UDP** are selected.
Operation	Available operations include: + Add : Used to add a port forwarding rule. : Used to delete a port forwarding rule.

9.6.2 Example of enabling Internet users to access LAN resources

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

Requirements: 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 port forwarding function to reach the requirements.

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
- WAN IP address of the router: 102.33.66.88

Note

- Ensure that the 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. 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 ISP may not support unreported web services accessed using the default port 80. Therefore, when setting port mapping, you are recommended to set the external port to an unfamiliar port (1024 to 65535), such as 9999, to ensure normal access.
- The LAN port number can be different from the WAN port number.

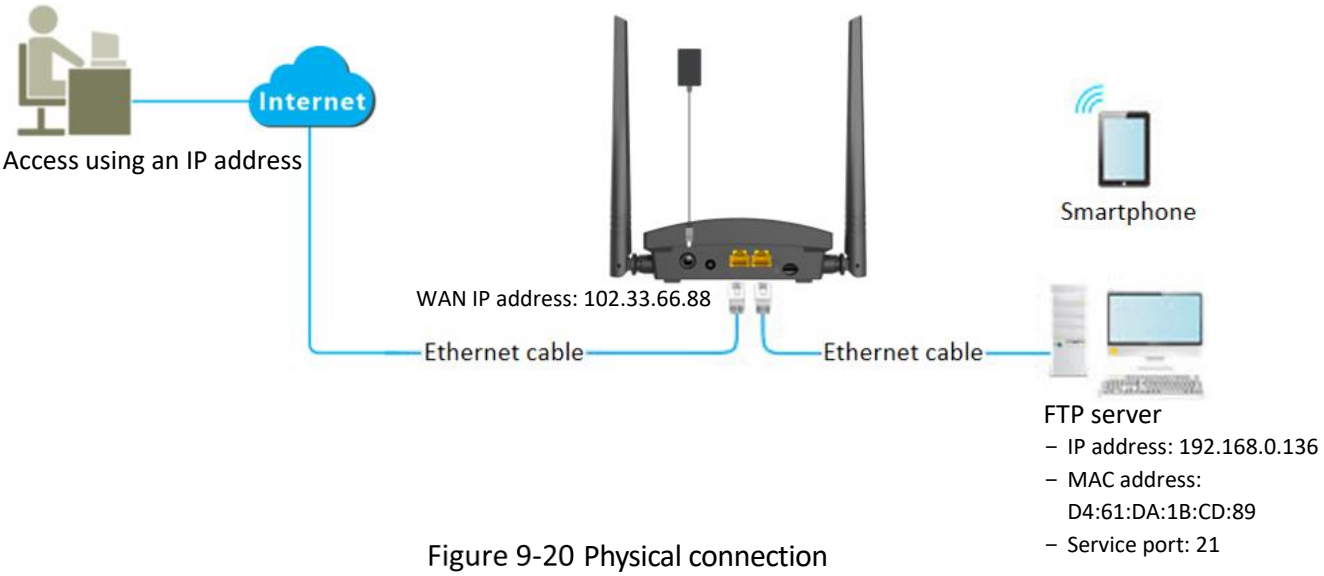


Figure 9-20 Physical connection

Procedure:

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

Step 2 Configure the port forwarding rule.

1) Navigate to **Advanced Settings** > **Port Forwarding**.

2) Enter the IP address of internal server in **Internal IP Address**, which is **192.168.0.136** in this example.
3) Click the drop-down list of **LAN Port** and select the service port of the Intranet server, which is **21** in this example.
4) The **WAN Port** will be automatically filled, which is **21** in this example.
   You can also customize the **WAN Port**.
5) Click the drop-down list of **Protocol** and select the protocol used by the intranet service. You are recommended to select **TCP&UDP**.
6) Click + Add .

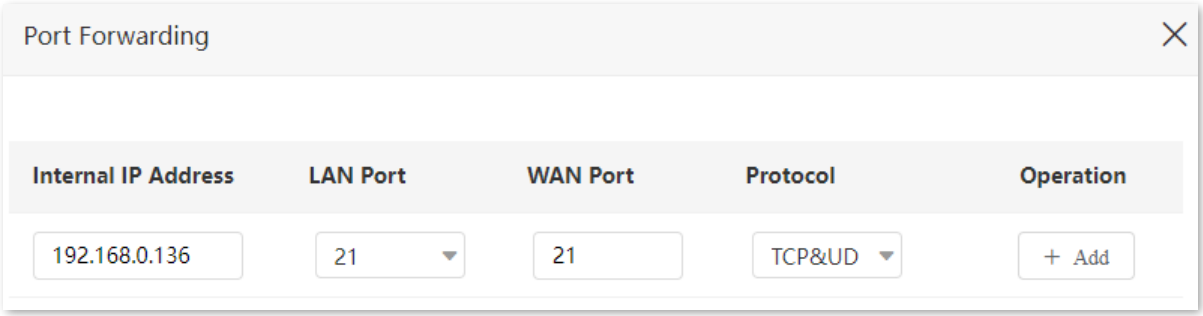


Figure 9-21 Configure the port forwarding rule

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

1) Navigate to **System Settings** > **DHCP Reservation**.
2) (Optional) Remark the **Device Name**, which is **FTP server** in this example.
3) Enter the **MAC Address** of the host to which a fixed IP address is to be assigned, which is **D4:61:DA:1B:CD:89** in this example.
4) Set the **IP Address** for the server host, which is **192.168.0.136** in this example.
5) Click + Add .

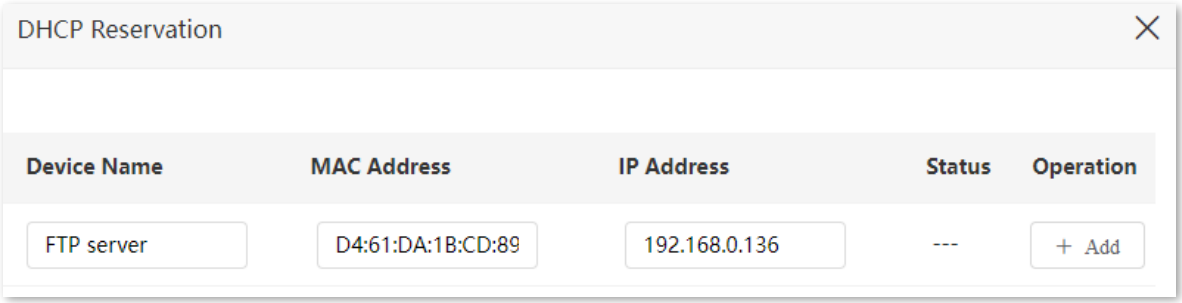


Figure 9-22 Configure the DHCP reservation rule

After the configuration is completed, Internet users can successfully access the FTP server by using the "*Intranet service application layer protocol name://WAN IP address of the router:WAN port number*". In this example, the address is **ftp://102.33.66.88:21**. You can find the WAN IP address of the router on the View WAN status page.

To access the FTP server from the Internet:

Open the file explorer on a computer that can access the Internet, and visit **ftp://102.33.66.88:21**.

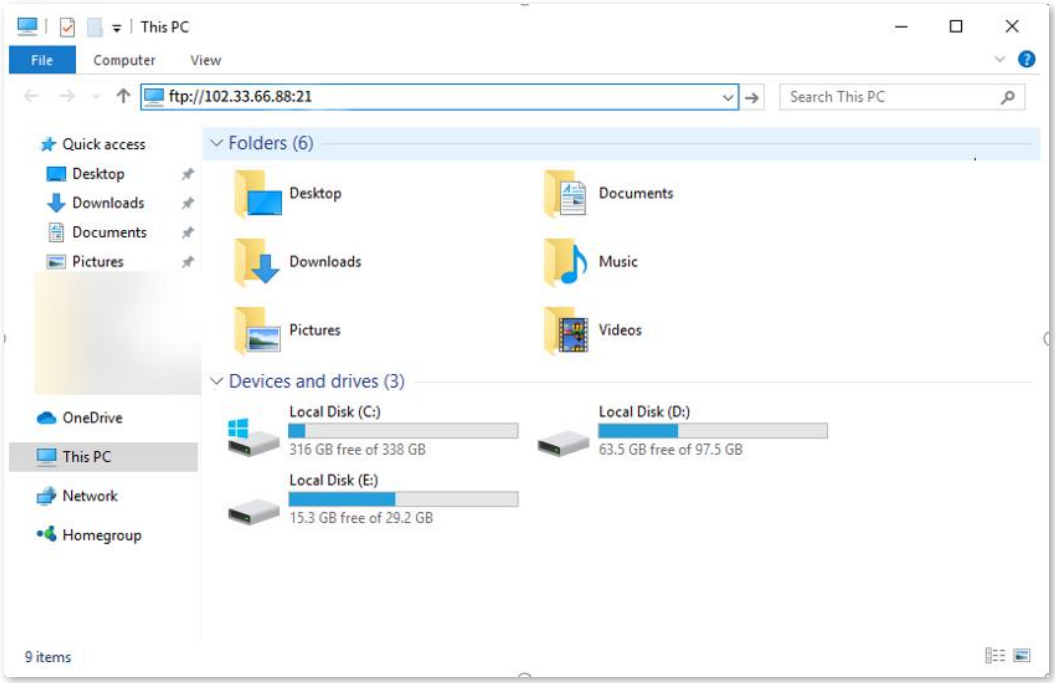


Figure 9-23 Visit ftp://102.33.66.88:21

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

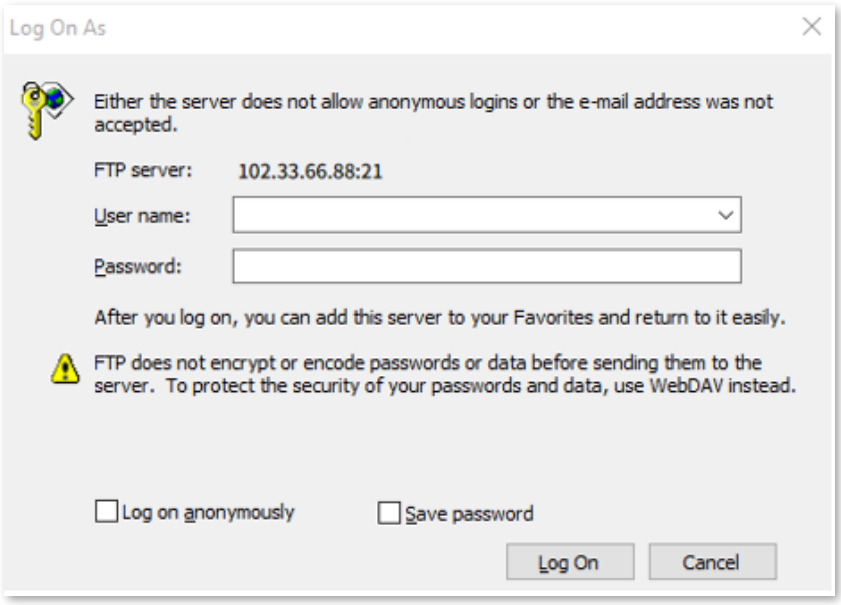


Figure 9-24 Enter the user name and password

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

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 port forwarding 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.

9.7 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 enter the page, log in to the web UI of the router, and navigate to **Advanced Settings** > **Firewall**.

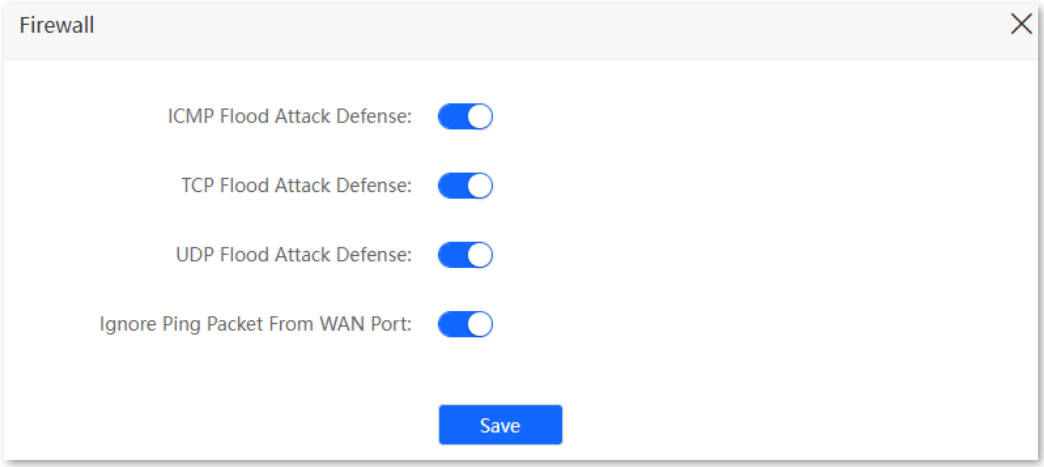


Figure 9-25 Configure firewall function

Table 9-7 Parameter description

Parameter	Description
ICMP Flood Attack Protection	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	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	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.

Parameter	Description
Ignore Ping Packet From WAN Port	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.

9.8 SSH

Secure Shell (SSH) uses encryption and authentication mechanisms to achieve remote access and file transmission services.

The router supports SSH server, and allows SSH client to connect to it.

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

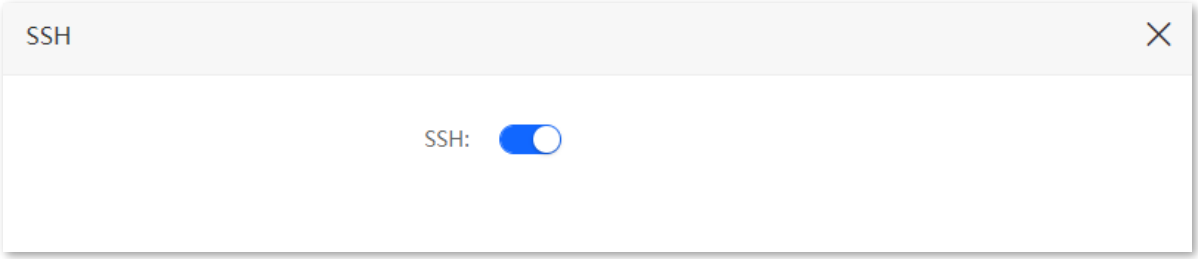


Figure 9-26 Enable SSH

Assume that you want to log in to the router (192.168.0.1) and configure it form the computer installed with the SSH client software.

Procedure:

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

Step 2 Navigate to **Advanced Settings** > **SSH**.

Step 3 Enable the **SSH** function.

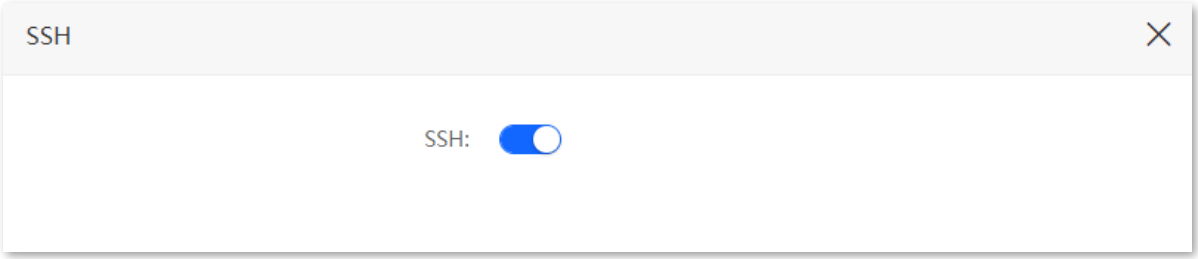


Figure 9-27 Enable SSH

Step 4 Run the SSH client software on the management computer. PuTTY is used for illustration.

1) Run the **PuTTY**.
2) Set **Connection type** to **SSH**.
3) Set **Host Name (or IP address)** to **192.168.0.1**.
4) Click **Open**.

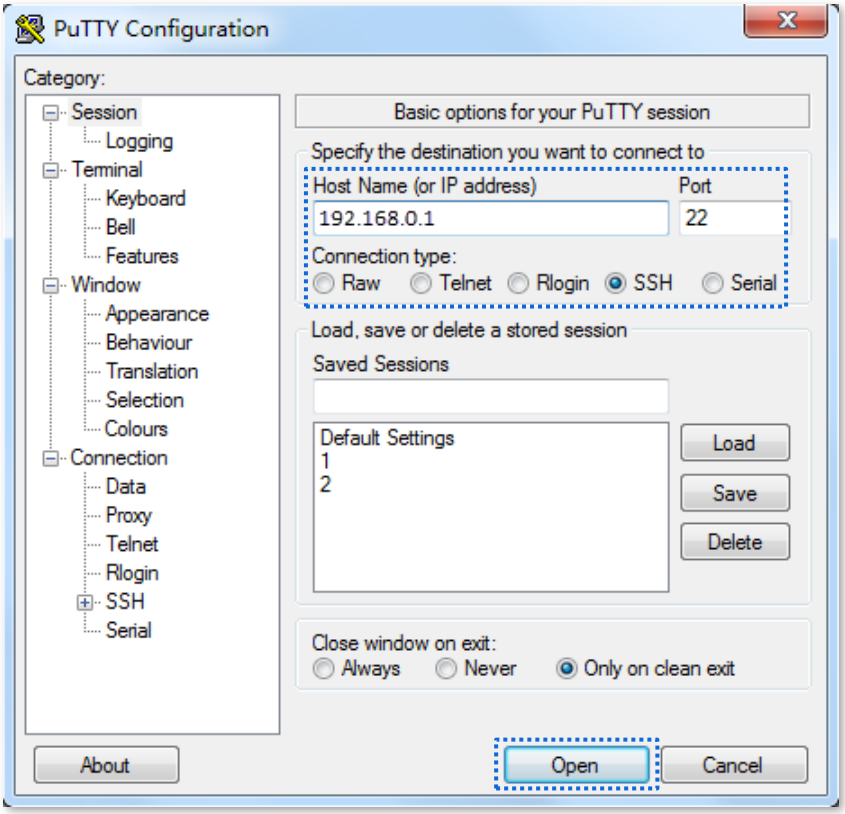


Figure 9-28 Configure PuTTY parameters

Step 5 Enter the user name (admin) and login password of the router according to the instructions to log in to the configuration page.

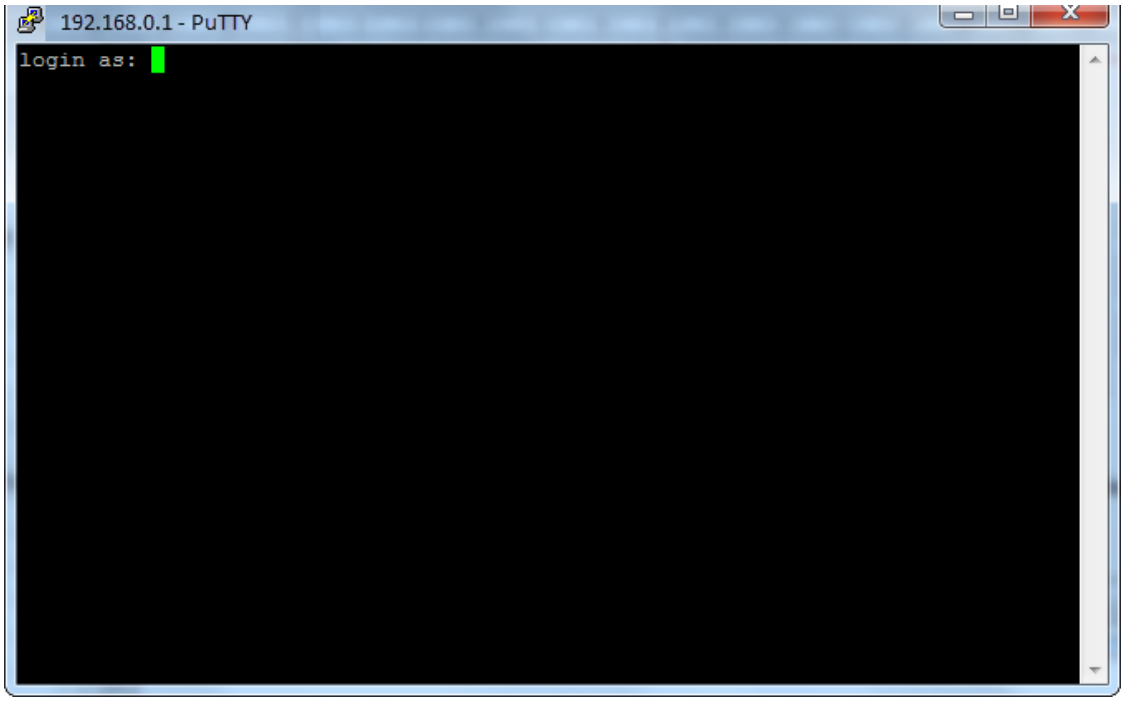


Figure 9-29 Enter the user name and login password of the router

9.9 DMZ host

9.9.1 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 host 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 host function. If the DMZ host function is not required, you are recommended to disable it and enable your firewall, security, and antivirus software.

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

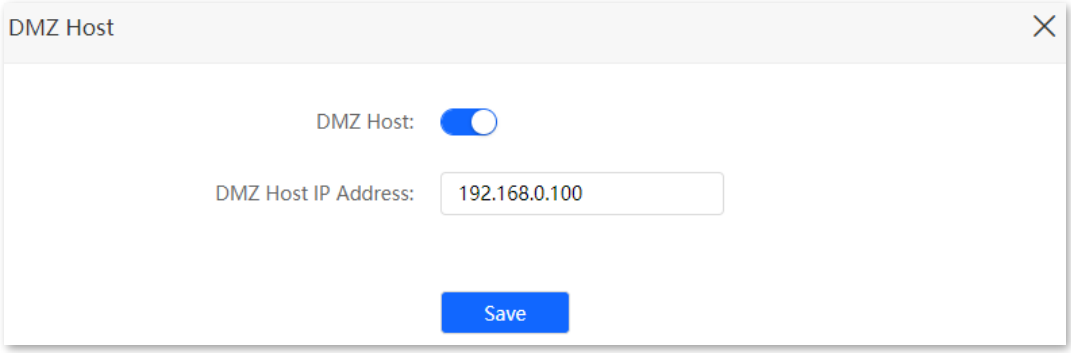


Figure 9-30 DMZ host

Table 9-8 Parameter description

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

9.9.2 Example of enabling Internet users to access LAN resources

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

Requirements: 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 requirements.

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

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.

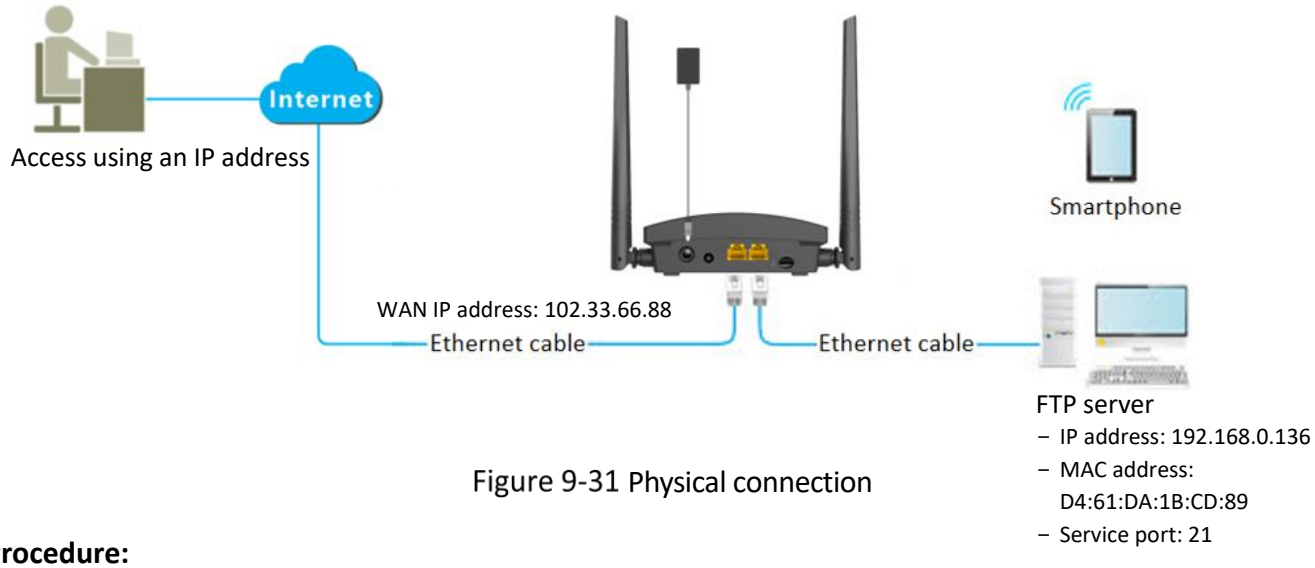


Figure 9-31 Physical connection

Procedure:

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

Step 2 Set the server host as the DMZ host.

1) Navigate to **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**.

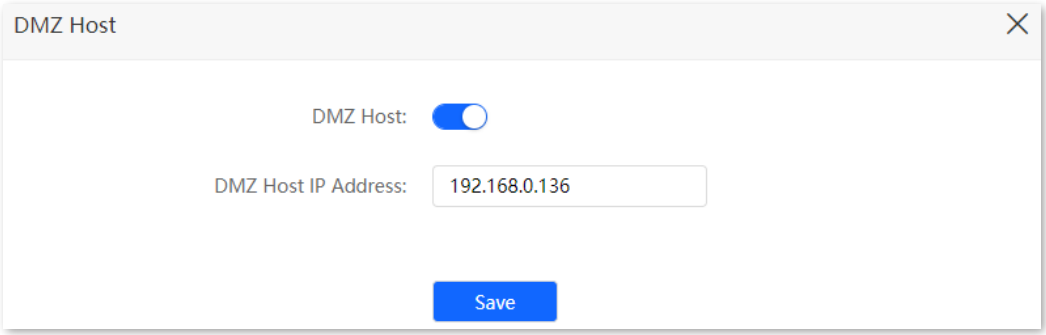


Figure 9-32 Configure the DMZ host rule

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

1) Navigate to **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**.

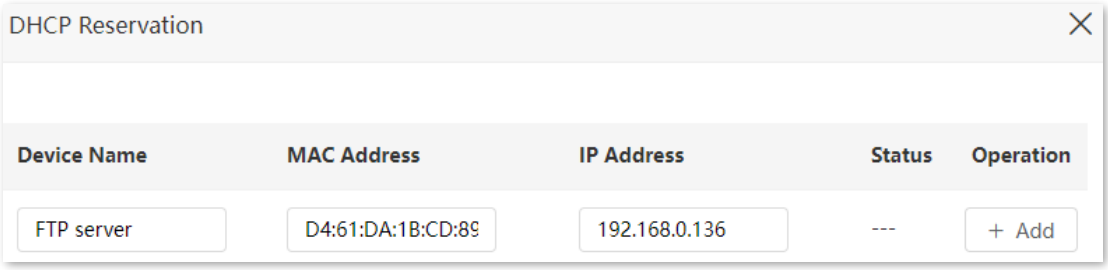


Figure 9-33 Configure the DHCP reservation rule

After the configuration is completed, Internet users can successfully access the DMZ host by using the "*Intranet service application layer protocol name*://*WAN IP address of the router*:*intranet service port number*". In this example, the address is **ftp://102.33.66.88:21**. You can find the WAN IP address of the router on the View WAN status page.

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.

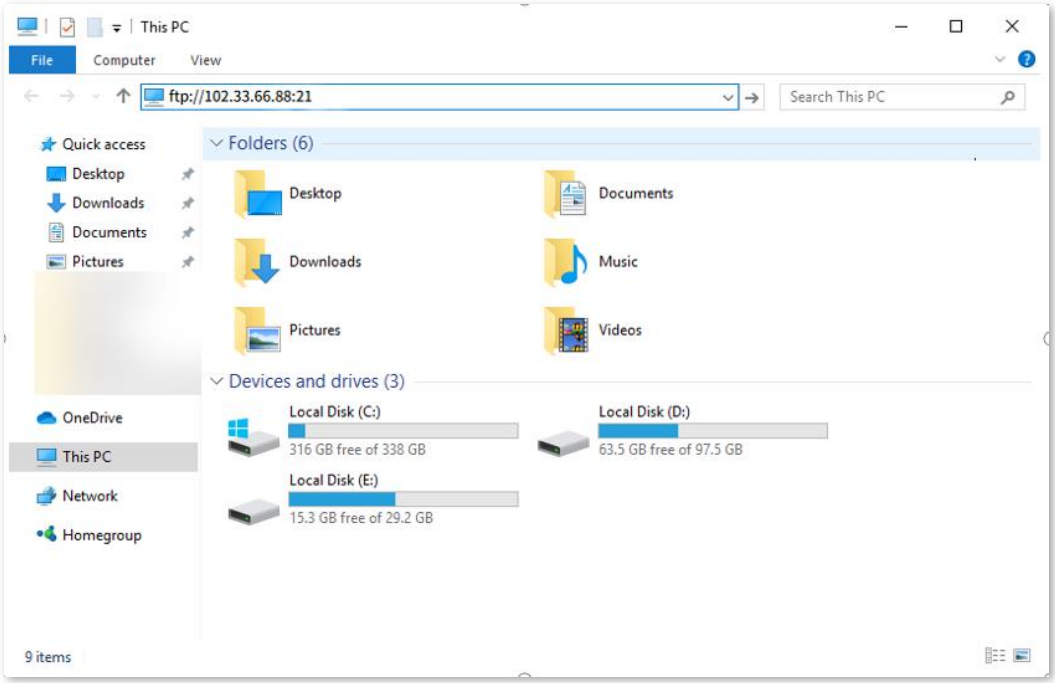


Figure 9-34 Visit ftp://102.33.66.88:21

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

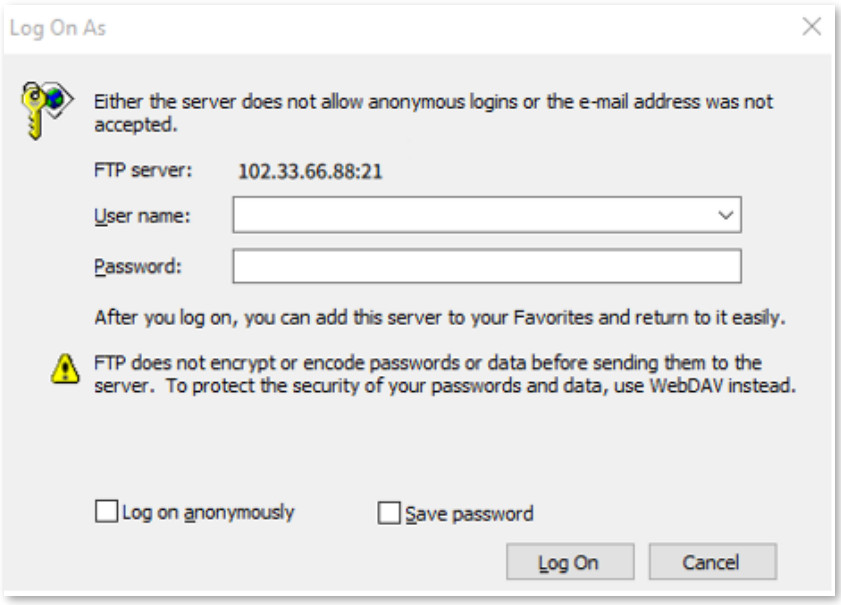


Figure 9-35 Enter the user name and password

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

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.

9.10 DDNS

9.10.1 Overview

DDNS normally interworks with port forwarding, 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 enter the page, log in to the web UI of the router, and navigate to **Advanced Settings** > **DDNS**. This function is disabled by default. When it is enabled, the page is shown as below.

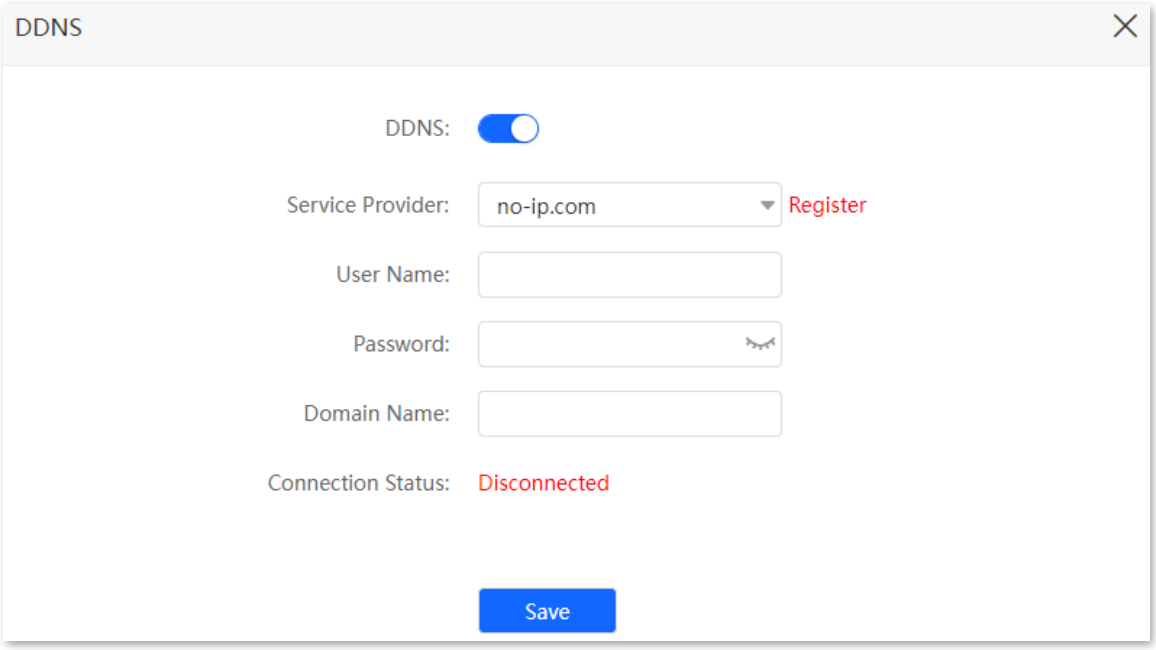


Figure 9-36 DDNS

Table 9-9 Parameter description

Parameter	Description
DDNS	Used to enable or disable the DDNS function.
Service Provider	Specifies the DDNS service provider.
User Name	Specify the user name and password registered on a DDNS service provider's website for logging in to the DDNS service.
Password	
Domain Name	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	Specifies the current connection status of the DDNS service.

9.10.2 Example of enabling Internet users to access LAN resources using a domain name

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

Requirements: 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 requirements.

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

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.

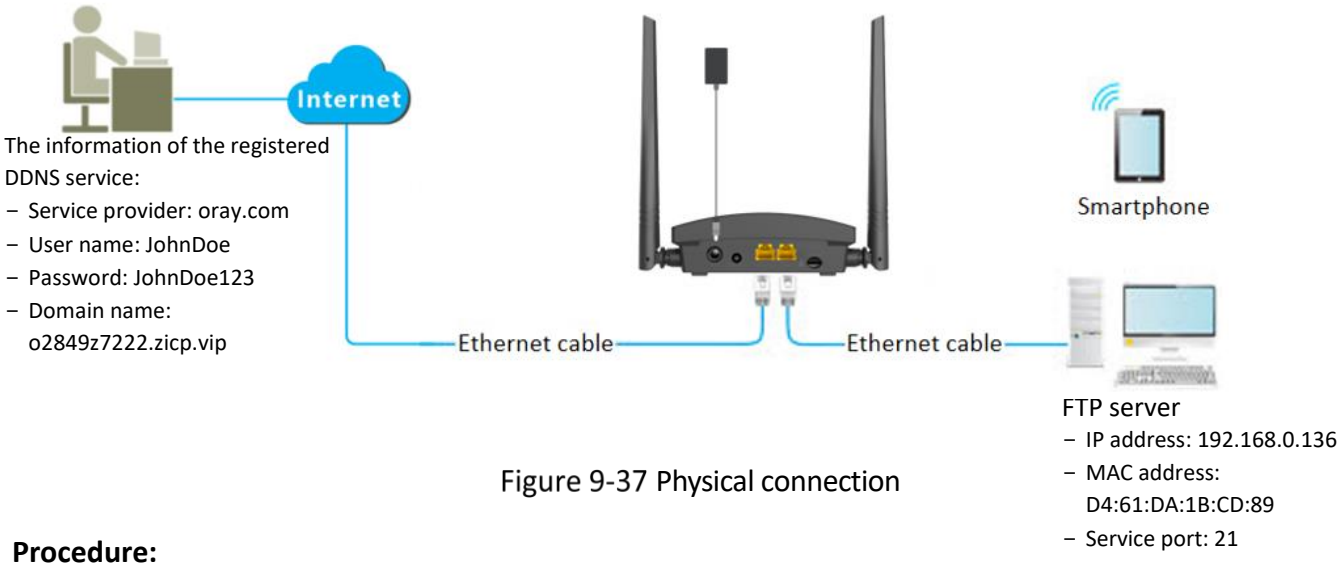


Figure 9-37 Physical connection

Procedure:

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

Step 2 Configure the DDNS function.

1) Navigate to **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**.

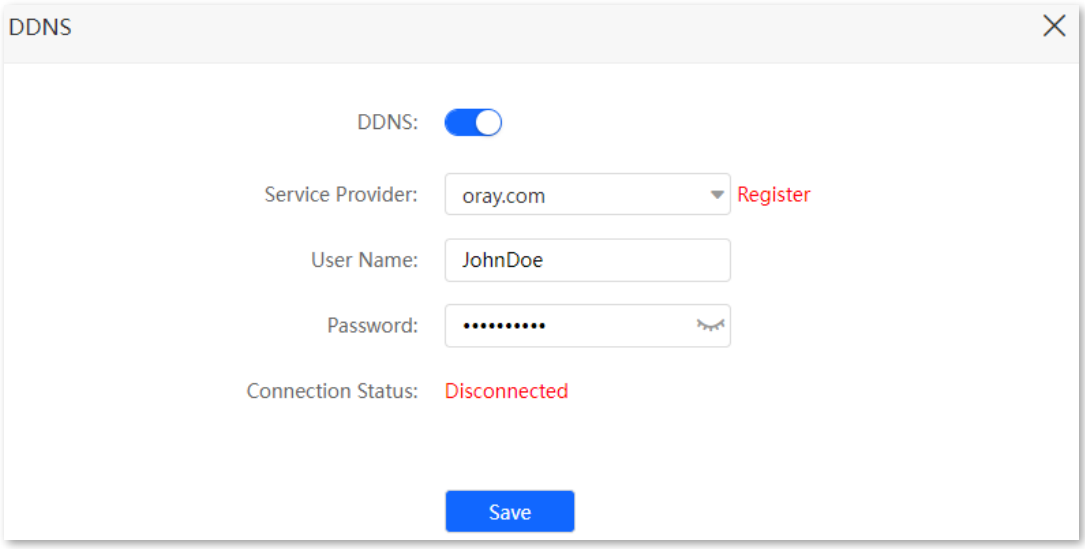


Figure 9-38 Configure the DDNS rule

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

Step 3 Configure the port forwarding function (refer to port forwarding).

After the configuration is completed, Internet users can successfully access the FTP server by using the "*Intranet service application layer protocol name://the domain name:WAN port number*". In this example, the address is **ftp://o2849z7222.zicp.vip:21**.

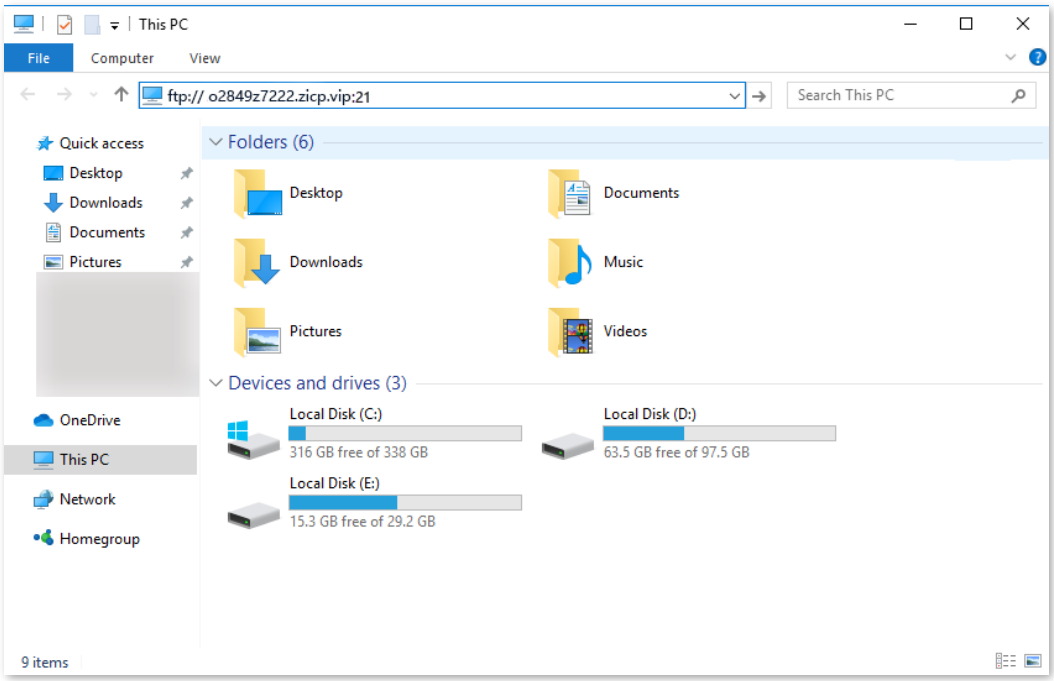


Figure 9-39 Visit ftp://o2849z7222.zicp.vip:21

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

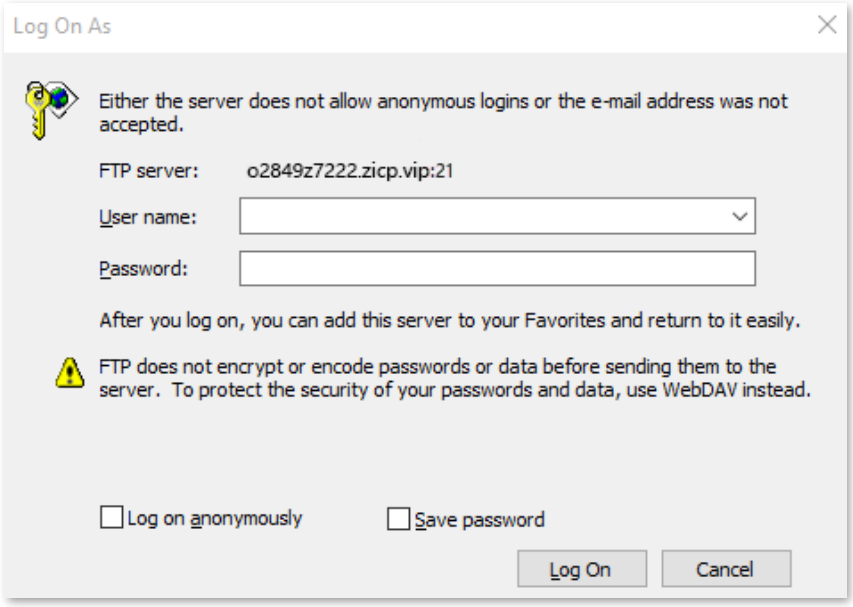


Figure 9-40 Enter the user name and password

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 port forwarding 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.

Chapter 10 System settings

10.1 DHCP reservation

10.1.1 Overview

Through the DHCP reservation function, specified clients can always obtain the same IP address when connecting to the router. This function takes effect only when the DHCP server function of the router is enabled.

To enter the page, log in to the web UI of the router, and navigate to **System Settings** > **DHCP Reservation**.

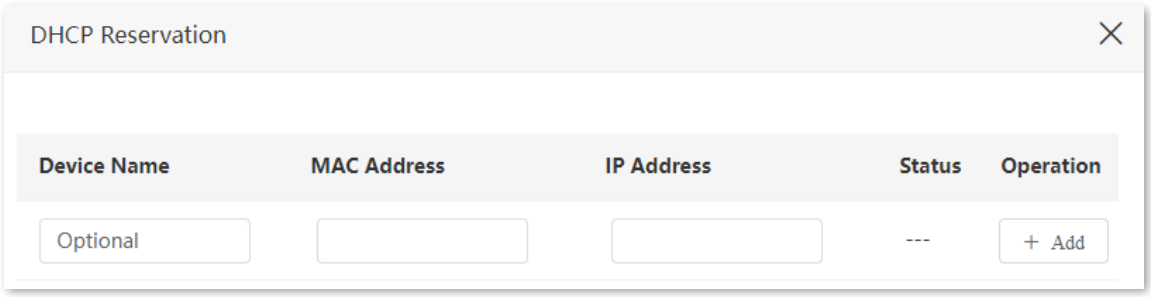


Figure 10-1 DHCP reservation

Table 10-1 Parameter description

Parameter	Description
Device Name	Specifies the device name of the client.
MAC Address	Specifies the MAC address of the client.
IP Address	Specifies the IP address reserved for the client.
Status	Specifies whether the client is online or not.
Operation	The available options include: + Add : Used to add a new DHCP reservation rule. : Used to bind the MAC address to the reserved IP address. : Used to unbind the MAC address from the reserved IP address. : Used to delete the DHCP reservation rule.

10.1.2 Assign static IP addresses to LAN clients

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

Requirements: 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 requirements.

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

Procedure:

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

Step 2 Navigate to **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**.

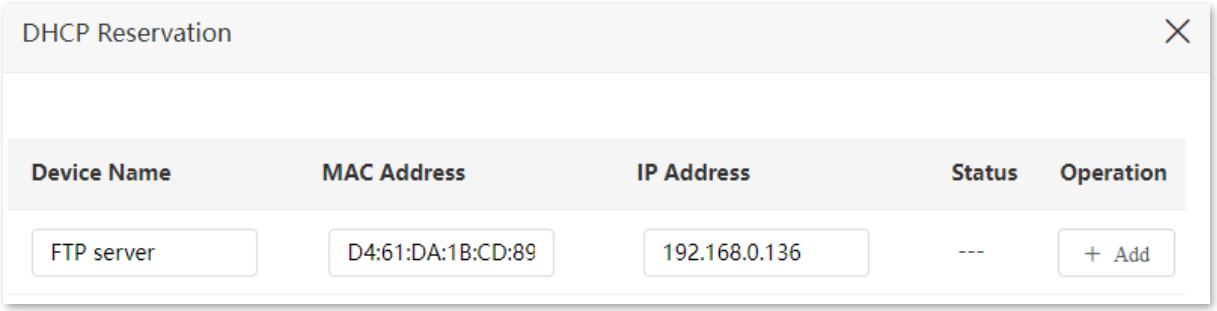


Figure 10-2 Add the DHCP reservation rule

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.

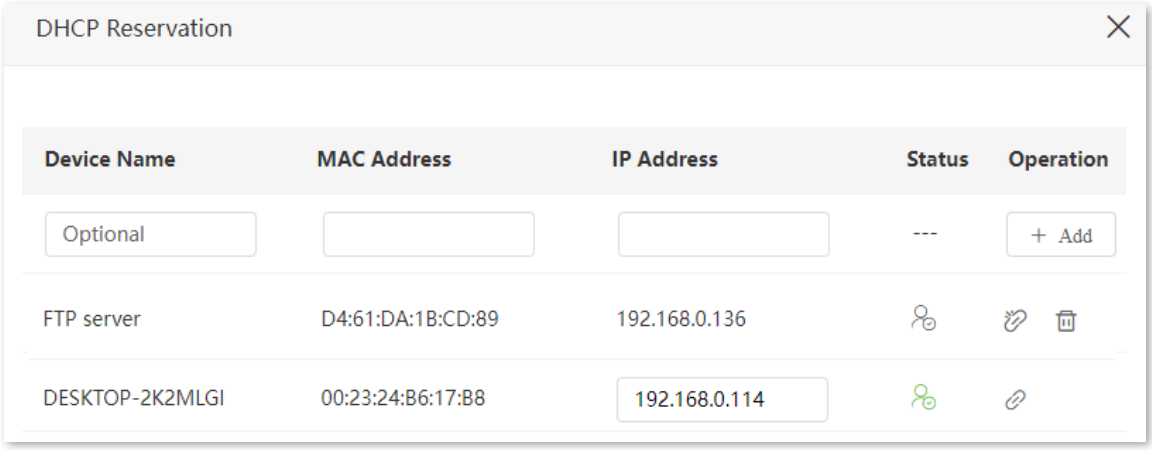


Figure 10-3 DHCP reservation rule added successfully

10.2 Time settings

To enter the page, log in to the web UI of the router, and navigate to **System Settings** > **Time Settings.**

You can change the time settings. 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.

10.2.1 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.

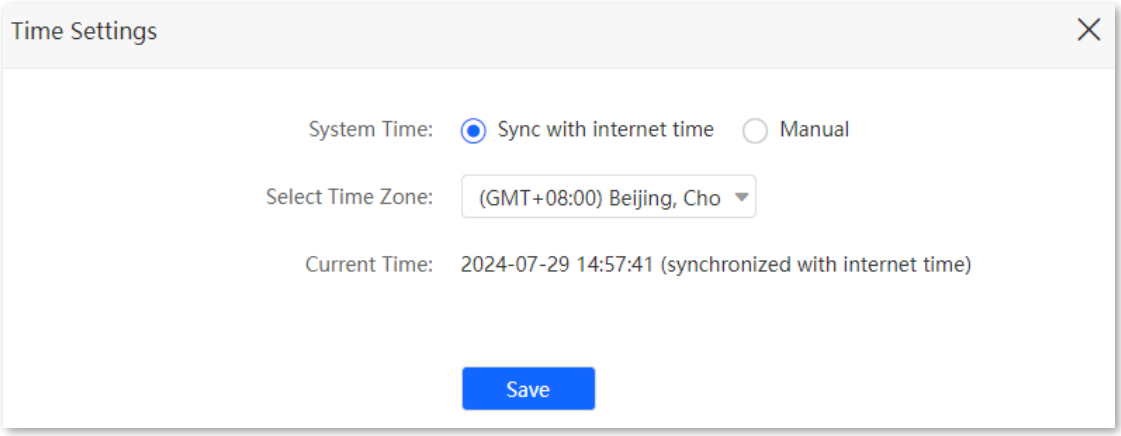


Figure 10-4 Sync with the Internet time

10.2.2 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.

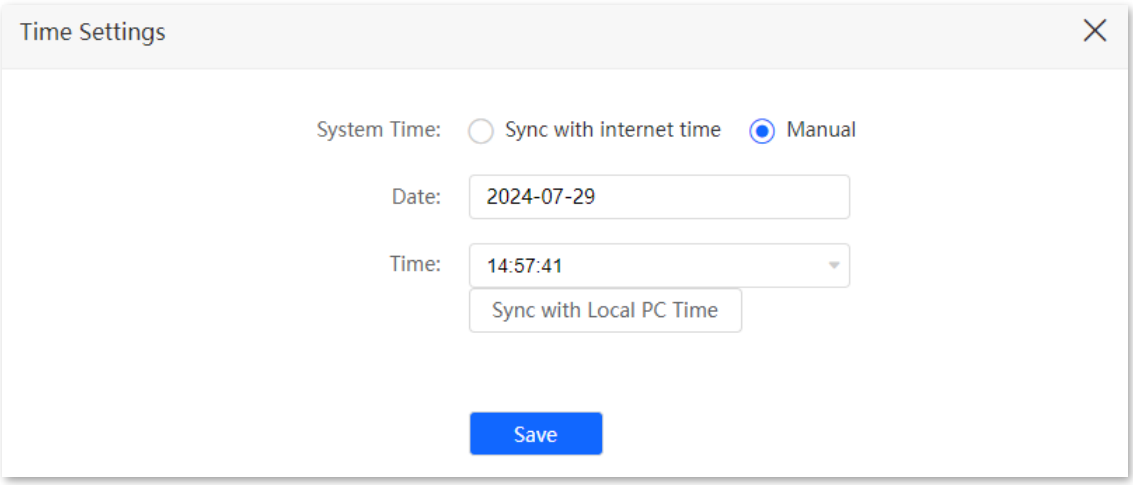


Figure 10-5 Set system time manually

10.3 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 enter the page, log in to the web UI of the router, and navigate to **System Settings** > **Login Password**. You can change the password and the old password is required to enter.

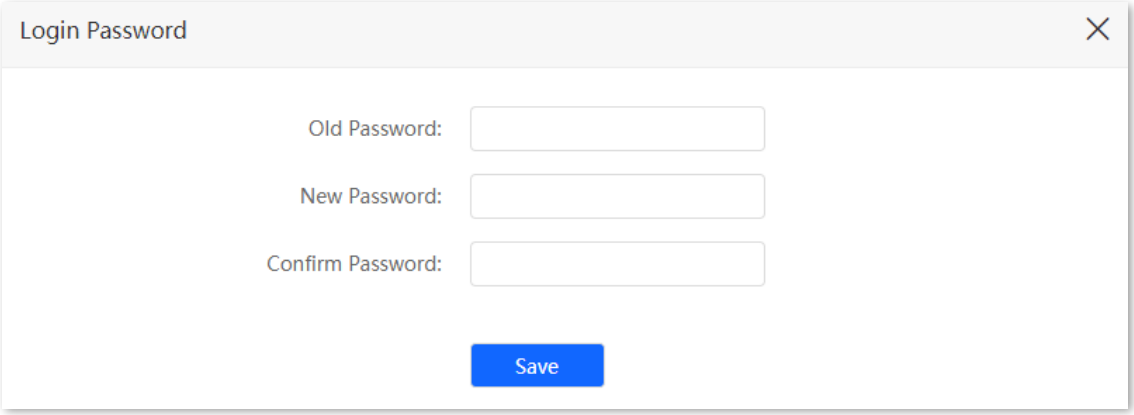


Figure 10-6 Configure login password

Note

- For initial setup or after a reset, set new login password for privacy and security (The longer the password, the stronger the protection). The character limit and composition rules for passwords are subject to software user interface prompts.
- If you forgot 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.

10.4 Reboot and reset

10.4.1 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 during leisure times.

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

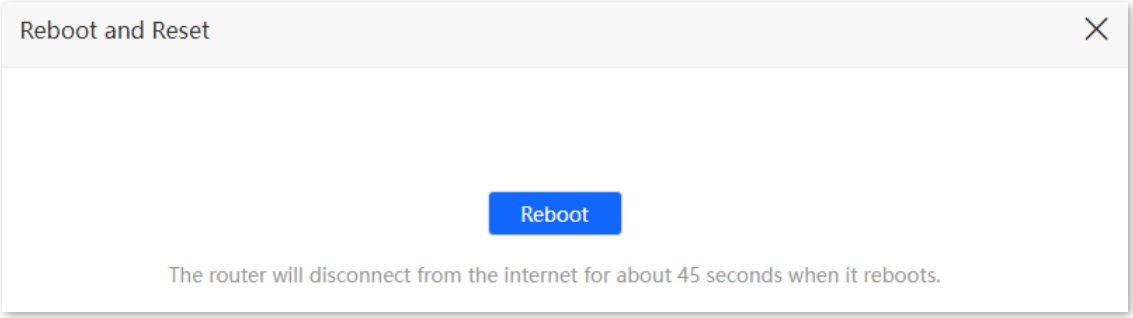


Figure 10-7 Reboot the router

Wait for a moment until the ongoing process finishes.

10.4.2 Reset the router

If you are uncertain about why the Internet is inaccessible through the router or you forgot 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 **WPS/RST** button on the rear panel of the router for about 8 seconds and release it when all indicators blink once. The router is restored to factory settings.

Reset the router on the web UI

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

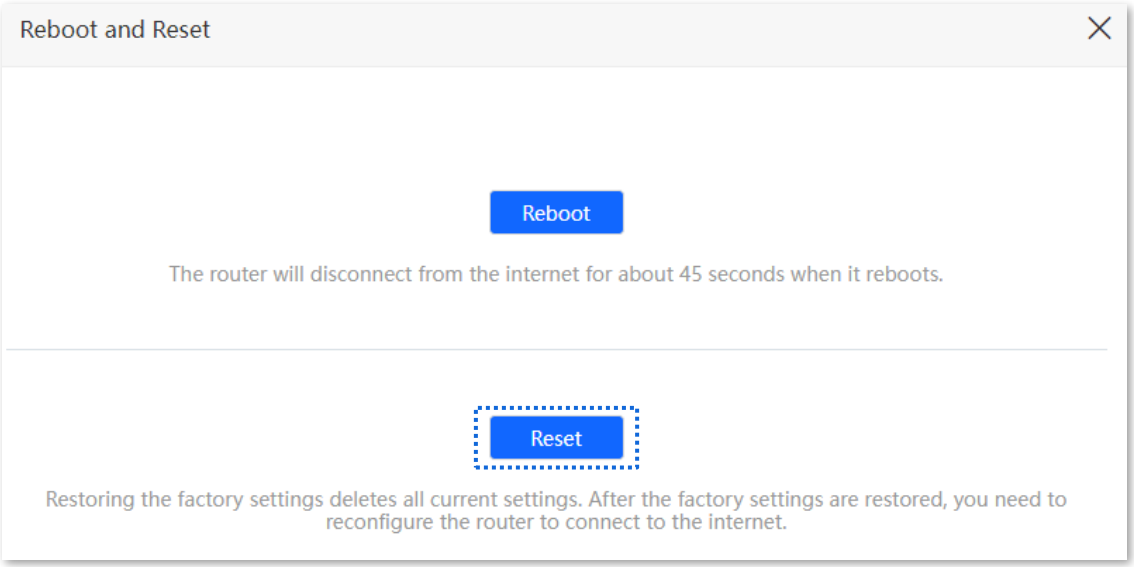


Figure 10-8 Reset the router

Wait for a moment until the ongoing process finishes.

10.5 Firmware upgrade

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

10.5.1 Online upgrade

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.

Procedure:

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

Step 2 Navigate to **System Settings** > **Firmware Upgrade**.

Step 3 Wait until a new firmware version is detected.

Step 4 Click **Update**.

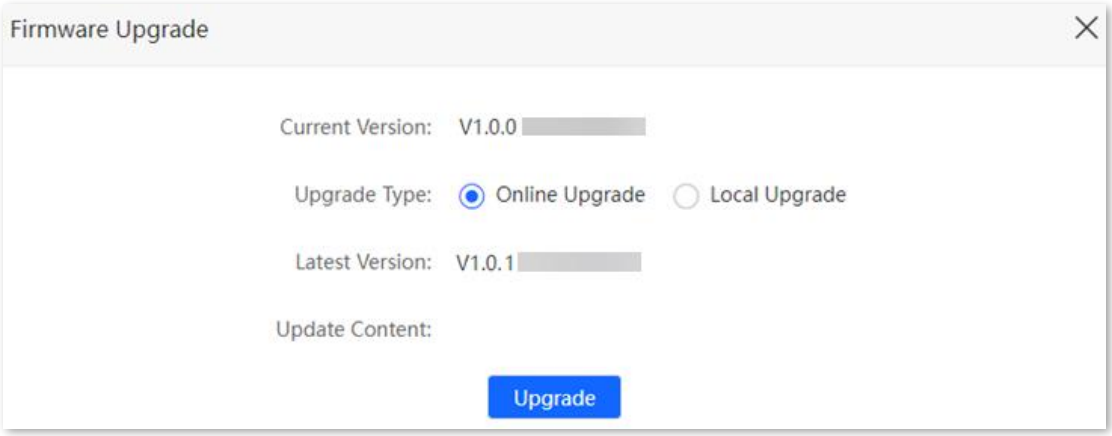


Figure 10-9 Online upgrade

Wait for a moment until the ongoing process finishes. Log in to the web UI of the router again. you can check whether the upgrade is successful based on the **Firmware Version** on the Internet Status page.

10.5.2 Local upgrade

Caution

To prevent the router from being damaged:

- Ensure that the firmware is applicable to the router.
- It is recommended to upgrade the firmware by connecting a LAN port to a computer and performing the upgrade on the web UI.
- When you are upgrading the firmware, do not power off the router.

Step 1 Go to https://www.hikvision.com/. Download an applicable firmware of the router to your local computer and unzip it.

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

Step 3 Navigate to **System Settings** > **Firmware Upgrade.**

Step 4 Choose **Local Upgrade**.

Step 5 Click **Select a file**. Select and upload the firmware that has been downloaded to your computer in step 1, and click **Upgrade**.

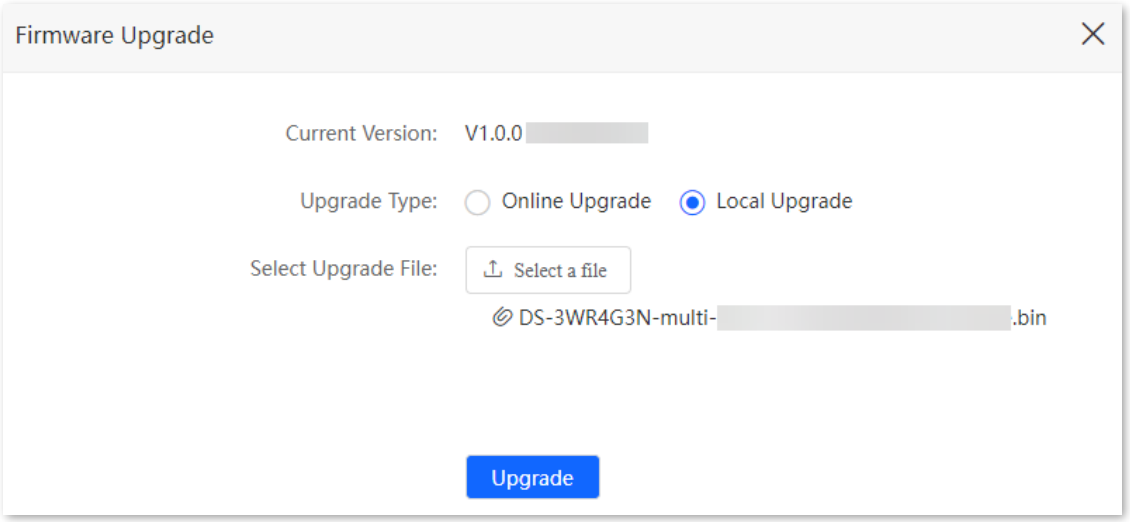


Figure 10-10 Local upgrade

Wait for a moment until the ongoing process finishes. Log in to the web UI of the router again, you can check whether the upgrade is successful based on the **Firmware Version** on the Internet Status page.

10.6 LAN settings

To enter the page, log in to the web UI of the router, and navigate to **System Settings** > **LAN Settings**.

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.

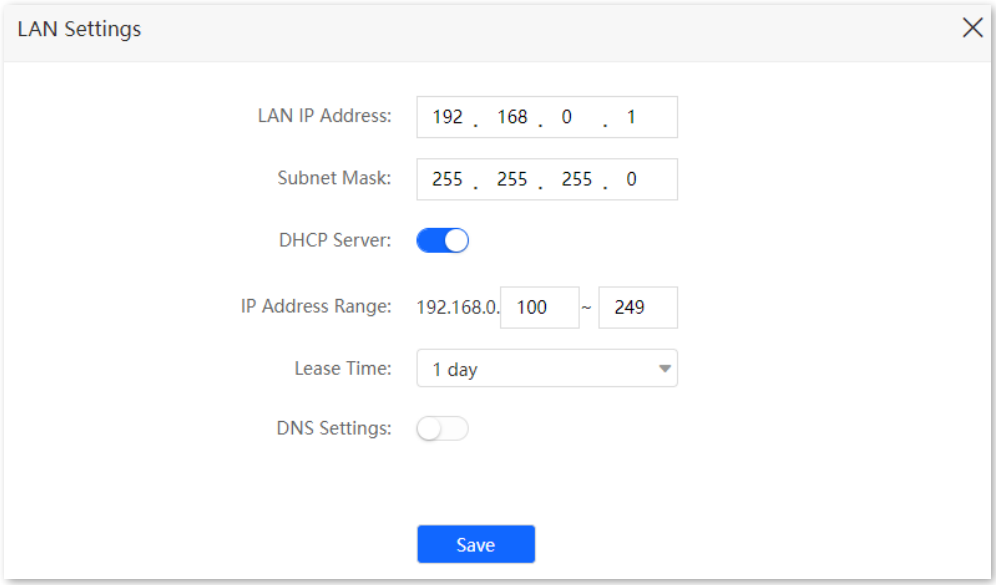


Figure 10-11 Configure LAN settings

Table 10-2 Parameter description

Parameter	Description
LAN IP Address	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	Specifies the subnet mask of the LAN port, used to identify the IP address range of the local area network.
DHCP Server	Used to enable or disable the DHCP server. Once enabled, the DHCP server automatically assigns Internet parameters such as IP address, subnet mask and gateway address to the client device. This function is recommended to be enabled.
IP Address Range	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. It is available only when **DHCP Server** is enabled.

Parameter	Description
Lease Time	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. The default value is recommended. It is available only when **DHCP Server** is enabled.
DNS Settings	Specifies whether to allocate another DNS address to the client. When it is disabled, the LAN port IP address of the router is used as the DNS address of the client. When it is enabled, **Primary DNS Server** must be set and **Secondary DNS Server** is optional. It is available only when **DHCP Server** is enabled.
Primary DNS Server	Specifies the primary DNS address of the router, which is assigned to the clients. You can change it if necessary. Ensure 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. It is available only when **DNS Settings** is enabled
Secondary DNS Server	Specifies the secondary DNS address of the router used to assign to the clients. It is an optional field and is left blank. It is available only when **DNS Settings** is enabled.

10.7 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 enter the page, log in to the web UI of the router, and navigate to **System Settings** > **Backup/Restore.**

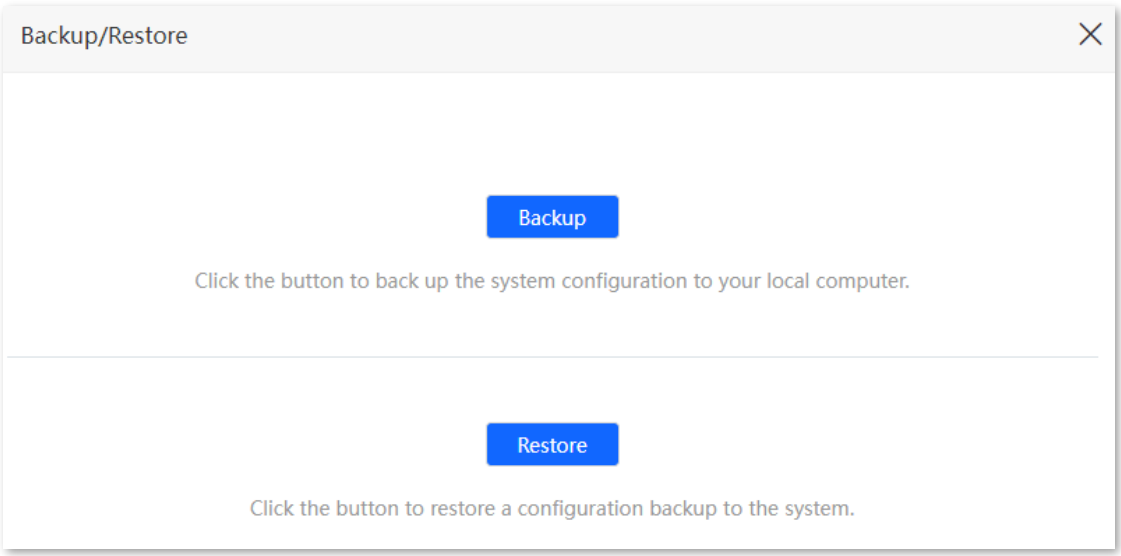


Figure 10-12 Backup and restore

10.7.1 Back up the configurations of the router

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

Step 2 Navigate to **System Settings** > **Backup/Restore**.

Step 3 Click **Backup**.

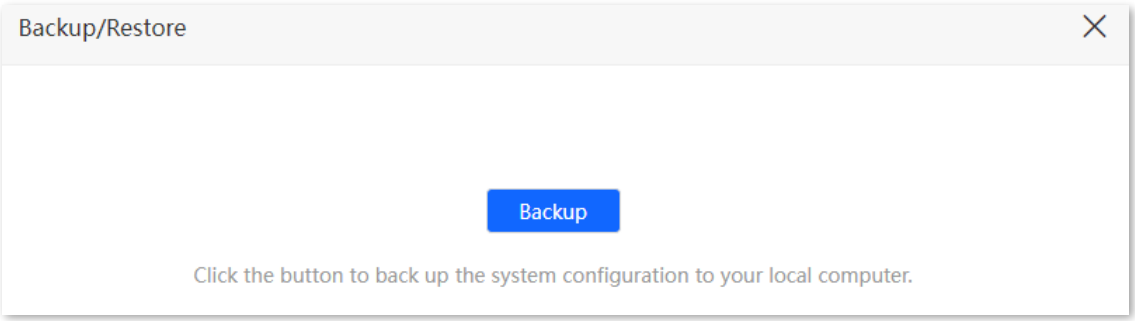


Figure 10-13 Back up the configurations

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

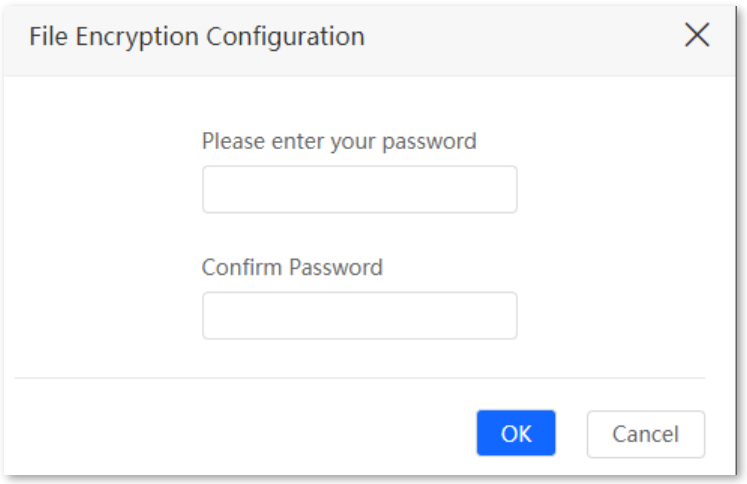
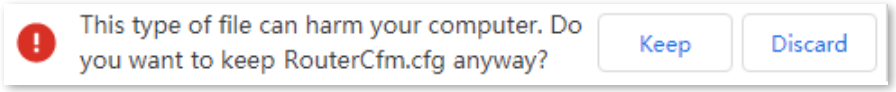


Figure 10-14 Enter the login password

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.



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

10.7.2 Restore previous configurations of the router

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

Step 2 Navigate to **System Settings** > **Backup/Restore**.

Step 3 Click **Restore**.

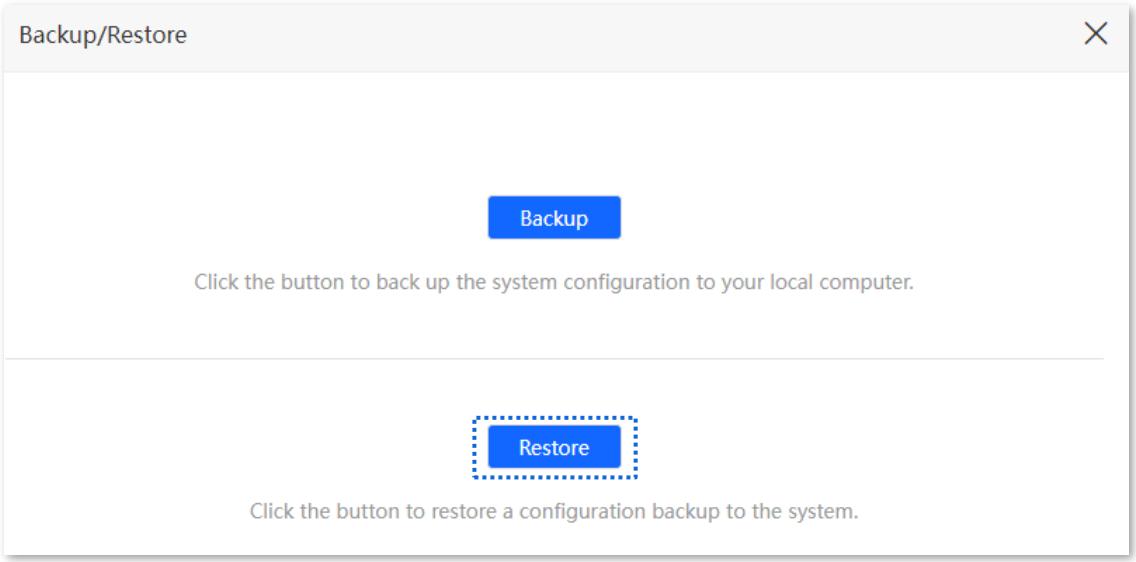


Figure 10-15 Restore previous configurations

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

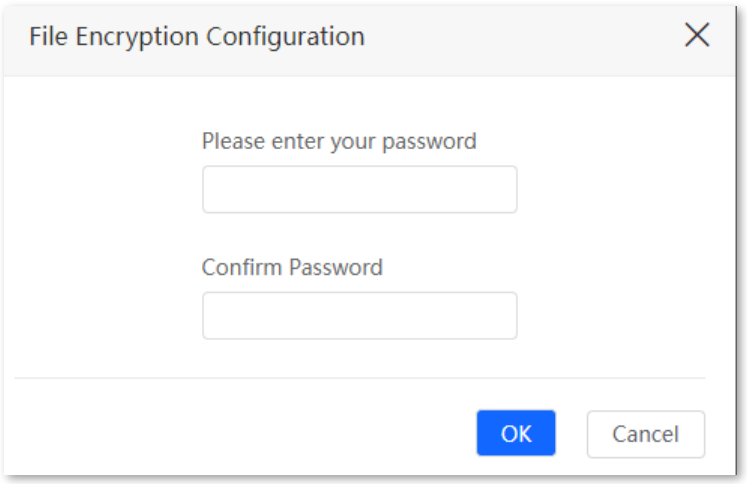


Figure 10-16 Enter the login password

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

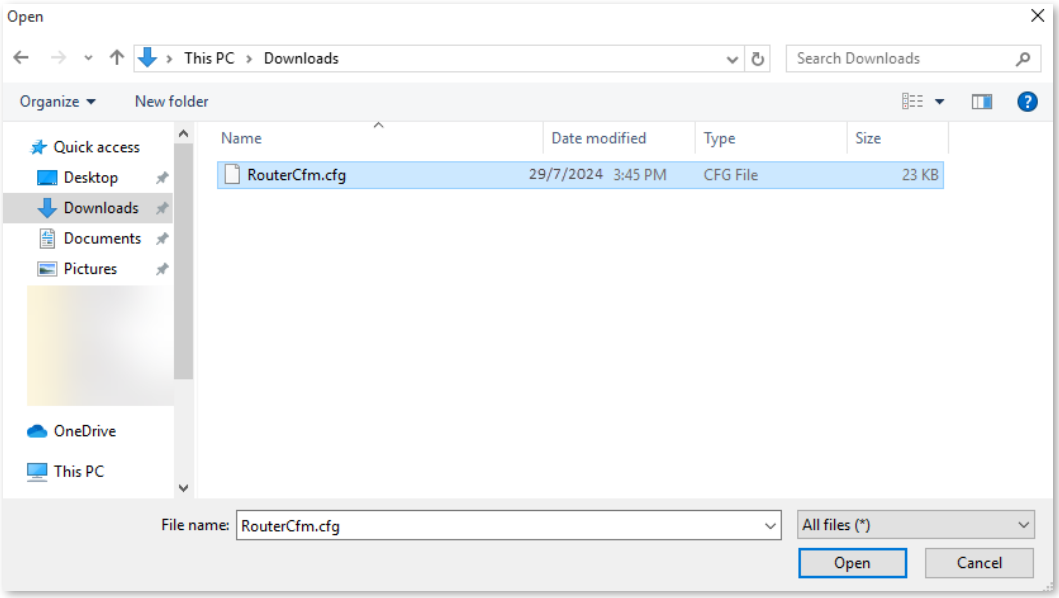


Figure 10-17 Upload the configuration file

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

10.8 Remote management

10.8.1 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 enter the page, log in to the web UI of the router, and navigate to **System Settings** > **Remote Management.**

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

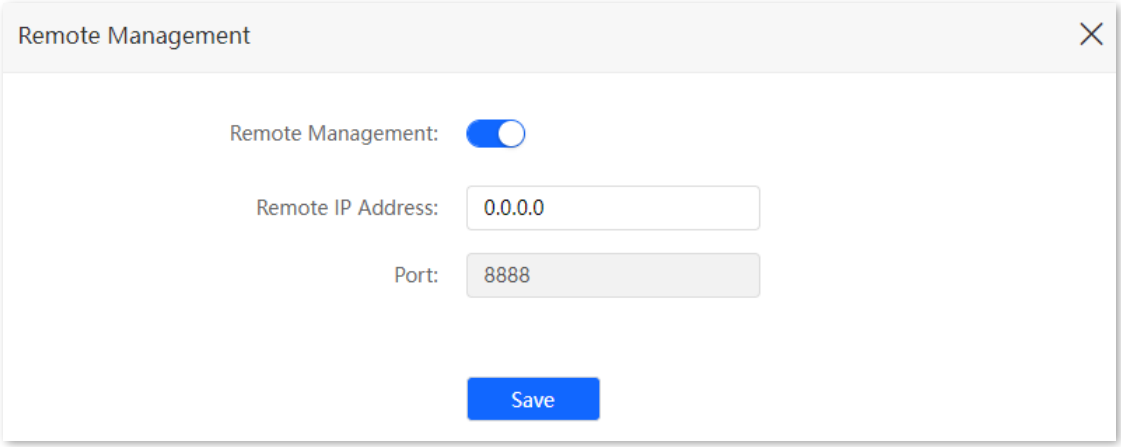


Figure 10-18 Enable remote management

Table 10-3 Parameter description

Parameter	Description
Remote Management	Used to enable or disable the remote management function of the router.
Remote IP Address	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	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”.

10.8.2 Example of configuring remote management function

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

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

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

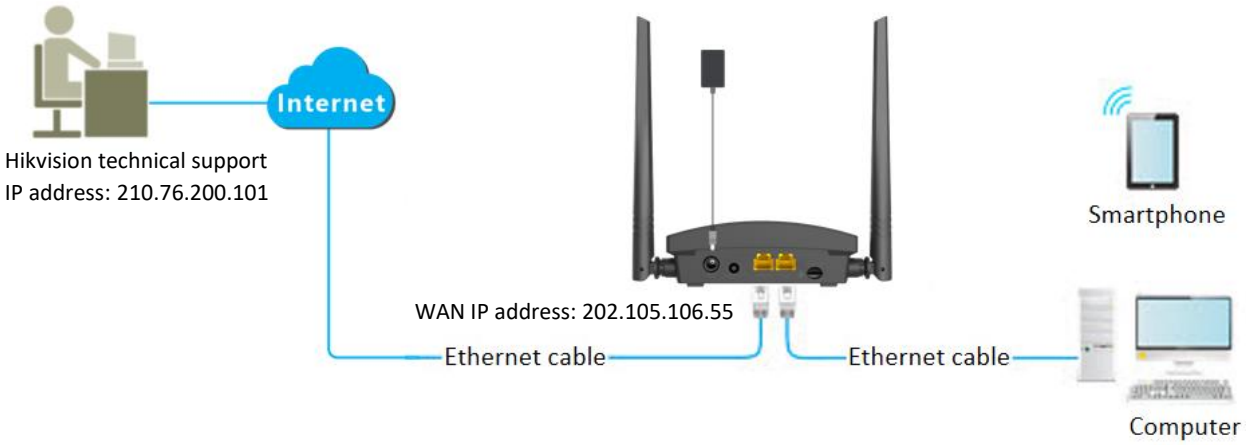


Figure 10-19 Physical connection

Procedure:

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

Step 2 Navigate to **System Settings** > **Remote Management**.

Step 3 Enable the **Remote Management**.

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

Step 5 Click **Save**.

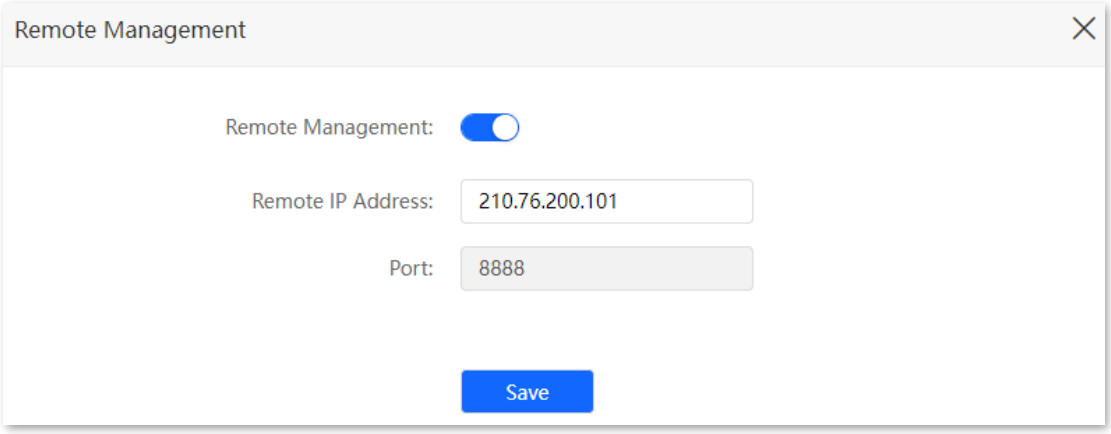


Figure 10-20 Configure remote management

After the configurations is 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.

10.9 System status

You can find the basic information of the router, LAN status and Wi-Fi status.

To enter the page, log in to the web UI of the router, and navigate to **System Settings** > **System Status.**

10.9.1 Basic information

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

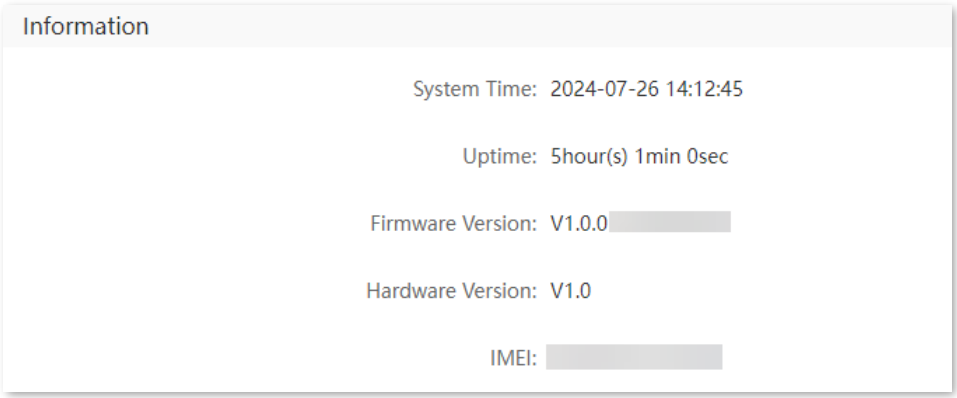


Figure 10-21 View basic information

For details about parameter description, refer to Basic information.

10.9.2 LAN status

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

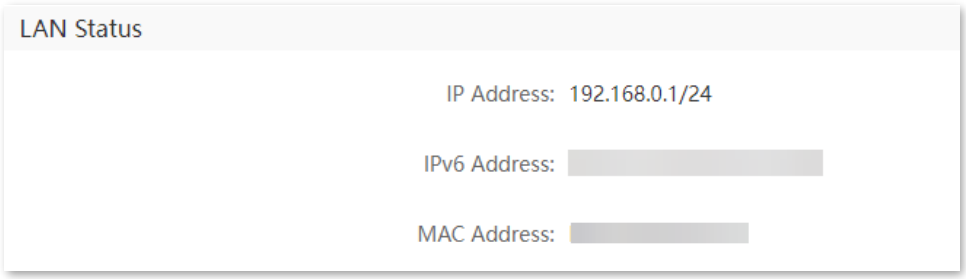


Figure 10-22 View LAN status

For details about parameter description, refer to LAN status.

10.9.3 Wi-Fi status

In this part, you can view the information of Wi-Fi network, including the visibility, Wi-Fi name, bandwidth, channel and MAC address.

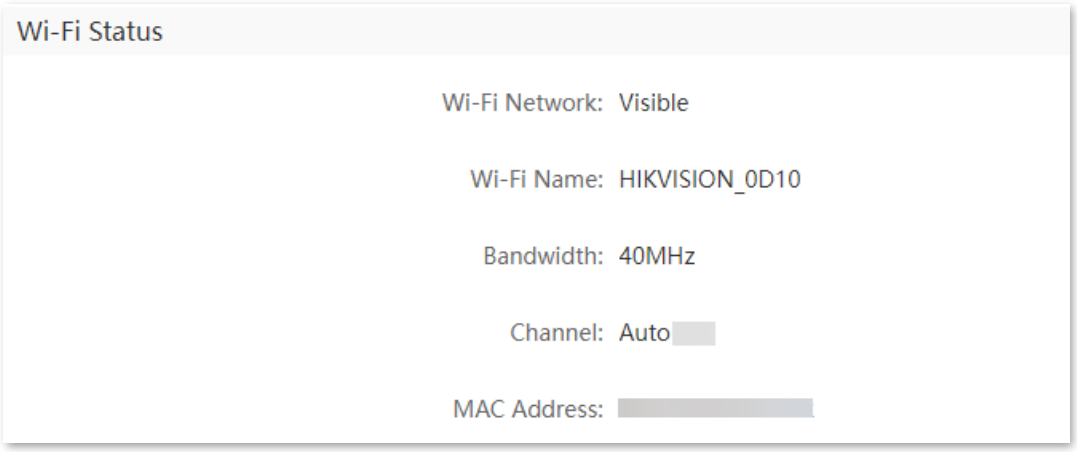


Figure 10-23 View Wi-Fi status

For details about parameter description, refer to Wi-Fi status.

10.10 System log

To enter the page, log in to the web UI of the router, and navigate to **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**. Then, enter the login password in the pop-up **File Encryption Configuration** window, and click **OK**.

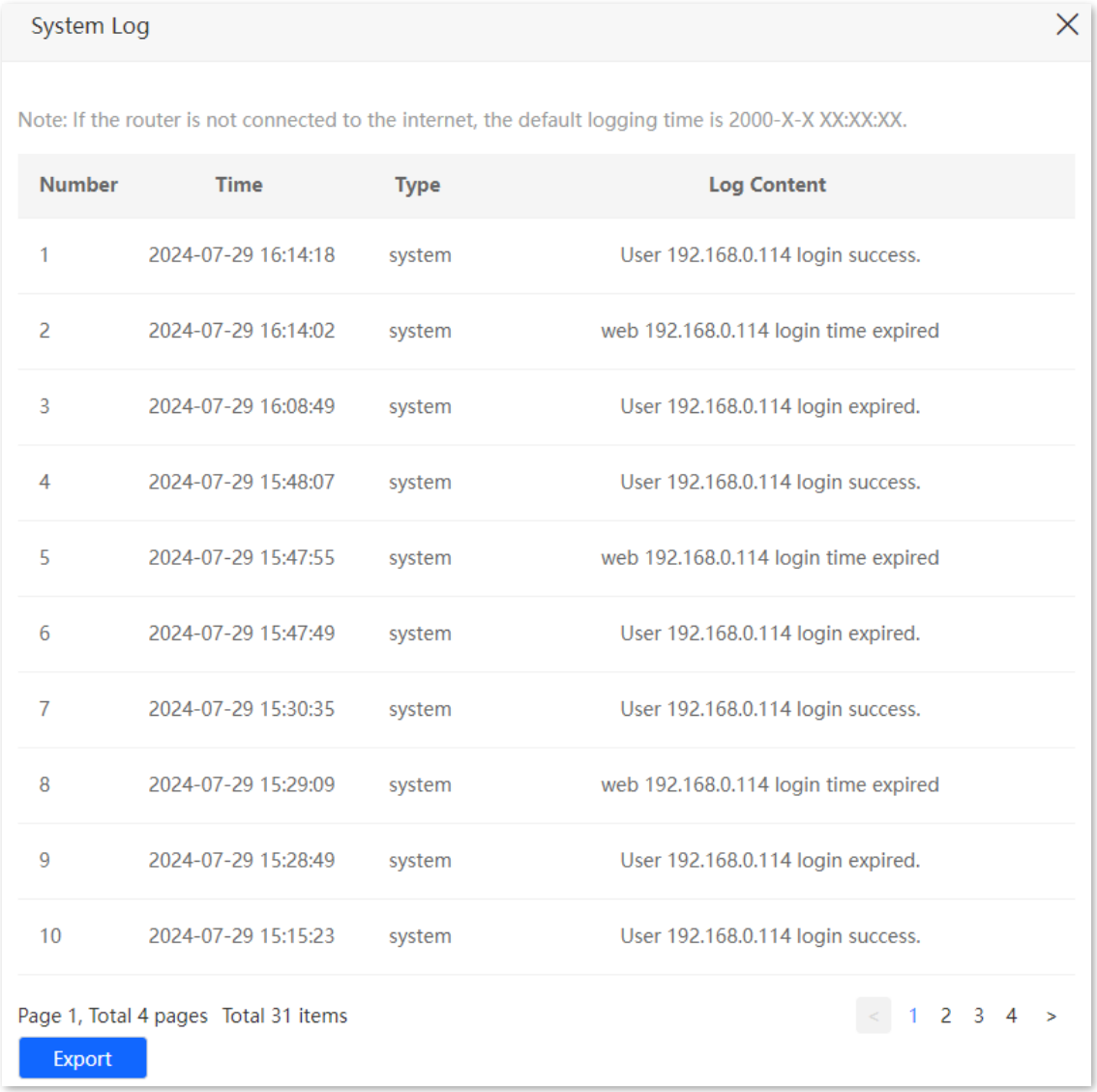


Figure 10-24 System log

Note

Rebooting the router will clear all previous system logs.

10.11 Automatic maintenance

Automatic maintenance enables you to make the router restart regularly and help improve the stability and service life of the router.

To enter the page, log in to the web UI of the router, and navigate to **System Settings** > **Automatic Maintenance.**

This function is enabled by default.

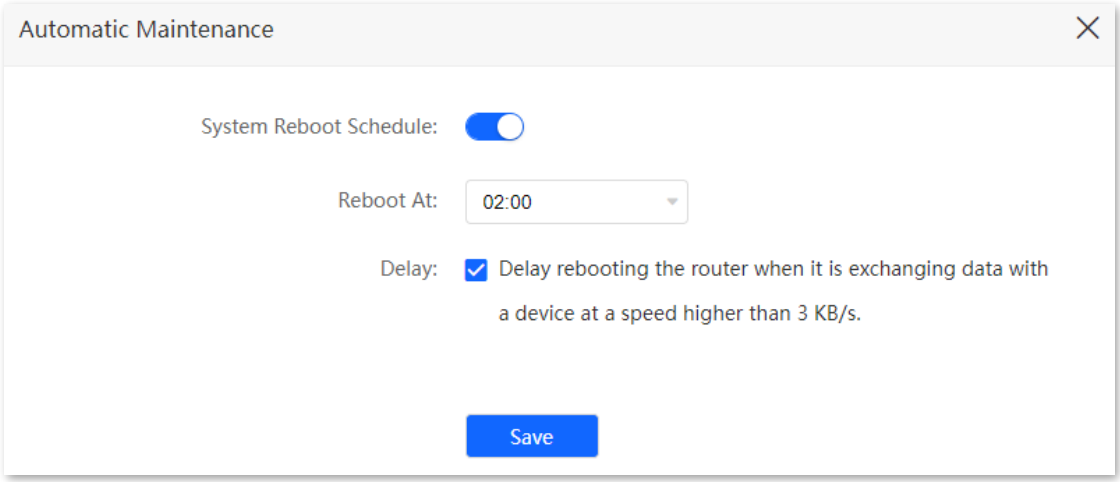


Figure 10-25 Configure automatic maintenance

Table 10-4 Parameter description

Parameter	Description
System Reboot Schedule	Used to enable or disable the automatic reboot function.
Reboot At	Specifies the time when the router reboots automatically every day.
Delay	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

Configure the computer to obtain an IPv4/IPv6 address automatically

Windows 10 is used for illustration here.

Step 1 Click  in the lower right corner of the desktop and choose **Network & Internet settings**.

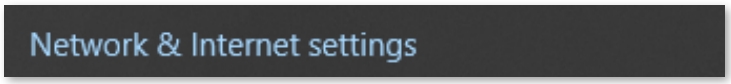


Figure 10-26 Choose Network & Internet settings

Step 2 Click **Change adapter options**.

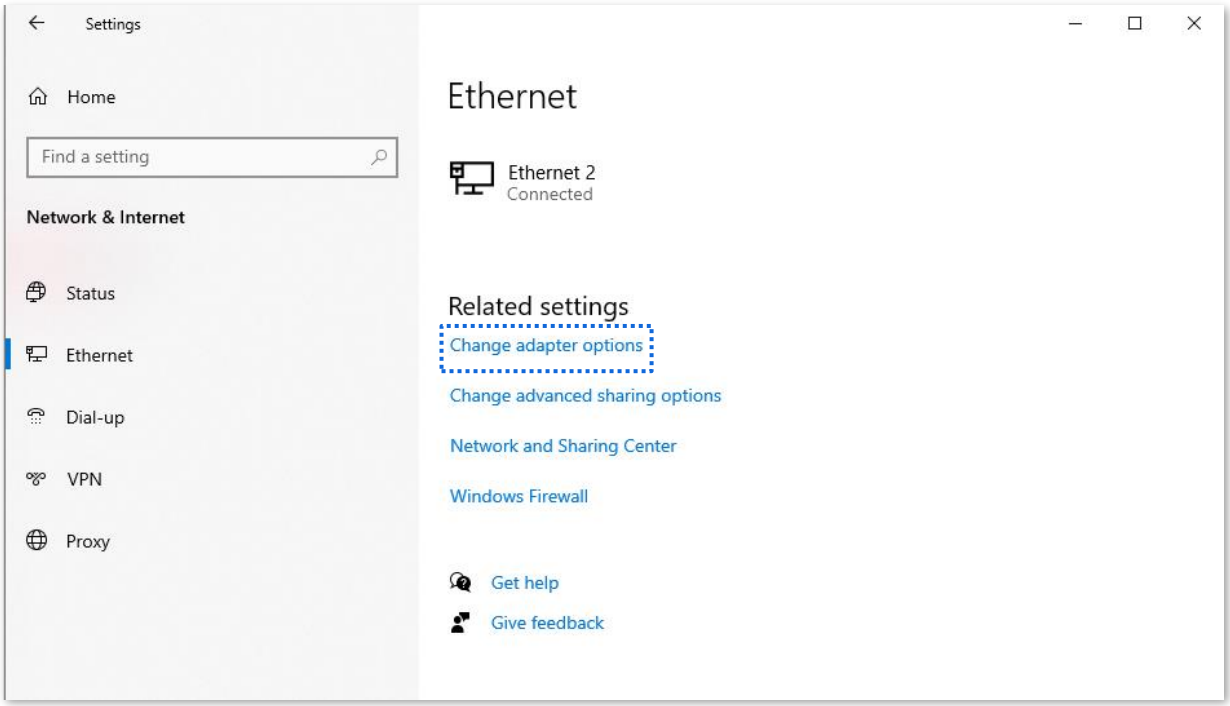


Figure 10-27 Click Change adapter options

Step 3 Right click on the connection which is being connected, and then click **Properties**.

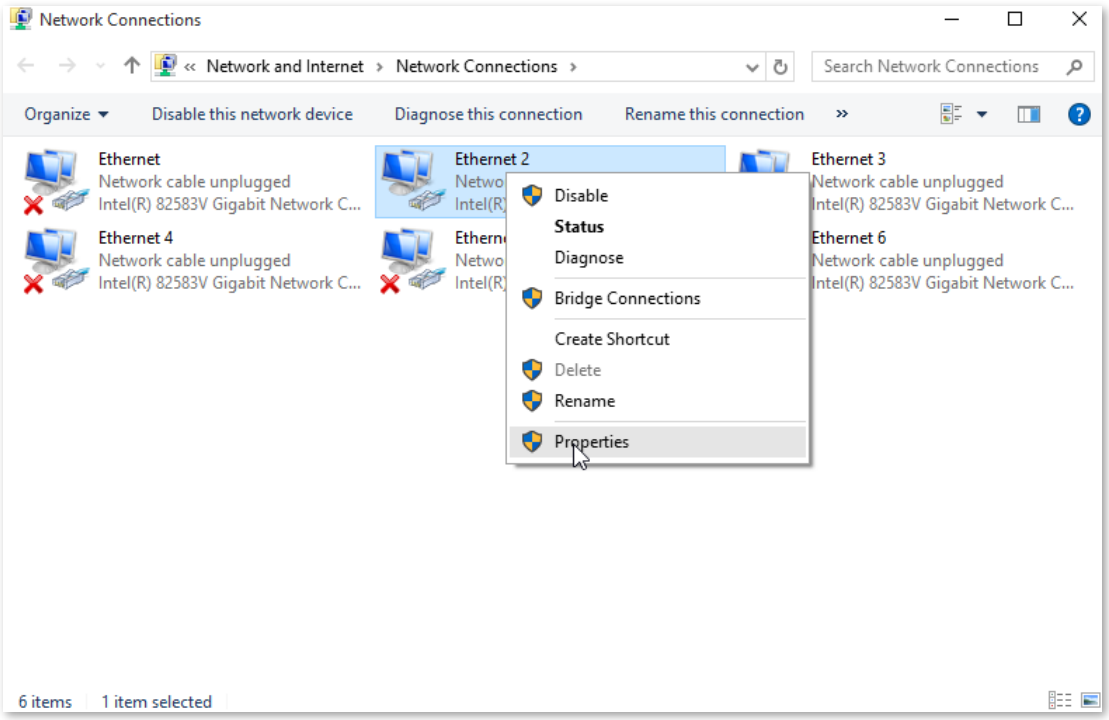


Figure 10-28 Click Properties

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)**.

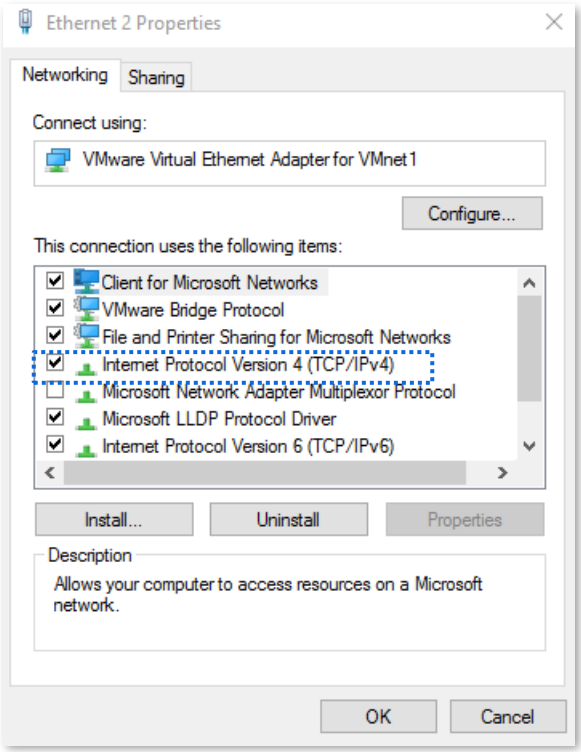


Figure 10-29 Double-click Internet Protocol Version 4 (TCP/IPv4)

Step 5 Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**, and click **OK**.

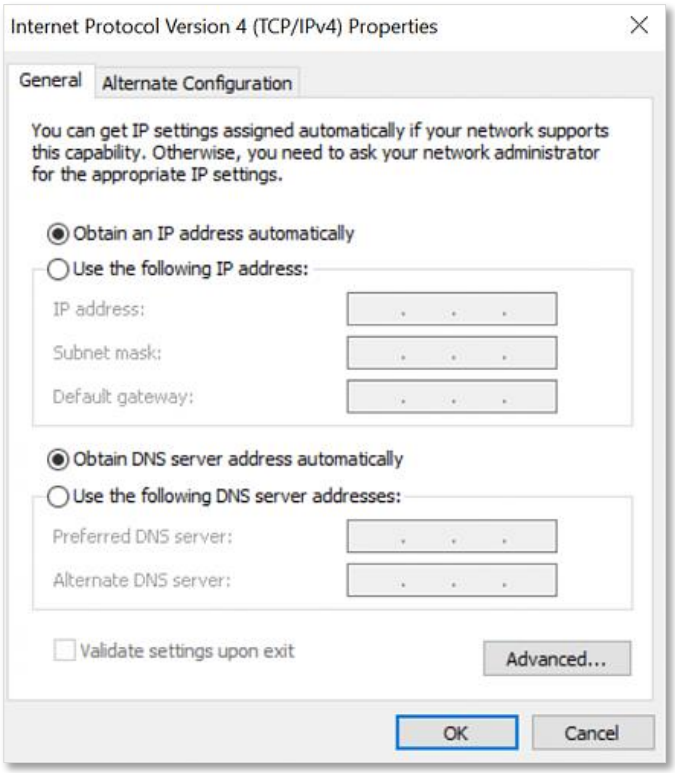


Figure 10-30 Configure Internet Protocol Version 4 (TCP/IPv4) Properties

Step 6 Click **OK** in the **Ethernet Properties** window.

Acronyms and abbreviations

Acronym or Abbreviation	Full Spelling
AES	Advanced Encryption Standard
DDNS	Dynamic Domain Name System
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
GMT	Greenwich Mean Time
IP	Internet Protocol
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
SSH	Secure Shell
SSID	Service Set Identifier
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
USSD	Unstructured Supplementary Service Data
WAN	Wide Area Network
WISP	Wireless Internet Service Provider

Acronym or Abbreviation	Full Spelling
WPA-PSK	WPA-Pre-shared Key


See Far, Go Further