User Guide

AC1200 Dual-Band Wi-Fi 4G+ LTE Router

4G08

Copyright Statement

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, Tenda reserves the right to make changes to the products without obligation to notify any person or organization of such revisions or changes. Tenda does not assume any liability that may occur due to the use or application of the product described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute the warranty of any kind, express or implied.

Preface

This guide describes how to configure each feature of the AC1200 Dual-Band Wi-Fi 4G+ LTE Router. In this guide, unless otherwise specified, all screenshots are taken from 4G08 V1.0.

NOTE

Features available in the router may vary by model and software version. Router availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual router experience.

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	Meaning
NOTE	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configurations, loss of data or damage to device.
TIP	This format is used to highlight a procedure that will save time or resources.

More information and support

Visit www.tendacn.com and search for the product model to get your questions answered and get the latest documents.

Revision history

Tenda is constantly searching for ways to improve its products and documentation. The following table indicates any changes that might have been made since this guide was first published.

Version	Date	Description
V1.0	2025-04-05	Original publication.

Contents

1 Get to know your device

1.1 Indicators

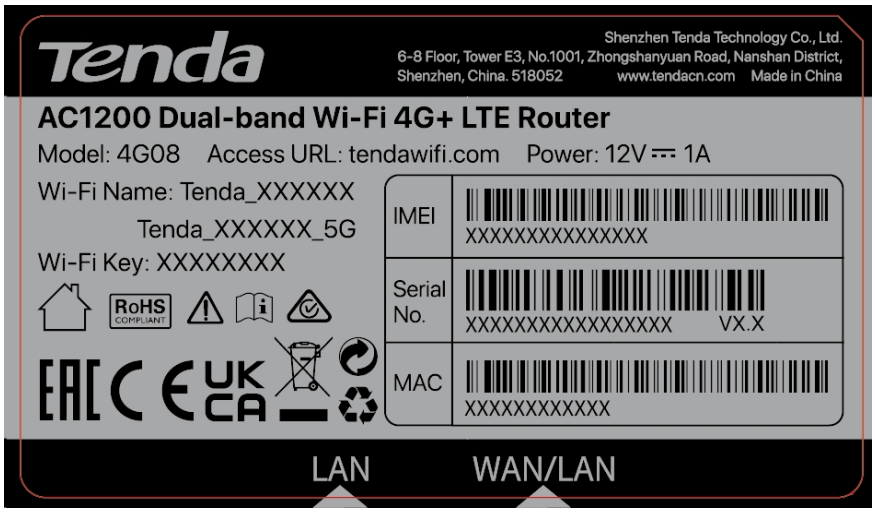
Indicator		Status	Description
	Internet	Solid on	Router is connected to internet
		Blinking	No internet access
	Wi-Fi	Solid on	Wi-Fi is enabled
		Blinking fast	Perform Mesh networking or WPS negotiation
		Off	Wi-Fi is disabled
	Ethernet port	Solid on	Device is connected to the Ethernet port
		Off	No device is connected to the Ethernet port
4G	3G/4G signal	3 bars	Excellent signal
		2 bars	Good signal
		1 bar	Fair signal
		Off	No signal

1.2 Button, ports and jack

Button/Port/Jack	Description
MESH/RST	- Mesh: Press the button for 1-3 seconds to enable Mesh networking of the router. - Reset: Press the button for 8 seconds to reset the router.
LAN	Used to connect to such devices as computers, switches or game machines.
WAN/LAN	LAN port by default. Used to connect to such devices as computers, switches or game machines. When the failover function is enabled, the **WAN/LAN** port only serves as a WAN port.
POWER	Use the power adapter to connect the router to a power source.
NANO SIM	Insert your Nano SIM card into this slot on the bottom of the router.

1.3 Label

The back label shows the model, access URL, power, Wi-Fi name, Wi-Fi key, IMEI, serial number and MAC address of the router. The following figure is for reference only.



Model: Model of the router

Access URL: URL used to log in to the web UI of the router

Power: Power supply for the router

Wi-Fi Name: Default Wi-Fi name of the router

Wi-Fi Key: Default Wi-Fi password of the router

IMEI: Unique mobile device identification code of the router

Serial No.: Serial number of the router

MAC: MAC address of the router

2 Quick setup

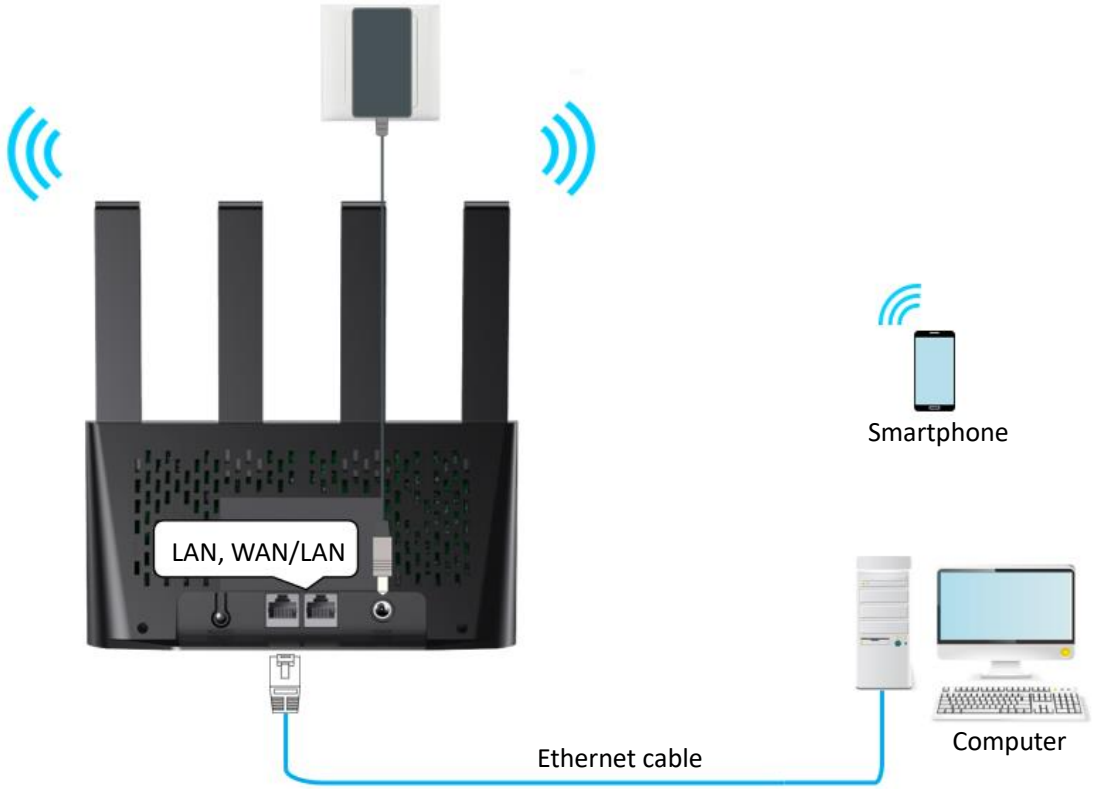
This chapter describes how to connect the devices and enable internet access through the quick setup wizard. You can complete quick setup for internet access by following the instructions on the web UI wizard. This wizard only occurs upon your first setup.

Procedure:

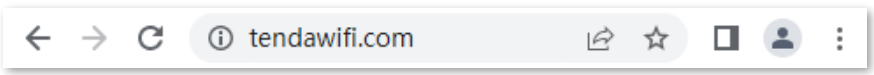
1. Connect your smartphone to the Wi-Fi network, or connect your computer to a LAN port of the router.

   TIP

   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.



2. Start a web browser on the device connected to the router, and visit **tendawifi.com** (computer used as an example).



3. Click **Start**.

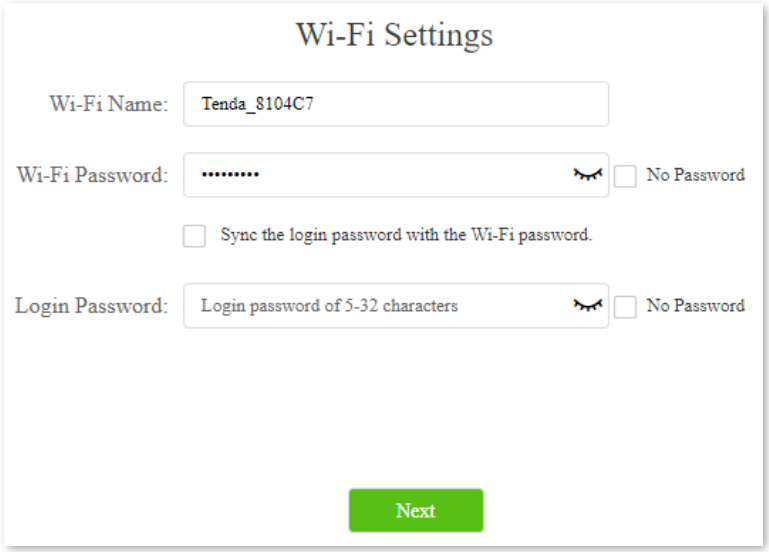
TIP

- If the SIM card is inserted properly and the internet connection is normal, you can continue the setup in step **4**.
- If **No SIM Card** is shown on the page, refer to No SIM card detected.
- If **SIM card blocked** is shown on the page, refer to Unlock the SIM card in the quick setup wizard.

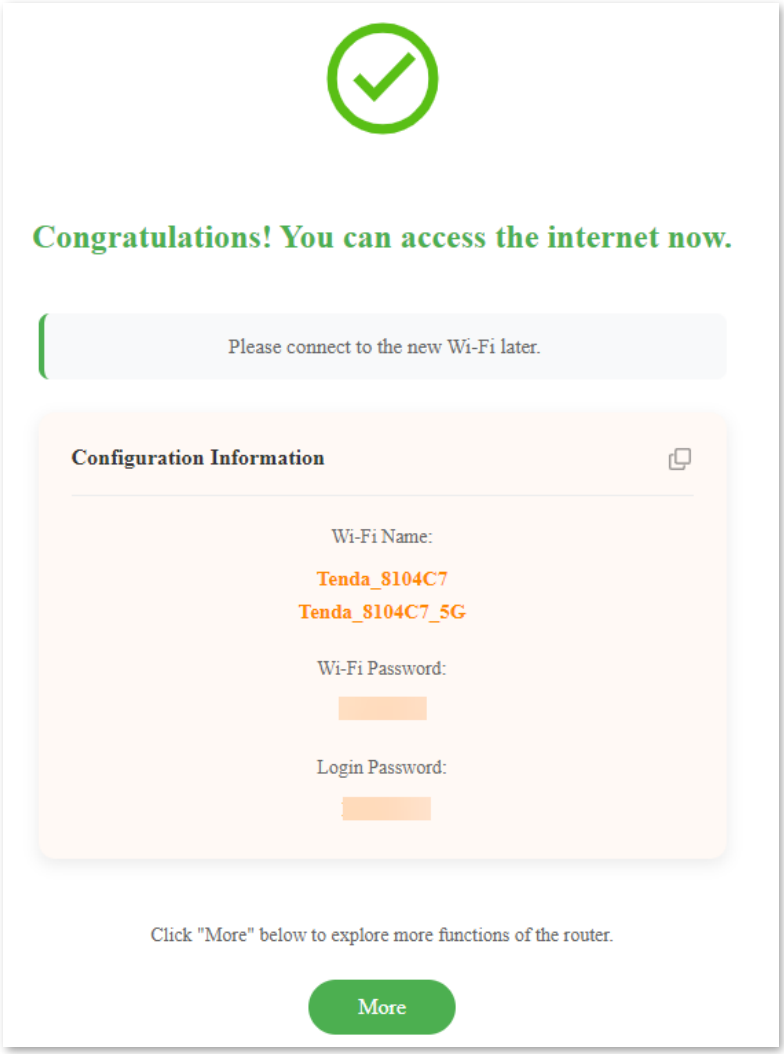
4. Set parameters as required, and click **Next**.

TIP

- If you do not want to use a password, tick **No Password**. In this case, any client can access the network without a password. **No Password** is not recommended as it leads to low network security.
- To use the same password for Wi-Fi access and web UI login, tick **Sync the login password with the Wi-Fi password**.
- To use different passwords for Wi-Fi access and web UI login, set Wi-Fi name and Wi-Fi password for Wi-Fi access and login password for web UI login.



5. If the following information is displayed, the quick setup for internet access is finished. Click **More**.



---End

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

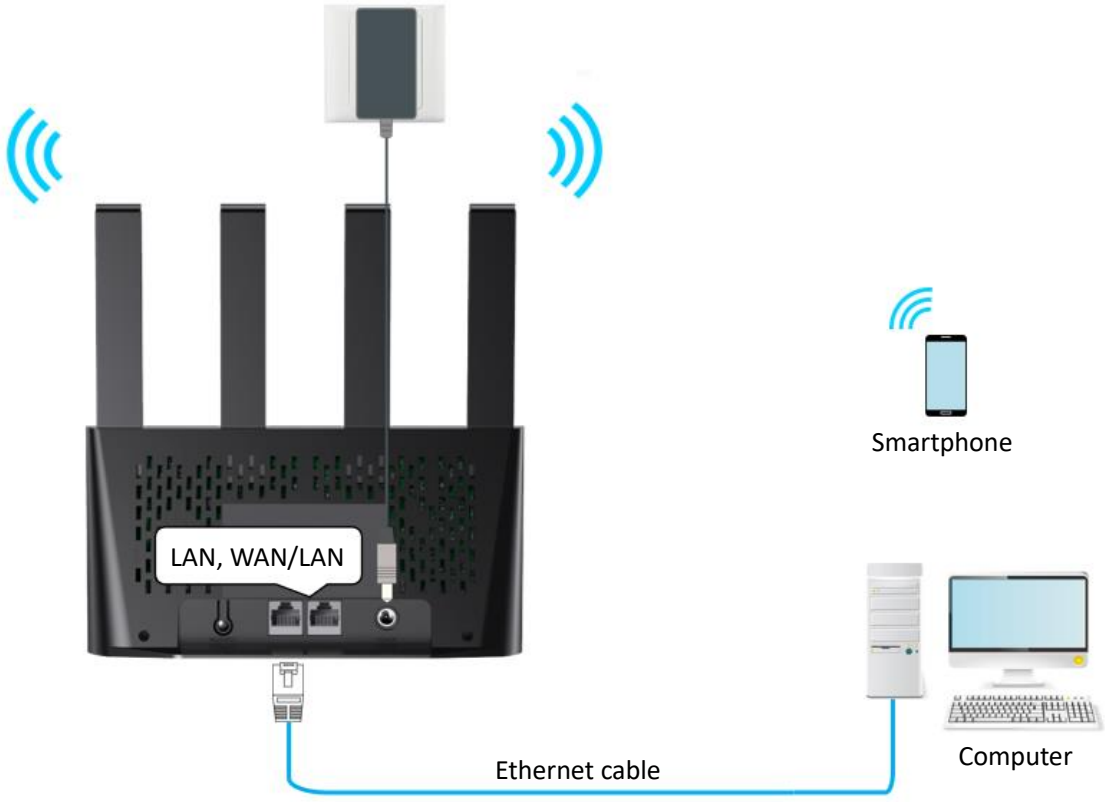
3 Web UI

3.1 Log in to the web UI

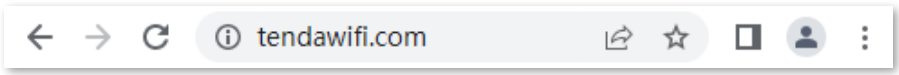
1. Connect your smartphone to the Wi-Fi network, or connect your computer to a LAN port of the router.

TIP

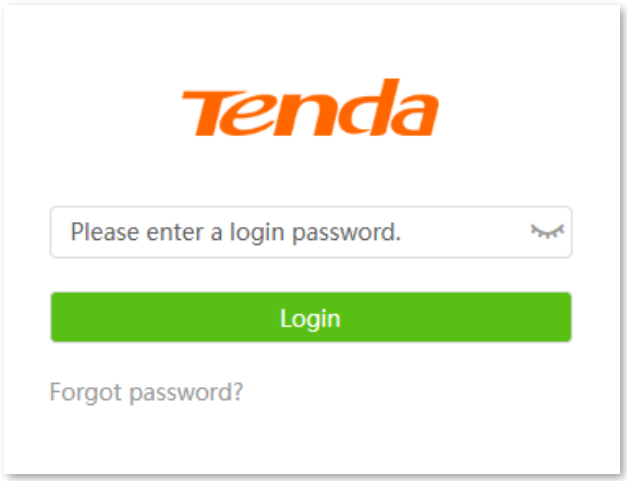
By default, the WAN/LAN and LAN port are both LAN ports. When the failover function is enabled, the WAN/LAN port only serves as a WAN port.



2. Start a web browser on the device connected to the router, and visit **tendawifi.com** (computer used as an example).



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



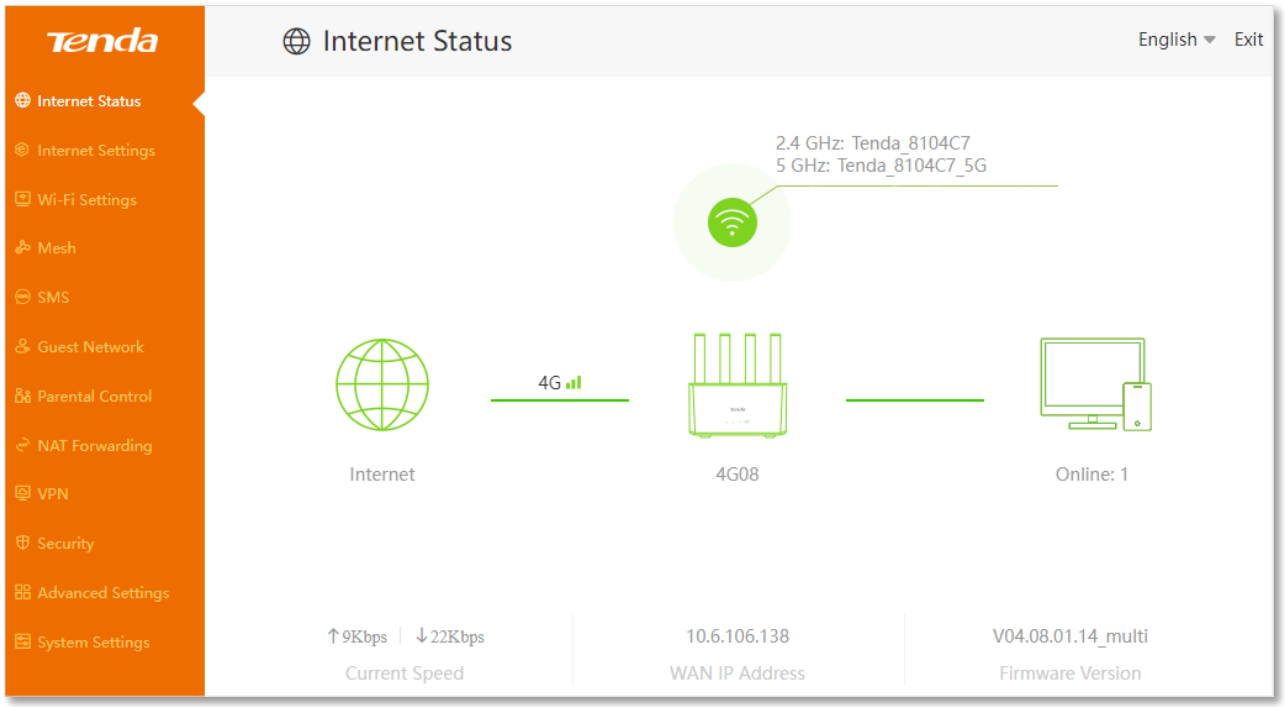
---End

TIP

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 properly.
- Clear the cache of your web browser or try again with another web browser.
- Try to enter **http://tendawifi.com** or **http://192.168.0.1** in the browser address bar (not the search bar).
- Ensure that the computer is set to **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
- Restore the router to factory settings and try again.

The following page appears.

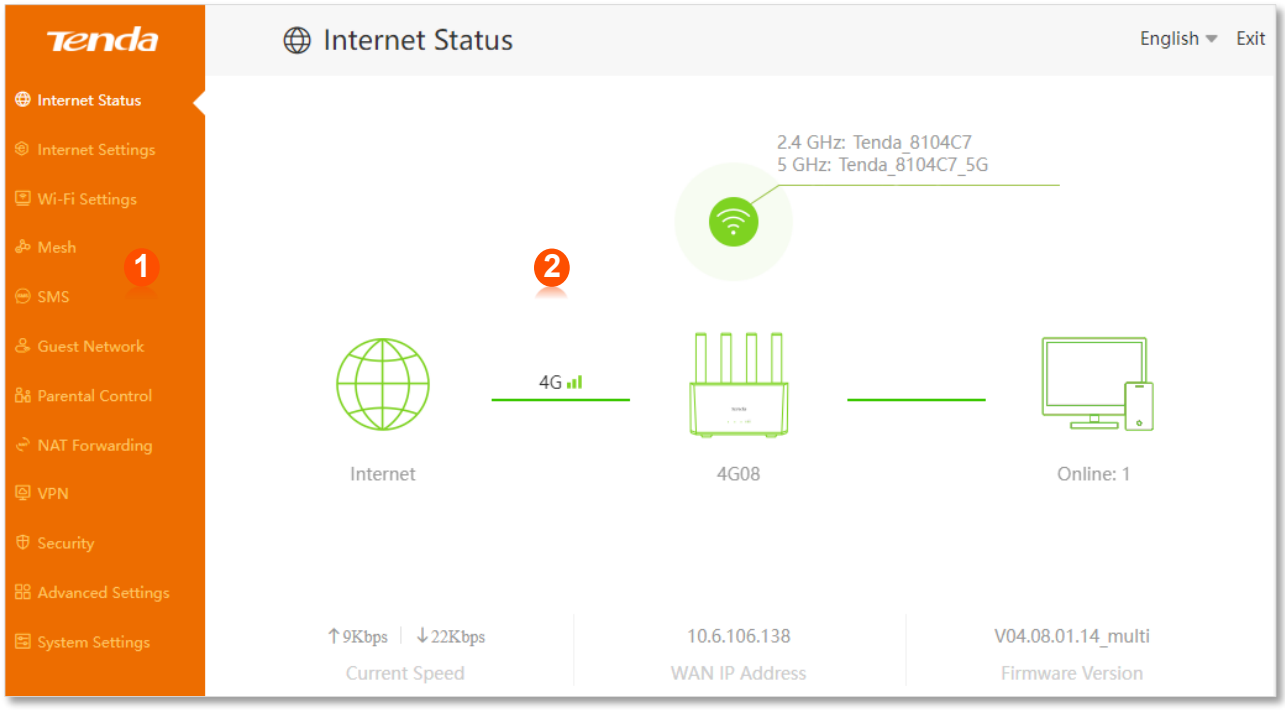


3.2 Log out of the web UI

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

3.3 Web UI layout

The web UI of the router consists of two sections, including the navigation bar and the configuration area. The following figure is for reference only.



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.

4 Internet status

4.1 View internet status

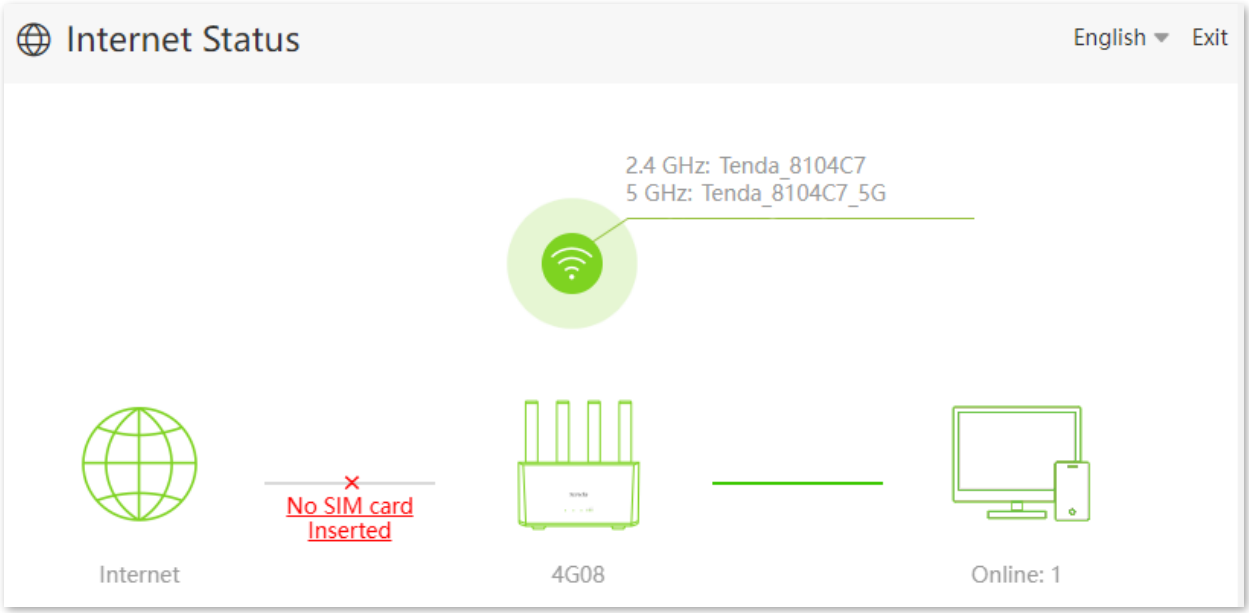
4.1.1 Through the SIM card

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

On this page, you can perform troubleshooting as prompted on the page when you access the internet through the SIM card.

No SIM card detected

When "No SIM card Inserted" is shown between the internet and the router, ensure the SIM card is inserted properly.



SIM card blocked

When "Please unlock the SIM card" is shown between the internet and the router, it indicates that the SIM card is locked. Refer to Unlock the SIM card on the web UI.

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 between the internet and the router, 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 between the internet and the router, 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 between the internet and the router, 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 between the internet and the router, 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 between the internet and the router, 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.

4.1.2 Through the WAN port

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

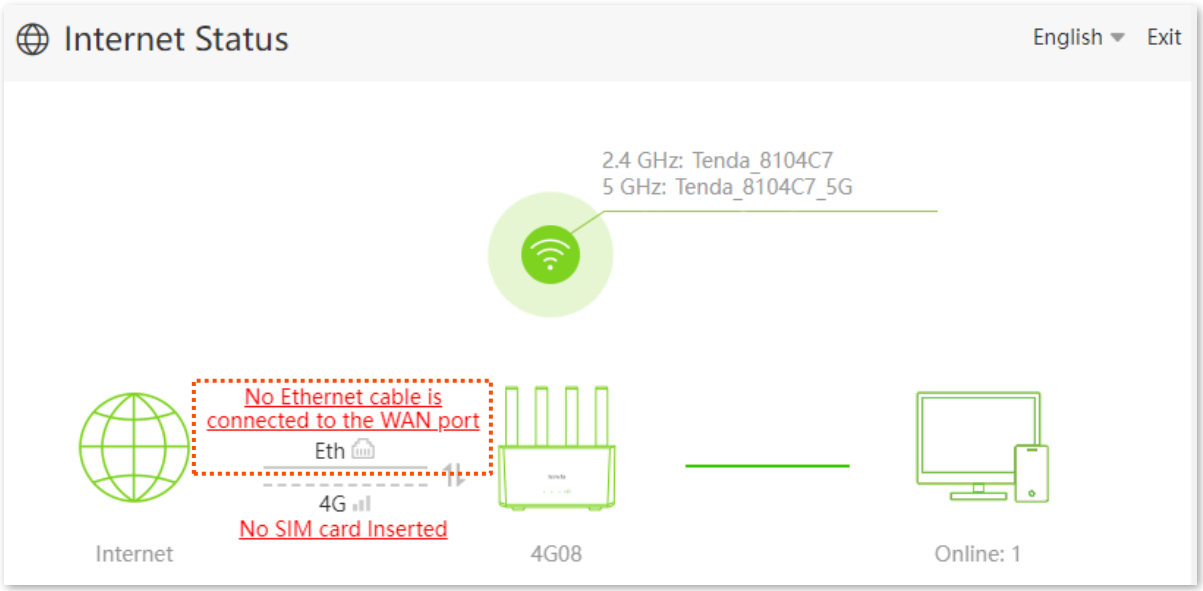
On this page, you can perform troubleshooting as prompted on the page when you access the internet through the WAN port.

TIP

- Before checking the internet status, you should connect the WAN/LAN port of the router to the internet using an Ethernet cable, enable the failover function and configure internet parameters on the **Internet Settings** page.
- The connection type **PPPoE** is used for illustration here.

Ethernet cable disconnected

When "No Ethernet cable is connected to the WAN port" is shown between the internet and the router, ensure the Ethernet cable is connected to the WAN port properly.



Incorrect user name and password

When "The user name and password are incorrect." is shown between the internet and the router, ensure 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 between the internet and the router, it indicates that the upstream server network may be abnormal. Contact your ISP for help.

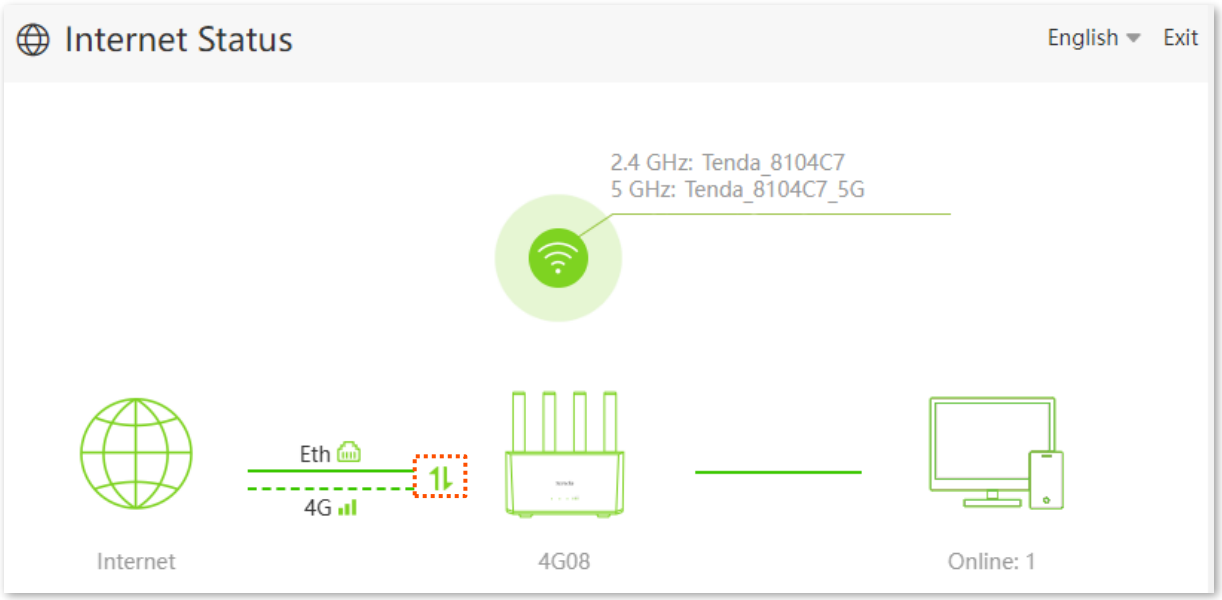
Connection disconnected

- When “Disconnected” is shown between the internet and the router, 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 between the internet and the router, it indicates that the connection is abnormal. Contact your ISP for help.

4.1.3 Through SIM card and WAN port

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

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 as required.



TIP

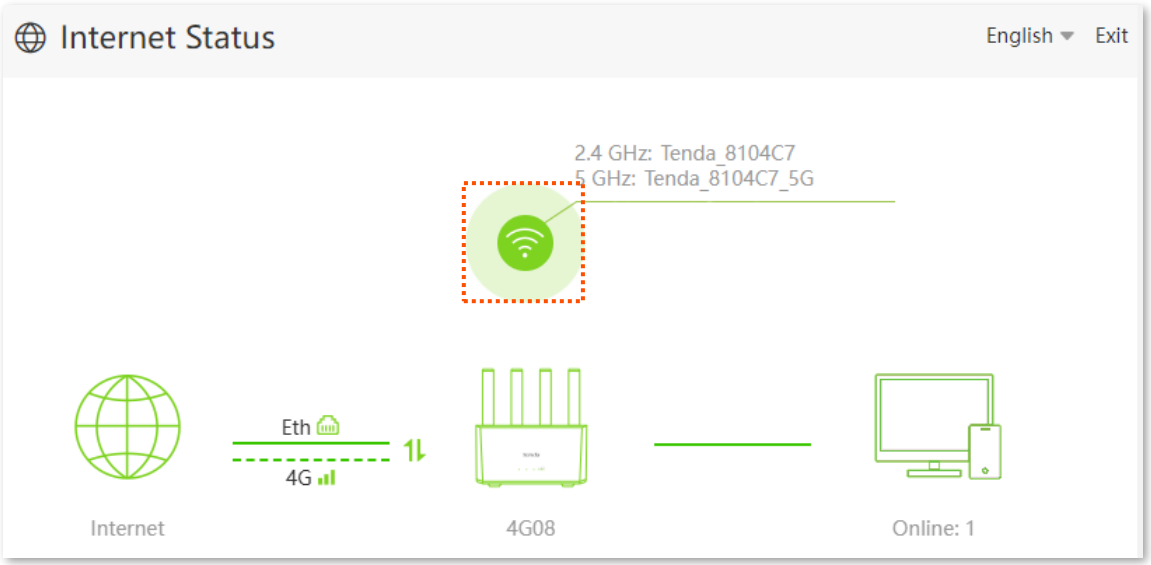
- If there is a network failure, the router will automatically switch to an available internet connection mode.
- If the other abnormal information is shown between the internet and the router, refer to access the internet through the SIM card or through the WAN port to find a solution.

4.2 View wireless information

On this page, you can view or configure the wireless information.

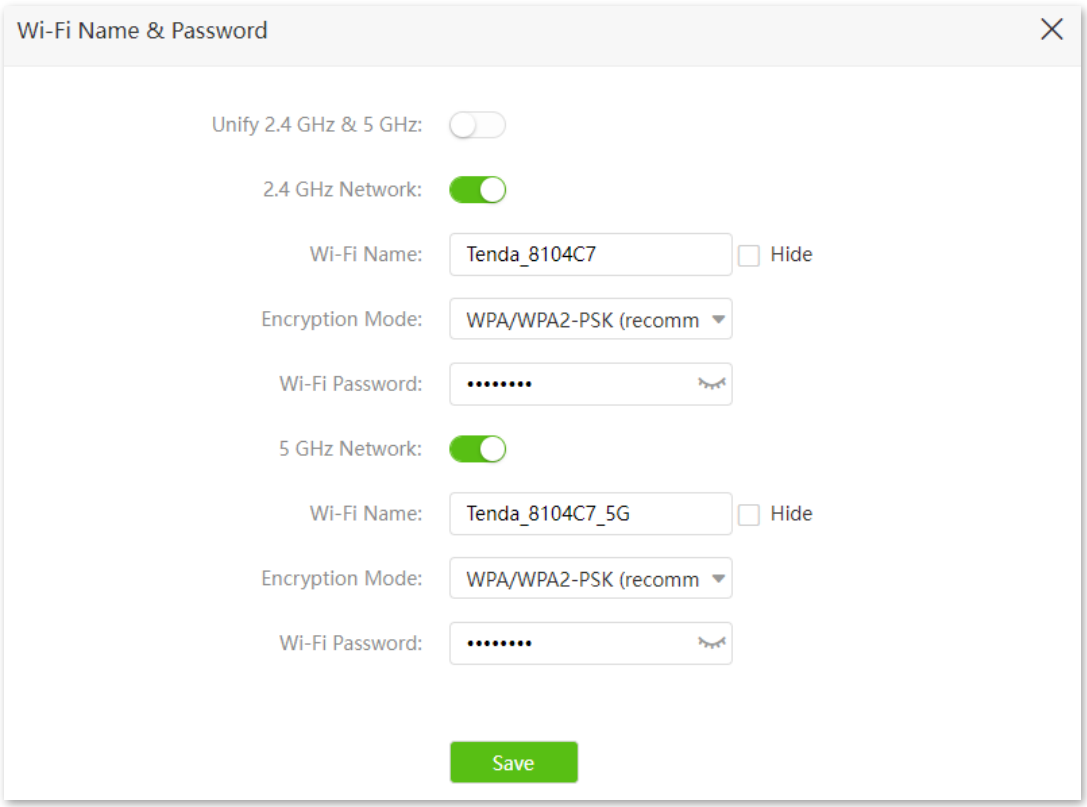
Procedure:

1. Log in to the web UI of the router.
2. Navigate to **Internet Status**.
3. Click  .



---End

You can change wireless parameters as required.



4.3 View WAN status

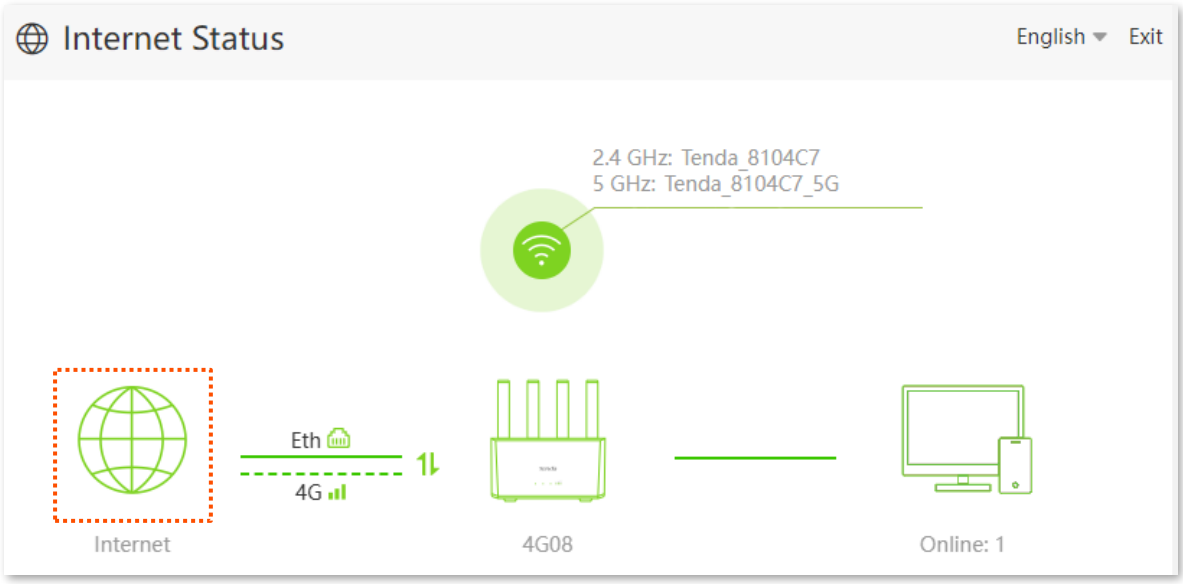
On this page, you can view the WAN status, including 3G/4G and Ethernet WAN status.

TIP

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

Procedure:

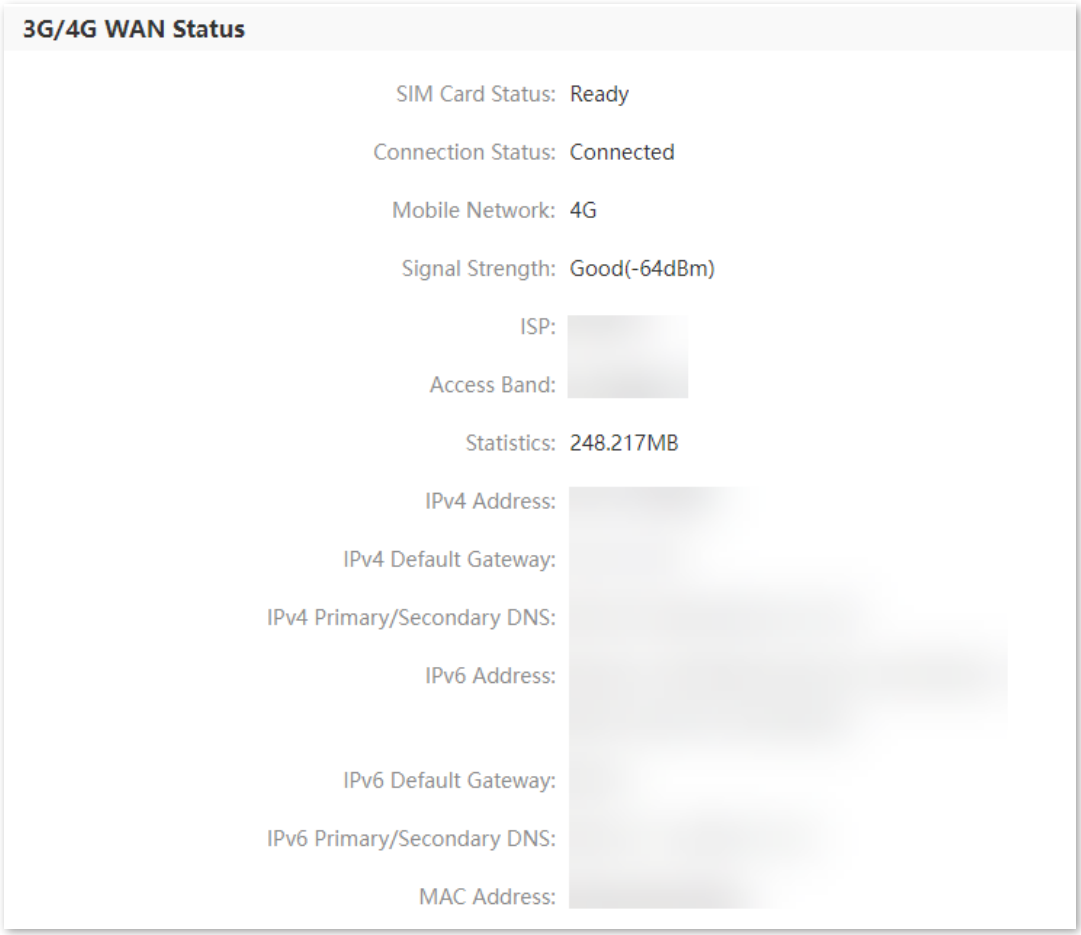
1. Log in to the web UI of the router.
2. Navigate to **Internet Status**.
3. Click .



---End

4.3.1 3G/4G WAN status

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



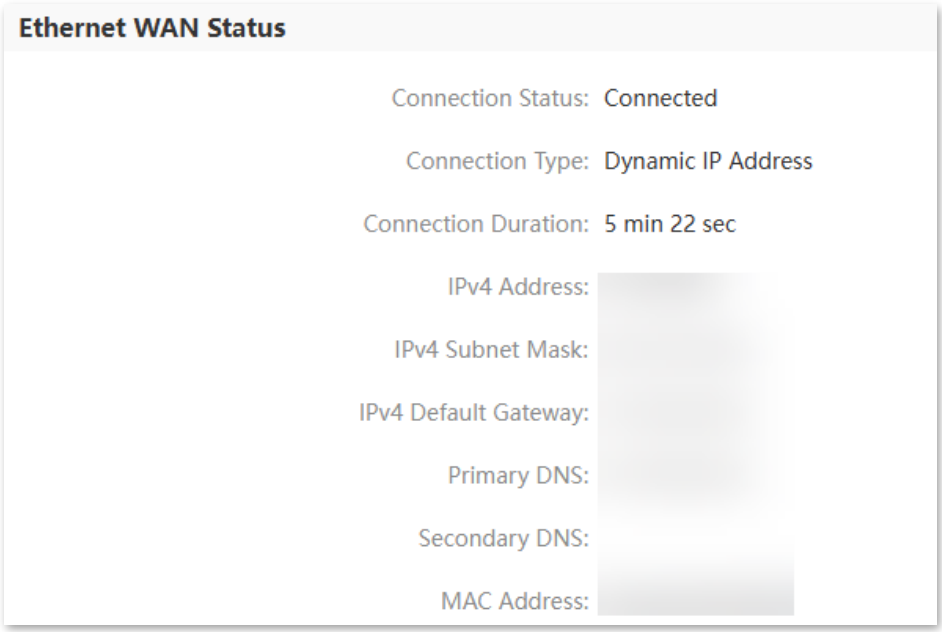
Parameter description

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.
Mobile Network	Specifies the current network type for internet access.
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.
Access Band	Specifies the access band of the mobile network of the router.
Statistics	Specifies the data traffic of the SIM card that has been used.

Parameter	Description
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.
MAC Address	Specifies the 3G/4G MAC address of the router.

4.3.2 Ethernet WAN status

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



Parameter description

Parameter	Description
Connection Status	Specifies internet connection status of WAN/LAN port connected to the Ethernet cable.

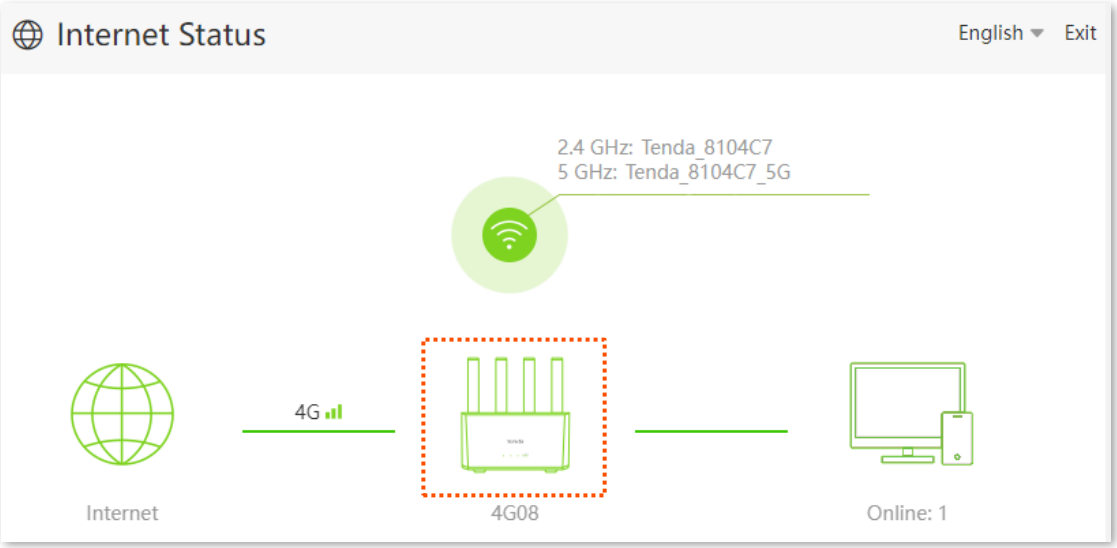
Parameter	Description
Connection Type	Specifies how your router connects to the internet, including: - **PPPoE**: Select this type if you access the internet using the PPPoE user name and PPPoE password. - **Dynamic IP Address**: Select this type if you can access the internet by simply plugging in an Ethernet cable. - **Static IP Address**: Select this type if you want to access the internet using fixed IP information.
Connection Duration	Specifies the connection duration of WAN/LAN port connected to the Ethernet cable.
IPv4 Address	Specifies the WAN IP address of the router.
IPv4 Subnet Mask	Specifies the WAN subnet mask of the router.
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.
MAC Address	Specifies the Ethernet MAC address of the router.

4.4 View system information

On this page, you can view the system information, including system time, uptime, firmware version, hardware version, LAN status and Wi-Fi status.

Procedure:

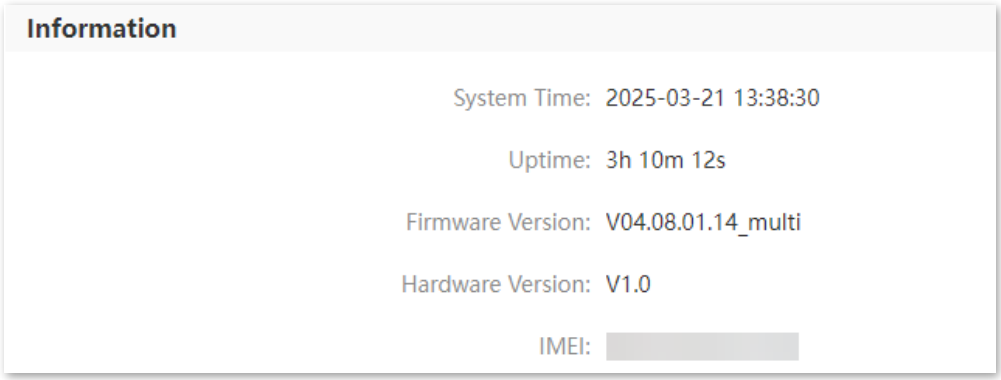
1. Log in to the web UI of the router.
2. Navigate to **Internet Status**.
3. Click  .



---End

4.4.1 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.

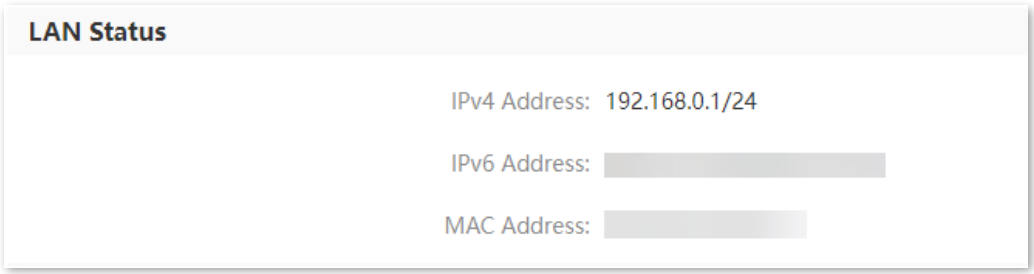


Parameter description

Parameter	Description
System Time	Specifies the system time of the router.
Uptime	Specifies 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.

4.4.2 LAN status

In this part, you can view the LAN information, such as LAN IPv4 address, IPv6 address and MAC address.

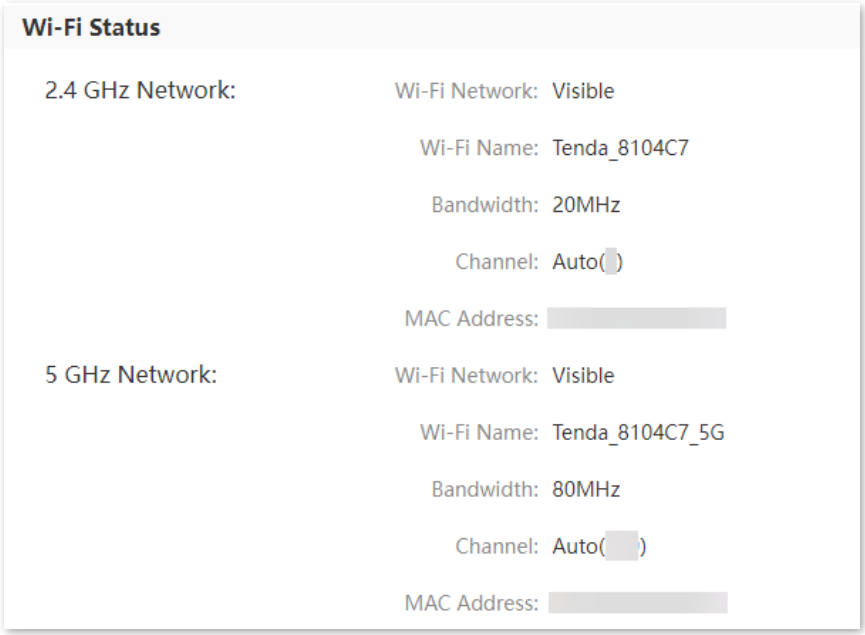


Parameter description

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.

4.4.3 Wi-Fi status

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



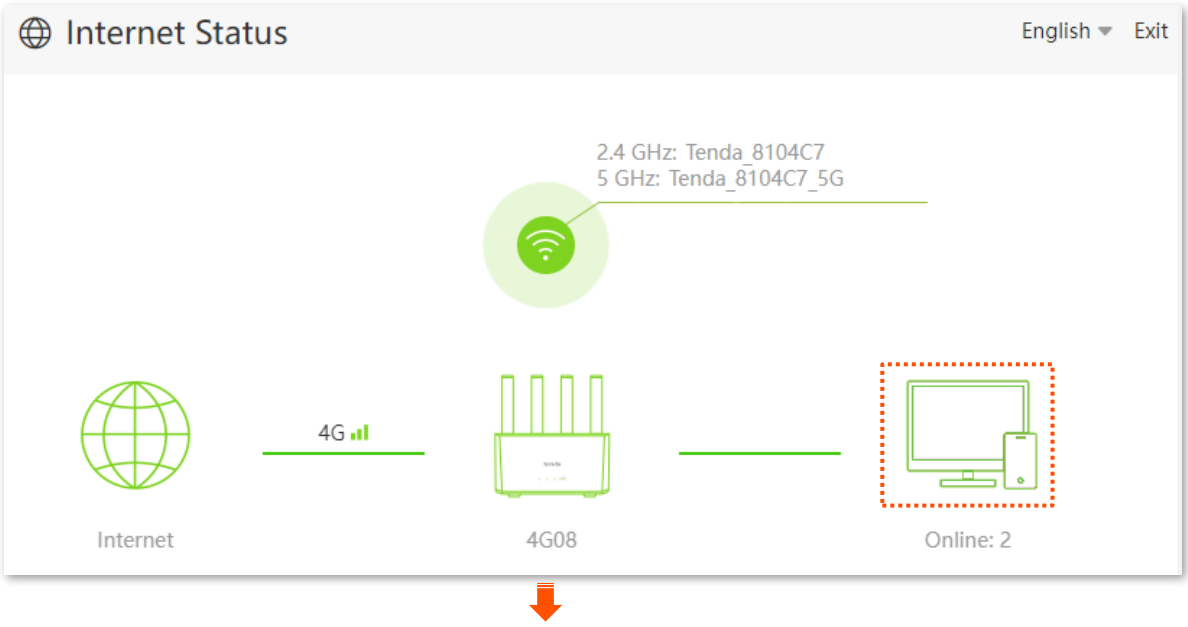
Parameter description

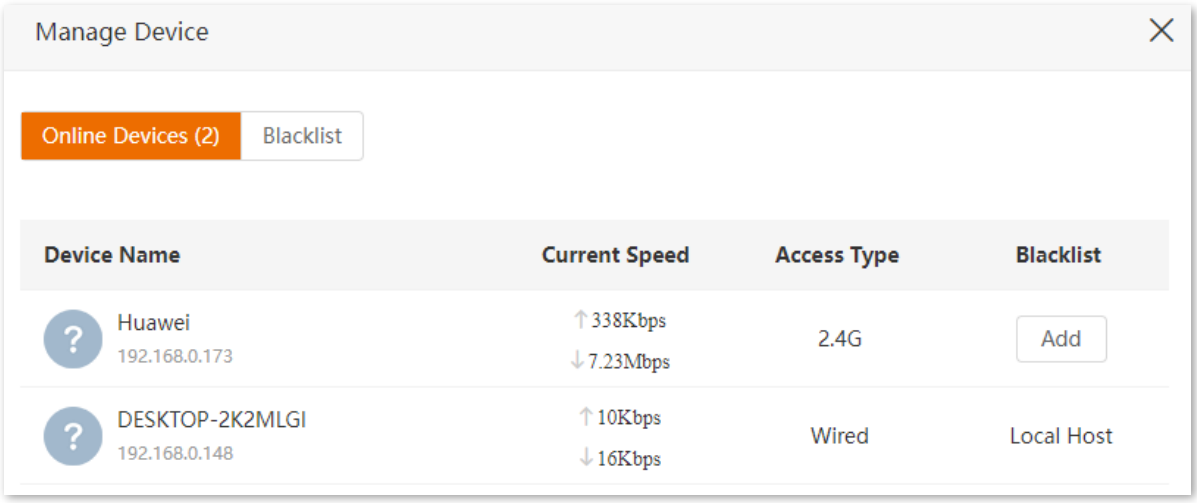
Parameter	Description
Wi-Fi Network	Specifies whether the Wi-Fi network is hidden.
Wi-Fi Name	Specifies the Wi-Fi name of the router.
Bandwidth	Specifies the bandwidth of the Wi-Fi network.
Channel	Specifies the channel that the Wi-Fi network works in.
MAC Address	Specifies the MAC address of the Wi-Fi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

4.5 View online or blacklist device information

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

On this page, 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.





Parameter description

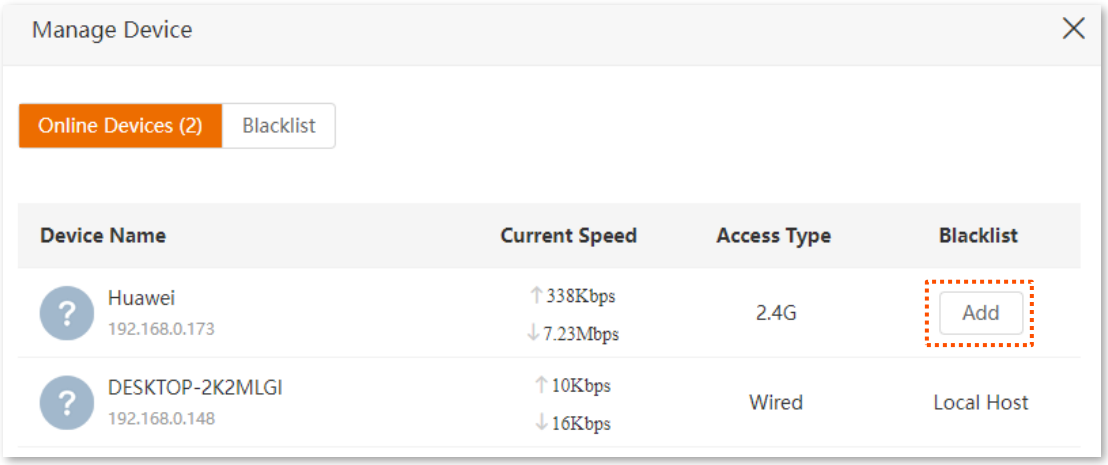
Parameter		Description
Online Devices	Device Name	Specifies the name of online device connected to the router.
	Current Speed	Specifies the upload speed and download speed of the device.
	Access Type	Specifies the access type of online device connected to the router.
	Blacklist	Specifies whether to add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

4.5.1 Add devices to the blacklist

On this page, you can add devices to the blacklist to block the internet access.

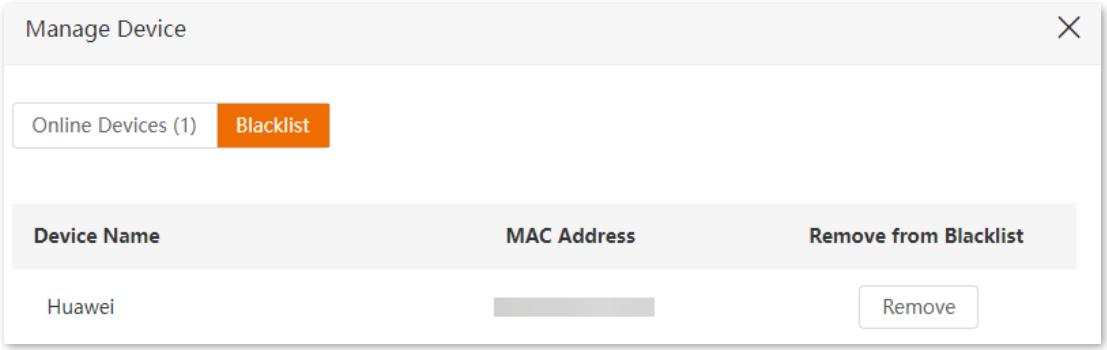
Procedure:

1. Log in to the web UI of the router.
2. Navigate to **Internet Status**.
3. Click .
4. Locate the device to be added in **Online Devices** and click **Add**.



---End

On the **Internet Status** page, click , and then click **Blacklist**, you can view the information of devices that are added to the blacklist.

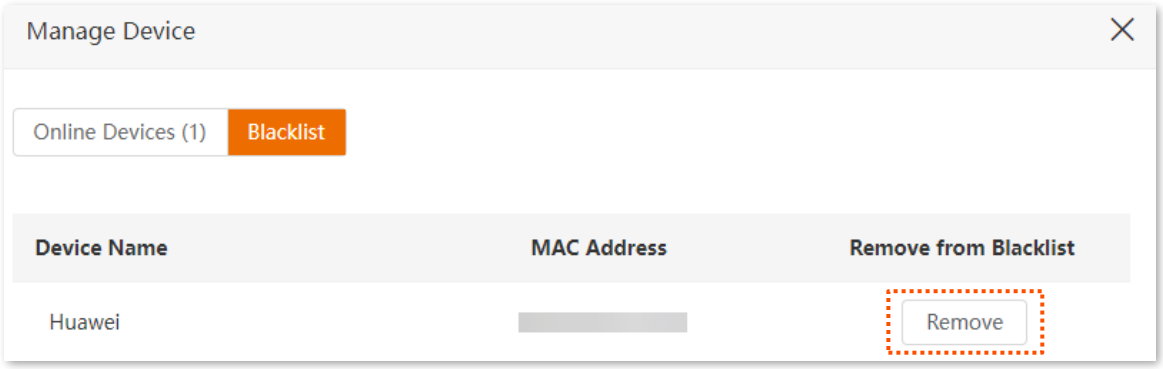


4.5.2 Remove devices from the blacklist

On this page, you can remove devices from the blacklist as required.

Procedure:

1. Log in to the web UI of the router.
2. Navigate to **Internet Status**.
3. Click .
4. Choose **Blacklist**, and locate the device to be removed from the blacklist.
5. Click **Remove**.



---End

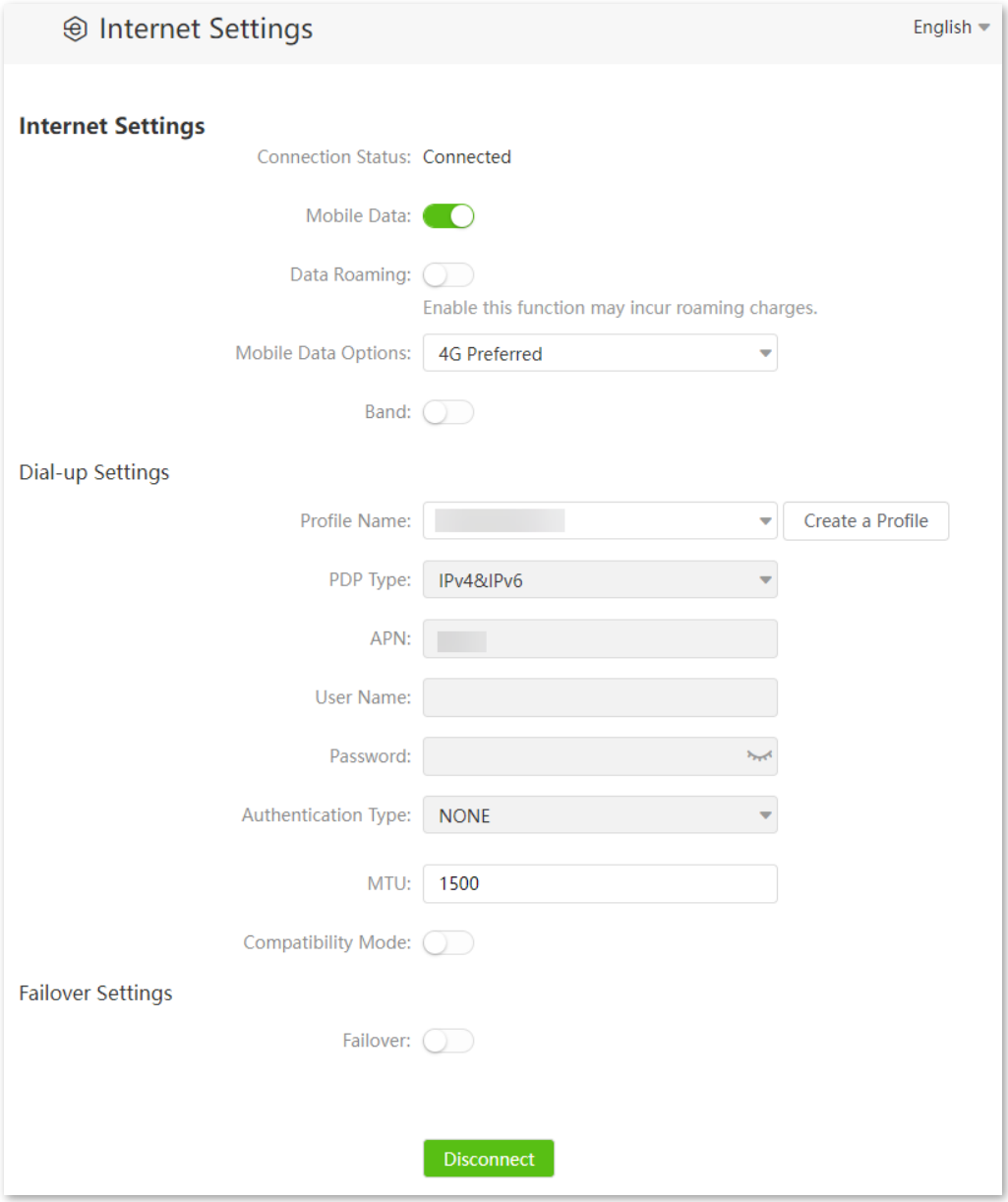
After the configuration is completed, the device is removed from the blacklist and can be connected to the router again.

5 Internet settings

5.1 Access the internet with a SIM card

On this page, you can change the internet settings when you access the internet through the SIM card.

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



Parameter description

Parameter		Description
Internet Settings	Connection Status	Specifies the internet connection status of the SIM card.
	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. Data roaming means the data usage produced when you are outside the coverage of your ISP. You can disable data roaming to avoid roaming data usage and charges.
	Mobile Data Options	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).
Dial-up Settings	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 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. TIP If the router cannot identify these parameters, get these parameters from your ISP.
	Create a Profile	Used to create an APN dial-up profile when the router fails to identify these parameters automatically.

Parameter		Description
	MTU	Maximum Transmission Unit (MTU) is the largest data packet transmitted by a network device. The default MTU value is 1500. Do not change the value unless necessary.
	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. TIP It is applicable to some ISPs limited plans. The TTL and HL values can be modified for packet capture analysis as required.

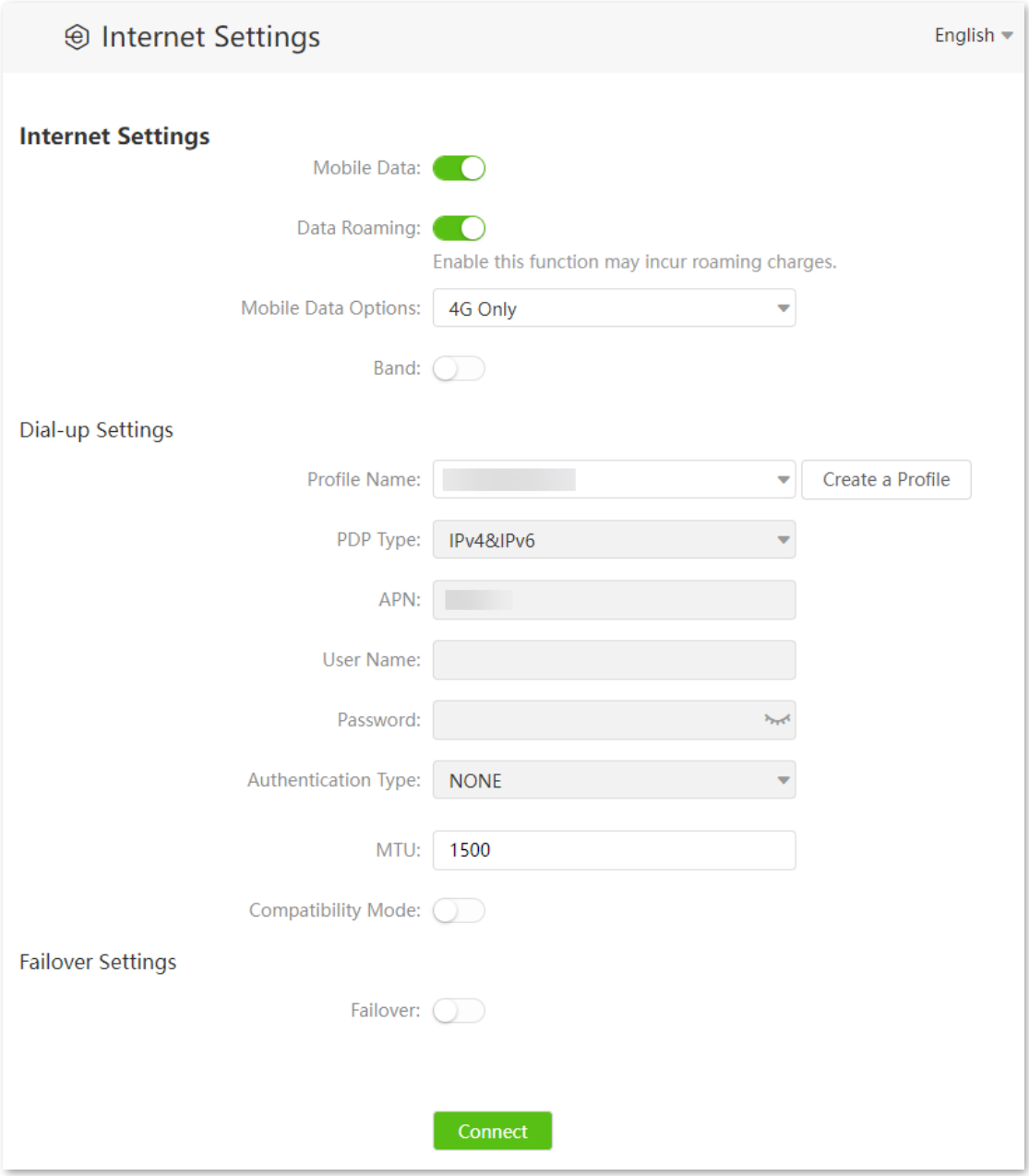
5.1.1 Change mobile network preference

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:

1. Log in to the web UI of the router.
2. Navigate to **Internet Settings**.
3. Enable **Mobile Data** and **Data Roaming**.
4. Set **Mobile Data Options** to **4G Only**.
5. Click **Connect**.



---End

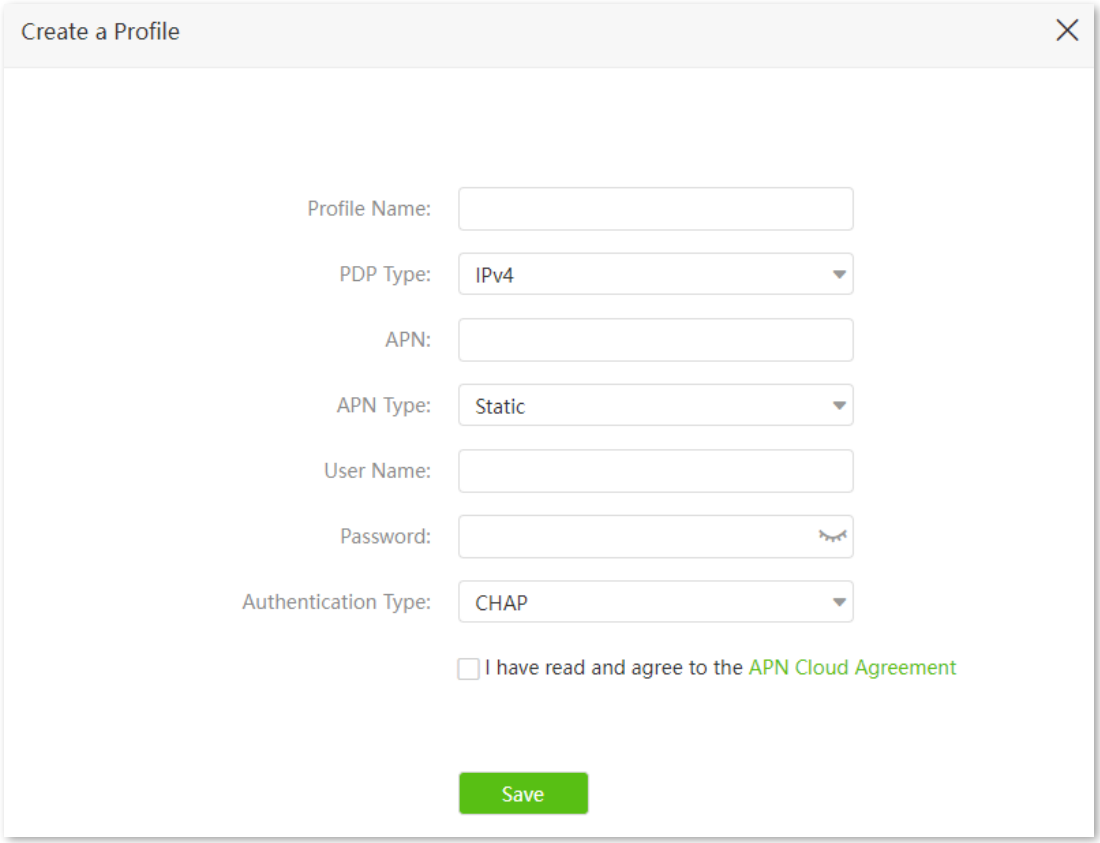
After the configuration is completed, you can refresh the configuration page. When **Connected** is shown after **Connection Status,** you can use the 4G network only to access the internet outside the coverage of your ISP.

5.1.2 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. Get these parameters from your ISP.

Procedure:

1. Log in to the web UI of the router.
2. Navigate to **Internet Settings**.
3. Click **Create a Profile**.
4. Enter required parameters from your ISP.
5. Click **Save**.



---End

Wait a moment. The router will use the parameters you entered to dial up for internet access, and you can access the internet with the APN profile you create.

5.2 Access the internet through the WAN port

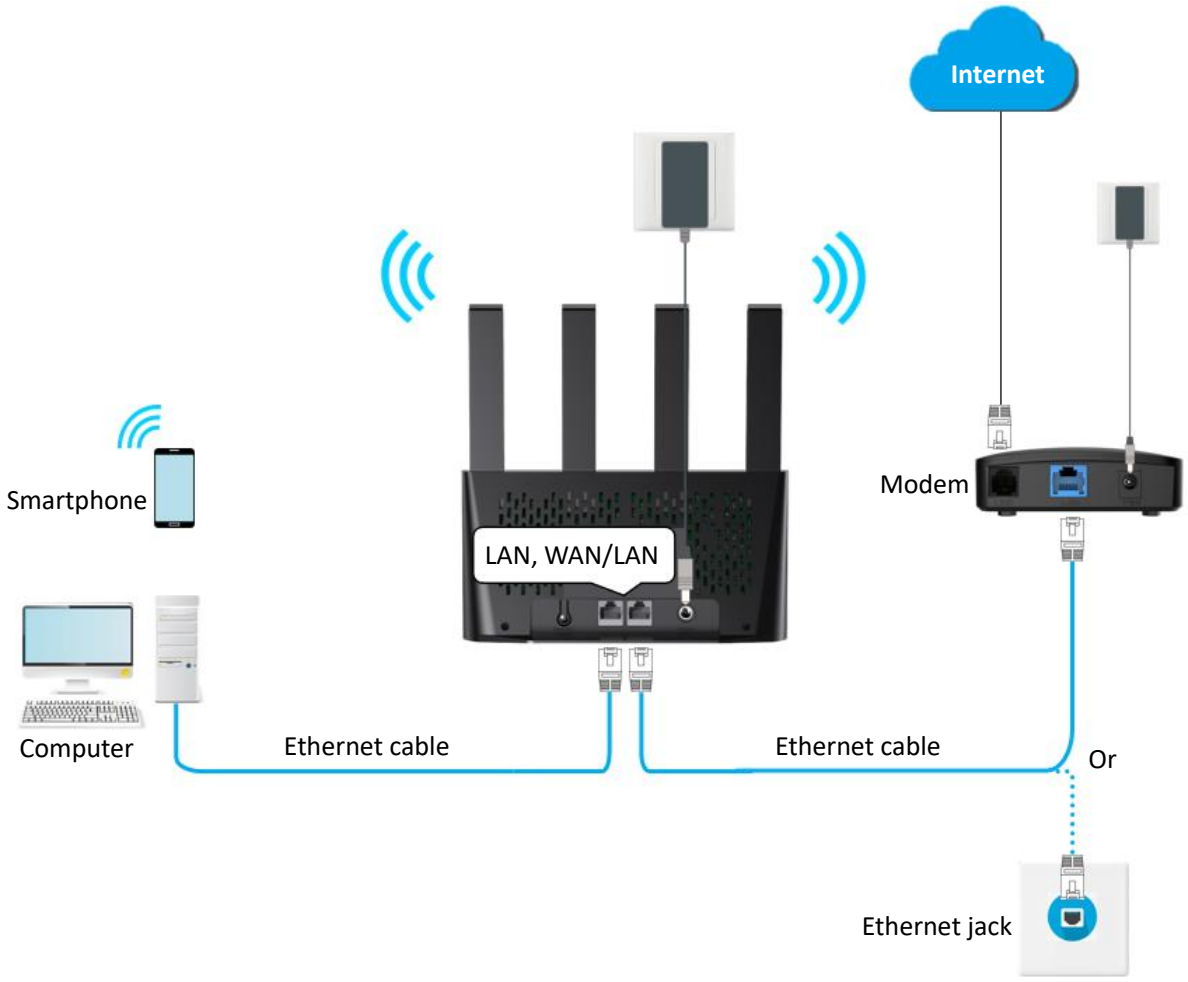
If you want to connect your broadband to the router to access the internet, you can access the internet through the WAN port.

TIP

Parameters for accessing the internet are provided by your ISP. If you have any doubt, contact your ISP.

5.2.1 Access the internet with a PPPoE account

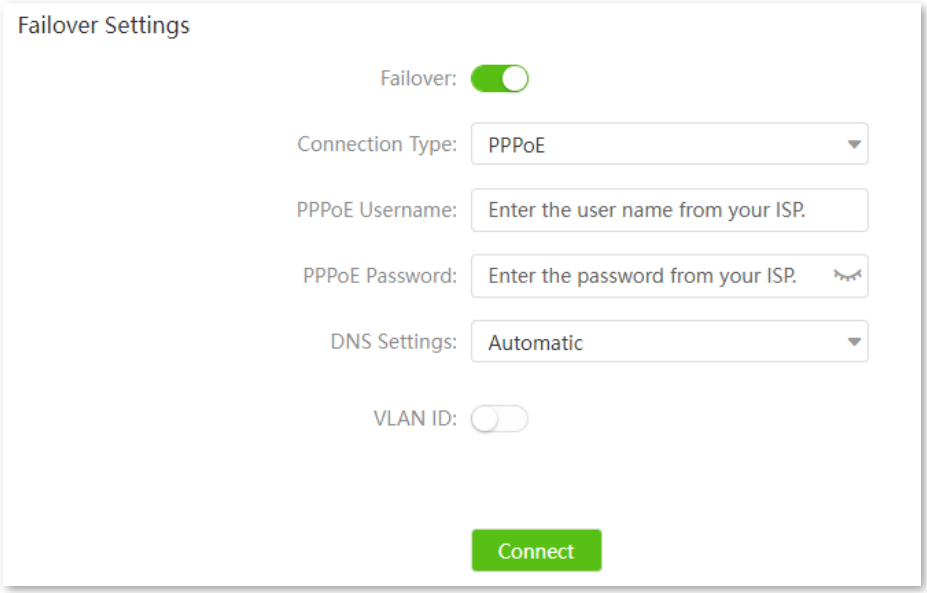
If the ISP provides you with PPPoE user name and password, you can choose this connection type to access the internet. The application scenario is shown below.



Procedure:

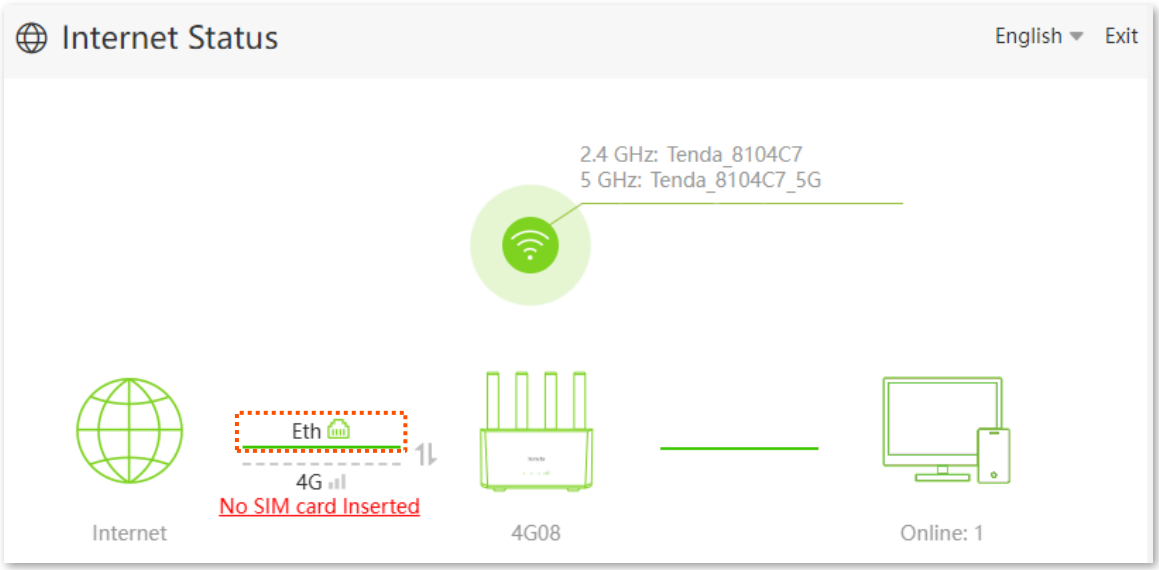
1. Log in to the web UI of the router.
2. Navigate to **Internet Settings**.

3. Enable the **Failover** function.
4. Set **Connection Type** to **PPPoE**.
5. Enter the **PPPoE Username** and **PPPoE Password**.
6. Set **DNS Settings** and **VLAN ID** as required.
7. Click **Connect**.



---End

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



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

Parameter description

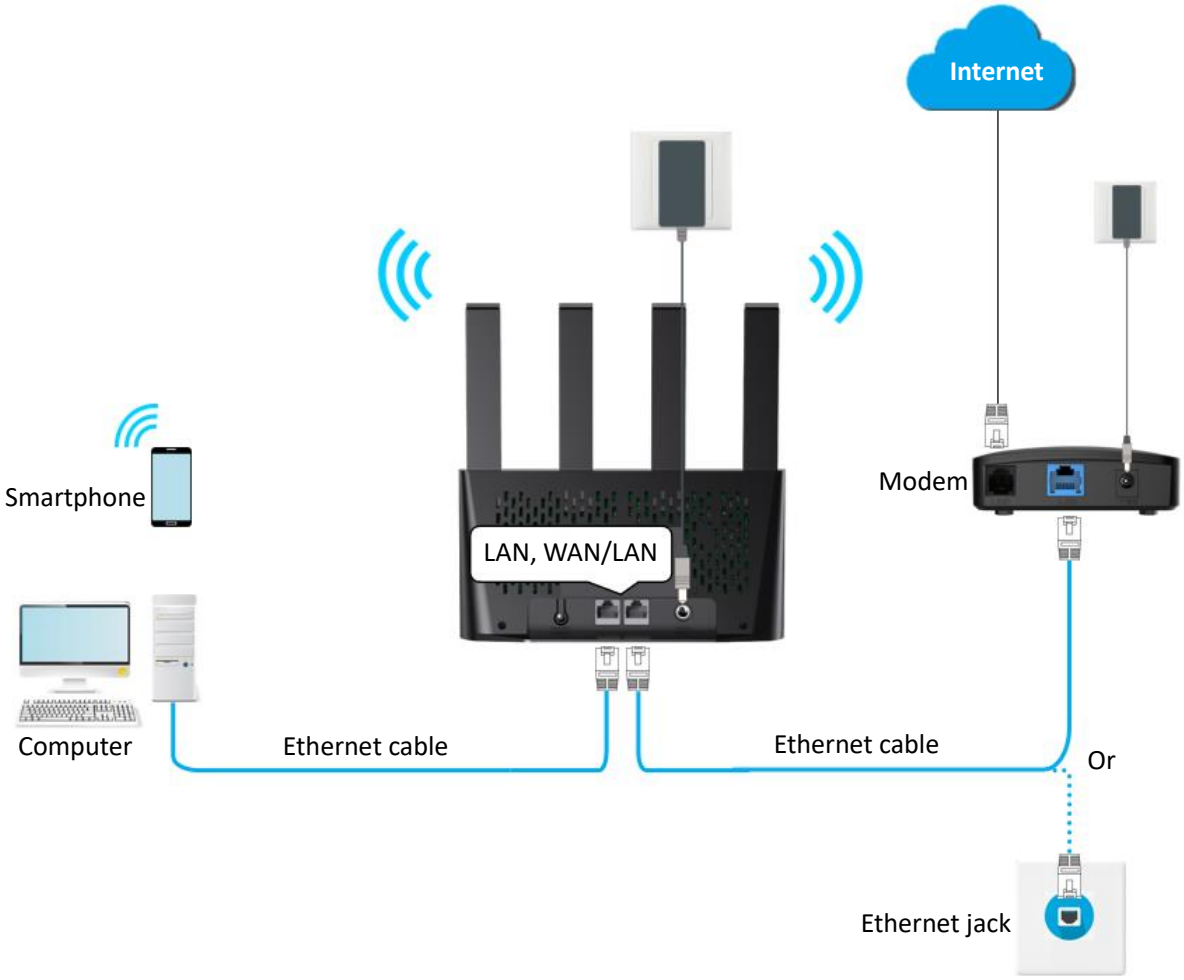
Parameter	Description
Failover	Used to enable or disable the failover function.
Connection Type	Specifies how your router connects to the internet, including: - **PPPoE**: Select this type if you access the internet using the PPPoE user name and PPPoE password. - **Dynamic IP Address**: Select this type 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.
PPPoE Username	When PPPoE is chosen as the connection type, you need to enter the user name and password provided by your ISP to access the internet.
PPPoE Password	
DNS Settings	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.

5.2.2 Access the internet through dynamic IP address

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

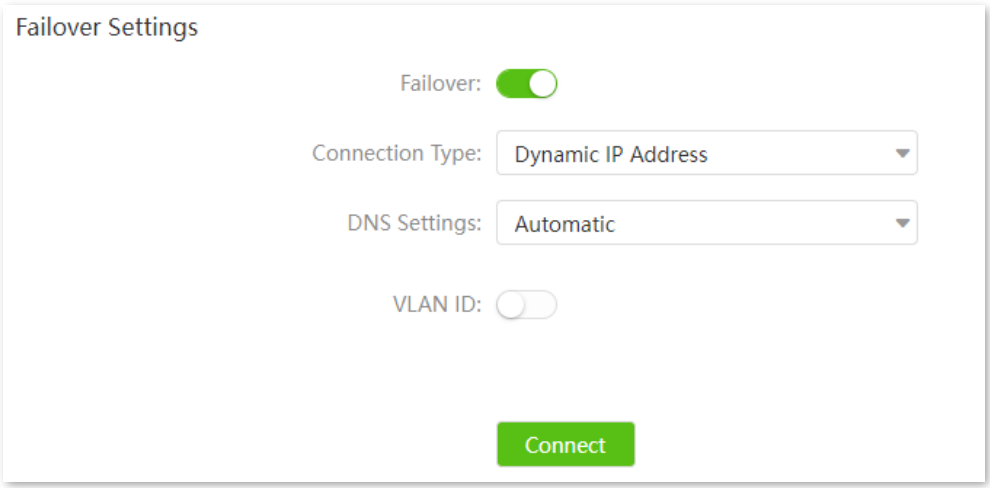
- Your ISP does not provide PPPoE user name and password, or any information including IP address, subnet mask, default gateway and DNS server.
- You have a router with internet access and want to add a 4G08 as the other one.

The application scenario is shown below.



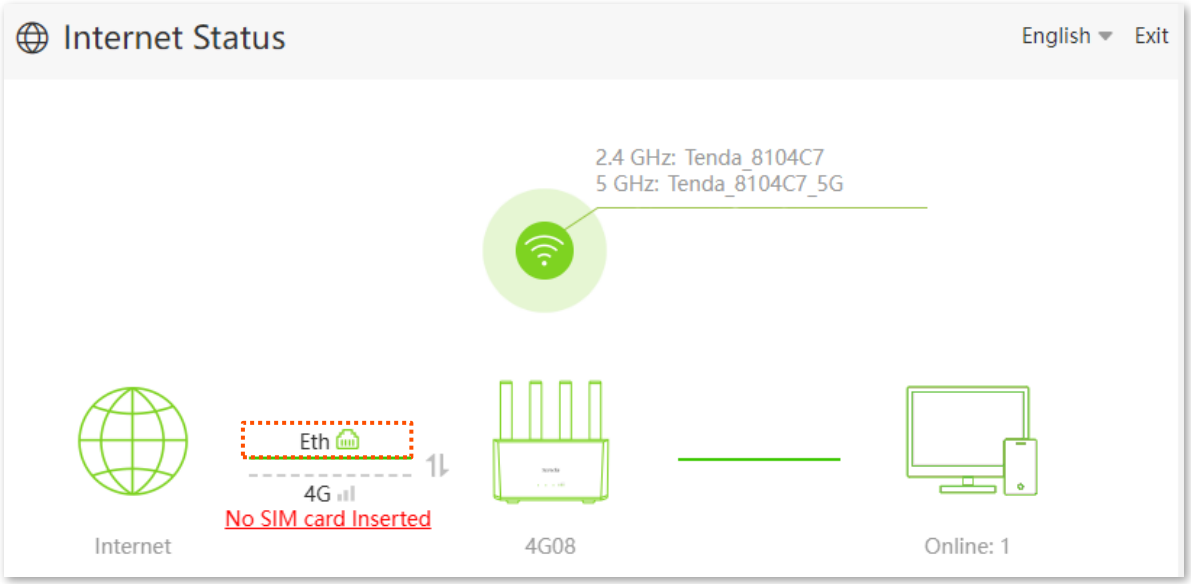
Procedure:

1. Log in to the web UI of the router.
2. Navigate to **Internet Settings**.
3. Enable the **Failover** function.
4. Set **Connection Type** to **Dynamic IP Address**.
5. Set **DNS Settings** and **VLAN ID** as required.
6. Click **Connect.**



---End

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



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

Parameter description

Parameter	Description
Failover	Used to enable or disable the failover function.

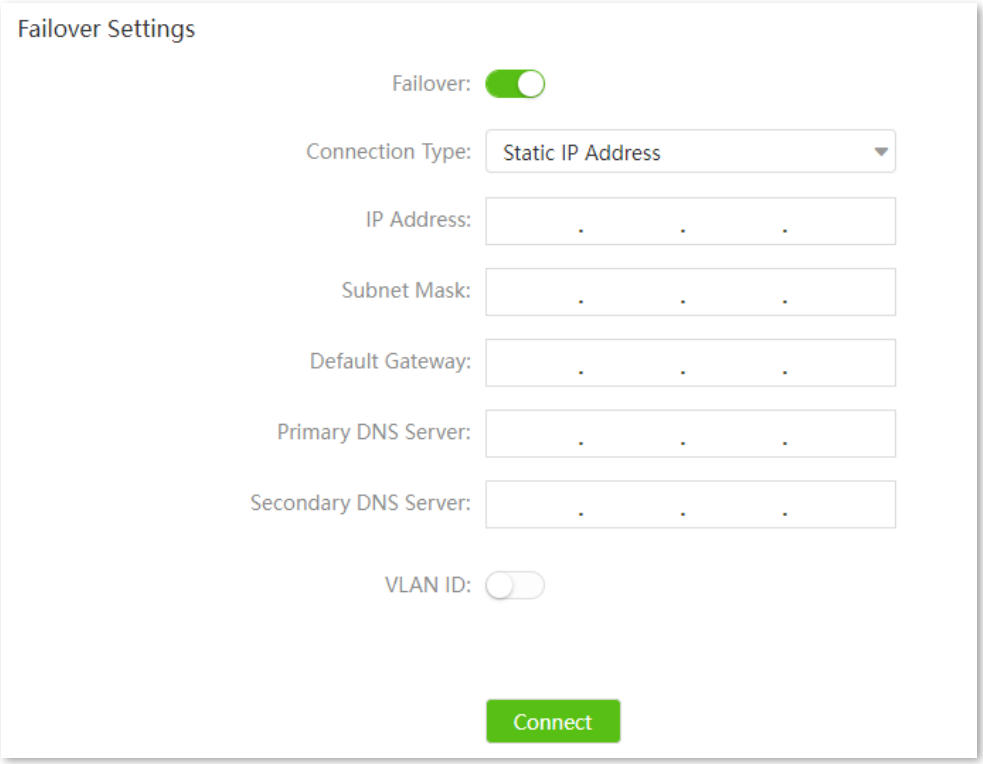
Parameter	Description
Connection Type	Specifies how your router connects to the internet, including: - **PPPoE**: Select this type if you access the internet using the PPPoE user name and PPPoE password. - **Dynamic IP Address**: Select this type if you can access the internet by simply plugging in an Ethernet cable. - **Static IP Address**: Select this type if you want to access the internet using fixed IP information.
DNS Settings	Specifies the obtaining method of WAN DNS address, which is **Automatic** by default. - **Automatic:** Obtain a DNS server address from the DHCP server of the upstream network. - **Manual:** Configure the DNS server address 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.

5.2.3 Access the internet with static IP address information

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

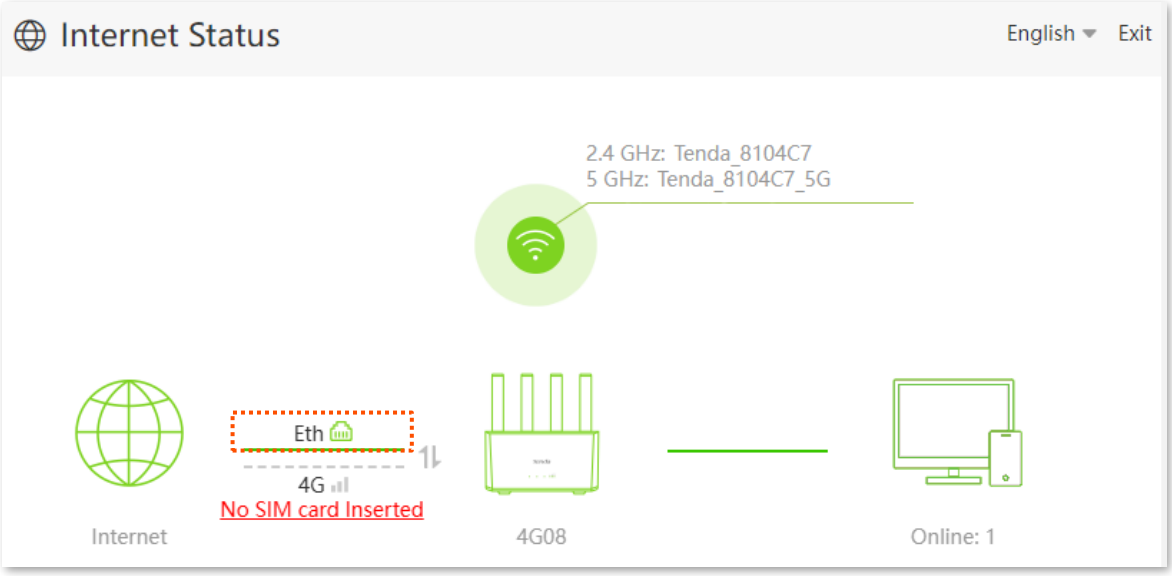
Procedure:

1. Log in to the web UI of the router.
2. Navigate to **Internet Settings**.
3. Enable the **Failover** function.
4. Set **Connection Type** to **Static IP Address**.
5. Enter **IP Address**, **Subnet Mask**, **Default Gateway** and **Primary/Secondary DNS Server**.
6. Set **VLAN ID** as required.
7. Click **Connect**.



---End

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



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

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

5.3 Set failover connection

5.3.1 Overview

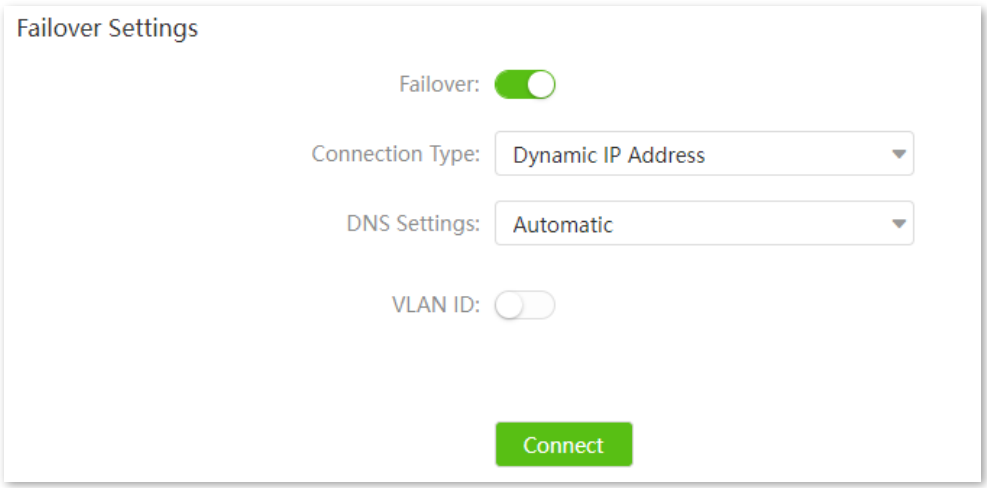
By configuring the failover function, you can set parameters of the internet connection mode other than the current one. If there is a network failure, the router will automatically switch to an available internet connection mode, therefore ensuring an uninterrupted internet access for clients under the router.

TIP

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

To access the 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.



5.3.2 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.

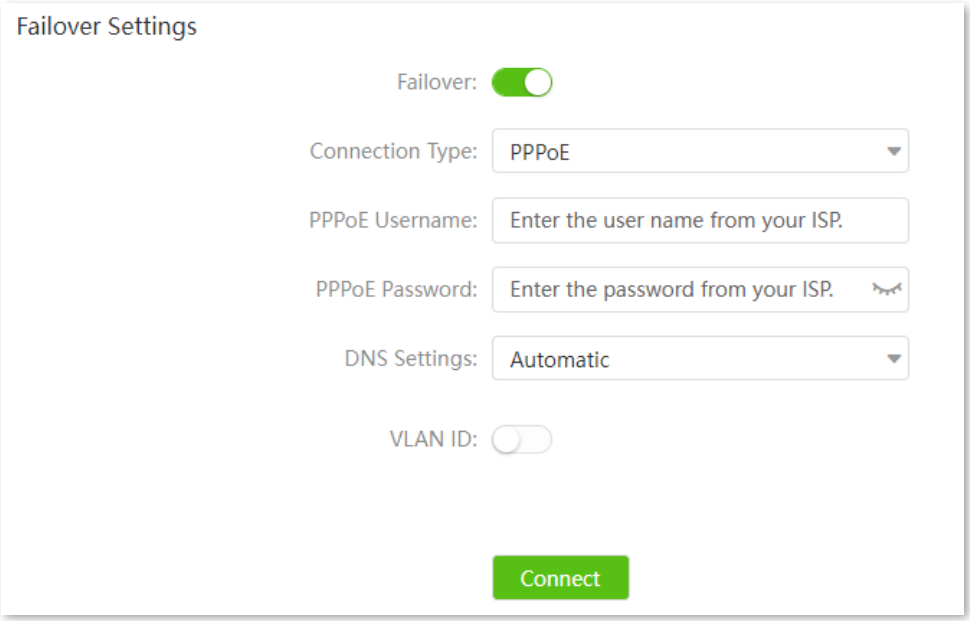
Requirement: Set the router to access the internet through the broadband, and use the SIM card as backup in case of broadband failure.

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.

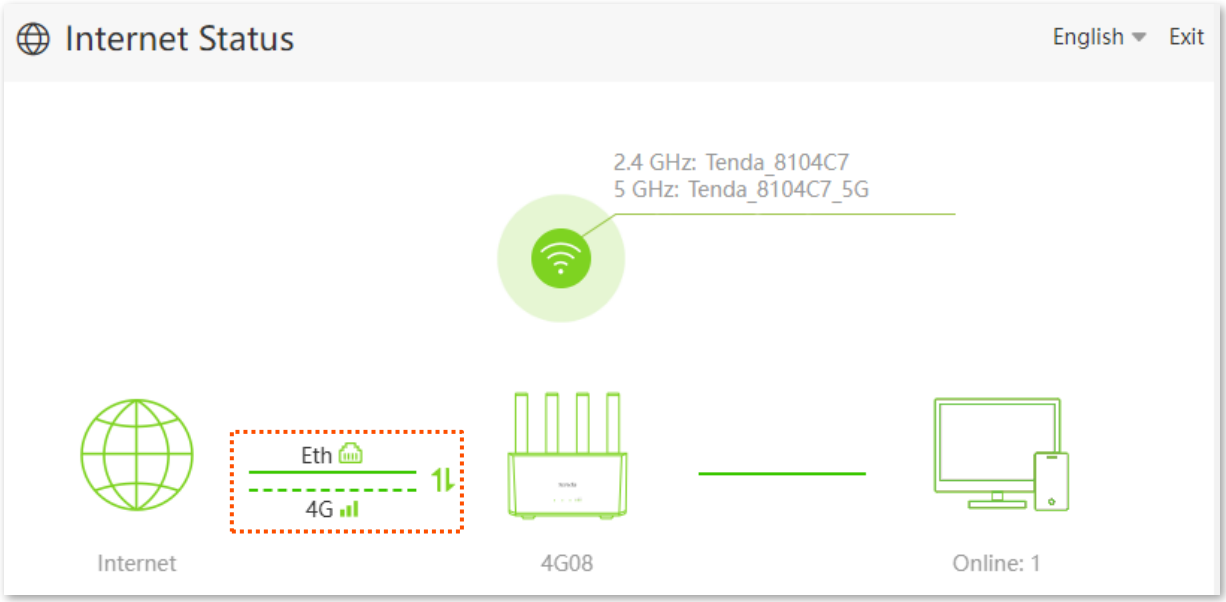
Procedure:

1. Connect the WAN/LAN port of the router to the LAN port of your smart home gateway.
2. Log in to the web UI of the router.
3. Navigate to **Internet Settings**.
4. Enable the **Failover** function.
5. Set **Connection Type** to **PPPoE**, and enter the **PPPoE Username** and **PPPoE Password** provided by your ISP.
6. Set **DNS Settings** and **VLAN ID** as required.
7. Click **Connect**.



---End

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.



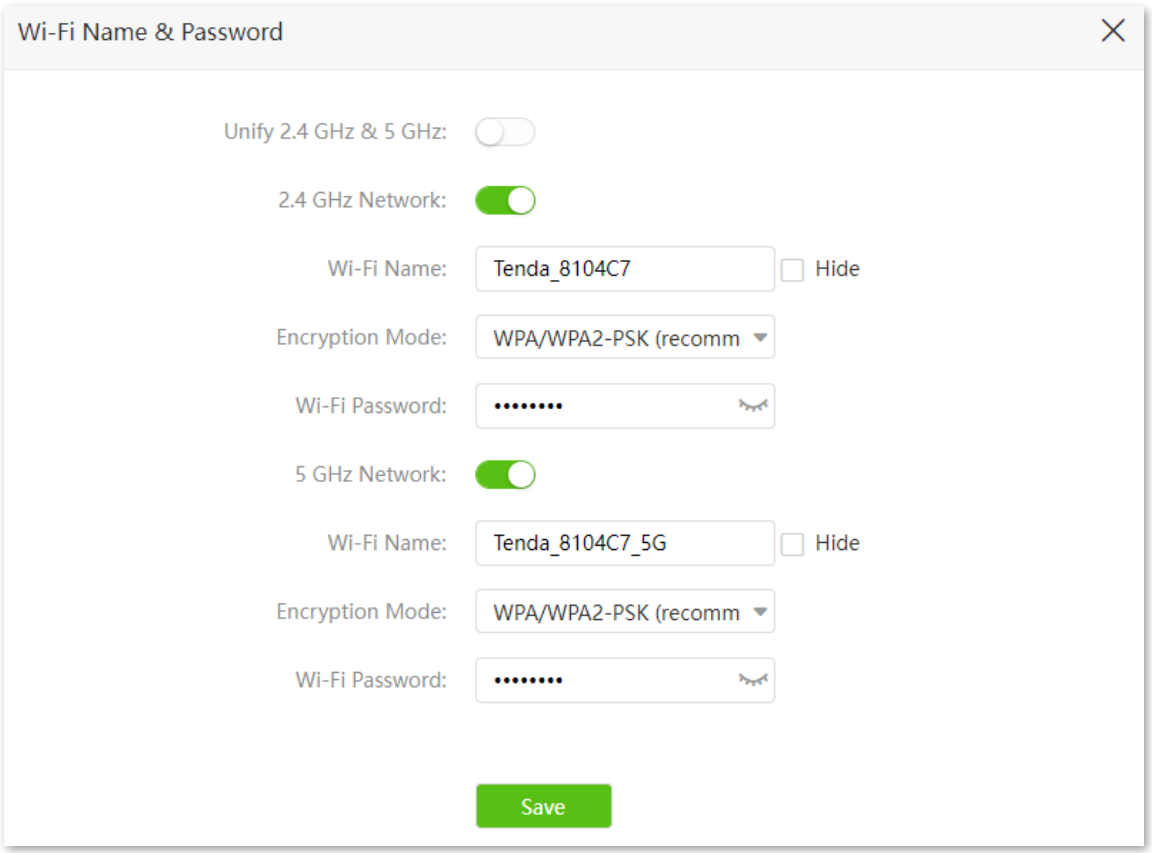
6 Wi-Fi settings

6.1 Wi-Fi name & password

6.1.1 Overview

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

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



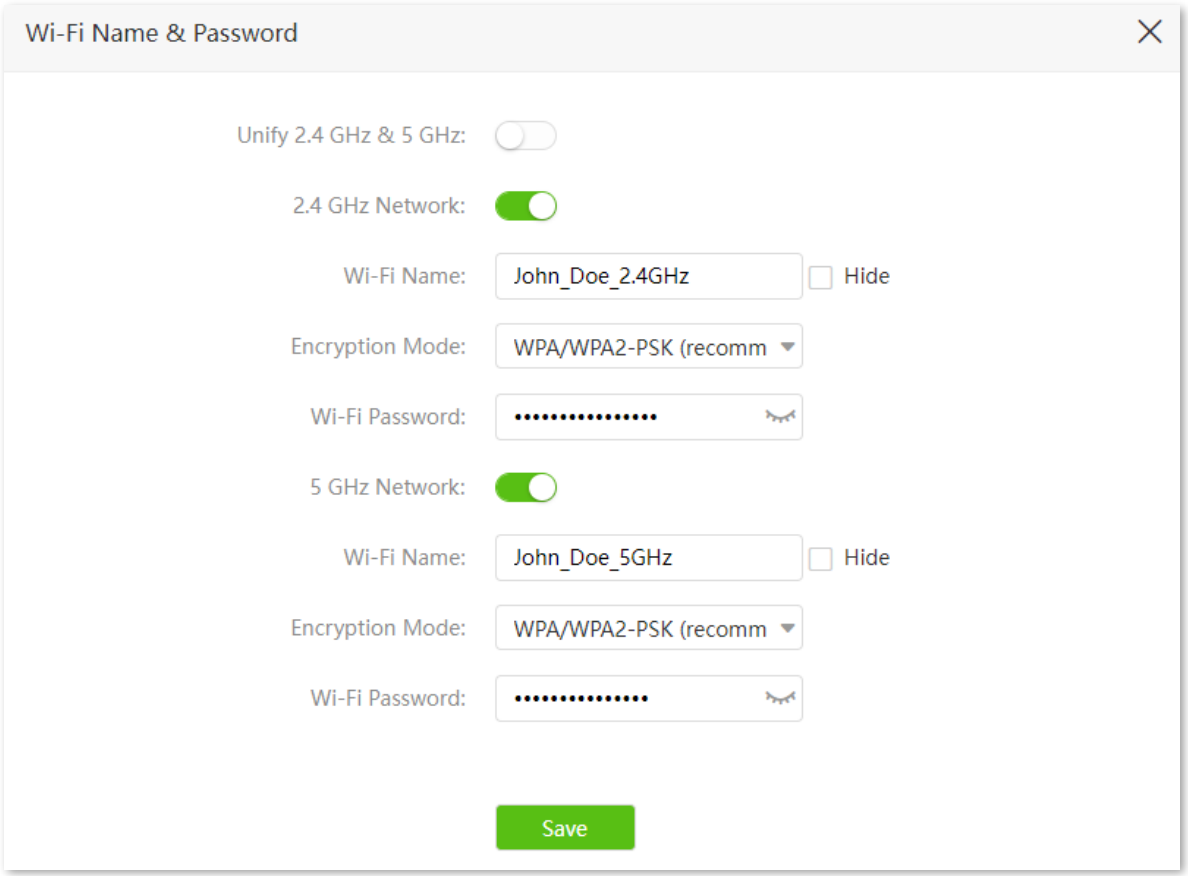
Parameter description

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

Parameter	Description
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. TIP It is recommended to use the combination of digits, uppercase letters, lowercase letters, and special symbols in the password to enhance the security of the Wi-Fi network.

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

1. Log in to the web UI of the router.
2. Navigate to **Wi-Fi Settings** > **Wi-Fi Name & Password.**
3. Enable or disable the **Unify 2.4 GHz & 5 GHz** function as required. The following figure shows an example of disabling the Unify 2.4 GHz & 5 GHz.
4. Change the parameters of the 2.4 GHz network.
   1) Change the **Wi-Fi Name** of the 2.4 GHz network, which is **John_Doe_2.4GHz** in this example.
   2) Set the **Encryption Mode**, which is **WPA/WPA2-PSK (recommended)** in this example.
   3) Set the **Wi-Fi Password** of the 2.4 GHz network, which is **Tenda+Wireless24** in this example.
5. Change the parameters of the 5 GHz Wi-Fi network.
   1) Change the **Wi-Fi Name** of the 5 GHz network, which is **John_Doe_5GHz** in this example.
   2) Set the **Encryption Mode**, which is **WPA/WPA2-PSK (recommended)** in this example.
   3) Set the **Wi-Fi Password** of the 5 GHz network, which is **Tenda+Wireless5** in this example.
6. Click **Save**.

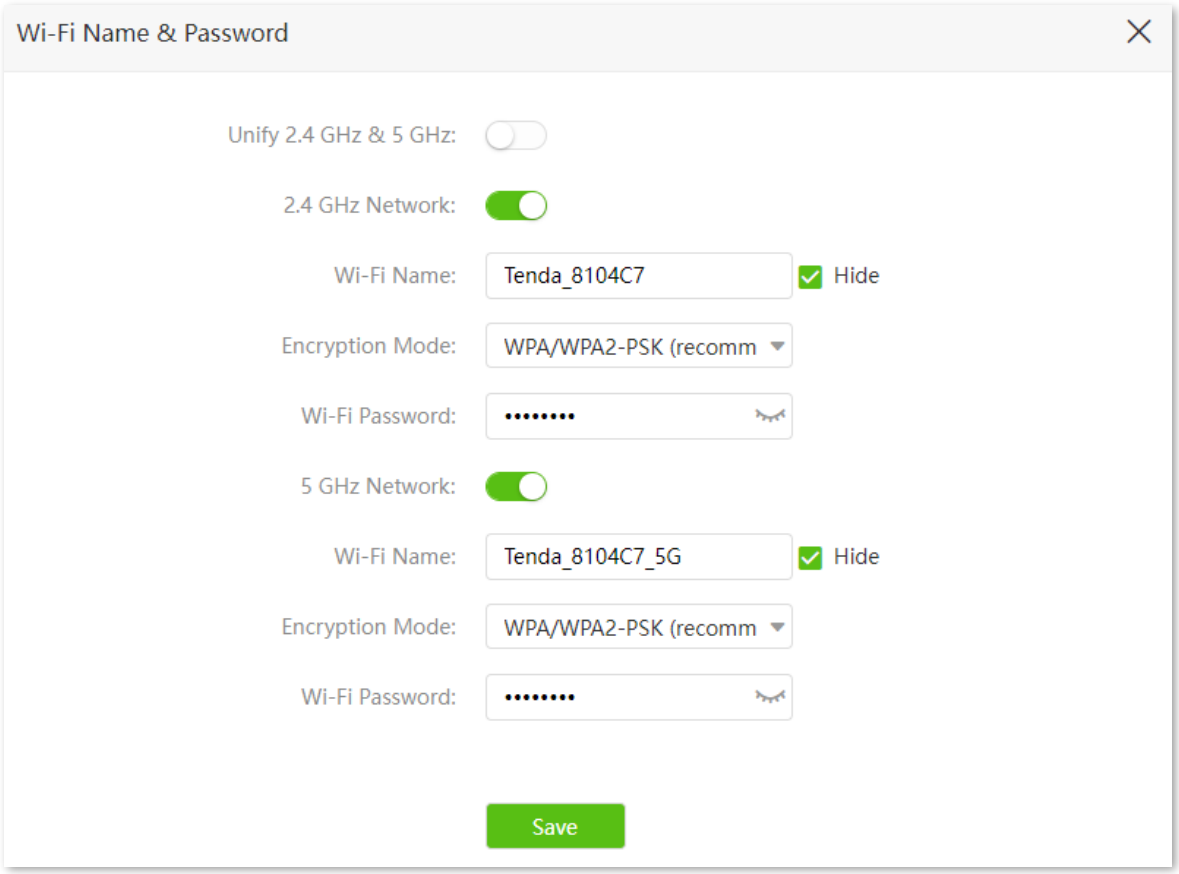


---End

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

6.1.3 Hide the Wi-Fi network

1. Log in to the web UI of the router.
2. Navigate to **Wi-Fi Settings** > **Wi-Fi Name & Password.**
3. Tick **Hide** of the target network.
4. Confirm the prompt information, and click **OK**.
5. Click **Save**.



---End

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

6.1.4 Connect to a hidden Wi-Fi network

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

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

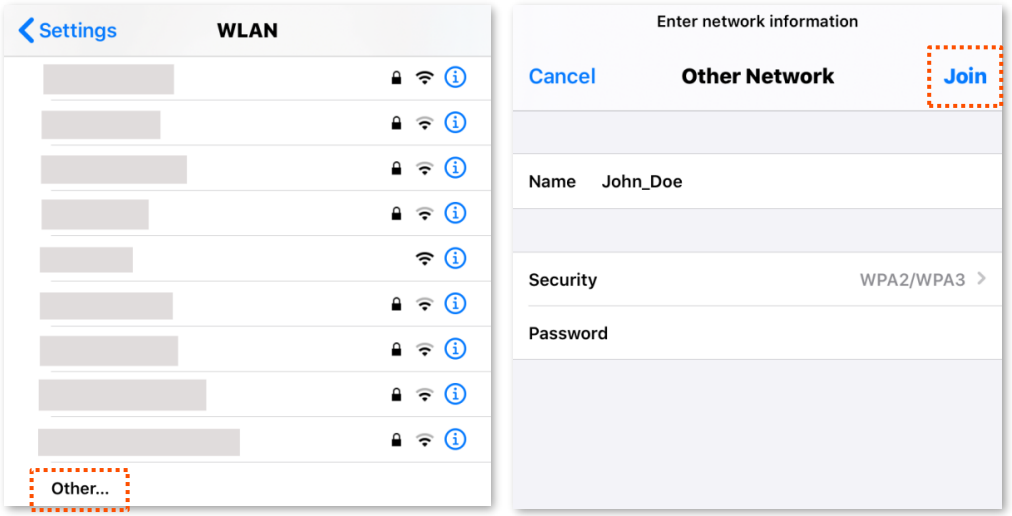
- Wi-Fi name: Jone_Doe
- Encryption type: WPA/WPA2-PSK (recommended)
- Wi-Fi password: Tenda+Wireless245

TIP

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)**:**

1. Tap **Settings** on your smartphone, and choose **WLAN**.
2. Enable **WLAN**.
3. Scroll the Wi-Fi list to the bottom, and tap **Other…**.
4. Enter the Wi-Fi name and password, which are **John_Doe** and **Tenda+Wireless245** in this example.
5. Set **Security** to **WPA2/WPA3** (If WPA2/WPA3 is not available, choose **WPA2**).
6. Tap **Join**.



---End

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

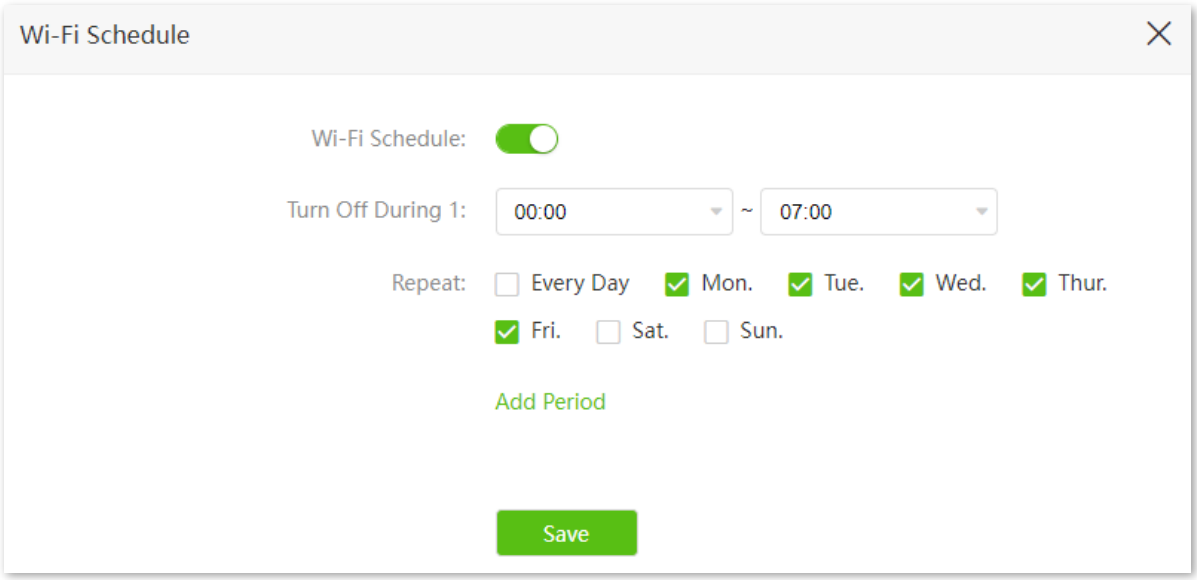
6.2 Wi-Fi schedule

6.2.1 Overview

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

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

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



NOTE

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

Parameter description

Parameter	Description
Wi-Fi Schedule	Used to enable or disable the Wi-Fi schedule function.
Turn Off During	Specifies the period when the Wi-Fi networks are disabled.
Repeat	Specifies the days on which the Wi-Fi networks are disabled during the specified period.
Add Period	Used to add a new Wi-Fi schedule rule.

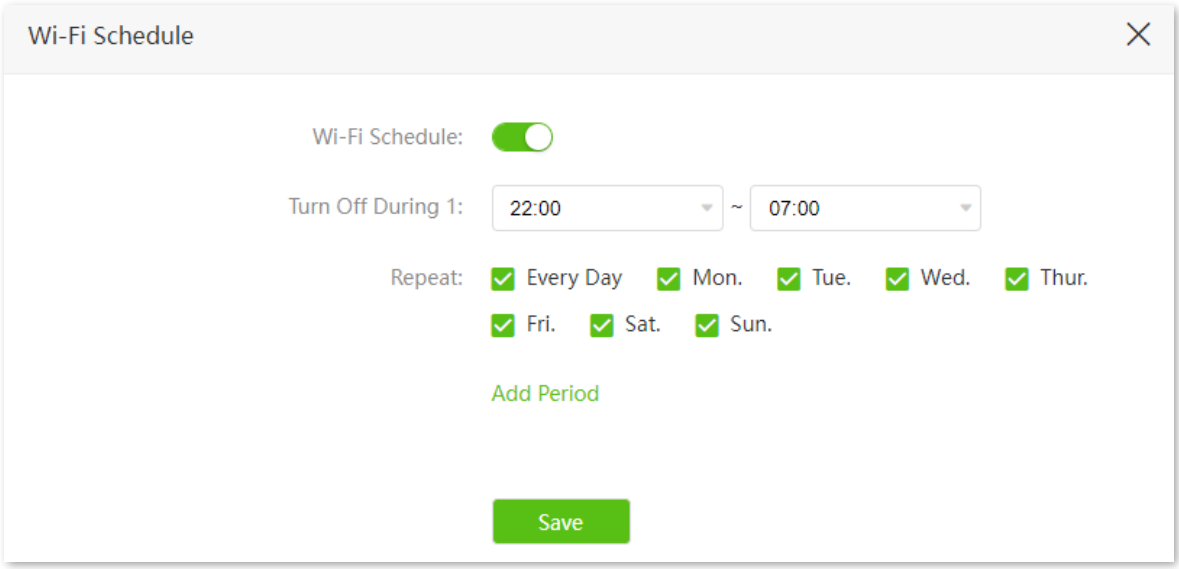
6.2.2 Example of configuring Wi-Fi schedule

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

Procedure:

1. Log in to the web UI of the router.
2. Navigate to **Wi-Fi Settings** > **Wi-Fi Schedule**.
3. Enable the **Wi-Fi Schedule** function.
4. Set a period for the Wi-Fi networks to be disabled, which is **22:00~07:00** in this example.
5. Set the days when the function works, which is **Every Day** in this example.

6. Click **Save**.



---End

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

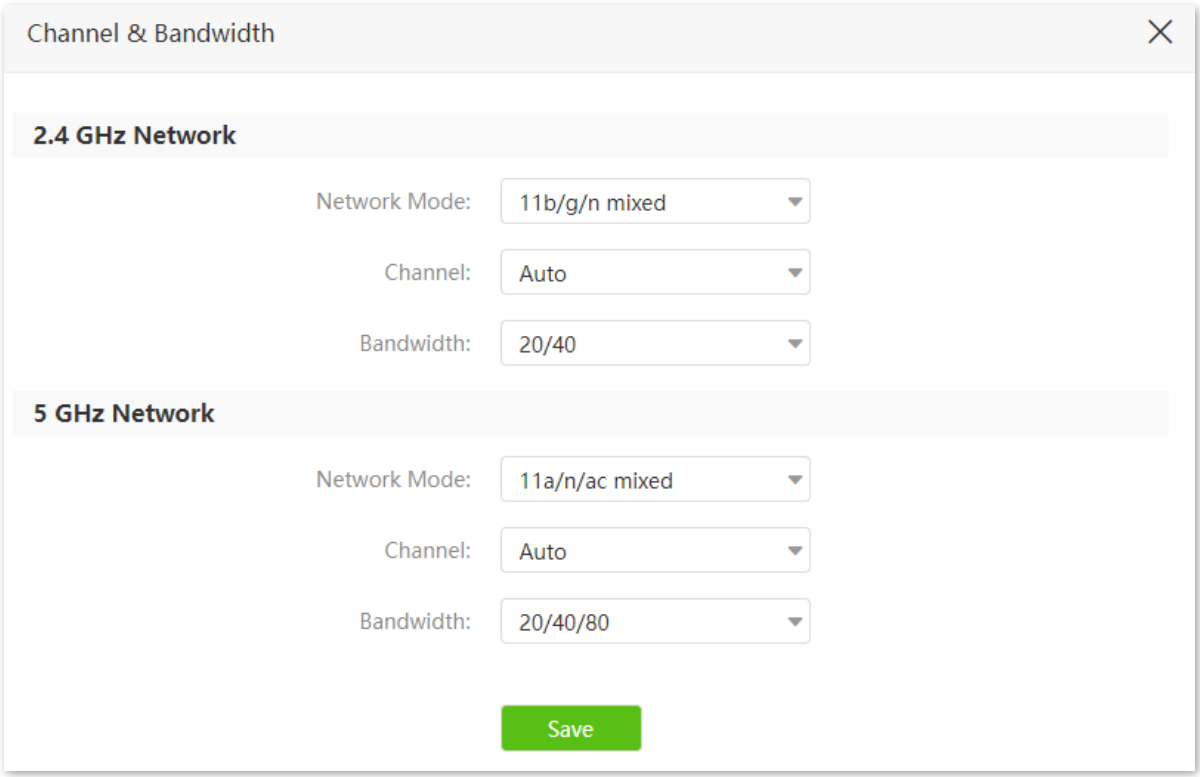
6.3 Channel & bandwidth

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

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

TIP

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



Parameter description

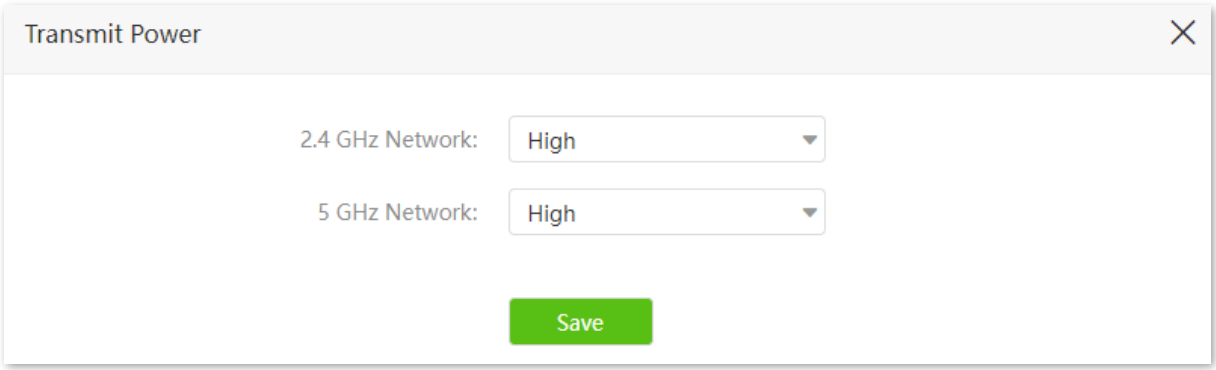
Parameter	Description
Network Mode	Specifies various protocols adopted for wireless transmission. 2.4 GHz Wi-Fi network includes 11b/g mixed and 11b/g/n mixed modes. - **11b/g mixed**: It indicates that devices compliant with IEEE 802.11b or IEEE 802.11g protocol can connect to the 2.4 GHz Wi-Fi network of the router. - **11b/g/n mixed**: It indicates that all devices can connect to the router if they are compliant with IEEE 802.11b or IEEE 802.11g protocol, or work at 2.4 GHz with IEEE 802.11n protocol. 5 GHz Wi-Fi network includes11ac and 11a/n/ac mixed modes. - **11ac**: It indicates that devices complaint with IEEE 802.11ac protocol can connect to the router. - **11a/n/ac mixed**: It indicates that all devices that are compliant with IEEE 802.11a or IEEE 802.11ac protocol, or work at 5 GHz with IEEE 802.11n protocol can connect to the router.

Parameter	Description
Channel	Specifies the channel in which the Wi-Fi network works. By default, the wireless channel is **Auto**, which indicates that the router selects a channel for the Wi-Fi network automatically. You are recommended to choose a channel with less interference for better wireless transmission efficiency. You can use a third-party tool to scan the Wi-Fi signals nearby to understand the channel usage situations.
Bandwidth	Specifies the bandwidth of the wireless channel of a Wi-Fi network. Please change the default settings only when necessary. - **20**: It indicates that the channel bandwidth used by the router is 20 MHz. - **40**: It indicates that the channel bandwidth used by the router is 40 MHz. - **20/40**: It specifies that a router can switch its channel bandwidth between 20 MHz and 40 MHz based on the ambient environment. This option is available only at 2.4 GHz. - **80**: It indicates that the channel bandwidth used by the router is 80 MHz. This option is available only at 5 GHz. - **20/40/80**: It specifies that a router can switch its channel bandwidth among 20 MHz, 40 MHz, and 80 MHz based on the ambient environment. This option is available only at 5 GHz.

6.4 Transmit power

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

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



Parameter description

Parameter	Description
2.4 GHz Network 5 GHz Network	Specify the mode of signal strength. The default mode is **High**. - **High**: It is typically used to meet wireless coverage requirements in large or multi-barrier environments. - **Medium**: It is typically used to meet wireless coverage requirements in medium-area or less-obstacle environments. - **Low**: It is typically used to meet wireless coverage requirements in small area or barrier-free environments.

6.5 WPS

6.5.1 Overview

The WPS function enables wireless devices, such as smartphones, to quickly and easily connect to Wi-Fi network of the router without entering the Wi-Fi password. There are two ways to connect devices to the Wi-Fi network.

- Connect devices to the Wi-Fi network using the WPS button
- Connect devices to the Wi-Fi network through the web UI of the router

To enable or disable the WPS function, 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.
- If the WPS function is disabled, the internet cannot be connected through the WPS function of the router.

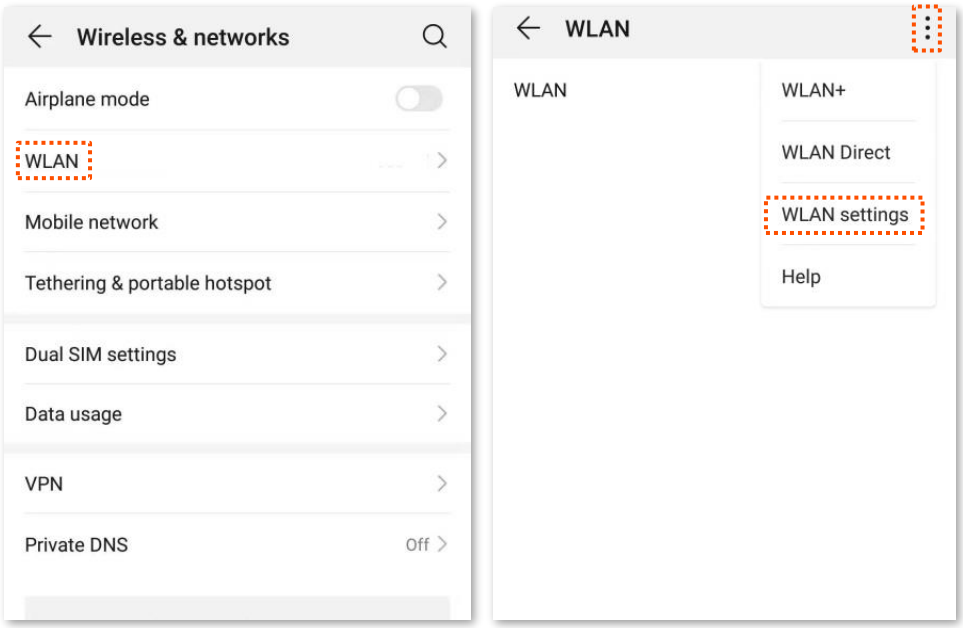
6.5.2 Connect devices to the Wi-Fi network using the WPS button

1. Find the **MESH/RST** button on the rear panel of the router, and hold it down for about 1 second. The Wi-Fi indicator blinks.
2. Configure the WPS function on your wireless devices **within 2 minutes**. Configurations on various devices may differ (Example: HUAWEI P10).

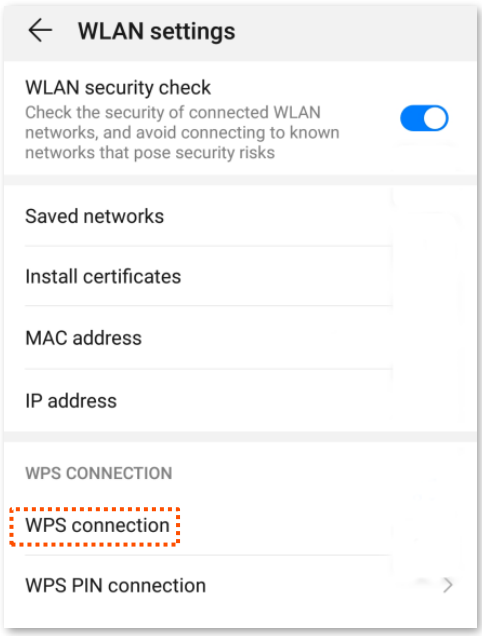
1) Find **Settings** on the smartphone.

2) Tap **WLAN**.

3) Tap ⋮, and choose **WLAN settings**.

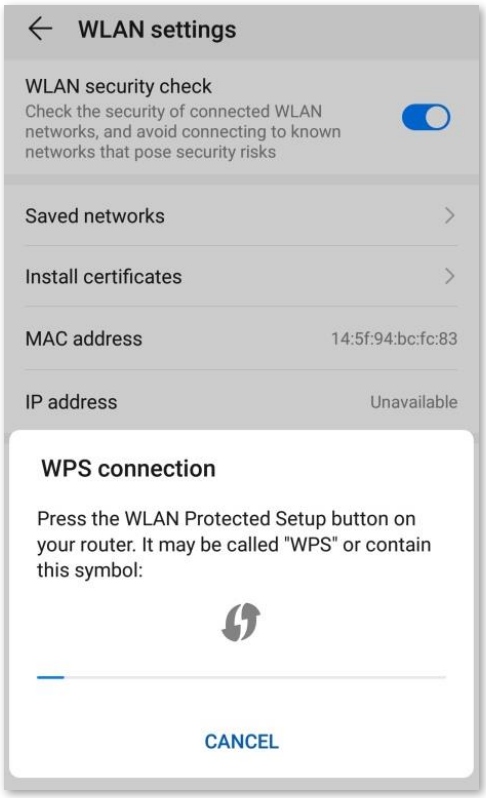


4) Tap **WPS connection**.



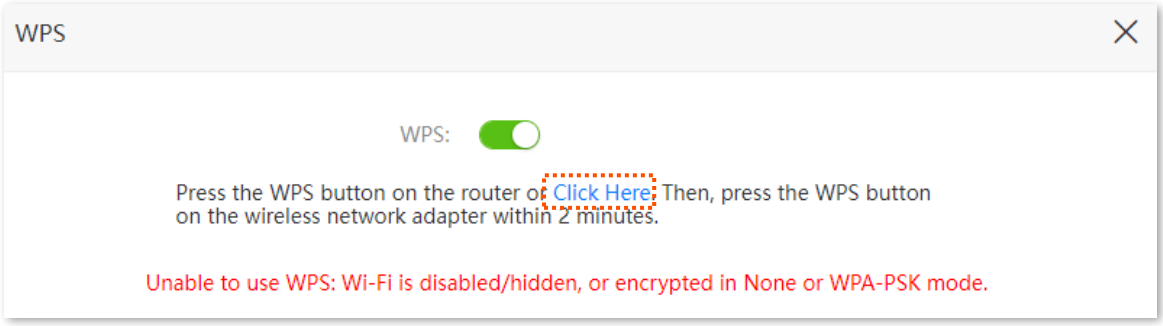
---End

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



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

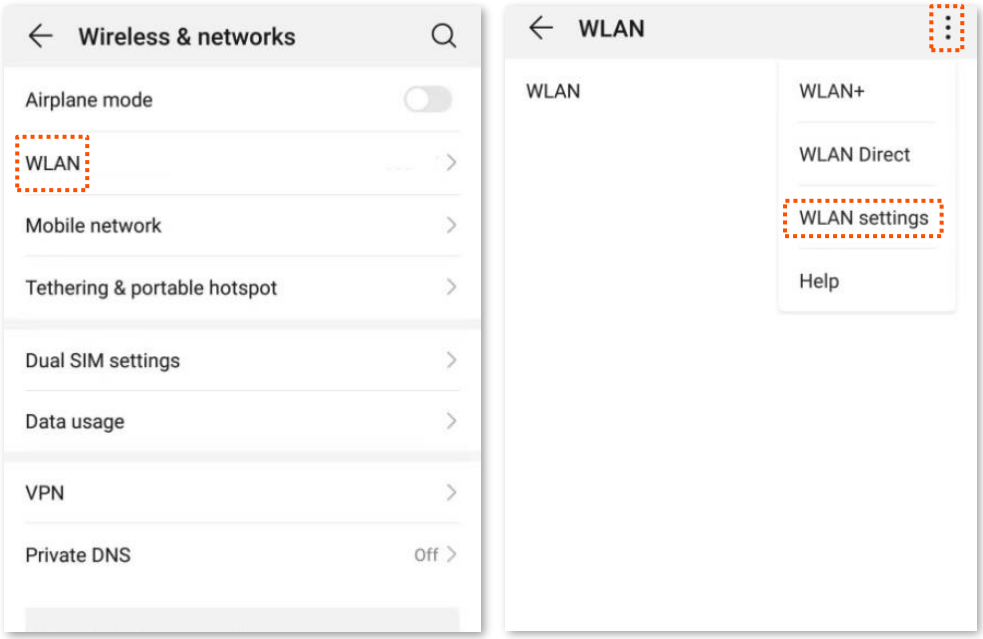
1. Log in to the web UI of the router.
2. Navigate to **Wi-Fi Settings** > **WPS.**
3. Enable **WPS**.
4. Click Click Here.



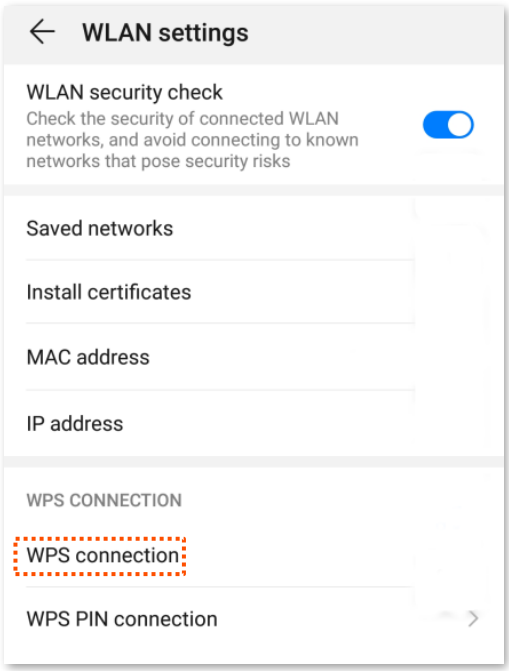
5. Configure the WPS function on your wireless devices **within 2 minutes**. Configurations on various devices may differ (Example: HUAWEI P10).

1) Find **WLAN** settings on the smartphone.

2) Tap ⋮, and choose **WLAN settings**.

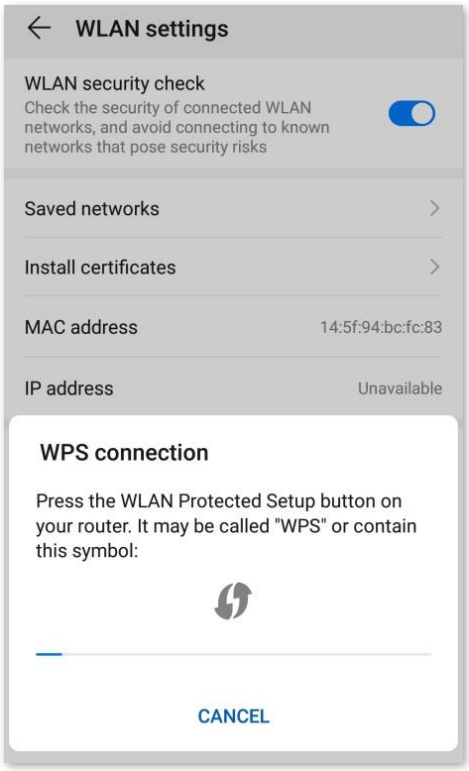


3) Tap **WPS connection**.



---End

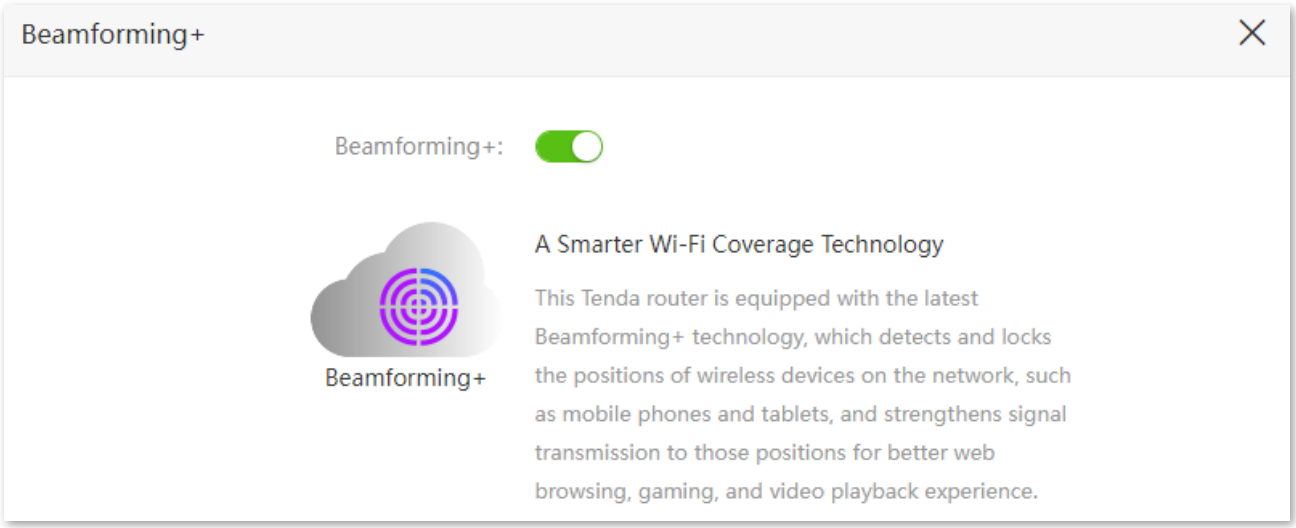
Wait a moment until the WPS negotiation is completed, and the smartphone is connected to the Wi-Fi network.



6.6 Beamforming+

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

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



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

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

7 Mesh

7.1 Overview

TIP

Currently, this router can be used as the primary node to network with devices that support the Tenda Mesh protocol.

The router support Mesh networking. Mesh networking has such advantages as automatic networking, self-repair, multi-skip cascade, unified management network, node self-management, which can greatly reduce the cost and complexity of network deployment.

The router supports the following three Mesh networking modes. You can choose the Mesh networking mode as required.

- **MESH button networking**

The networking button (MESH/RST) on the router body can be used to network with other routers without entering the management page.

- **Wired networking**

Connect the LAN port (such as LAN or WAN/LAN) of an existed router to a new router through an Ethernet cable for automatic networking. The wired network has good stability and small delay. If Ethernet cables have been deployed at home, you can use this mode.

- **Scanning networking**

Manually add other routers to the network of the existing router through the scanning networking of the router's web UI.

7.2 Set up as an add-on node

This section describes how to add a new router to extend the Wi-Fi network coverage when a router is connected to the internet.

If you are using the router for the first time or have restored the router to factory settings, follow the quick installation guide of the router to configure the router to the internet.

TIP

- If there are more than two secondary nodes, place the primary node in the key area and ensure that no more than one node is between the primary node and the secondary node.
- Before using a new router to extend the network, ensure that the existing router (primary node) has been connected to the internet and the new router (secondary node) is restored to the factory settings.
- The router can be networked with other routers that support the XMESH protocol. If the router fails to be added to an existing network, contact Tenda customer service for help. The following uses 4G08 (primary mode) and MX15 (secondary node) as an example.

7.2.1 MESH button networking

Procedure:

1. Add to the existed network.

   1) Power on the existing router (4G08) and connect it to the internet properly.

   2) Place the new router (MX15) near the existing router (within 5 meters) and power on. Wait until the startup of the new router is complete. The indicator blinks green slowly.

   3) Press (1 to 3 seconds) the networking button (MESH) of the new router. The indicator blinks green fast.

   4) Press (1 to 3 seconds) the networking button (MESH/RST) on the existing router.

      When the indicator of the new router turns solid green, the networking is successful. The MX15 becomes a secondary node in the network.

2. Select an appropriate position for the new router.

   1) For a better internet experience, you can relocate the wireless router by referring to the following relocation tips:

   - Place the new router within the wireless coverage range of the existing router.
   - Keep your nodes away from electronics with strong interference, such as microwave ovens, induction cookers, and refrigerators.
   - Place the nodes in a high position with few obstacles.

   2) Power on the new router, and wait until the indicator blinks green slowly.

TIP

- The indicators of the new router may vary with device models. Please refer to the product you purchased.
- If the indicator of the new router is still blink green slowly after 3 minutes. Please adjust the new router closer to the existing router.

Observe the indicator of the new router until it changes to one of the following status:

● Solid green	Networking succeeds. Excellent connection quality.
● Solid yellow	Networking succeeds. Fair connection quality.
● Solid red	Networking succeeds. Poor connection quality.

3) If the indicator of the new router is solid red, select a new location by referring to substep 1 of step 2 in this section to obtain the better connection quality.

---End

To access the internet with:

- **Wired devices:** Connect to a LAN port of the router using an Ethernet cable.
- **WiFi-enabled devices:** Connect to the Wi-Fi network using the Wi-Fi name and password you set.

Repeat this section to add other routers.

7.2.2 Wired networking

Assume that the Ethernet cable has been deployed in advance between the living room and the bedroom in the home, the existing router 4G08 (primary node) placed in the living room has been connected to the internet, and now you need to deploy a new router MX15 (planned as a secondary node) in the bedroom to extend the Wi-Fi network.

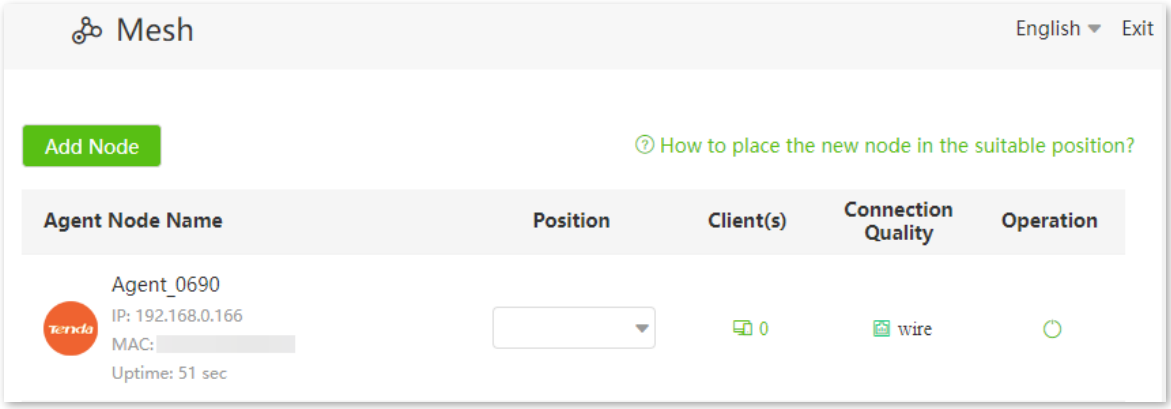
Procedure:

1. Power on the existing router (4G08) and connect it to the internet properly.
2. Place the new router (MX15) where you want to deploy it, which is **bedroom** in this example. Power on the new router. Wait until the startup of the new router is complete (the indicator blinks green slowly).
3. Connect the LAN port (LAN, WAN/LAN) of the existing router to the LAN port of the new router using an Ethernet cable.

---End

The wireless router will automatically network. Please wait about 1 minute. When the indicator of the new router turns solid green, the networking is successful. The MX15 becomes a secondary node in the network.

On the **Mesh** page, you can view and configure the added node.



To access the internet with:

- **Wired devices:** Connect to a LAN port of the router using an Ethernet cable.
- **WiFi-enabled devices:** Connect to the Wi-Fi network using the Wi-Fi name and password you set.

TIP

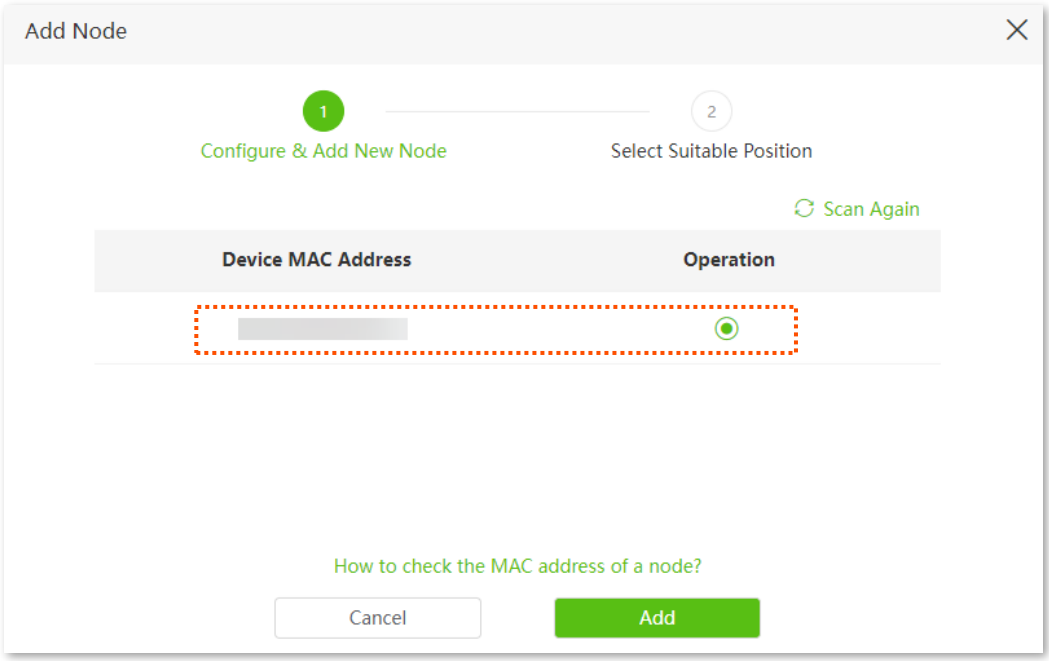
- After the wired networking is successful, if the Ethernet cable connecting the two routers are removed, the system automatically switches to the wireless networking. To obtain better internet access experience after switching to a Wi-Fi network, go to select an appropriate position for the new router.
- If there is still a router to network, repeat this section.

7.2.3 Scanning networking

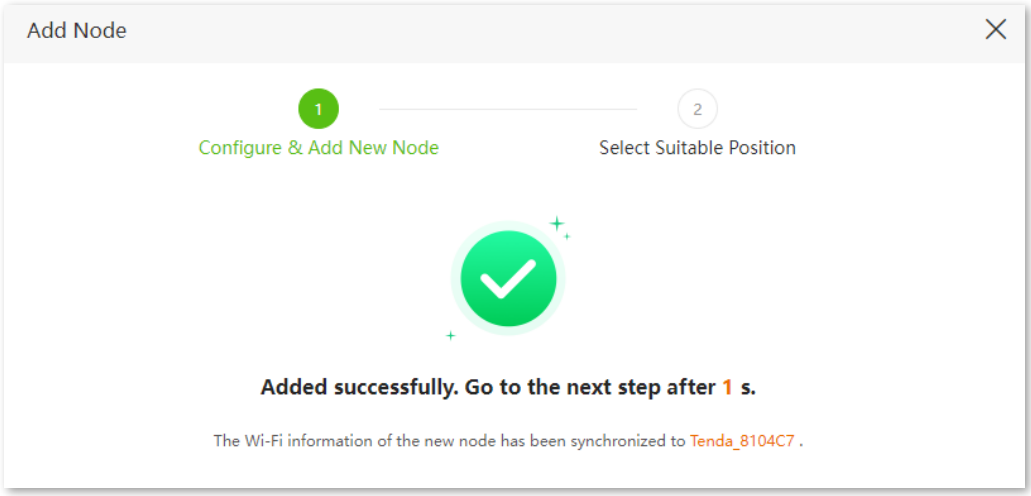
After you fail to add the node to the Mesh network using the Mesh button networking or wired networking, you can manually add other routers to the network of the existing router through the scanning networking.

Procedure:

1. Log in to the web UI of the router, and navigate to **Mesh**.
2. Click **Manually add** on the **Add Node** page.
3. The system discovers new nodes, ensure that the MAC address is the same as the MAC address on the label of the new router, select a node, and click **Add**.



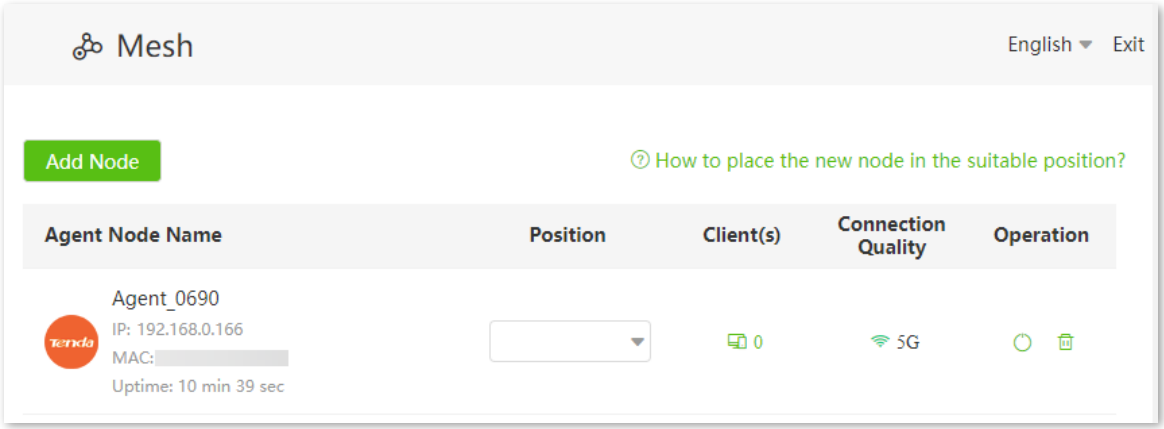
4. Wait until the ongoing process is complete. The new node is added successfully.



5. Select an appropriate position for the new router.

---End

On the **Mesh** page, you can view and configure the added node.



To access the internet with:

- **Wired devices:** Connect to a LAN port of the router using an Ethernet cable.
- **WiFi-enabled devices:** Connect to the Wi-Fi network using the Wi-Fi name and password you set.

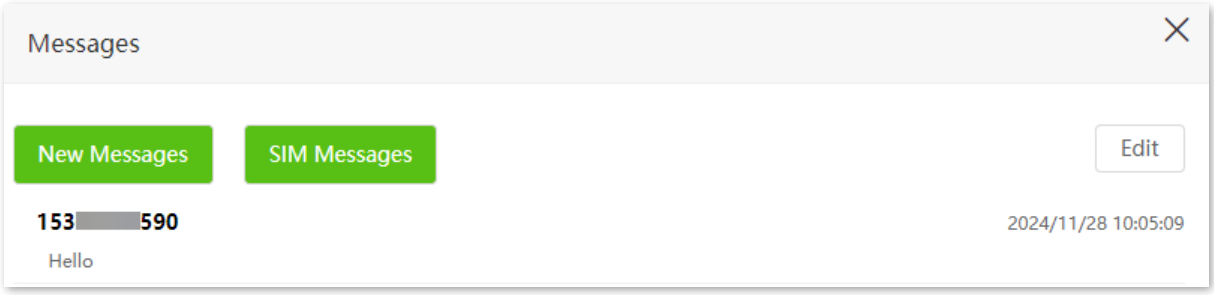
Repeat this section to add other routers.

8 SMS

8.1 Manage SMS messages

This router supports sending, receiving, deleting and exporting SMS messages on the web UI.

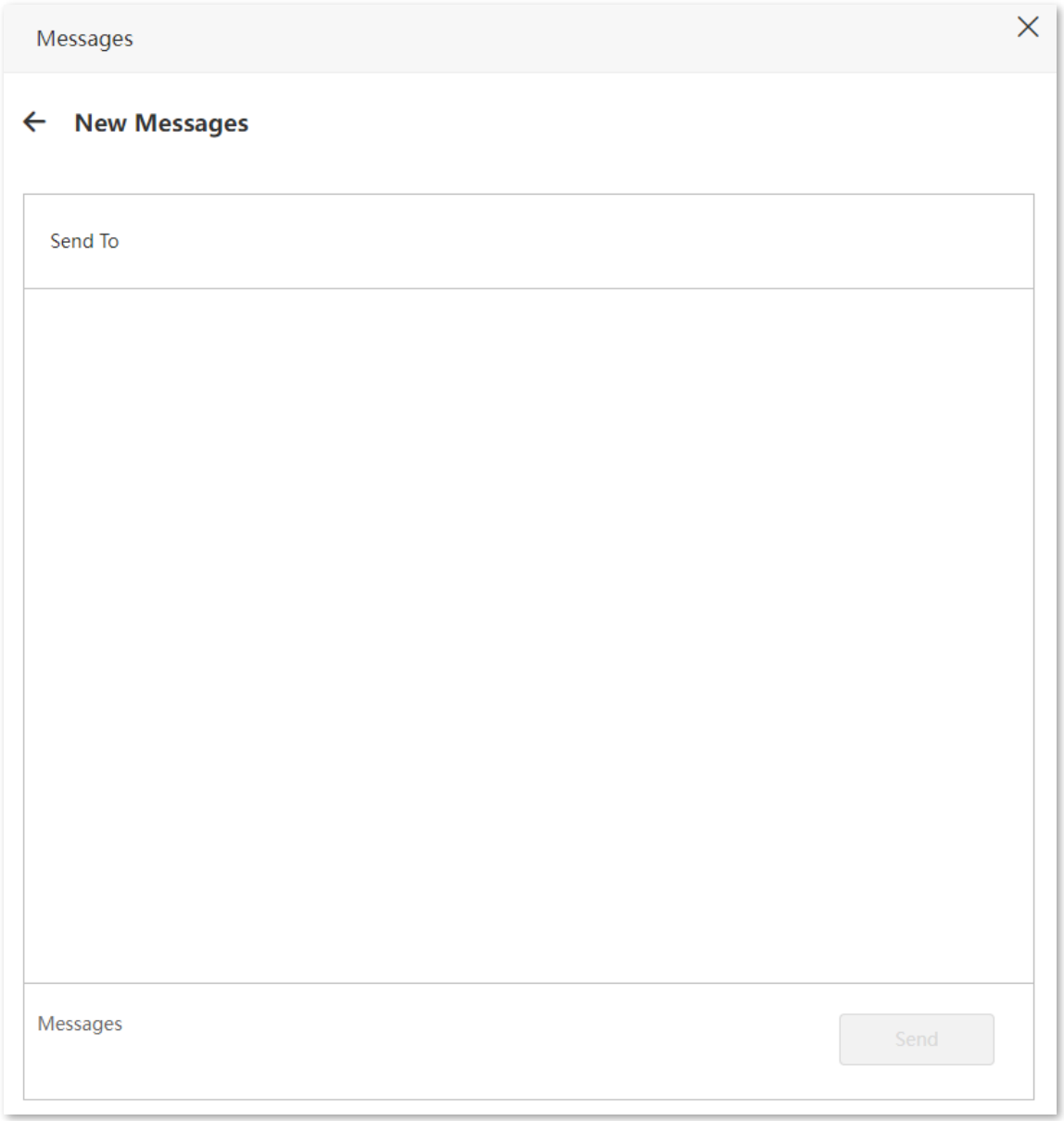
To access the page, log in to the web UI of the router, and navigate to **SMS** > **Messages**.



8.1.1 Send SMS messages

Send SMS messages to a new smartphone number

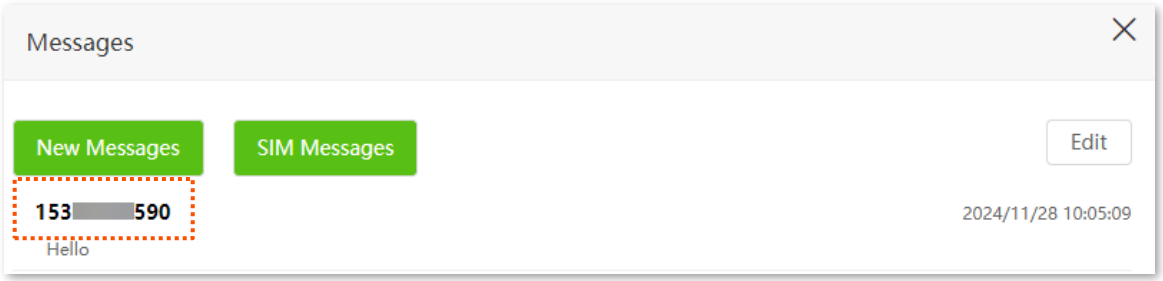
1. Log in to the web UI of the router.
2. Navigate to **SMS** > **Messages.**
3. Click **New Messages**.
4. Enter the smartphone number in the **Send To** column.
5. Enter the message content in the **Messages** column at the bottom.
6. Click **Send** at the bottom right corner.



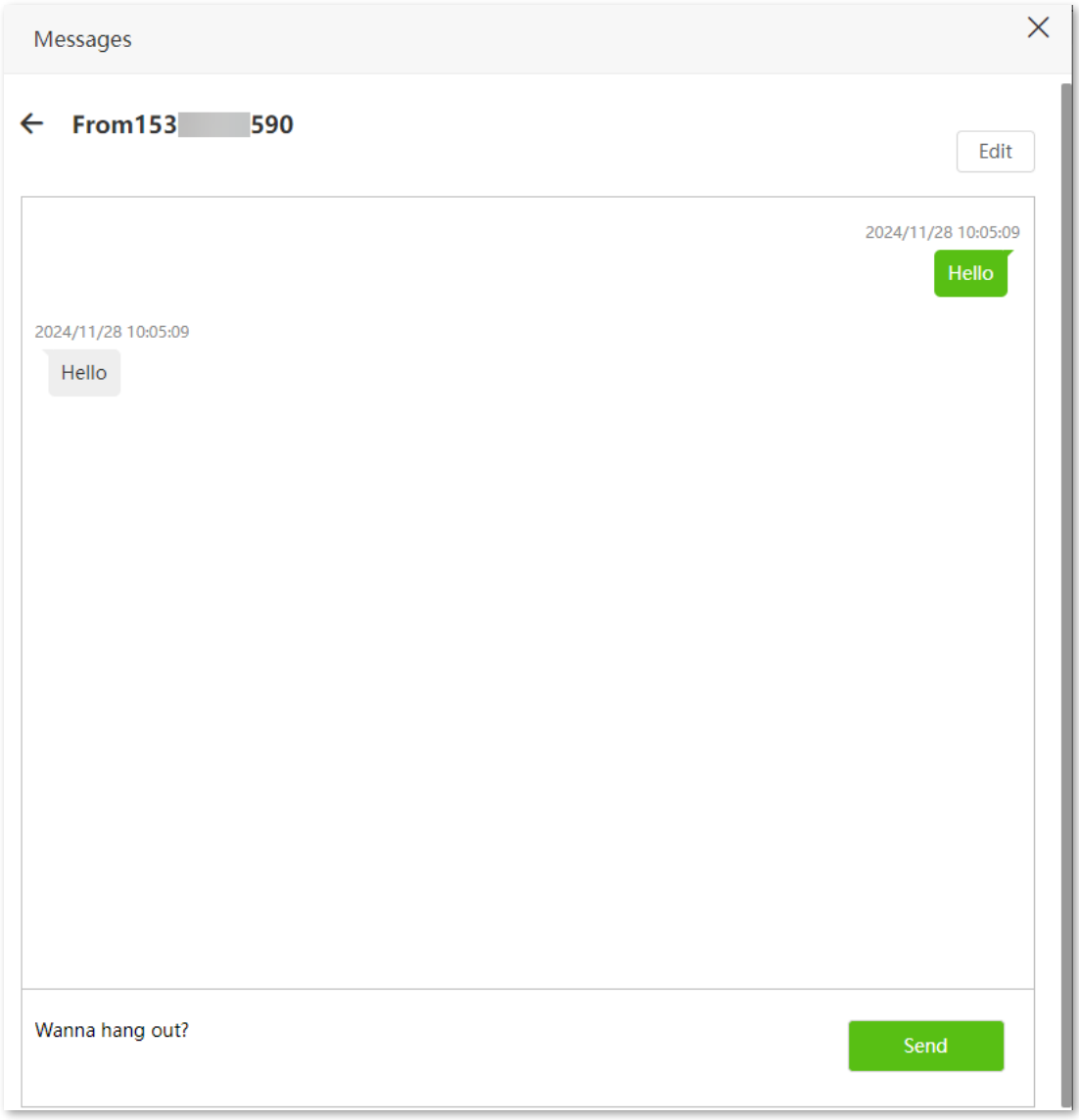
---End

Send messages to an existing smartphone number

1. Log in to the web UI of the router.
2. Navigate to **SMS** > **Messages.**
3. Click the targeted smartphone number.



4. Enter the message content in the **Messages** column at the bottom.
5. Click **Send**.



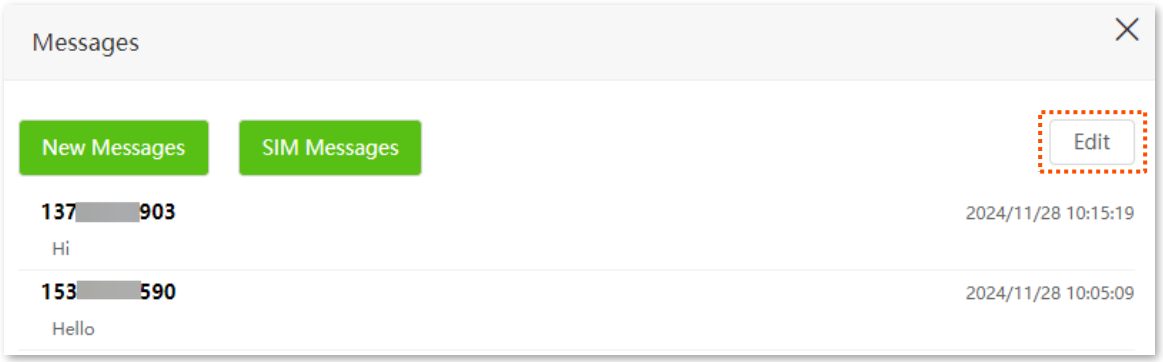
---End

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

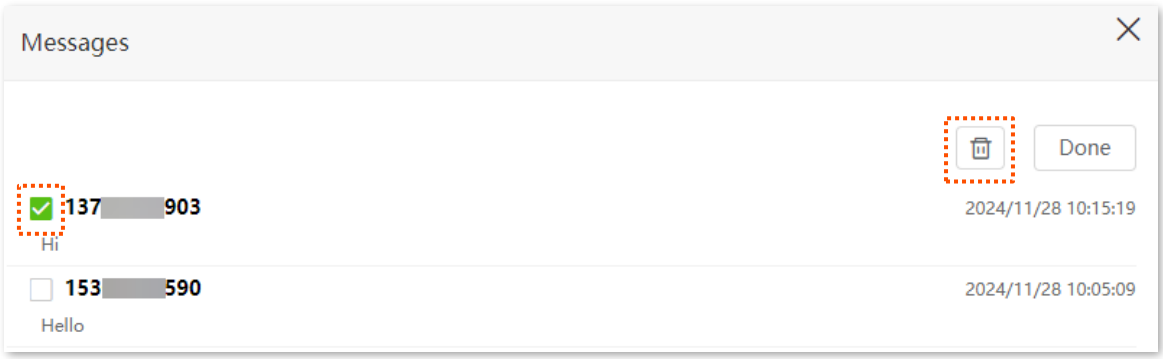
8.1.2 Delete SMS messages

Delete all messages of the same smartphone numbers

1. Log in to the web UI of the router.
2. Navigate to **SMS** > **Messages.**
3. Click **Edit** in the upper right corner.



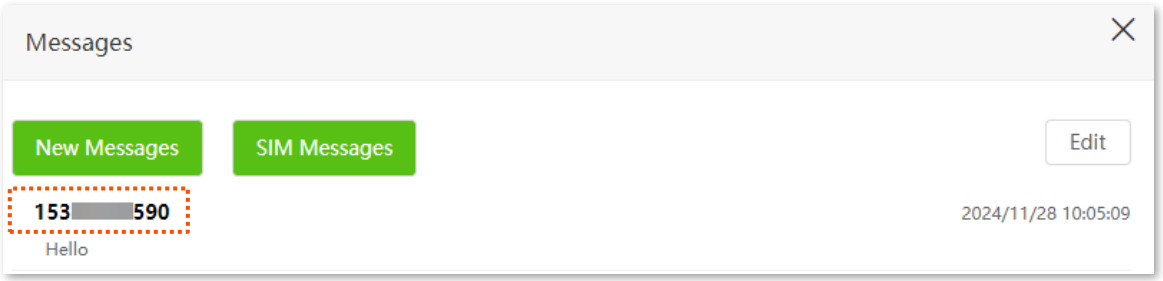
4. Select the smartphone number to be deleted.
5. Click .



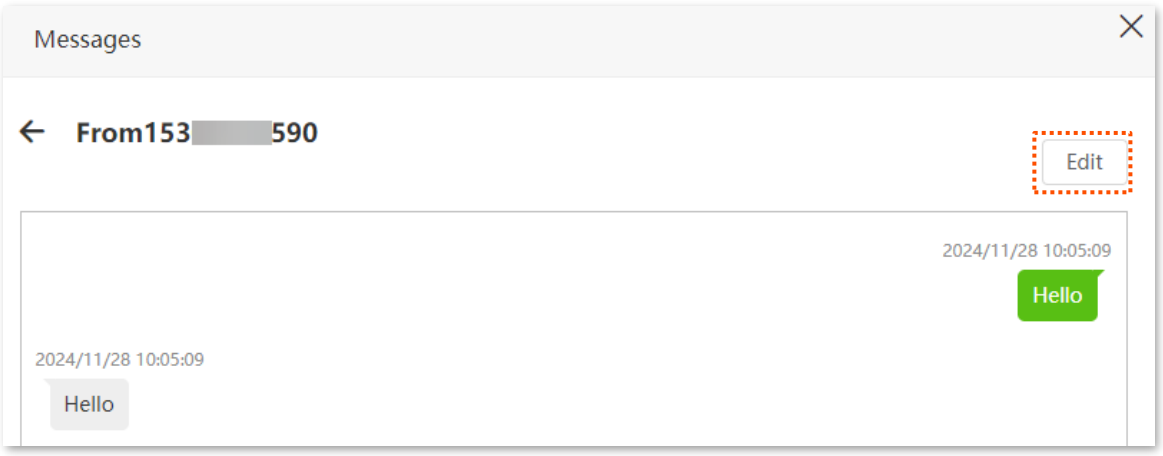
---End

Delete certain messages of the same smartphone number

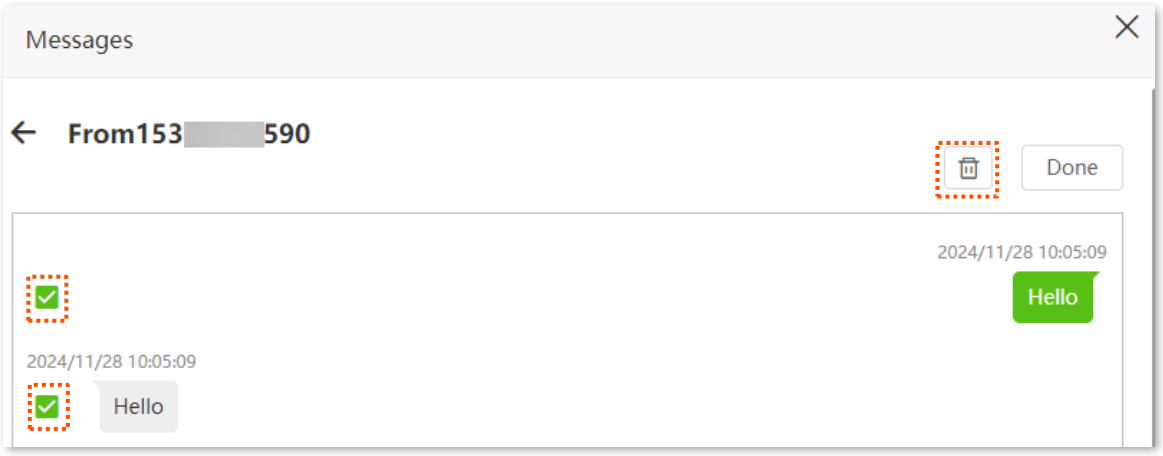
1. Log in to the web UI of the router.
2. Navigate to **SMS** > **Messages.**
3. Click the targeted smartphone number.



4. Click **Edit**.



5. Select the messages to be deleted.
6. Click  .



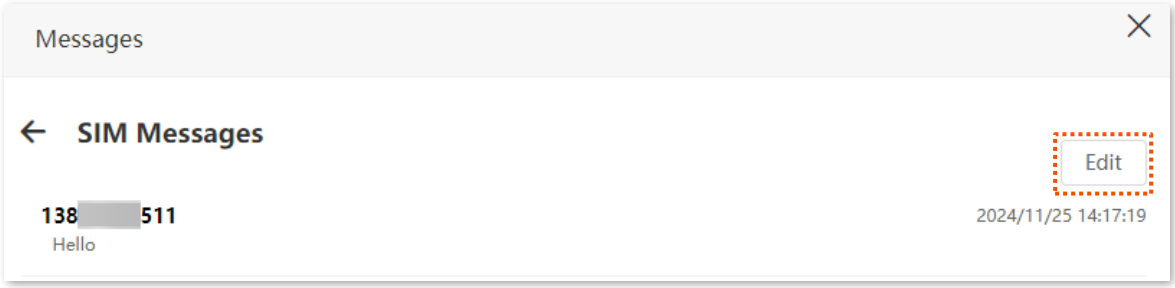
---End

Delete certain messages of the SIM card

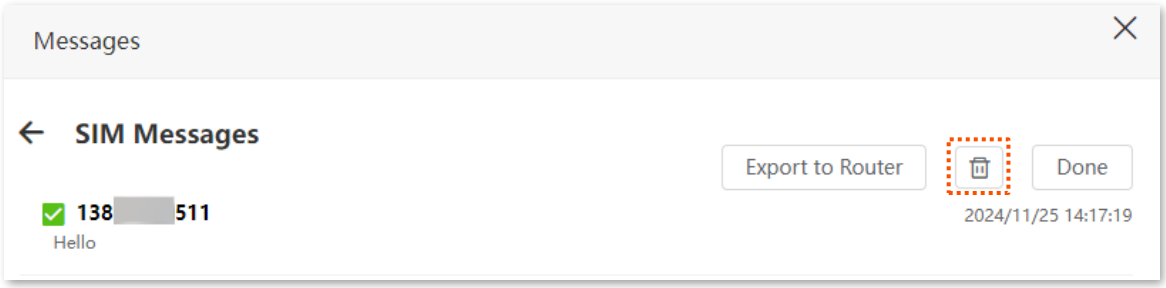
TIP

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

1. Log in to the web UI of the router.
2. Navigate to **SMS** > **Messages.**
3. Click **SIM Messages**.
4. Click **Edit** in the upper right corner.



5. Select the smartphone number to be deleted.
6. Click .



---End

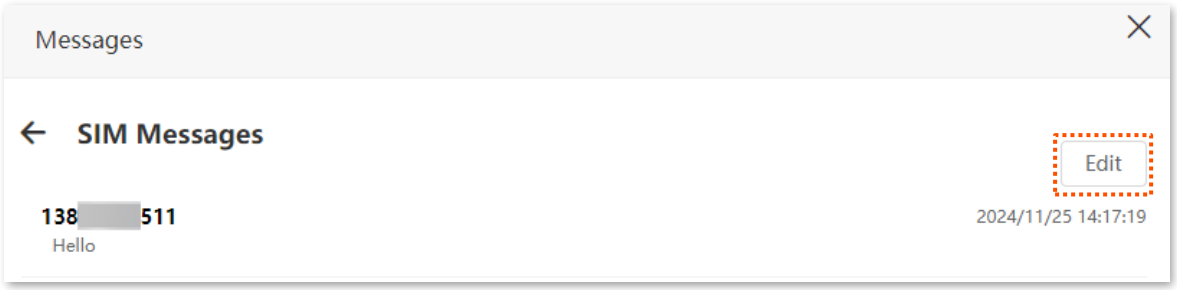
8.1.3 Export SMS messages

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.

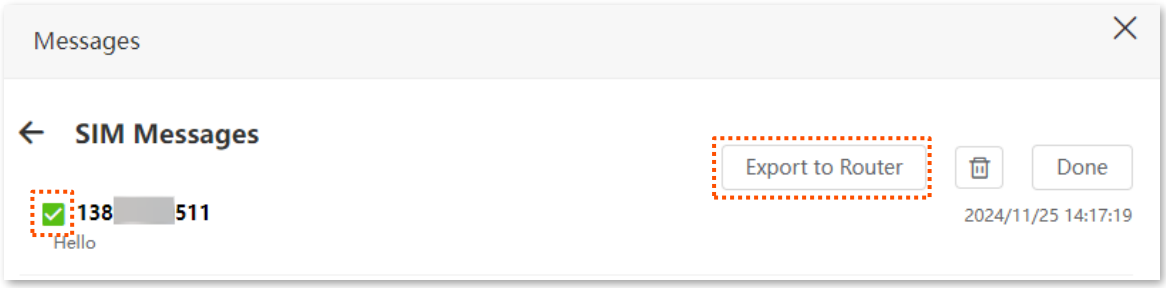
Procedure:

1. Log in to the web UI of the router.
2. Navigate to **SMS** > **Messages.**

3. Click **SIM Messages**.
4. Click **Edit** in the upper right corner.



5. Select the smartphone number to export messages.
6. Click **Export to Router**.



---End

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

8.2 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.

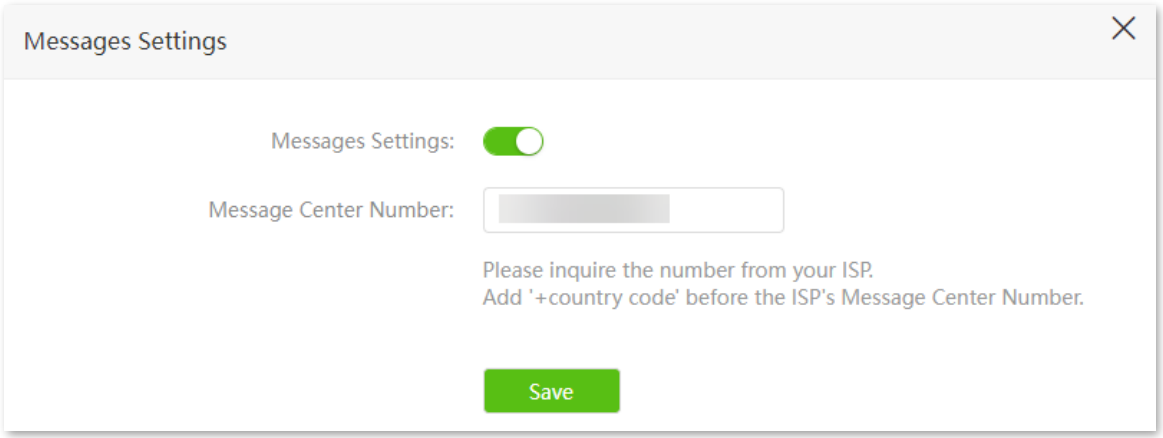
Procedure:

1. Log in to the web UI of the router.
2. Navigate to **SMS** > **Messages Settings**.
3. Enable **Message Settings**.
4. Enter the correct **Message Center Number**.

TIP

Contact your ISP for correct message center number.

5. Click **Save**.



---End

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

8.3 Inquire information by sending USSD commands

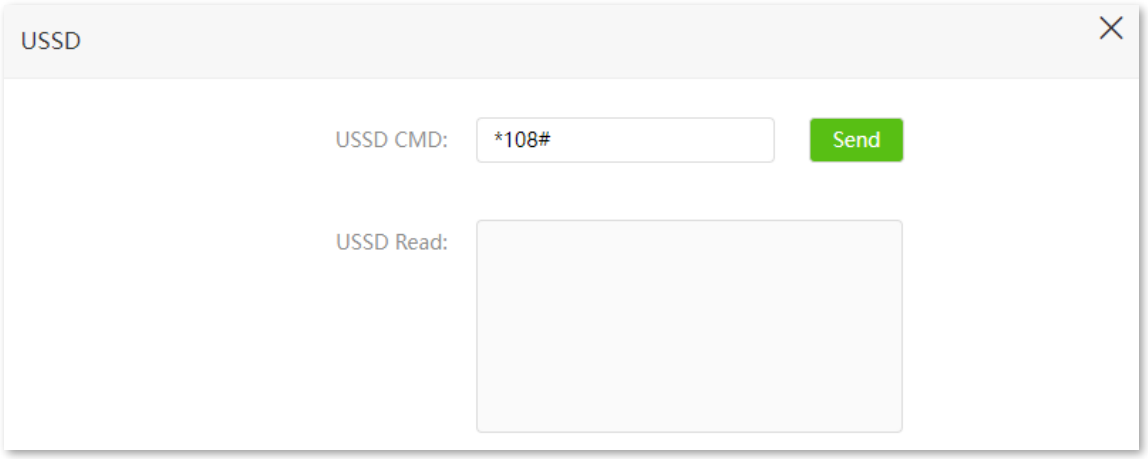
With the **USSD** function, you can inquire specific information or perform specific operations by send a special code or command to your ISP.

NOTE

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

Procedure:

1. Log in to the web UI of the router.
2. Navigate to **SMS** > **USSD**.
3. Set the **USSD CMD**, which is ***108#** in this example.
4. Click **Send**.



---End

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

9 Guest network

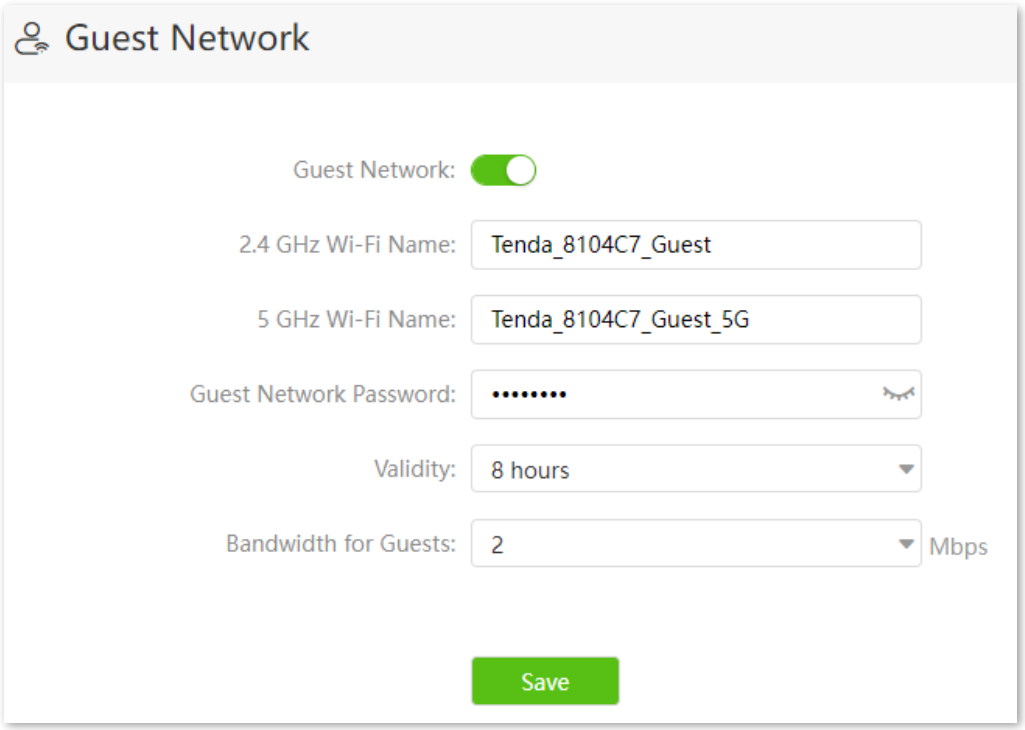
9.1 Overview

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

On this page, you can enable or disable the guest network function and change the Wi-Fi names and password of the guest networks.

To access the page, log in to the web UI of the router, and navigate to the **Guest Network**.

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



Parameter description

Parameter	Description
Guest Network	Used to enable or disable the guest network function.

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

9.2 Example of configuring the guest network

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

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

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

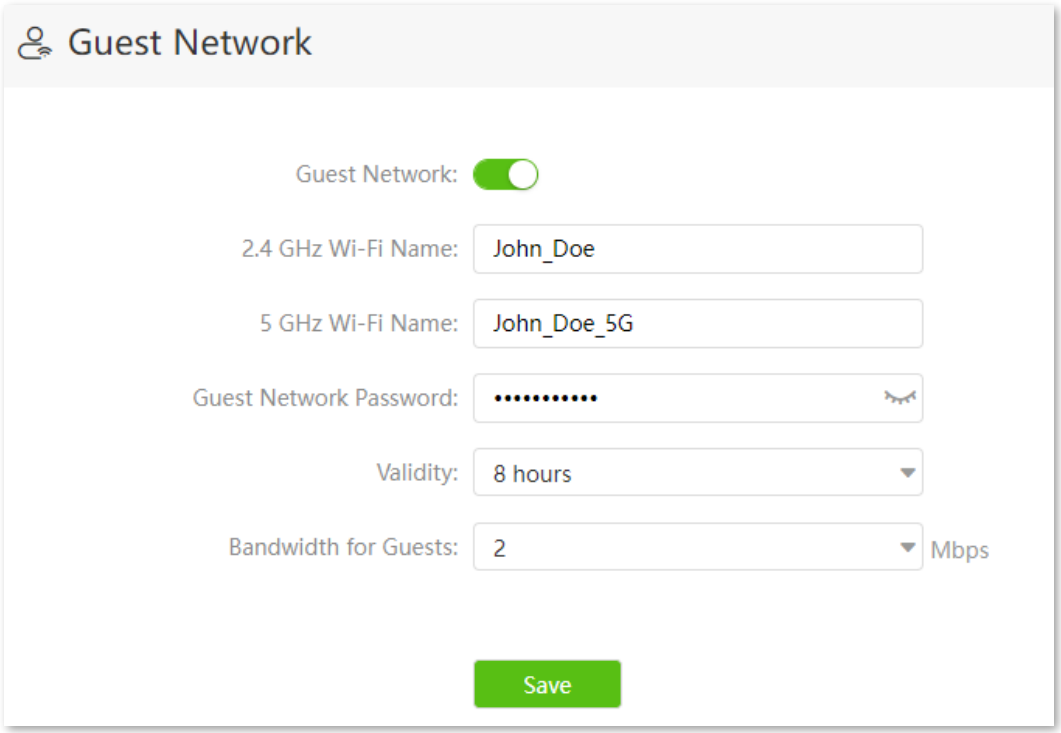
Assume that the parameters you are going to set for the guest Wi-Fi network:

- Wi-Fi names for 2.4 GHz and 5 GHz networks: John_Doe and John_Doe_5G
- Wi-Fi password for 2.4 GHz and 5 GHz networks: Tenda_12345
- The shared bandwidth for guests: 2 Mbps

Procedure:

1. Log in to the web UI of the router.
2. Navigate to **Guest Network**.
3. Enable the **Guest Network** function.
4. Set the **2.4 GHz Wi-Fi Name**, which is **John_Doe** in this example.
5. Set the **5 GHz Wi-Fi Name**, which is **John_Doe_5G** in this example.
6. Set the **Guest Network Password**, which is **Tenda_12345** in this example.
7. Select a validity time from the **Validity** drop-down box, which is **8 hours** in this example.
8. Set the bandwidth in the **Bandwidth for Guests** drop-down box, which is **2** in this example.

9. Click **Save**.



---End

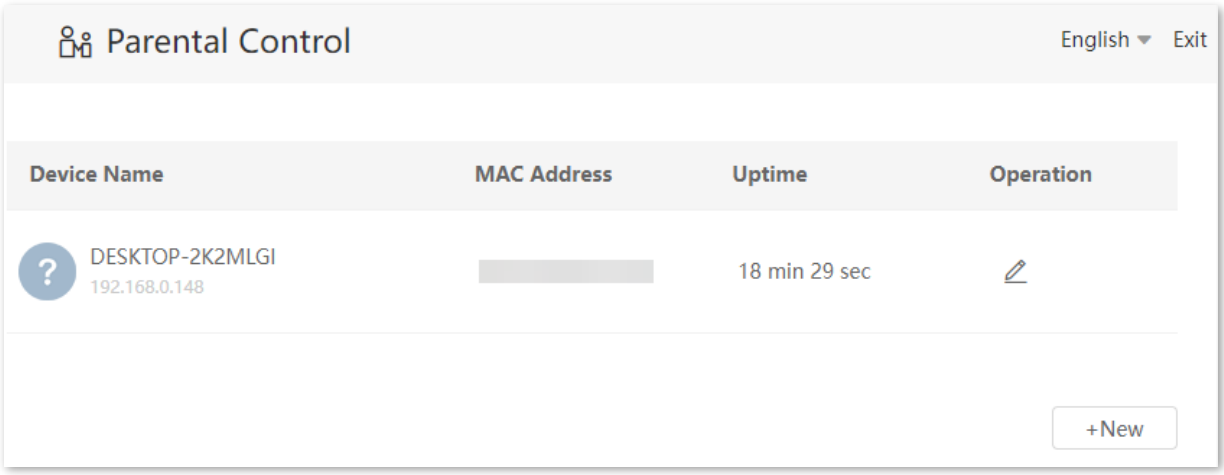
During the 8 hours after the configuration, guests can connect their wireless devices, such as smartphones, to **John_Doe** or **John_Doe_5G** to access the internet and enjoy the shared bandwidth of 2 Mbps.

10 Parental control

10.1 Overview

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

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

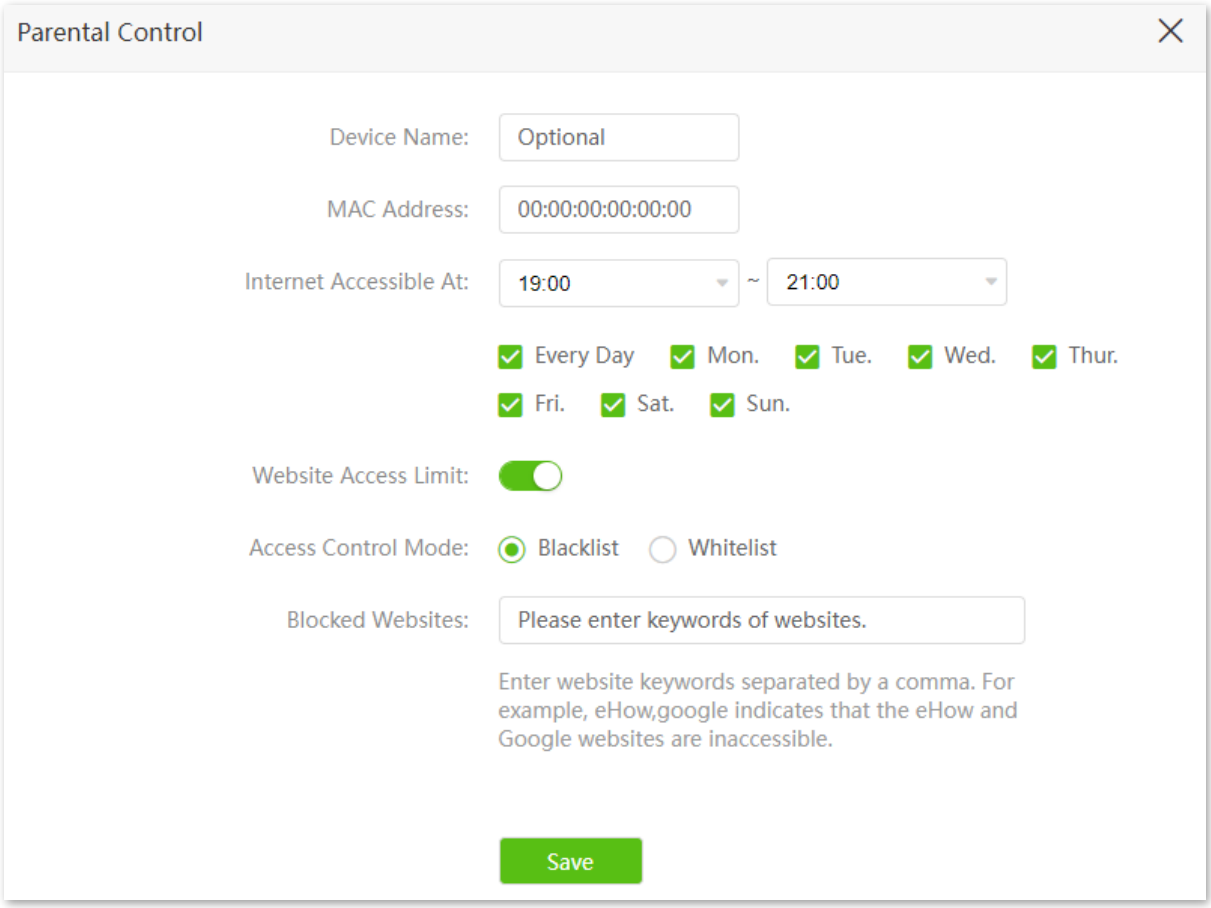


Parameter description

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	Click to configure the parental control rule for the device. After you have configured the parental control rule for the device, there should be a or button, which is used to enable or disable the configured rule.
+New	Click **+New** to add parental control rules for devices that are not connected to the router at the time.

10.2 Configure the parental control rule

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



Parameter description

Parameter	Description
Device Name	Specifies the name of the device 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.

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

10.3 Example of adding parental control rules

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

Requirement: 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.

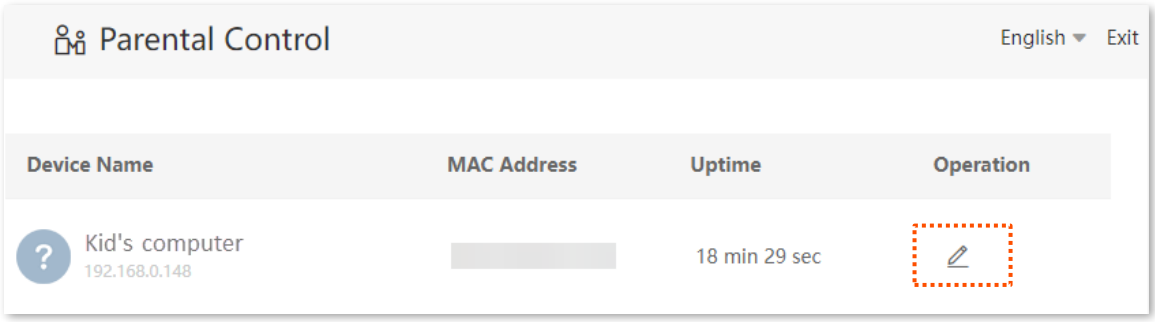
Procedure:

1. Log in to the web UI of the router.
2. Navigate to **Parental Control**.
3. Configure the parental control rule.

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

   TIP

   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.



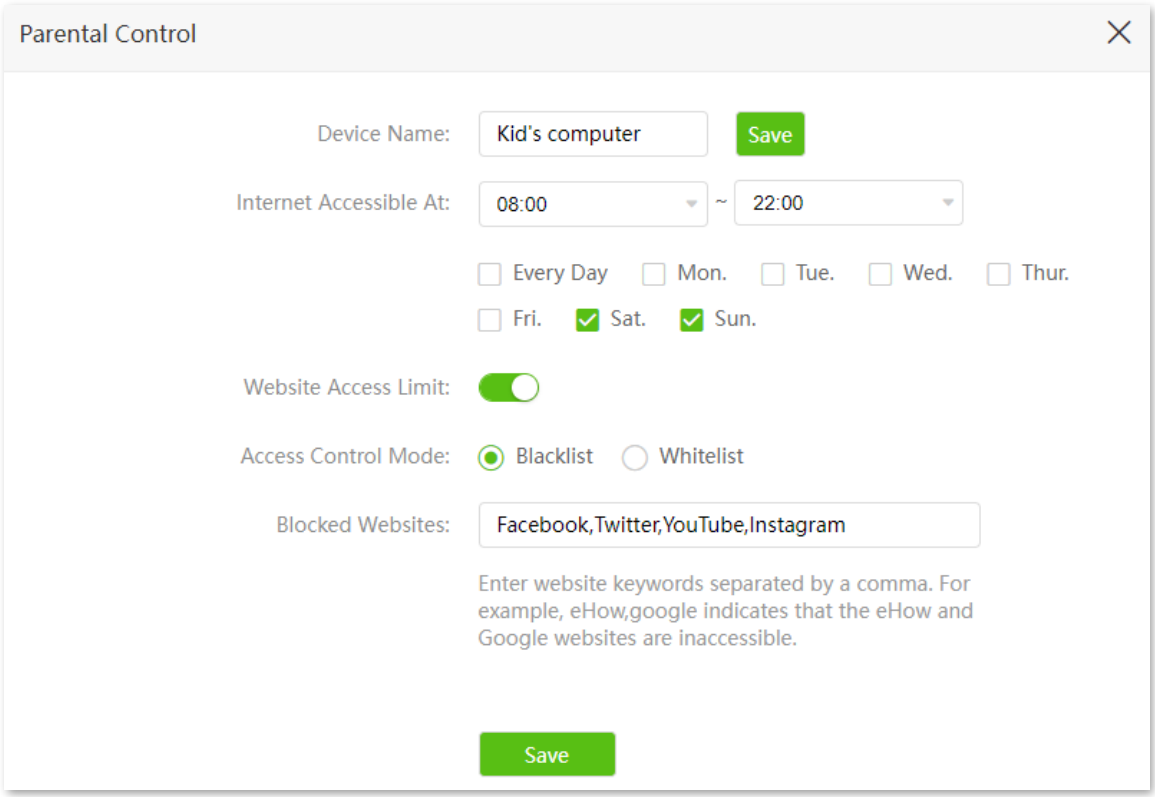
2) Specify the period when the internet can be accessed, which is **8:00 ~ 22:00** in this example.

3) Tick the days when the rule is applied, which are **Sat.** and **Sun.** in this example.

4) Enable **Website Access Limit**, and choose **Blacklist**.

5) Set **Blocked Websites**, which is **Facebook,Twitter,YouTube,Instagram** in this example.

6) Click **Save**.



---End

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.

11 NAT forwarding

11.1 Virtual server

11.1.1 Overview

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

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

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

To access the page, log in to the web UI of the router, and navigate to **NAT Forwarding** > **Virtual Server**.

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 this parameter, **TCP&UDP** is recommended.

Parameter	Description
Operation	Available operations include: + Add : Used to add a new virtual server rule. : Used to delete existing virtual server rules.

11.1.2 Enable internet users to access LAN resources

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

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

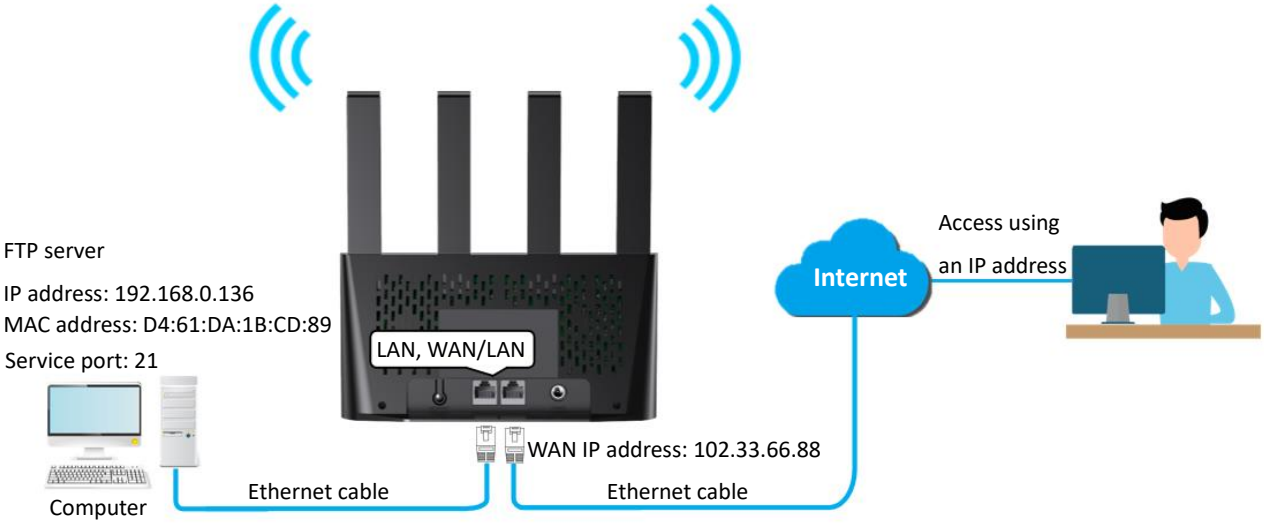
Solution: You can configure the virtual server function to reach the requirements.

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.

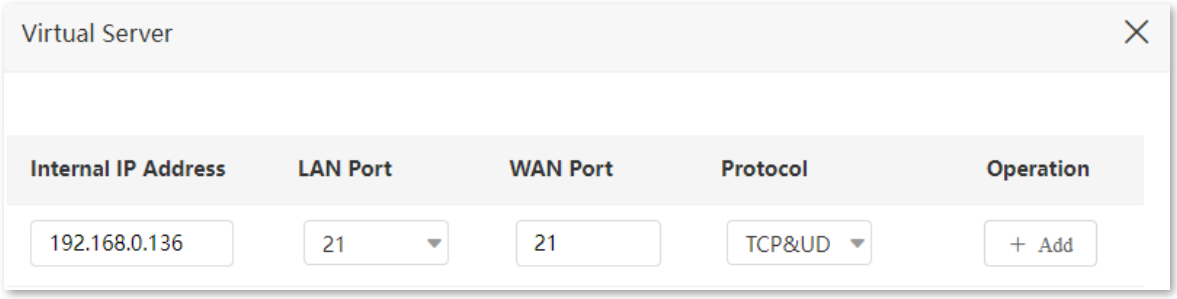
TIP

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



Procedure:

1. Log in to the web UI of the router.
2. Add a virtual server rule.
   1) Navigate to **NAT Forwarding** > **Virtual Server**.
   2) Enter the **Internal IP Address**, which is **192.168.0.136** in this example.
   3) Choose a **LAN Port** in the drop-down box, which is **21** in this example.
   4) Set a **WAN Port** in the drop-down box, which is **21** in this example.
   5) Choose a protocol, which is **TCP&UDP** in this example.
   6) Click **+ Add**.



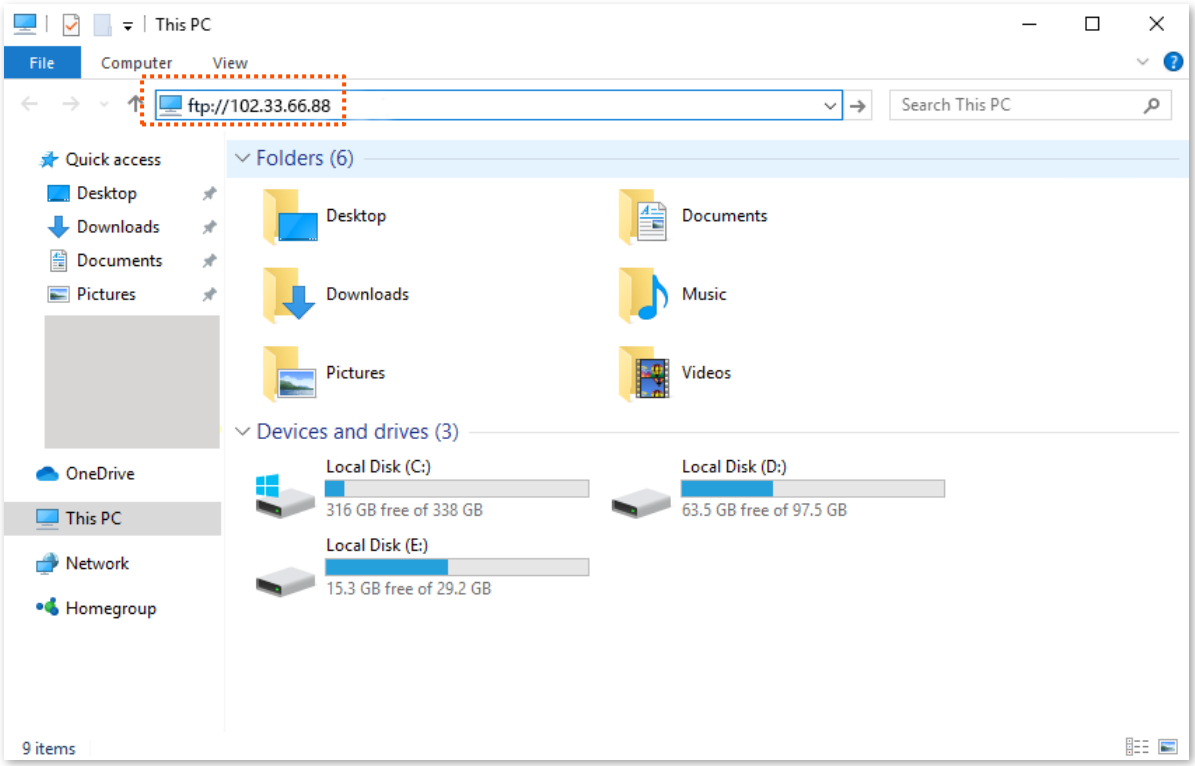
3. Assign a fixed IP address to the host where the server locates.
   1) Navigate to **Security** > **DHCP Reservation**.
   2) Specifies a **Device Name** for the host of the server, which is **FTP server** in this example.
   3) Enter the **MAC Address** of the host of the server, which is **D4:61:DA:1B:CD:89** in this example.

4) Set the **IP Address** reserved for the host, which is **192.168.0.136** in this example.

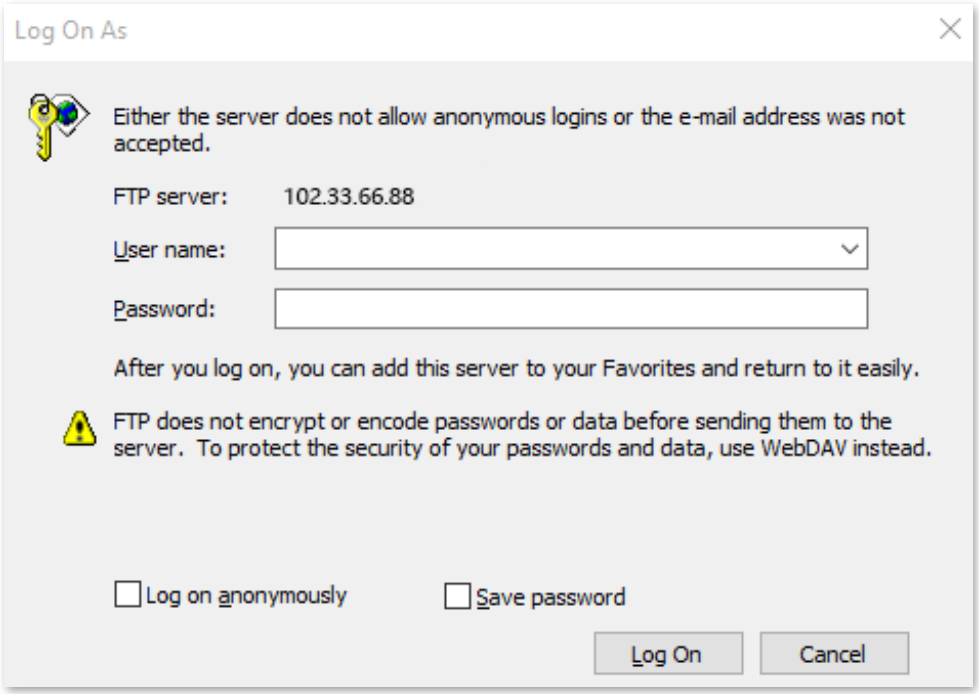
5) Click **+ Add**.

---End

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



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



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

TIP

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

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

11.2 DMZ host

11.2.1 Overview

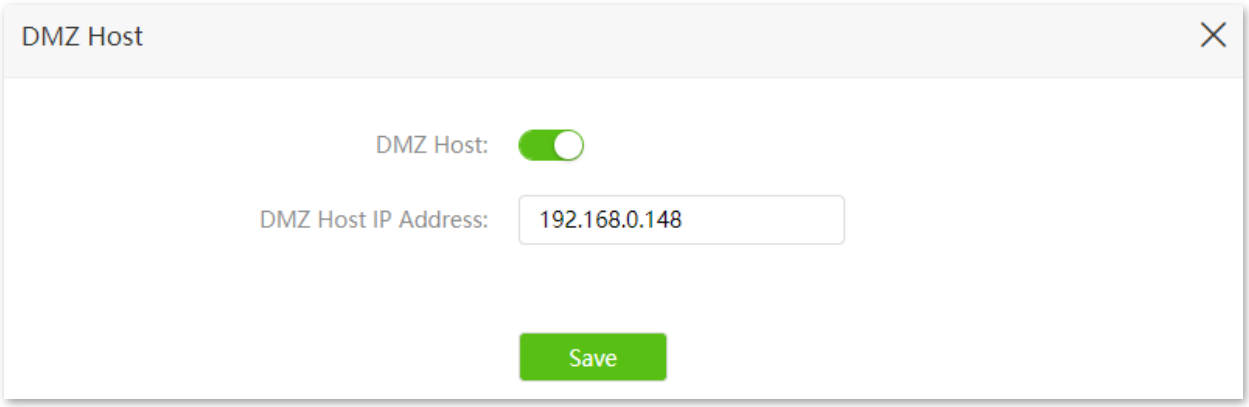
A DMZ host on a LAN is free from restrictions in communicating with the internet. It is useful for getting better and smoother experience in video conferences and online games. You can also set the host of a server within the LAN as a DMZ host when in need of accessing the server from the internet.

NOTE

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

To access the page, log in to the web UI of the router, and navigate to **NAT Forwarding** > **DMZ Host**.

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



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.

11.2.2 Enable internet users to access LAN resources

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

Requirement: 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.

TIP

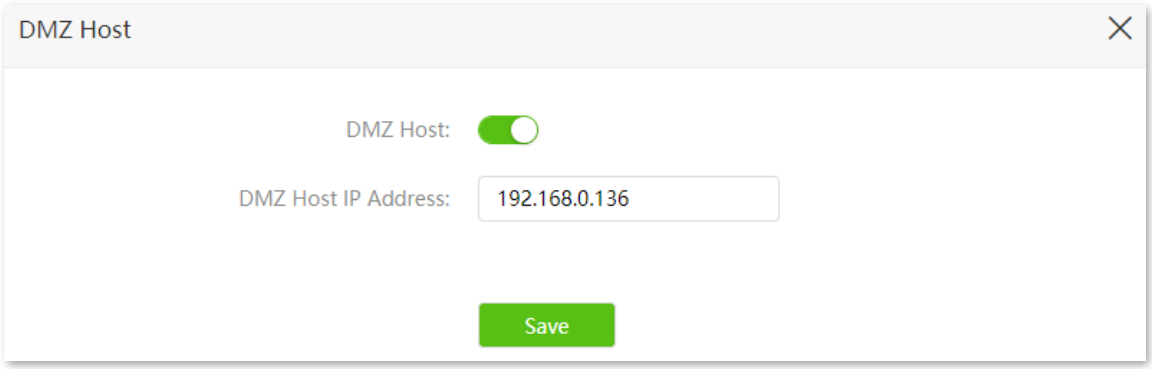
Please ensure that router obtains an IP address from the public network. This function may not work on a host with an IP address of a private network or an intranet IP address assigned by ISPs that start with 100. Common IPv4 addresses are classified into class A, class B and class C. Private IP addresses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

Procedure:

1. Log in to the web UI of the router.
2. Set the server host as the DMZ host.
   1) Navigate to **NAT Forwarding** > **DMZ Host**.
   2) Enable the **DMZ Host** function.

3) Enter the IP address of the host, which is **192.168.0.136** in this example.

4) Click **Save**.



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

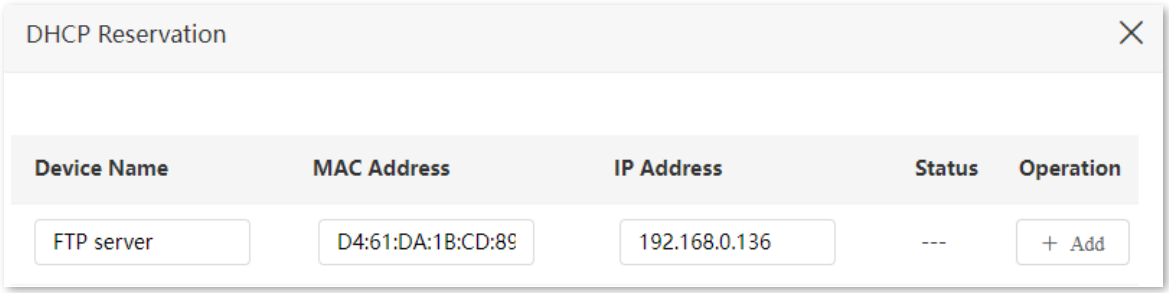
1) Navigate to **Security** > **DHCP Reservation**.

2) Specifies 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) Set the **IP Address** reserved for the host, which is **192.168.0.136** in this example.

5) Click **+ Add**.



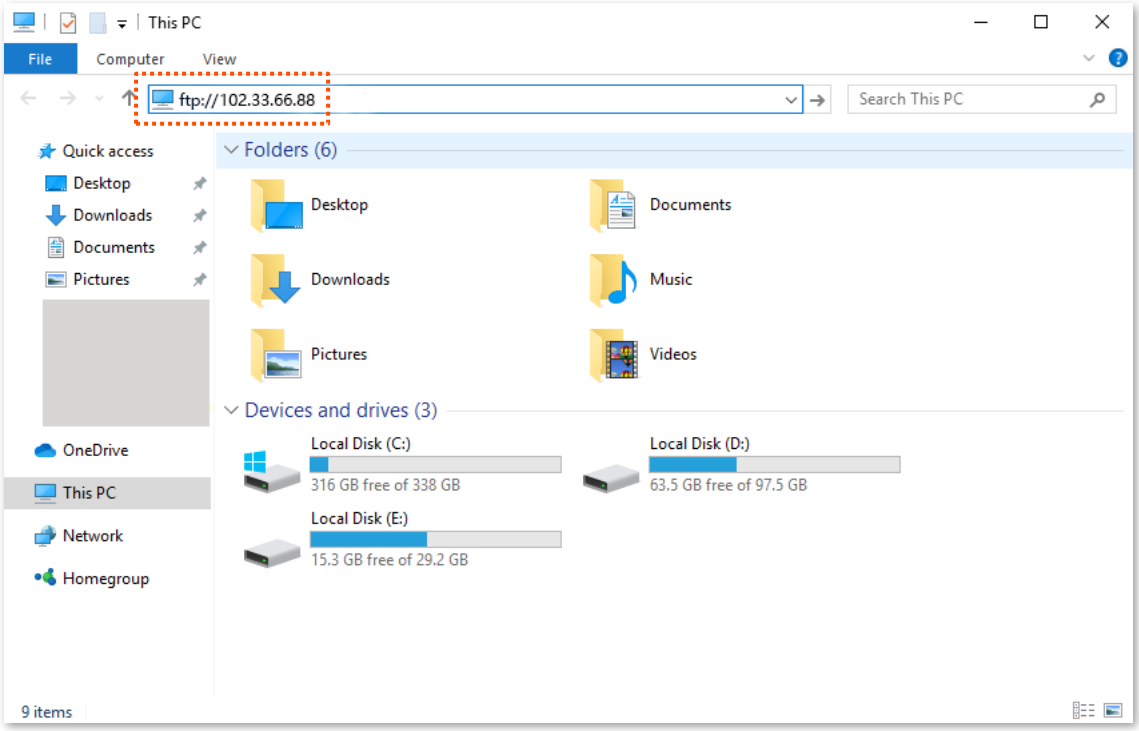
----End

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

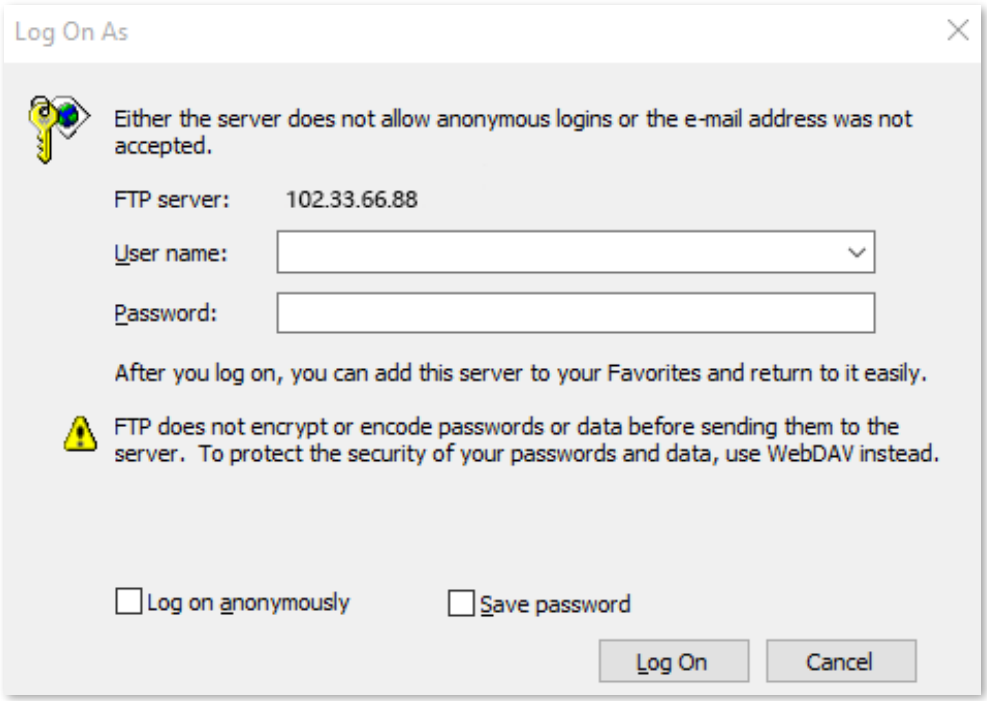
In this example, the address is "**ftp://102.33.66.88**". You can find the WAN IP address of the router in View system information.

TIP

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



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



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

TIP

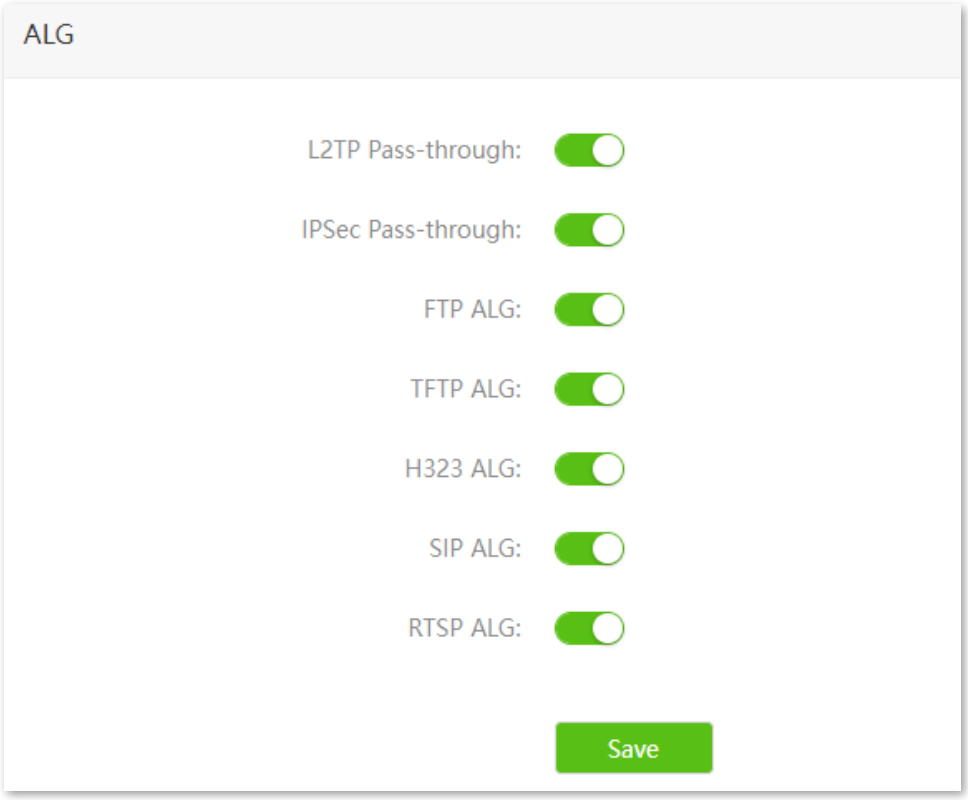
After the configurations, if internet users still cannot access the FTP server, close the firewall, antivirus software and security guards on the host of the FTP server and try again.

11.3 ALG

Application Layer Gateway (ALG) allows you to enable or disable FTP, TFTP, H323, SIP, RTSP functions and VPN pass through as required.

To access the page, log in to the web UI of the router, and navigate to **NAT Forwarding** > **ALG**.

The ALG function is enabled by default.



Parameter description

Name	Description
L2TP Pass-through	If you select L2TP protocol when you create a VPN connection on your computer in the LAN of the router, it takes effect only when this checkbox is selected.

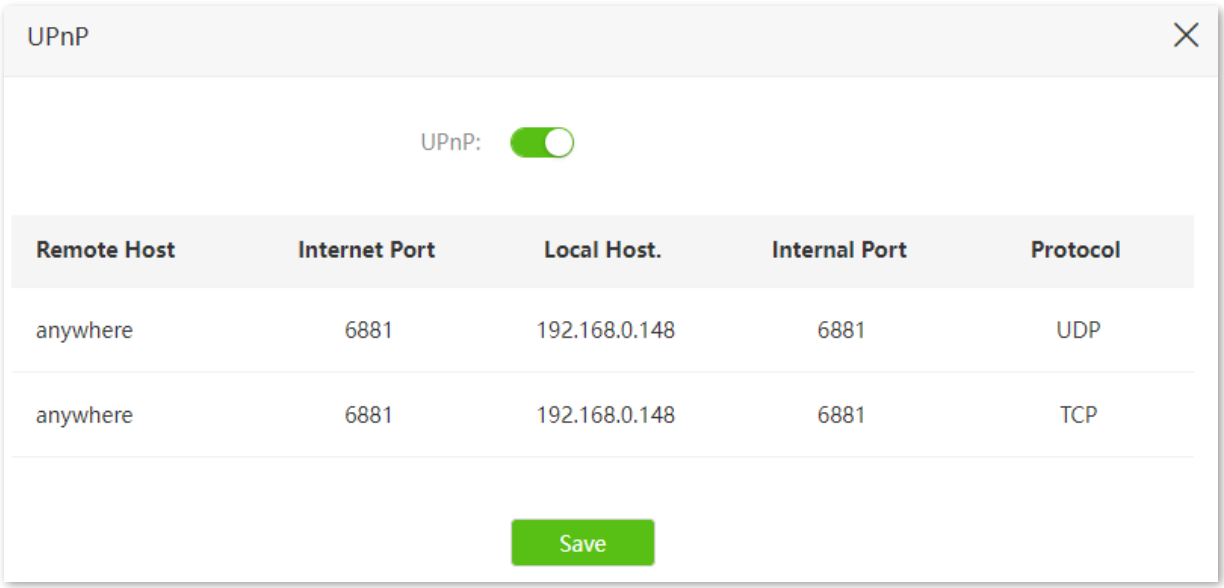
Name	Description
IPSec Pass-through	If you select IPsec protocol when you create a VPN connection on your computer in the LAN of the router, it takes effect only when this checkbox is selected.
FTP ALG	The users on LAN can share resources on the FTP server on WAN only when it is selected.
TFTP ALG	It is a simple protocol used for files transfer. The TFTP ALG processes TFTP packets that initiate the request and creates pinholes to allow return packets from the reverse direction.
H323 ALG	The IP phone and network conference function can be used on the computers connected to the router only when it is selected.
SIP ALG	The IP phone function can be used on the computers connected to the router only when it is selected.
RTSP ALG	The users on LAN can view video on demand when it is selected.

11.4 UPnP

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

To access the page, log in to the web UI of the router, and navigate to **NAT Forwarding** > **UPnP**.

With the UPnP function enabled, you can find the port conversion information on this page when the program sends any requests.



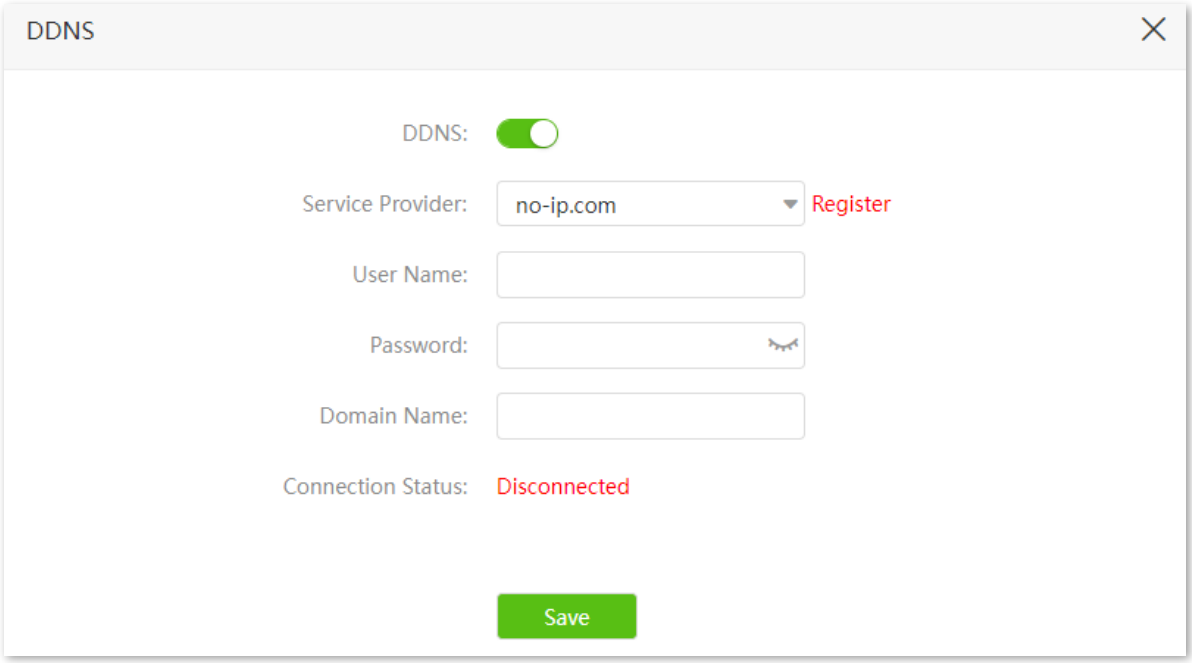
11.5 DDNS

11.5.1 Overview

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

To access the page, log in to the web UI of the router, and navigate to **NAT Forwarding** > **DDNS**.

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



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.

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

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

Requirement: 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:

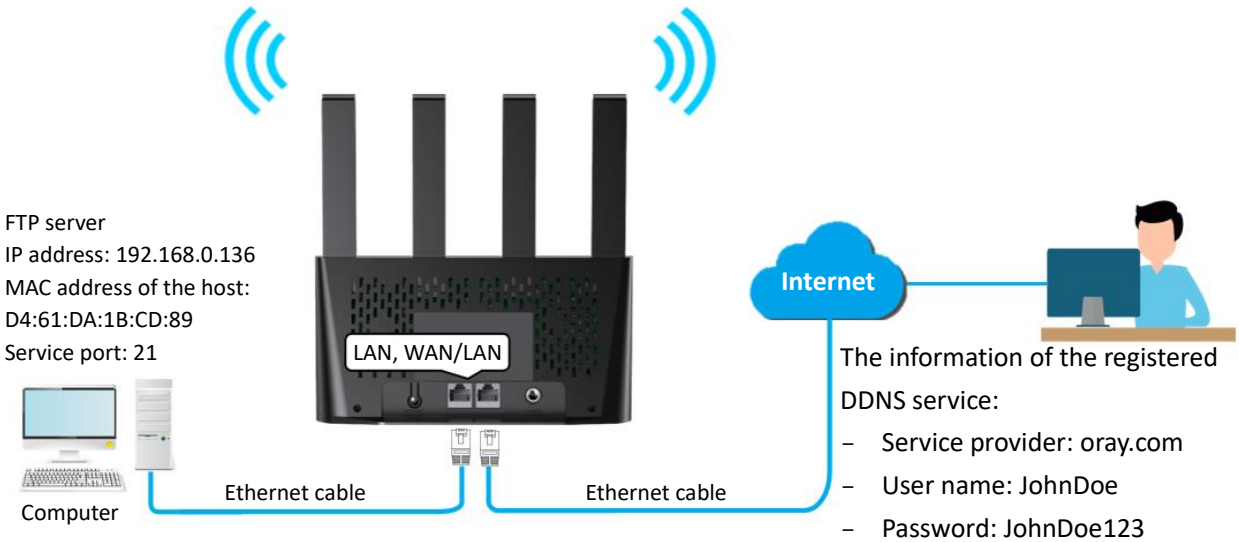
- IP address: 192.168.0.136
- MAC address of the host: D4:61:DA:1B:CD:89
- Service port: 21

The information of the registered DDNS service:

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

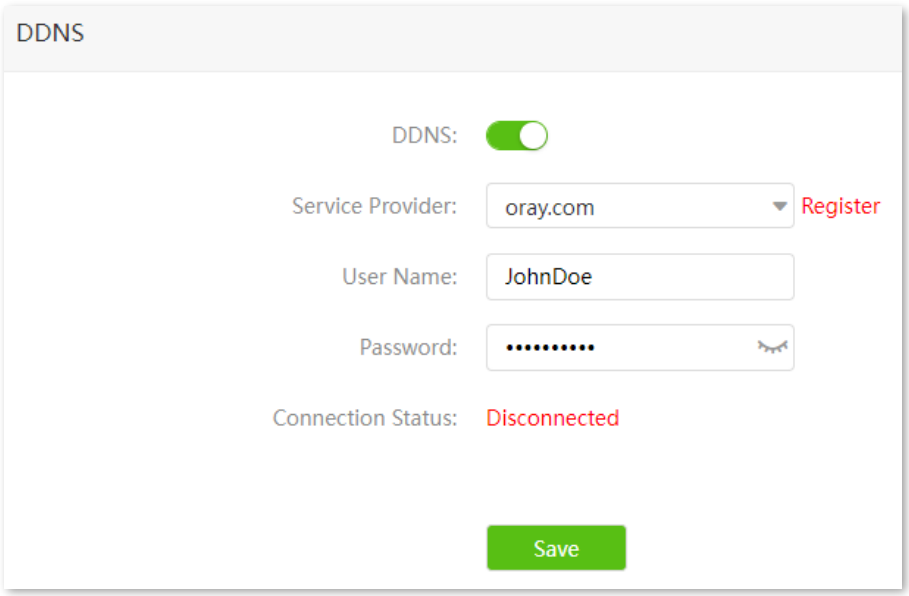
TIP

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



Procedure:

1. Log in to the web UI of the router.
2. Configure the DDNS function.
   1) Navigate to **NAT Forwarding** > **DDNS**.
   2) Enable 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**.

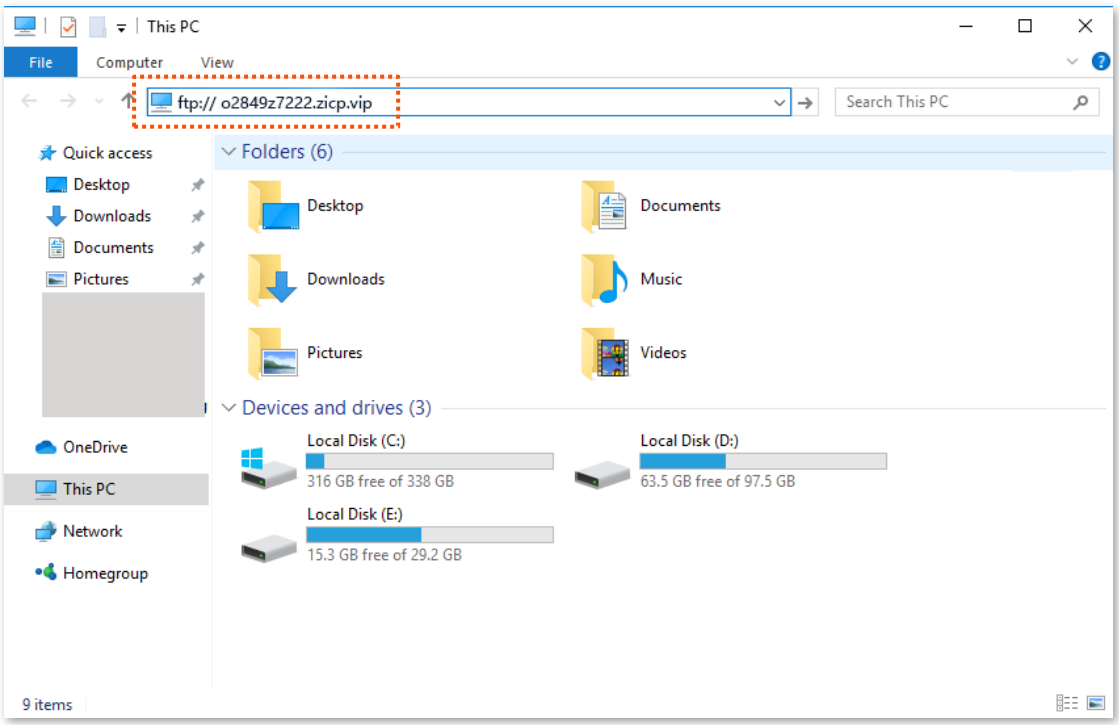


Wait a moment, when the **Connection Status** turns Connected, the configurations succeed.

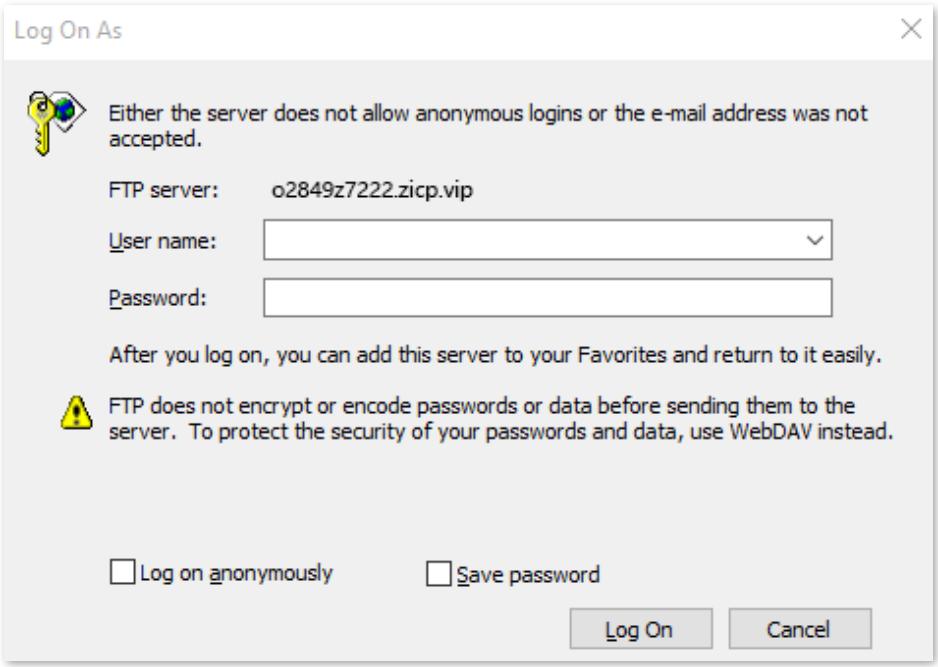
3. Configure the virtual server function (refer to Virtual server).

---End

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



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



TIP

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

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

12 VPN

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

The typology of a VPN network is shown below.

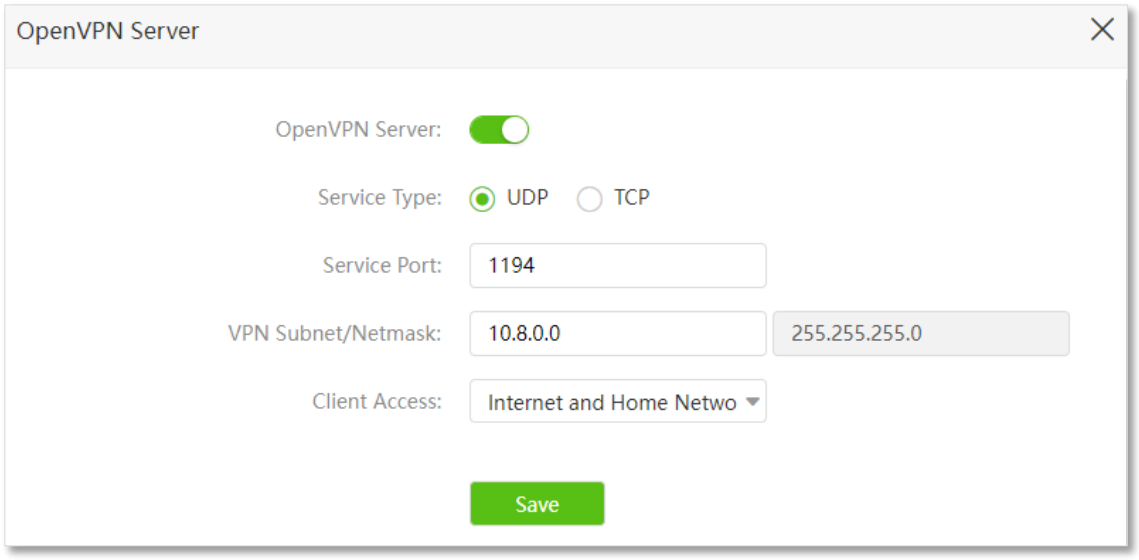
12.1 OpenVPN server

12.1.1 Overview

OpenVPN is a free virtual private network service that enables you to remotely access your internet or home network from anywhere with an open internet service, and access devices and services in use through your router.

To access the page, log in to the web UI of the router, and navigate to **VPN** > **OpenVPN Server**.

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



Parameter description

Parameter	Description
OpenVPN Server	Used to enable or disable the OpenVPN server.
Service Type	Specifies the service type, including **UDP** and **TCP**.
Service Port	Specifies the service port to be customized. The value range is 1025 – 65535.
VPN Subnet/Netmask	Specifies the VPN subnet IP address and subnet mask. The netmask cannot be changed.
Client Access	Specifies the type of the client access, including **Internet and Home Network** and **Home Network Only**. - **Internet and Home Network**: The client can access the home network, internet sites or services with a geographic limitation when you are abroad. The client's default route will be changed. - **Home Network Only**: The client can only access the home network, and the client's default route will not be changed.

12.1.2 Example of configuring OpenVPN server

Scenario: Enterprise employees need to remotely access the internal network resources of the Enterprise, such as internal websites, file shares or databases.

Requirement: Setting up an OpenVPN can connect to the internal network of the Enterprise through a public network (such as the internet), avoiding the risk of exposing the internal resources to the public network.

Solution: You can configure the OpenVPN server function to reach the requirements.

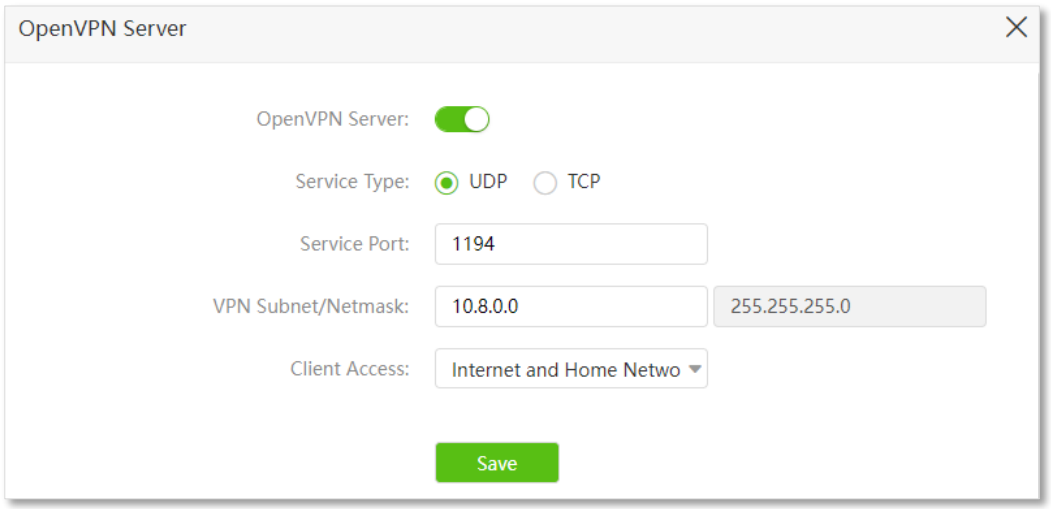
Assume that:

- Service type: UDP
- Server port: 1194
- VPN subnet/netmask: 10.8.0.0/255.255.255.0
- Client access: Internet and Home Network

Procedure:

I. Configure the router

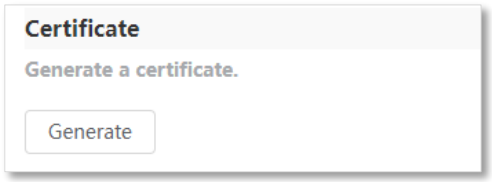
1. Log in to the web UI of the router.
2. Enable the OpenVPN server function, and set the relative parameters as required.
   1) Navigate to **VPN** > **OpenVPN Server**.
   2) Enable the **OpenVPN Server** function.
   3) Set **Service Type** and **Service Port**, which are **UDP** and **1194** respectively in this example.
   4) Set **VPN Subnet/Netmask**, which is **10.8.0.0/255.255.255.0** in this example.
   5) Set **Client Access**, which is **Internet and Home Network** in this example.
   6) Click **Save**.



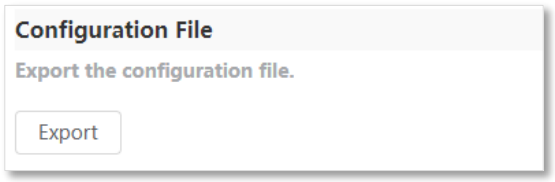
3. Click **Generate** in the **Certificate** module to generate a certificate.

TIP

If the WAN dial-up connection changes, the certificate must be regenerated, as it is only valid for the current WAN IP.

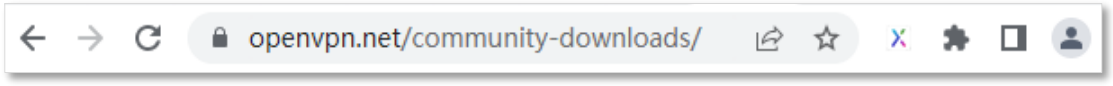


4. Click **Export** in the **Configuration File** module to download the configuration file to your computer.



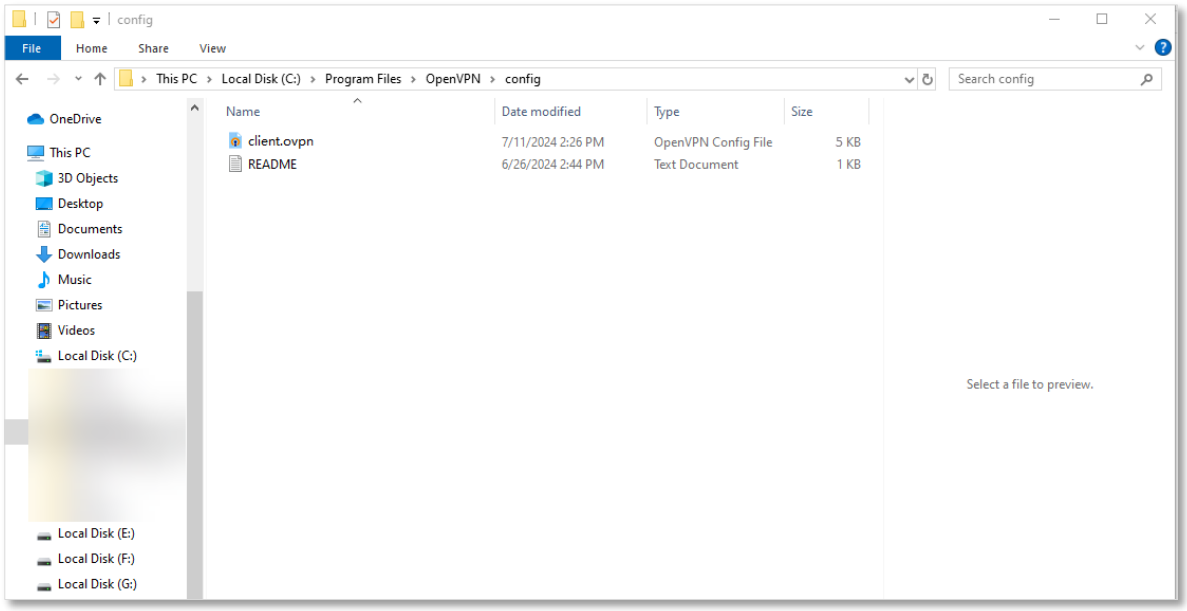
II. Connect the OpenVPN server

1. Start your browser, and enter https://openvpn.net/community-downloads/ in the address bar.



2. Select a version of OpenVPN as required, and click the link corresponding to the Windows version.

3. Download and run the OpenVPN client.
4. Find the Certificate in your download folder, copy the file, and paste the config file into the **config** folder located in the OpenVPN directory. The following figure is for reference only.



5. Launch the OpenVPN client. Right-click  in the bottom right corner of the desktop and choose **Connect.**

---End

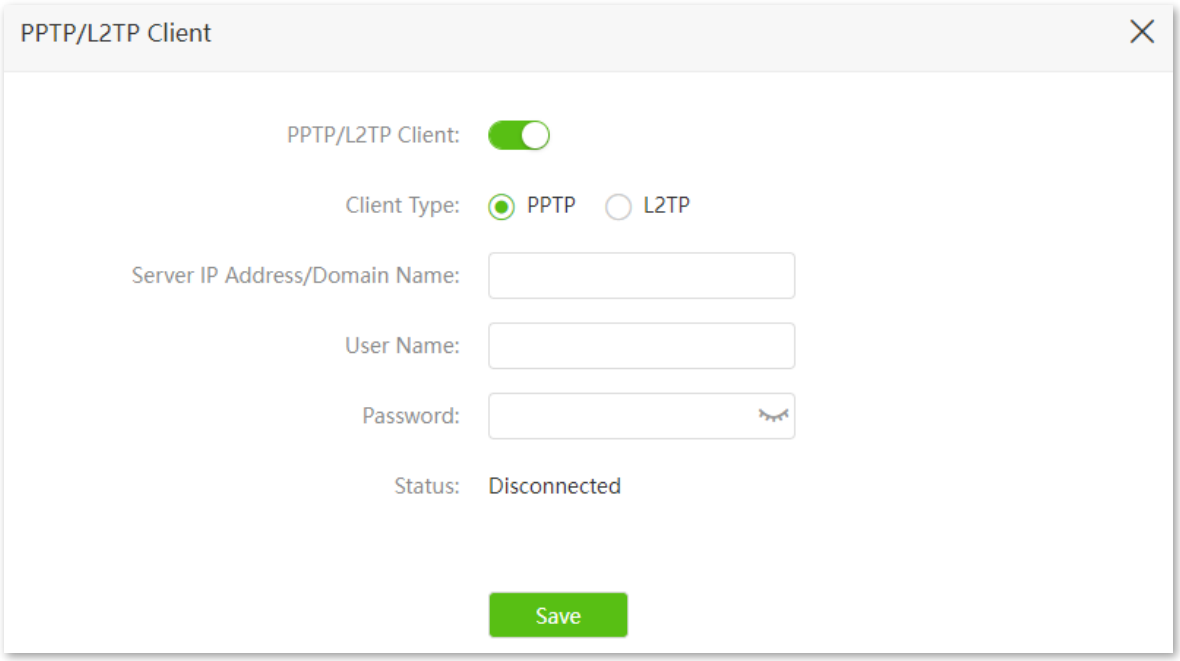
Wait for the icon to change to  . You are now connected to the internet and home network through the VPN. To verify, you can view the VPN connections in the **OpenVPN connection** module on the web UI of the router.

12.2 PPTP/L2TP client

12.2.1 Overview

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

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



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.

12.2.2 Access VPN resources with the router

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

Requirement: Access the VPN resources of your ISP.

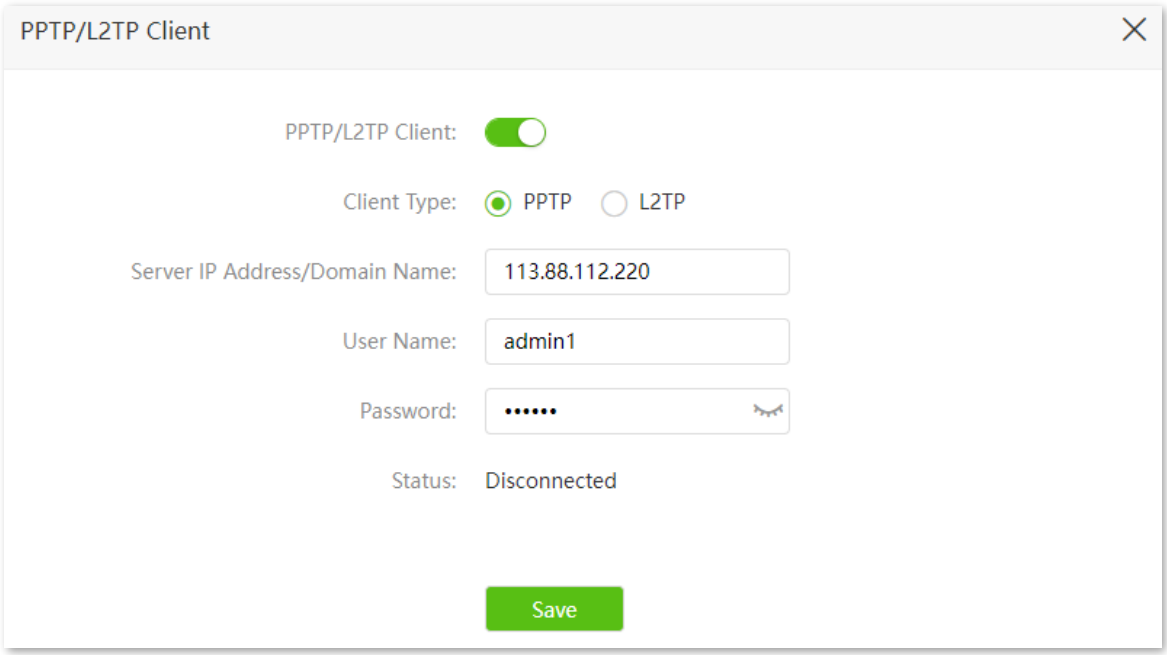
Solution: You can configure the PPTP/L2TP client function to reach the requirements.

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:

1. Log in to the web UI of the router.
1. Navigate to **VPN** > **PPTP/L2TP Client**.
2. Enable the **PPTP/L2TP Client**
3. Choose **PPTP** as the **Client Type**.
4. Set the **Server IP Address/Domain Name**, which is **113.88.112.220** in this example.
5. Set the **User Name** and **Password**, which are both **admin1** in this example.
6. Click **Save**.



---End

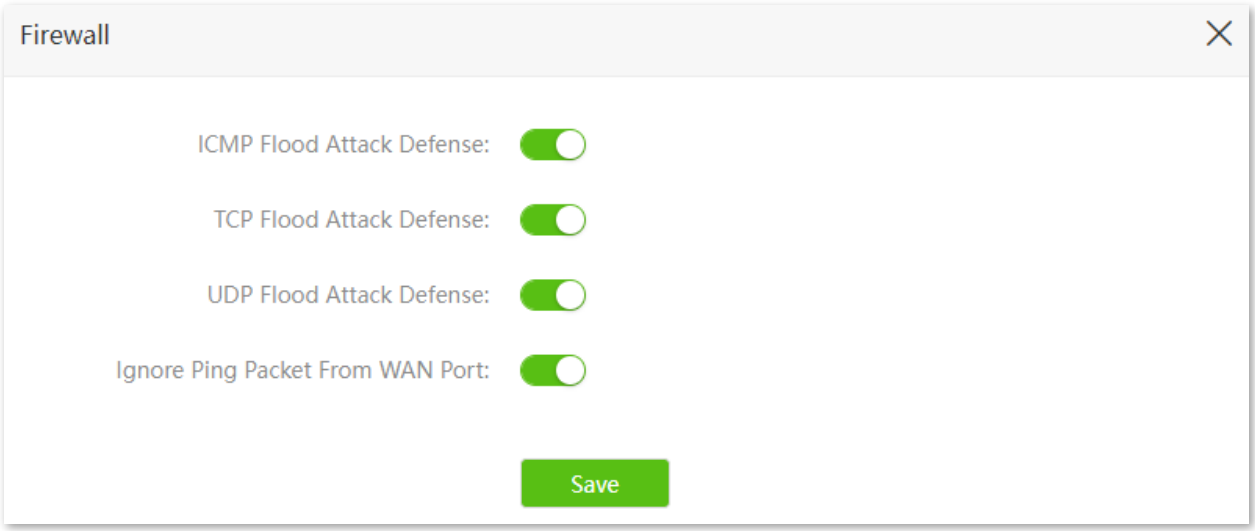
When **Connected** is shown in **Status**, you can access the VPN resources of your ISP.

13 Security

13.1 Firewall

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

To access the page, log in to the web UI of the router, and navigate to **Security** > **Firewall**.



Parameter description

Parameter	Description
ICMP Flood Attack Defense	Used to enable or disable the ICMP flood attack defense. 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 Defense	Used to enable or disable the TCP flood attack defense. 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.

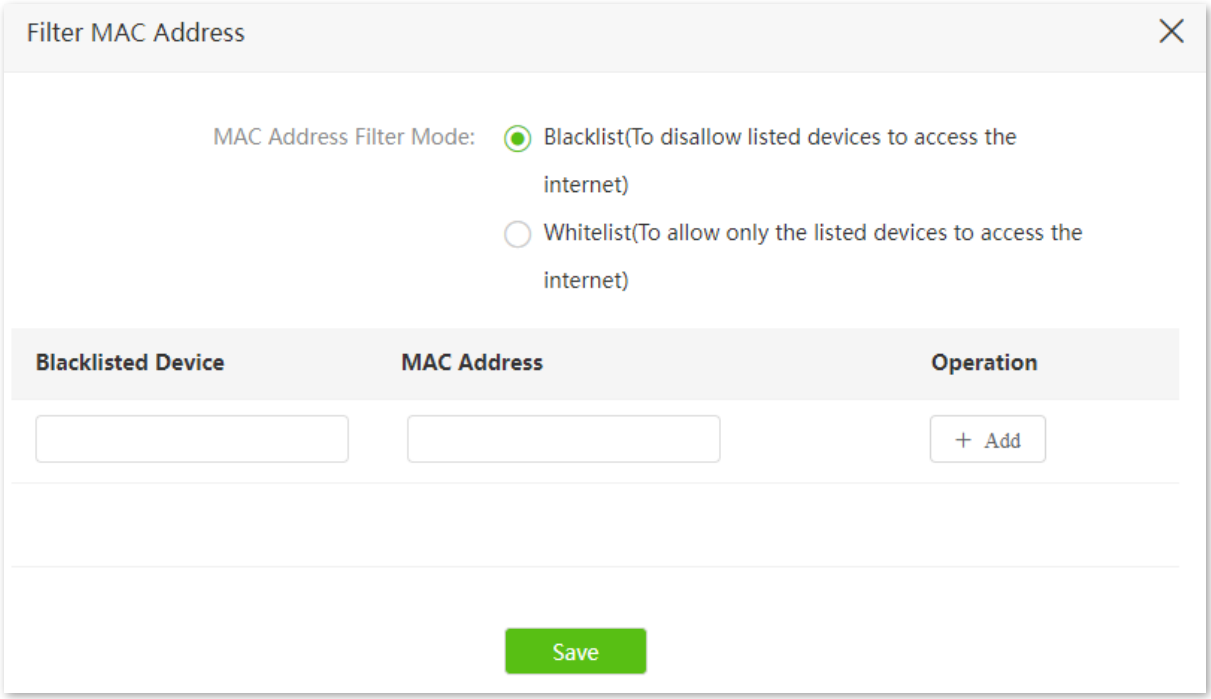
Parameter	Description
UDP Flood Attack Defense	Used to enable or disable the UDP flood attack defense. The UDP flood attack is implemented in a similar way with ICMP flood attack, during which the attacker sends many UDP packets to the target host, causing the target host to be busy processing these UDP packets, but unable to process normal packet requests or responses.
Ignore Ping Packet From WAN Port	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 prevent itself from being exposed, while preventing external ping attacks.

13.2 Filter MAC address

13.2.1 Overview

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

To access the page, log in to the web UI of the router, and navigate to **Security** > **Filter MAC Address**.



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	+ 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.

13.2.2 Only allow specified device to access the internet

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

Requirement: Only allow certain wireless devices of family members to access the internet using the Wi-Fi.

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

Assume that:

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

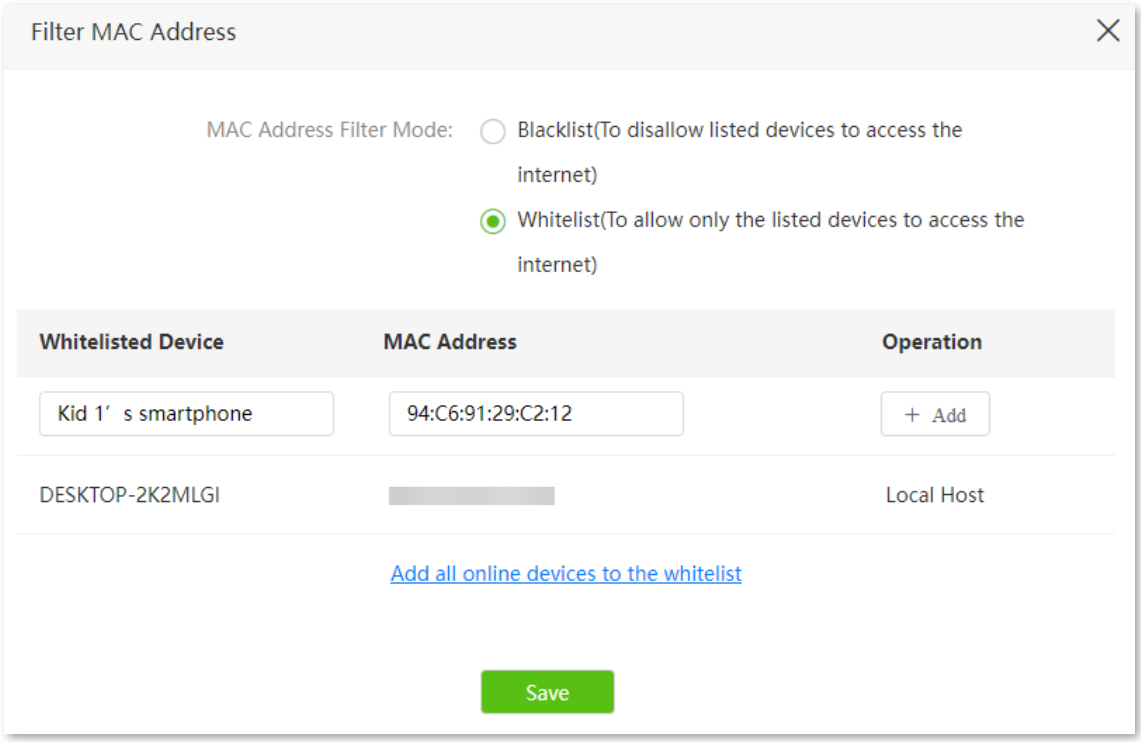
Procedure:

1. Log in to the web UI of the router.
2. Navigate to **Security** > **Filter MAC Address**.
3. Set the **MAC Address Filter Mode** to **Whitelist**.

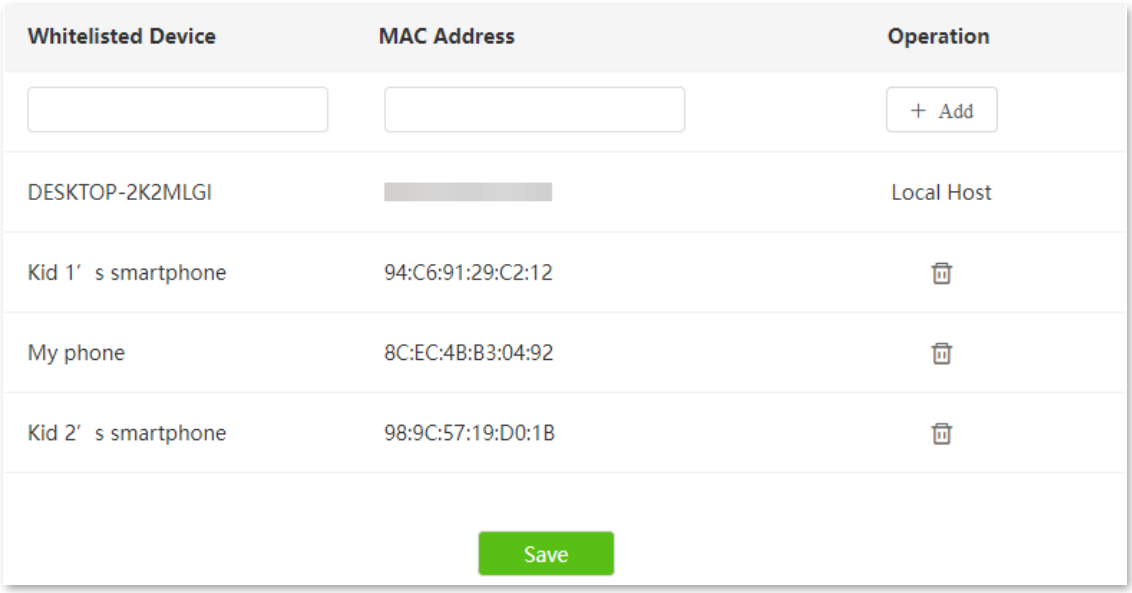
4. (Optional) Enter the device name in the **Whitelist Device** field, which is **Kid 1's smartphone** in this example.
5. Enter the **MAC Address** of the device, which is **94:C6:91:29:C2:12** in this example.
6. Click **+Add**.

TIP

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.



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



---End

After the configuration is completed, only the three wireless devices added can access the internet through the Wi-Fi of the router.

13.2.3 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.

Requirement: Disallow the certain device of family member to access the internet.

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

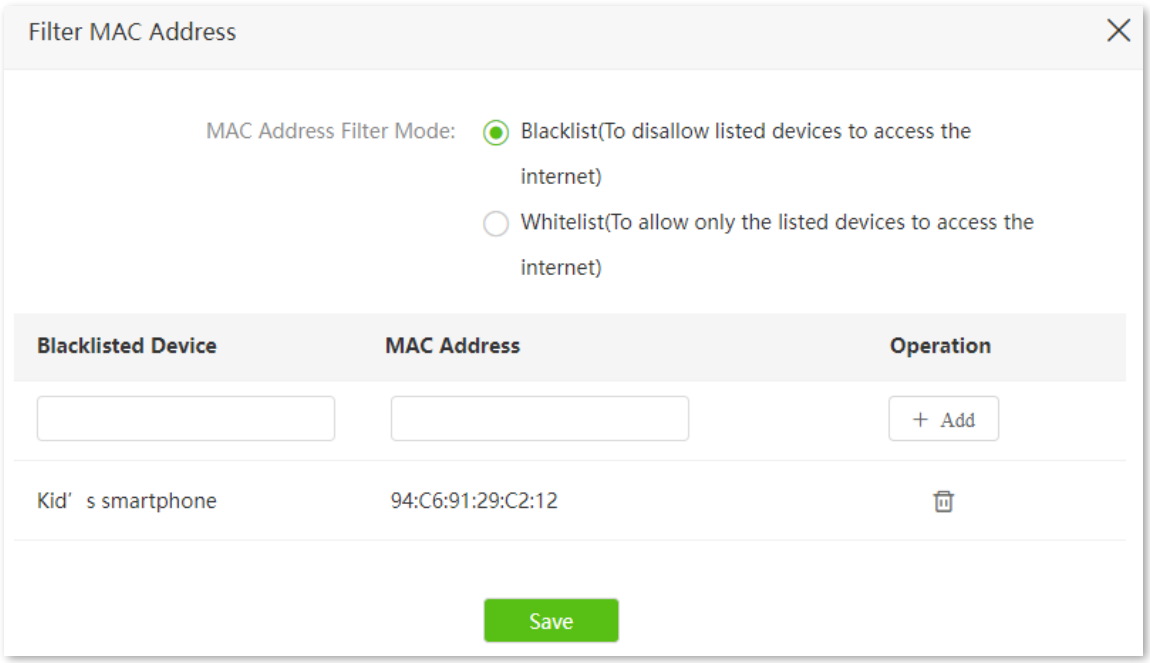
Assume that:

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

Procedure:

1. Log in to the web UI of the router.
2. Navigate to **Security** > **Filter MAC Address**.
3. Set the **MAC Address Filter Mode** to **Blacklist**.
4. (Optional) Enter the device name in the **Blacklisted Device** field, which is **Kid's smartphone** in this example.

5. Enter the **MAC Address** of the device, which is **94:C6:91:29:C2:12** in this example.
6. Click **+Add**.
7. Click **Save**.



---End

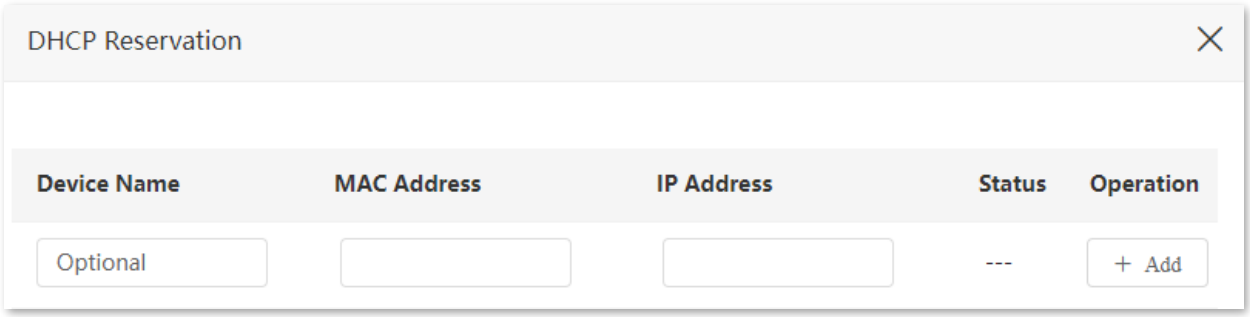
After the configuration is completed, the device added cannot access the internet through the router.

13.3 DHCP reservation

13.3.1 Overview

With 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 access the page, log in to the web UI of the router, and navigate to **Security** > **DHCP Reservation**.



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	Available operations include: + Add : It is used to add a new DHCP reservation rule. : It is used to bind the MAC address to the reserved IP address. : It is used to unbind the MAC address from the reserved IP address. : It is used to delete the DHCP reservation rule.

13.3.2 Assign static IP addresses to LAN clients

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

Requirement: 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.

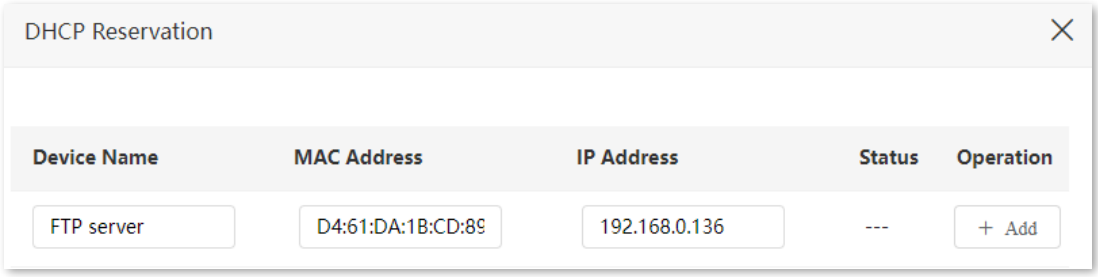
Assume that the information of the FTP server includes:

- 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:

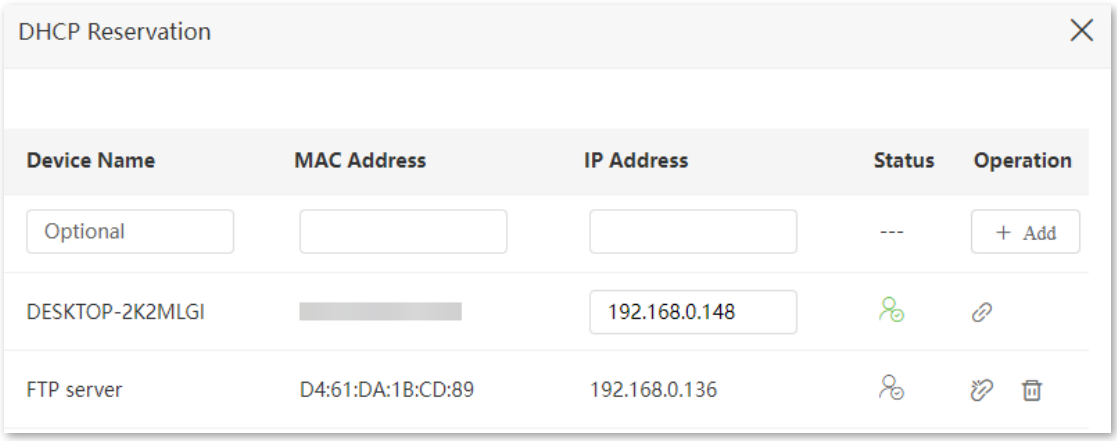
1. Log in to the web UI of the router.

2. Navigate to **Security** > **DHCP Reservation**.
3. (Optional) Set the **Device Name** for the host, which is **FTP server** in this example.
4. Set the **MAC Address** of the host, which is **D4:61:DA:1B:CD:89** in this example.
5. Set the **IP Address** reserved for the host, which is **192.168.0.136** in this example.
6. Click **+Add**.



---End

After 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.



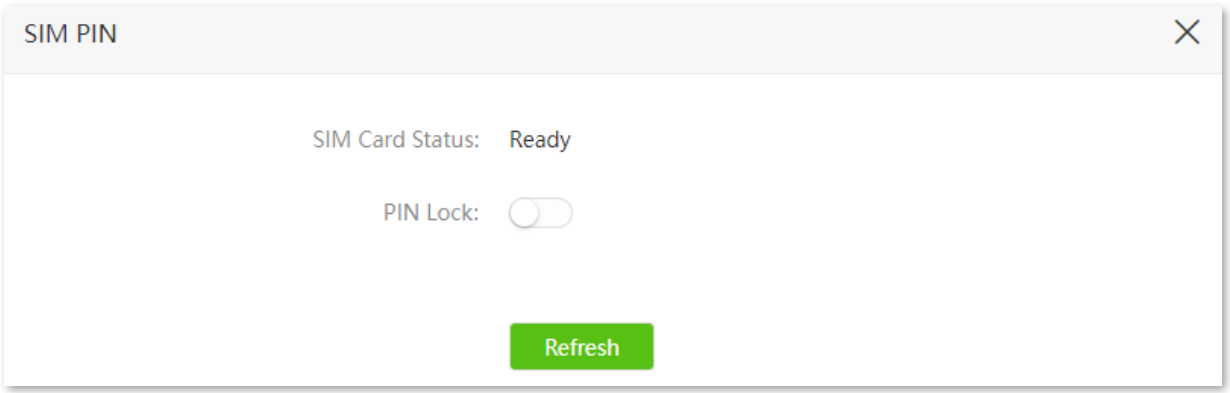
14 Advanced settings

14.1 SIM PIN

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 and specify a PIN code for an unlocked SIM card.

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

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



14.1.1 Unlock the SIM card

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

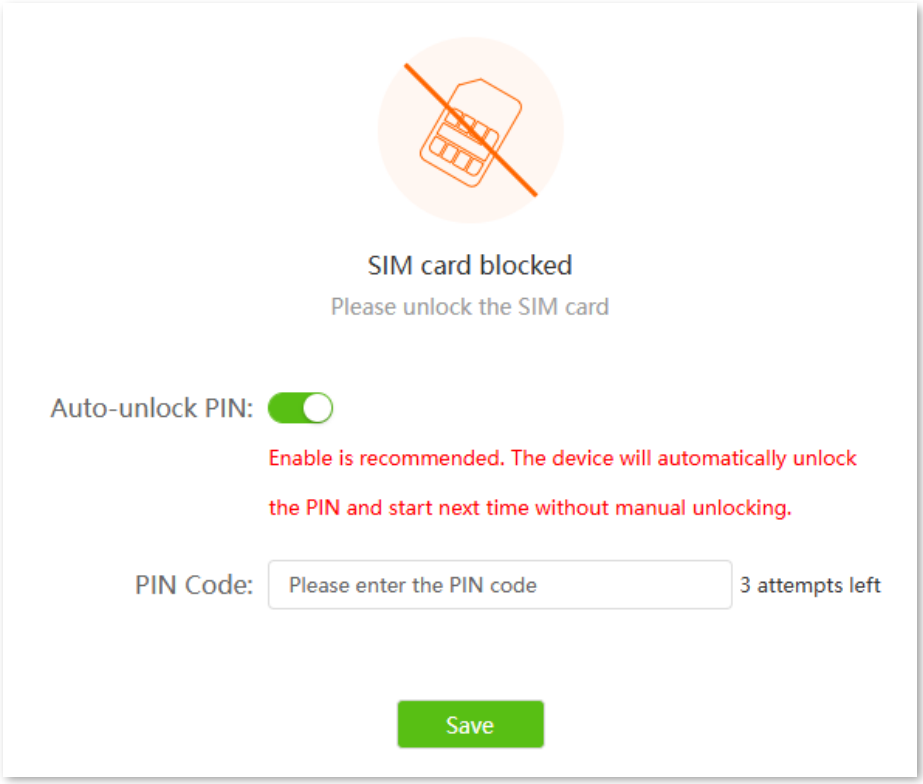
Unlock the SIM card in the quick setup wizard

Assume that you are required to unlock the SIM card in the quick setup wizard, the PIN code is needed.

Procedure:

1. Log in to the web UI of the router.
2. Click **Start**.

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



NOTE

- It is recommended to enable the Auto-unlock PIN function.
- Contact your ISP for the original PIN code.
- You can try the PIN code for only 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 will be locked permanently after you enter the wrong PUK code for 10 times.

4. Perform operations as prompted to complete the setup process.

---End

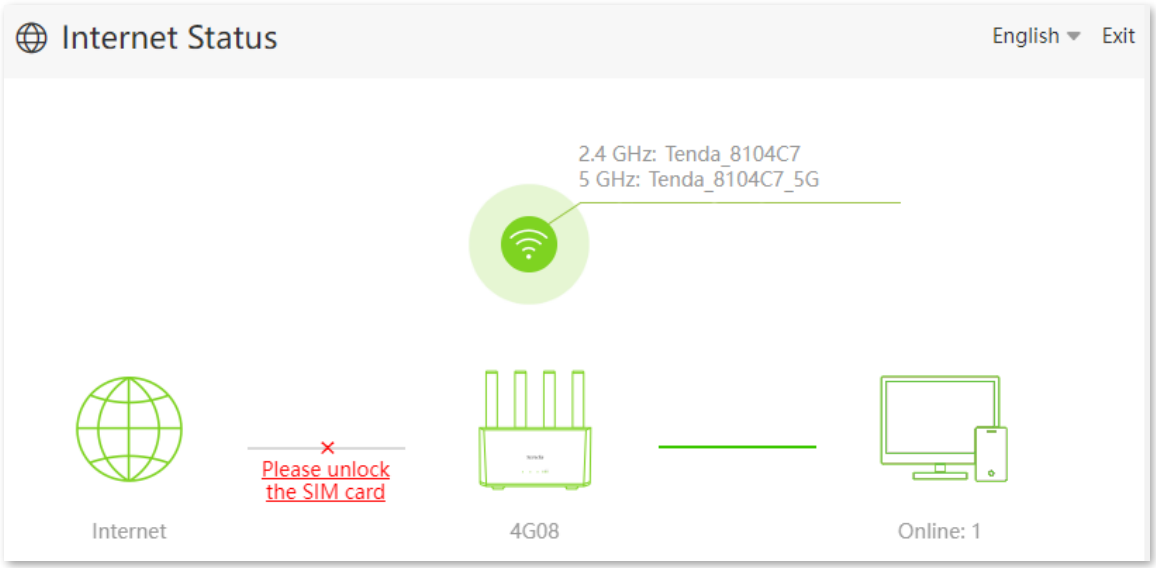
After the configuration is completed, you can log in to the web UI of the router to view and complete other configurations.

Unlock the SIM card on the web UI

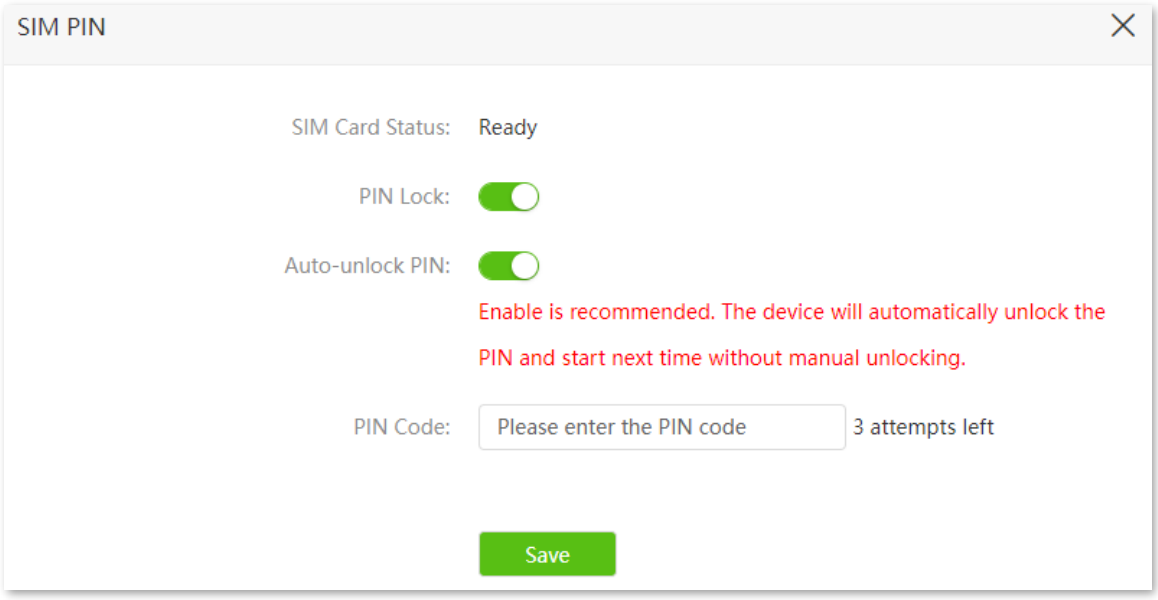
When "Please unlock the SIM card" is shown between the internet and the router, it indicates that you need to enter the PIN code. Click Please unlock the SIM card to navigate to the **SIM PIN** page and configure the related parameters.

Procedure:

1. Log in to the web UI of the router.
2. Click Please unlock the SIM card, or navigate to **Advanced Settings** > **SIM PIN**.



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



NOTE

- It is recommended to enable the Auto-unlock PIN function.
- Contact your ISP for the original PIN code.
- You can try the PIN code for only 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 will be locked permanently after you enter the wrong PUK code for 10 times.

---End

After the configuration is completed, you can access the internet normally.

14.1.2 Disable PIN lock for the SIM card

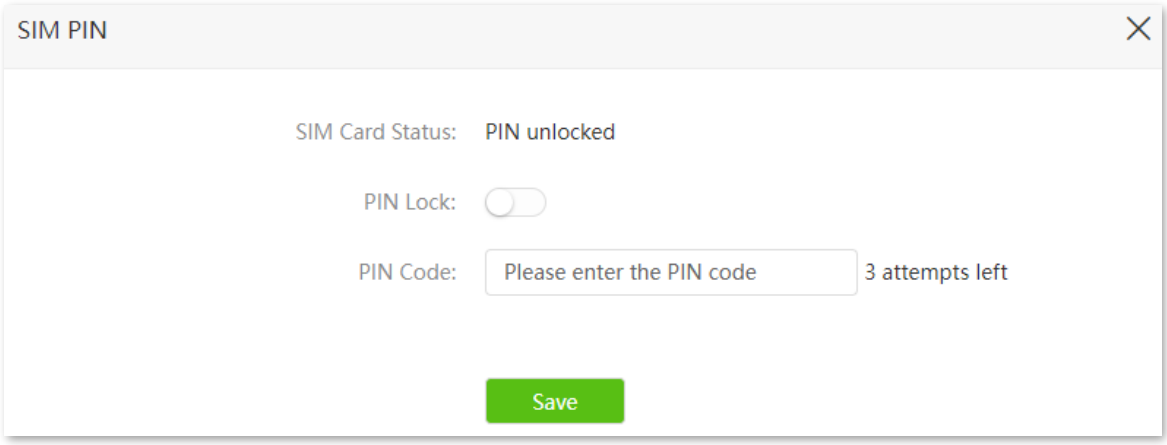
After PIN lock is disabled for the SIM card, your SIM card will not be protected by PIN lock.

NOTE

- Contact your ISP for the original PIN code.
- You can try the PIN code for only 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 will be locked permanently after you enter the wrong PUK code for 10 times.

Procedure:

1. Log in to the web UI of the router.
2. Navigate to **Advanced Settings** > **SIM PIN**.
3. Disable **PIN Lock**, enter the original **PIN Code**, and click **Save**.



---End

After the configuration is completed, the PIN lock function is disabled and the SIM card is not protected by PIN lock.

14.1.3 Enable PIN lock for the SIM card

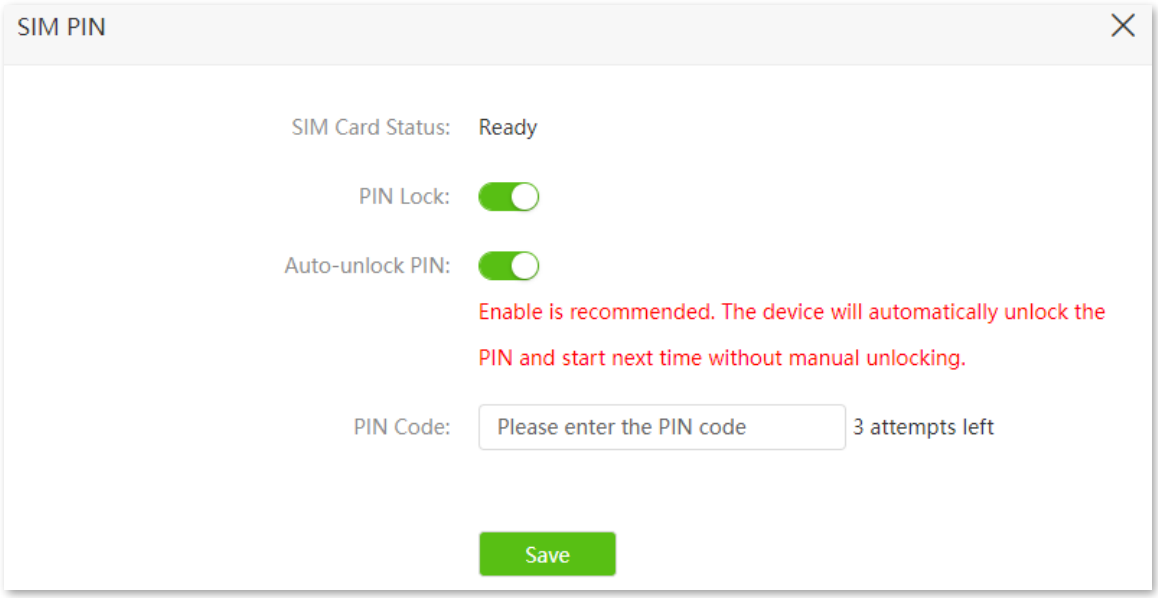
You can enable a PIN lock for a SIM card. SIM PIN is a protective measure to prevent your SIM card from misuse.

NOTE

- It is recommended to enable the Auto-unlock PIN function.
- Contact your ISP for the original PIN code.
- You can try the PIN code for only 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 will be locked permanently after you enter the wrong PUK code for 10 times.

Procedure:

1. Log in to the web UI of the router.
2. Enable **PIN Lock**.
3. Specify a **PIN Code**, and click **Save**.

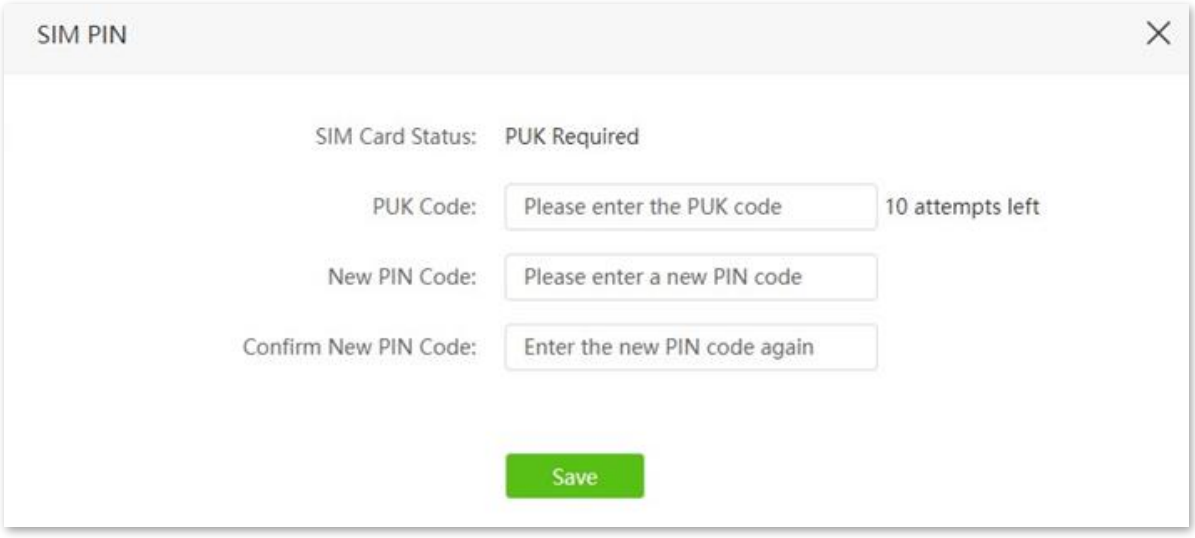


---End

After the configuration is completed, the SIM card is protected by PIN lock.

14.1.4 Use PUK code to set 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 you can set a new PIN code for the SIM card.

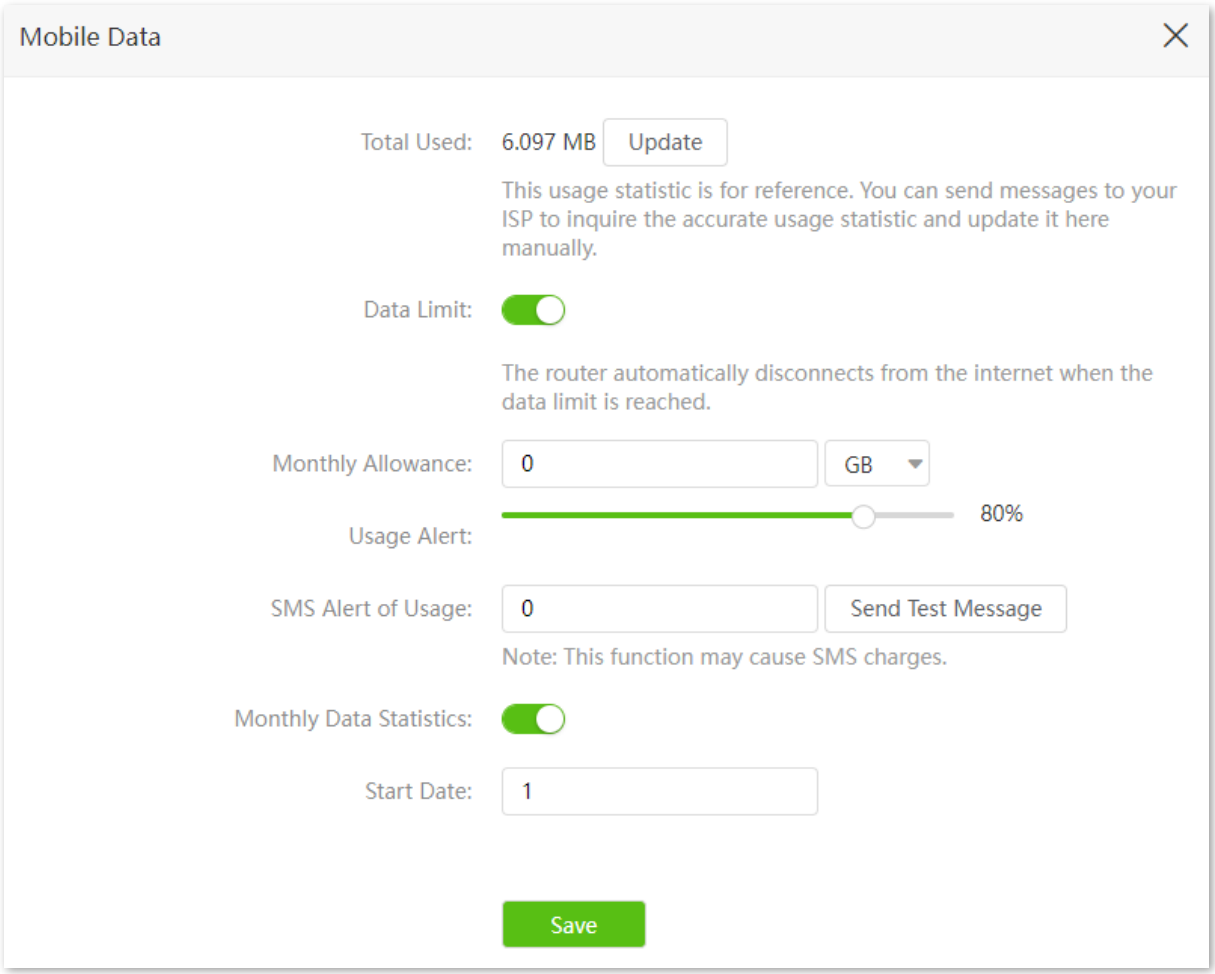


14.2 Mobile data

14.2.1 Overview

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

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



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**.

Parameter	Description
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.
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 data 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.

14.2.2 Example of configuring mobile data function

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

Requirement: 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.

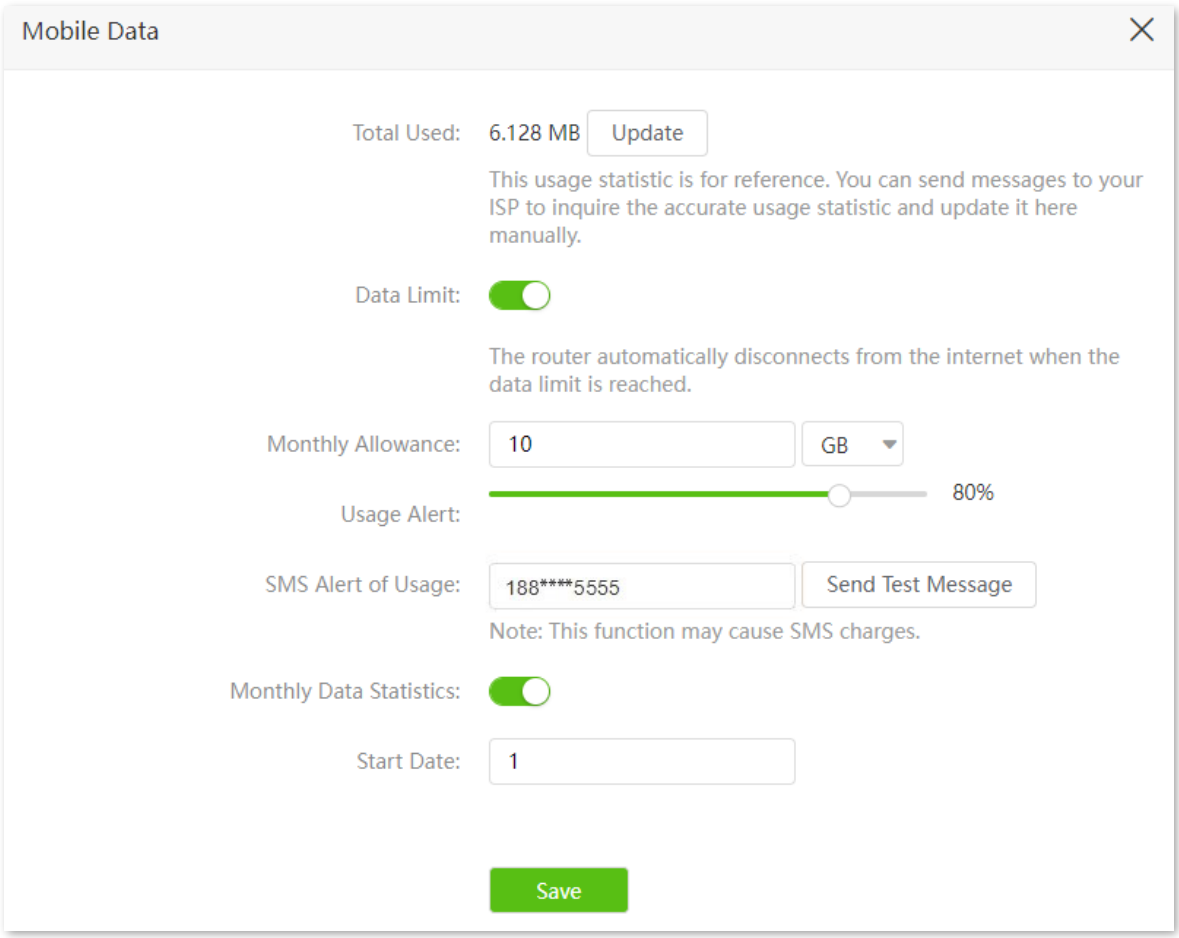
Assume that:

- Available data traffic: 10 GB
- Start date of data usage record: 1st each month
- Smartphone number: 188****5555
- Alert percentage: 80%

Procedure:

1. Log in to the web UI of the router.
2. Navigate to **Advanced Settings** > **Mobile Data**.
3. (Optional) Click **Update** to update the current usage data in **Total Used**.
4. Enable **Data Limit**.
5. Set **Monthly Allowance** to **10**, and choose **GB** in the drop-down box.

6. Set **Usage Alert** to **80%**.
7. Set **SMS Alert of Usage** to **188****5555**.
8. Enable **Monthly Data Statistics**.
9. Set **Start Date** to **1**, and click **Save**.



---End

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

TIP

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

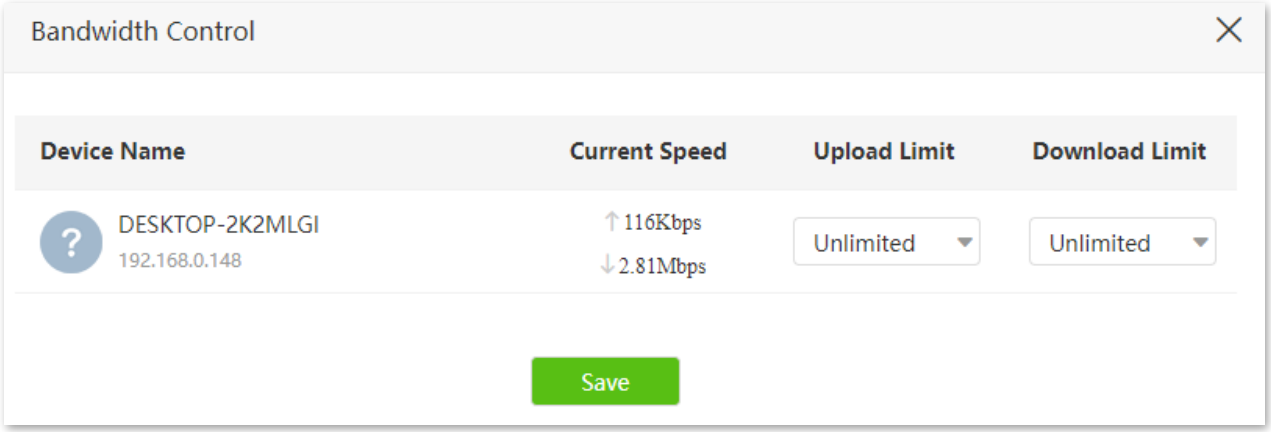
- Change the **Total Usage** by clicking **Update**.
- Disable **Data Limit**.
- Navigate to **Internet Settings**, and click **Connect** at the bottom of the page.

14.3 Bandwidth control

14.3.1 Overview

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

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



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	

14.3.2 Set the upload and download speed limit for users

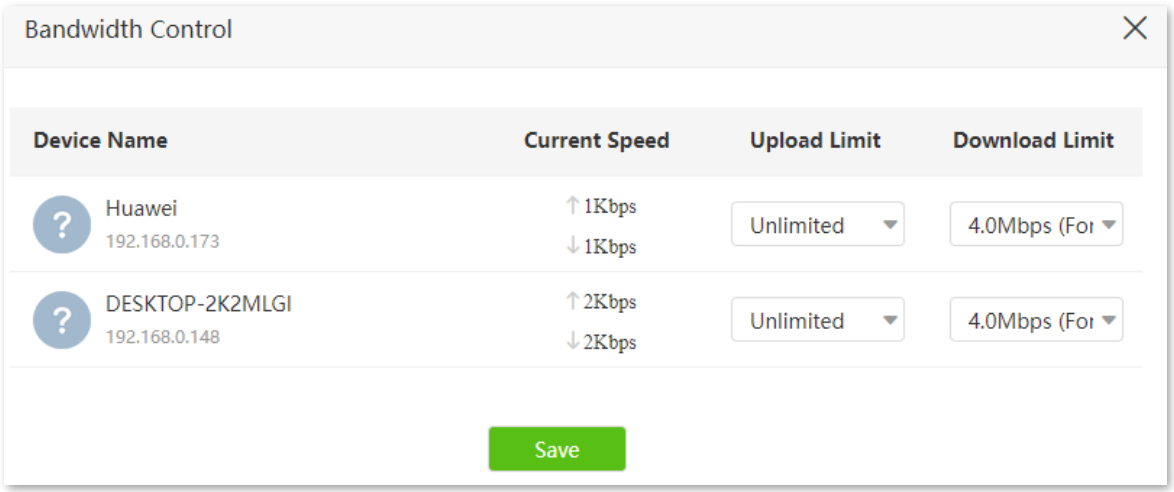
Scenario: You want to allocate bandwidth equally among connected and enable all connected devices to enjoy smooth 720p videos.

Solution: Configure the bandwidth control function to reach the requirements.

Procedure:

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

2. Navigate to **Advanced Settings** > **Bandwidth Control**.
3. Locate the devices to be controlled, and set the **Download Limit** to **4.0Mbps (For HD Video).**
4. Click **Save**.



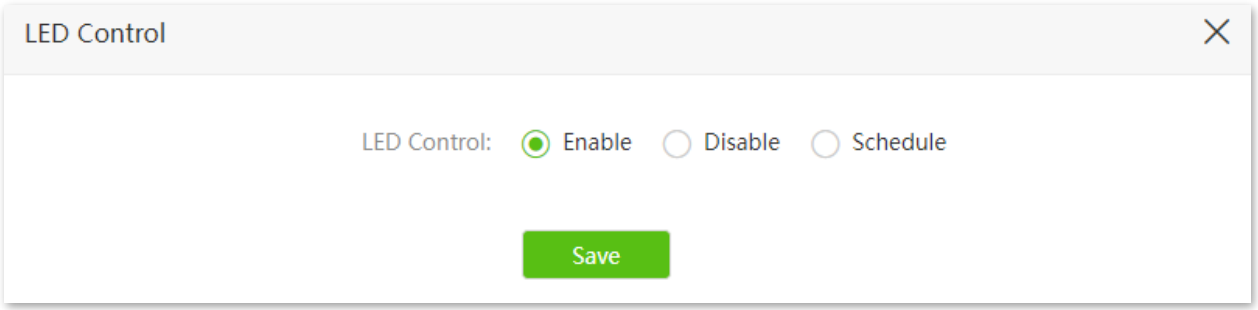
---End

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

14.4 LED control

To access the page, log in to the web UI of the router and navigate to **Advanced Settings** > **LED Control**.

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



Parameter description

Parameter	Description
Enable	All indicators stay in their normal status.

Parameter	Description
Disable	All indicators are turned off.
Schedule	Indicators are only turned off during the specified period.
Turn Off During	Specifies the period during which the indicators are turned off. Outside this period, all indicators work normally. It is available only when **Schedule** is selected.

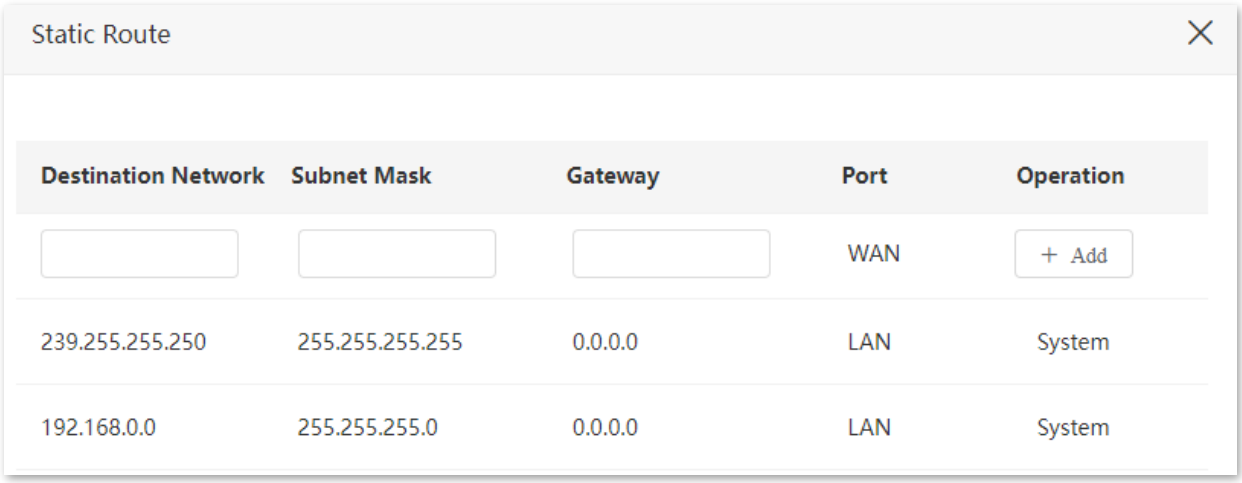
14.5 Static route

14.5.1 Overview

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

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

To access the page, log in to the web UI of the router and navigate to **Advanced Settings** > **Static Route**.



Parameter description

Parameter	Description
Destination Network	Specifies the IP address of the destination network. When the **Destination Network** and **Subnet Mask** are both 0.0.0.0, it indicates that this is the default route. TIP When the route of packets cannot be found in the routing table, the router will forward the packets using the default route.
Subnet Mask	Specifies the subnet mask of the destination network.
Gateway	Specifies the ingress IP address of the next hop route after the data packet exits from the interface of the router. 0.0.0.0 indicates that the destination network is directly connected to the router.
Port	Specifies the interface that the packet exits from.
Operation	+ Add : Used to add a static route rule. : Used to delete a static route rule.

14.5.2 Add a static route rule

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

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

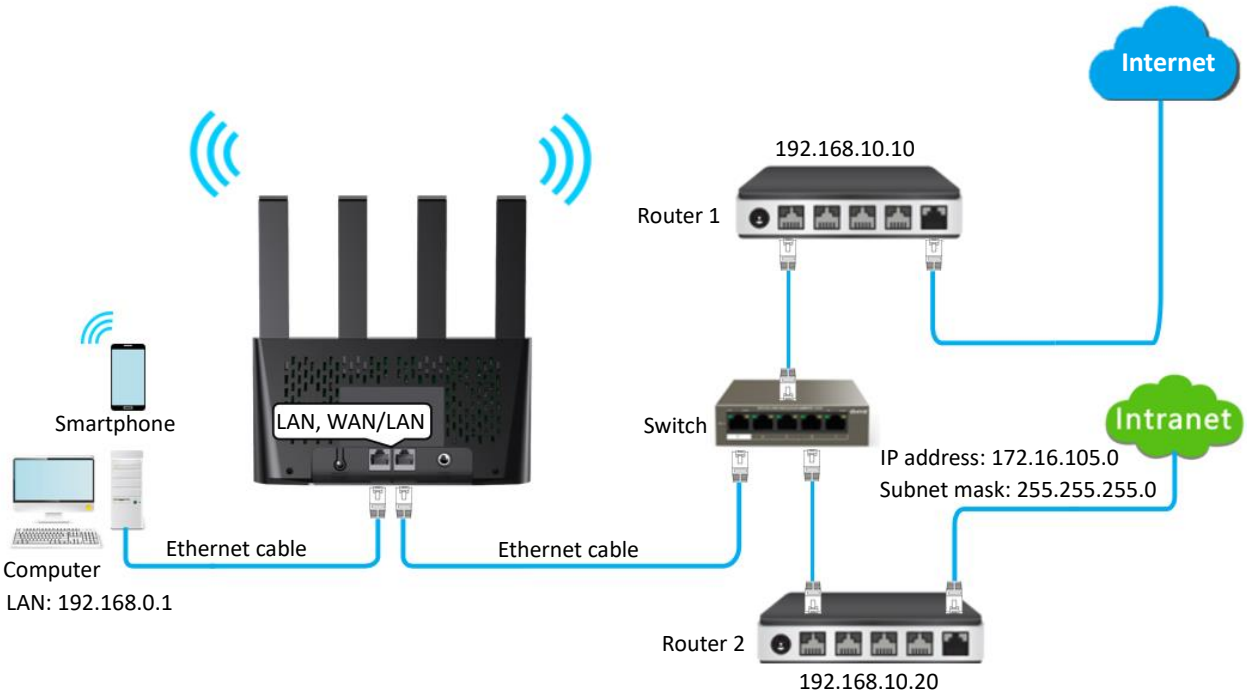
Solution: You can configure the static route function to reach the requirements.

Assume the LAN IP addresses of these devices are:

- Router: 192.168.0.1
- Router1: 192.168.10.10
- Router2: 192.168.10.20

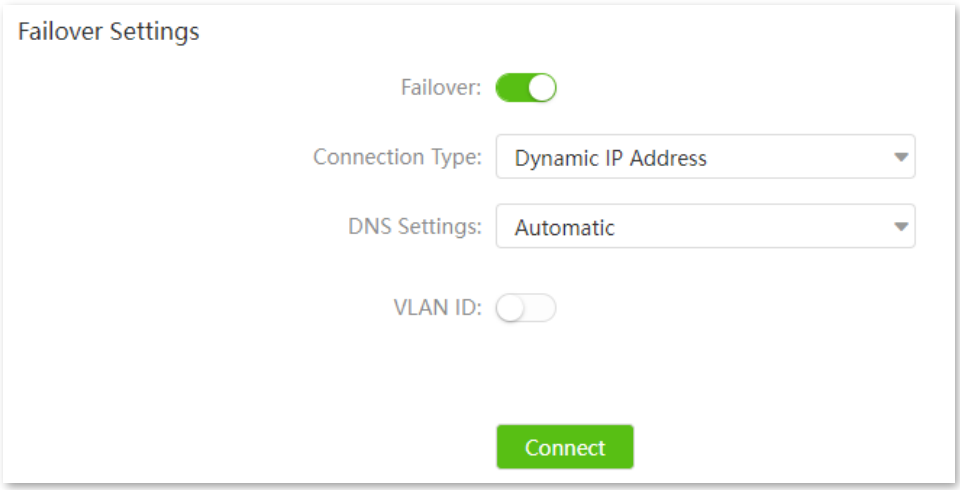
The information about the intranet:

- IP address: 172.16.105.0
- Subnet mask: 255.255.255.0



Procedure:

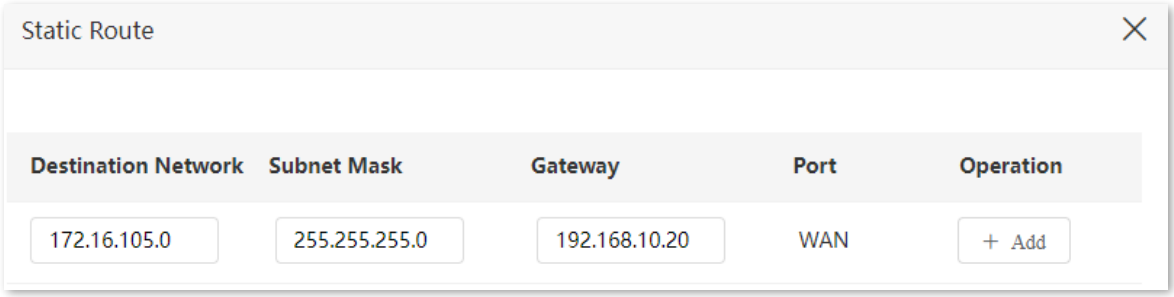
1. Log in to the web UI of the router.
2. Configure the router to access the internet in **Internet Settings**. For details, refer to Access the internet through dynamic IP address.



3. Add a static route rule.
   1) Navigate to **Advanced Settings** > **Static Route**.
   2) Enter the IP address of the destination network, which is **172.16.105.0** in this example.
   3) Enter the subnet mask of the destination network, which is **255.255.255.0** in this example.

4) Enter the ingress IP address of the next hop route, which is **192.168.10.20** in this example.

5) Click **+Add**.



---End

When the configuration is completed, you can access both the internet and intranet through the router at the same time.

15 System settings

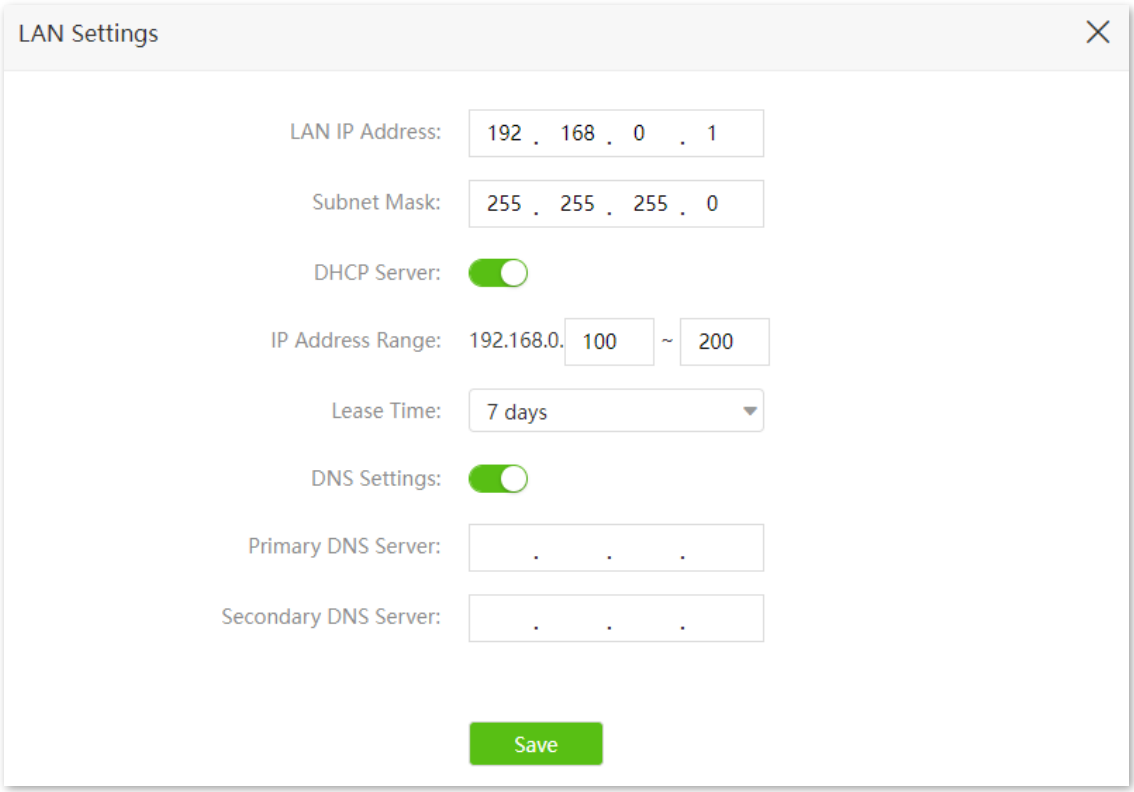
15.1 LAN settings

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

On this page, you can:

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

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



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, which is 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. 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. TIP It is available only when **DHCP Server** is enabled.
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 again 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. TIP 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. TIP - It is available only when **DHCP Server** is enabled. - This router has the DNS proxy function.
Primary DNS Server	Specifies the primary DNS address of the router, which is assigned to the clients. You can change it if necessary. Make sure that the primary DNS server is the IP address of the correct DNS server or DNS proxy. Otherwise, you may fail to access the internet. TIP It is available only when **DNS Settings** is enabled.

Parameter	Description
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 by default. TIP It is available only when **DNS Settings** is enabled.

15.2 Time settings

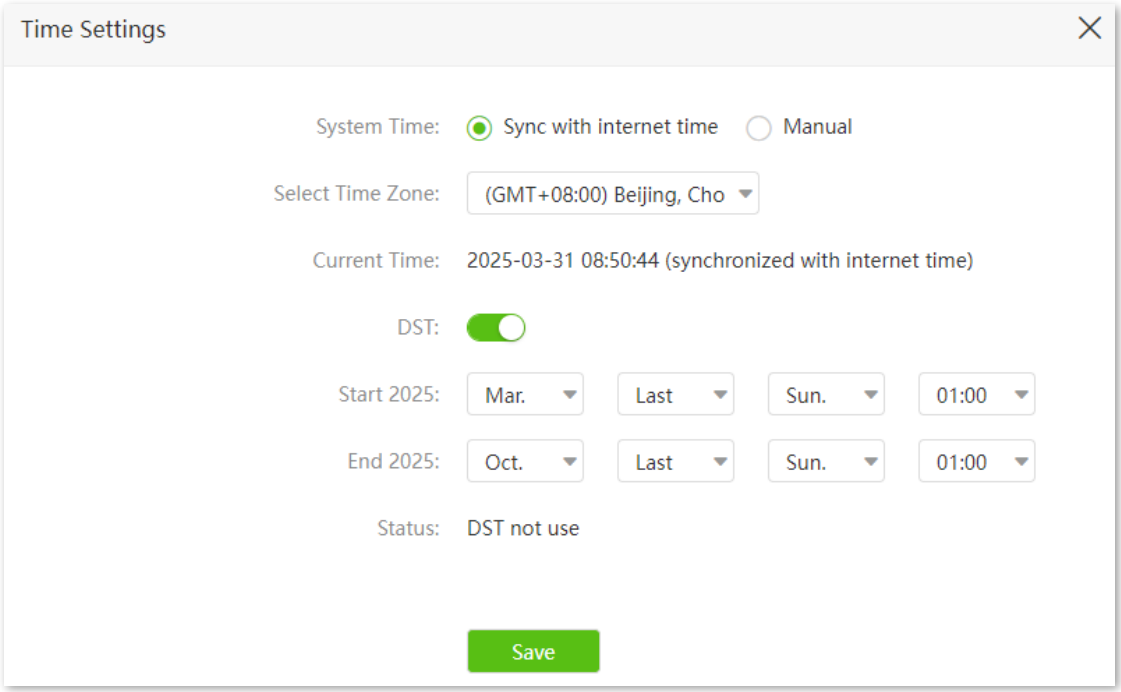
To access the page, log in to the web UI of the router, and navigate to **System Settings** > **Time Settings.**

You can change the time settings on this page. The time-based functions require 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.

15.2.1 Sync system time with the internet time

In 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.

After the configuration is completed, you can refresh the page to check whether the system time of the router is correct.



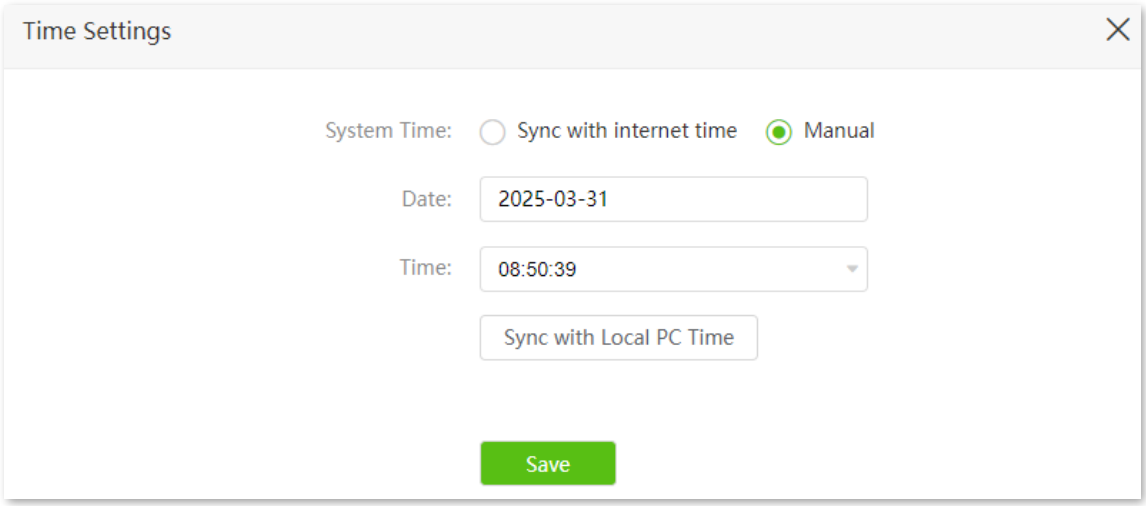
Parameter description

Parameter	Description
System Time	Used to set the system time of the router, which can be synchronized with the internet or set manually.
Select Time Zone	Specifies the time zone used for the system time. Select one option as required. It is available only when **Sync with internet time** is selected for **System Time**.
Current Time	Specifies the current system time. It is available only when **Sync with internet time** is selected for **System Time**.
DST	Used to enable or disable the Daylight Saving Time (DST) function. It is disabled by default.
Start 2024	Specifies the start time of DST. It is available only when DST is enabled.
End 2024	Specifies the end time of DST. It is available only when DST is enabled.
Status	Specifies whether the DST is used. It is available only when DST is enabled.

15.2.2 Set the time manually

When the system time is set to **Manual**, you can set 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.

After the configuration is completed, you can refresh the page to check whether the system time of the router is correct.



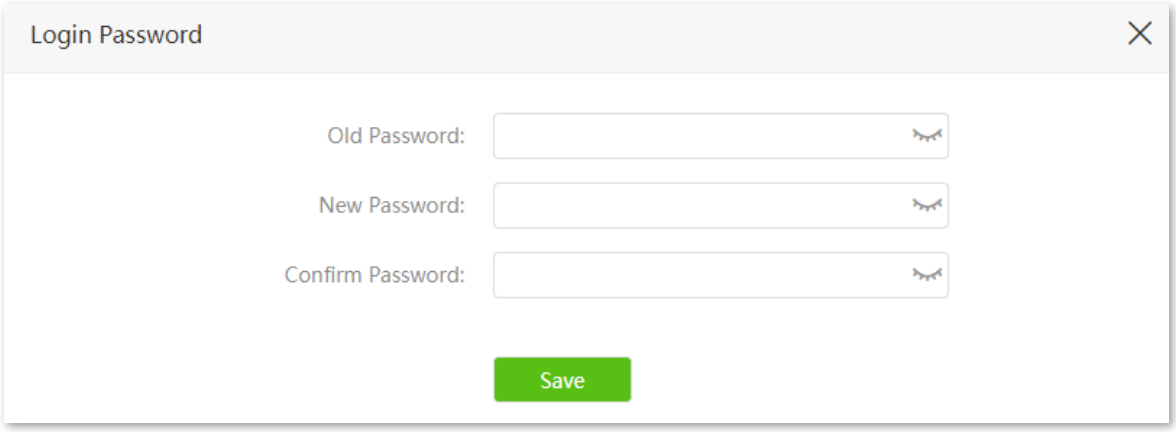
15.3 Login password

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 access the page, log in to the web UI of the router, and navigate to **System Settings** > **Login Password**.

TIP

- If you did not set a password before, you can set a login password on this page.
- If you have already set a login password, you can change the password on this page and the original password is required.



15.4 Reboot and reset

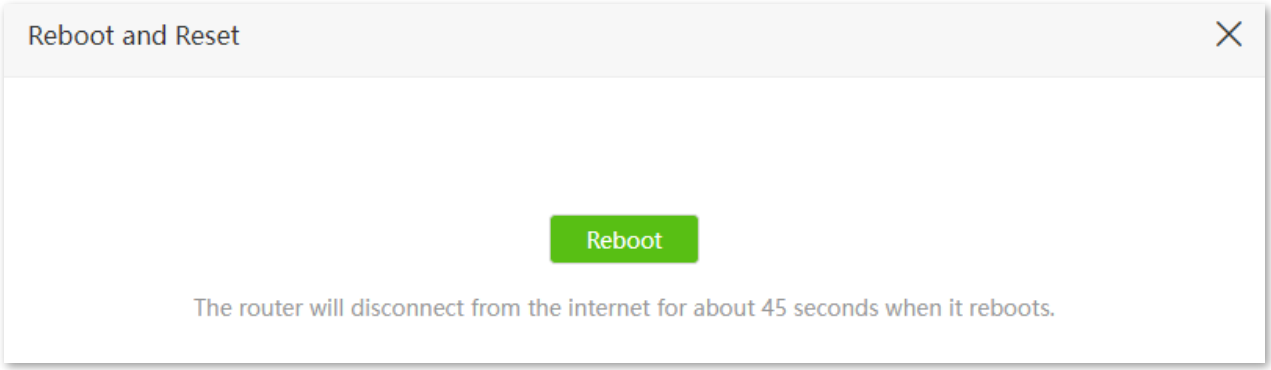
15.4.1 Reboot the router

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

TIP

Rebooting the router will disconnect all connections to the router. Reboot the router during leisure times.

To access the page, log in to the web UI of the router, navigate to **System Settings** > **Reboot and Reset**, and click **Reboot**.



Wait for a moment until the ongoing process finishes.

15.4.2 Reset the router

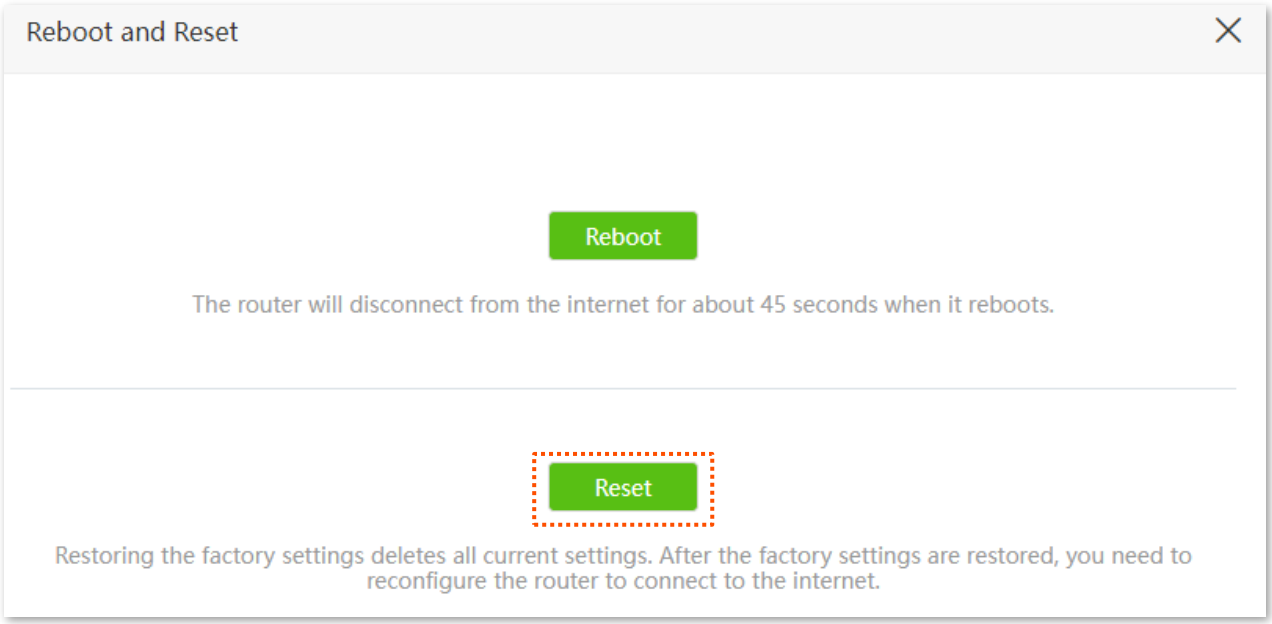
If you are uncertain about why the internet is inaccessible through the router or you forget the login password of the router, you can reset the router.

NOTE

- Resetting the router will clear all configurations and restores the router to factory settings. You need to reconfigure the router after it is reset. You are recommended to back up the configuration before restoring the factory settings.
- Ensure that the power supply of the router is normal when the router is reset. Otherwise the router could be damaged.
- After the router is restored to factory settings, the default login IP address of the router is **192.168.0.1**.

Reset the router on the web UI

To access the page, log in to the web UI of the router, navigate to **System Settings** > **Reboot and Reset**, and click **Reset**.



Wait for a moment until the ongoing process finishes.

Reset the router using the reset button

Hold down the **MESH/RST** button for about 8 seconds, and release it when all indicators light off and then light up. The router will be reset successfully in about two minutes.

15.5 Firmware upgrade

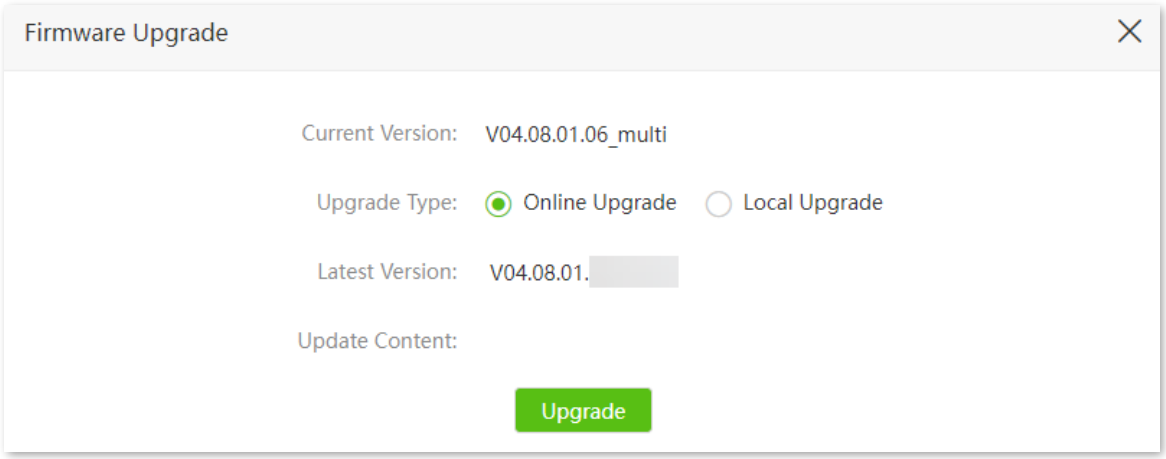
This function enables the router to obtain the latest functions and more stable performance. The router supports online firmware upgrade and local firmware upgrade.

15.5.1 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:

1. Log in to the web UI of the router.
2. Navigate to **System Settings** > **Firmware Upgrade**.
3. Wait until a new firmware version is detected. The following figure is for reference only.



4. Click **Upgrade**.

---End

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.

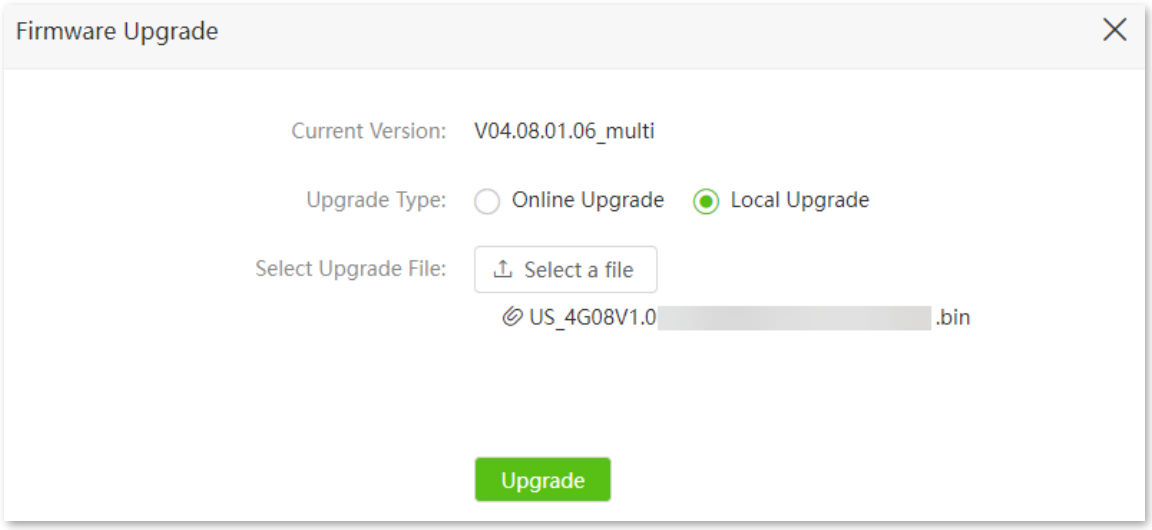
15.5.2 Local upgrade

NOTE

To prevent the router from being damaged:

- Ensure that the firmware is applicable to the router. Generally, the firmware upgrade file suffixed with **.bin**.
- 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.

1. Go to www.tendacn.com. Download an applicable firmware of the router to your local computer and unzip it.
2. Log in to the web UI of the router.
3. Navigate to **System Settings** > **Firmware Upgrade.**
4. Choose **Local Upgrade**.
5. Click **Select a file**. Select and upload the firmware that has been downloaded to your computer in step 1, and click **Upgrade**.



---End

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.

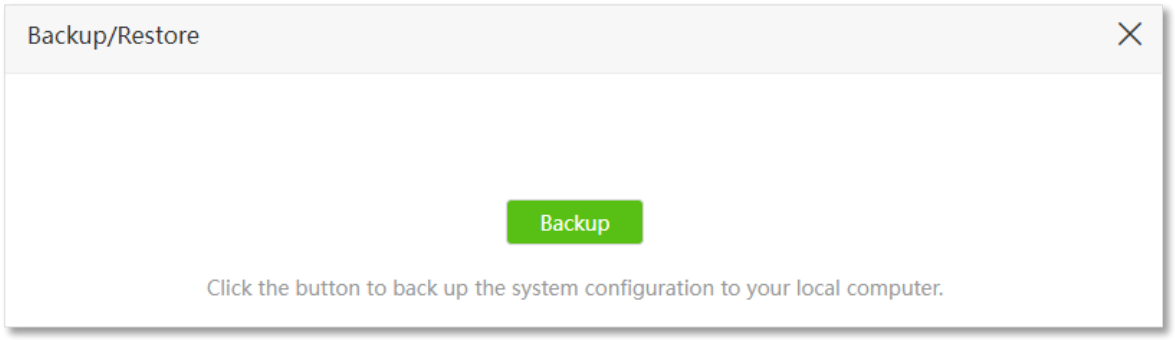
15.6 Backup & Restore

On this page, 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 the Backup function to restore the configurations that have been backed up.

15.6.1 Backup the configurations of the router

1. Log in to the web UI of the router.
2. Navigate to **System Settings** > **Backup/Restore.**
3. Click **Backup**.

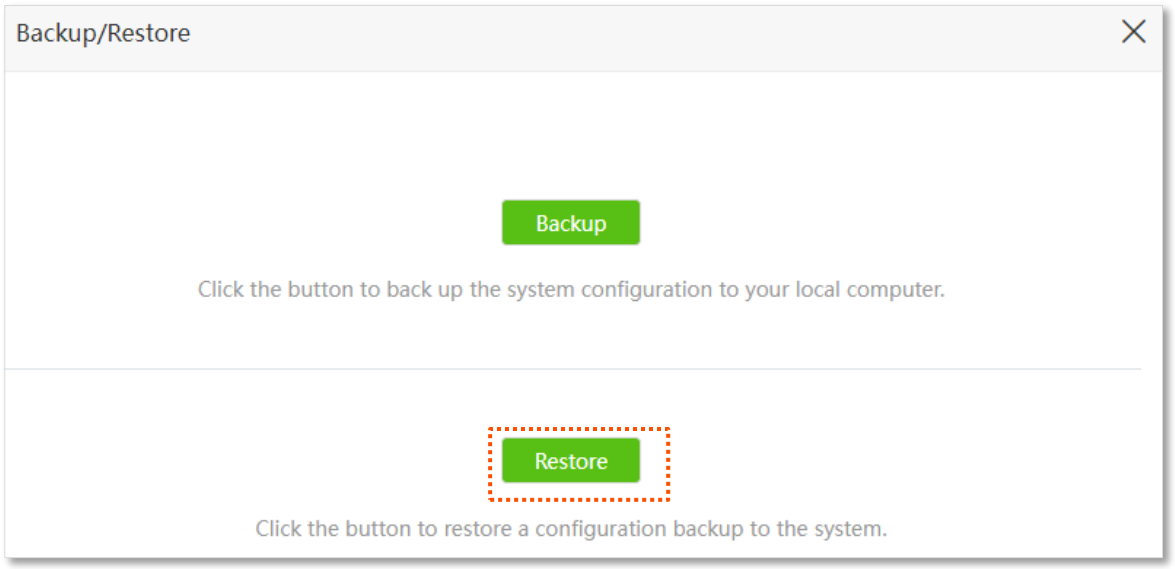


---End

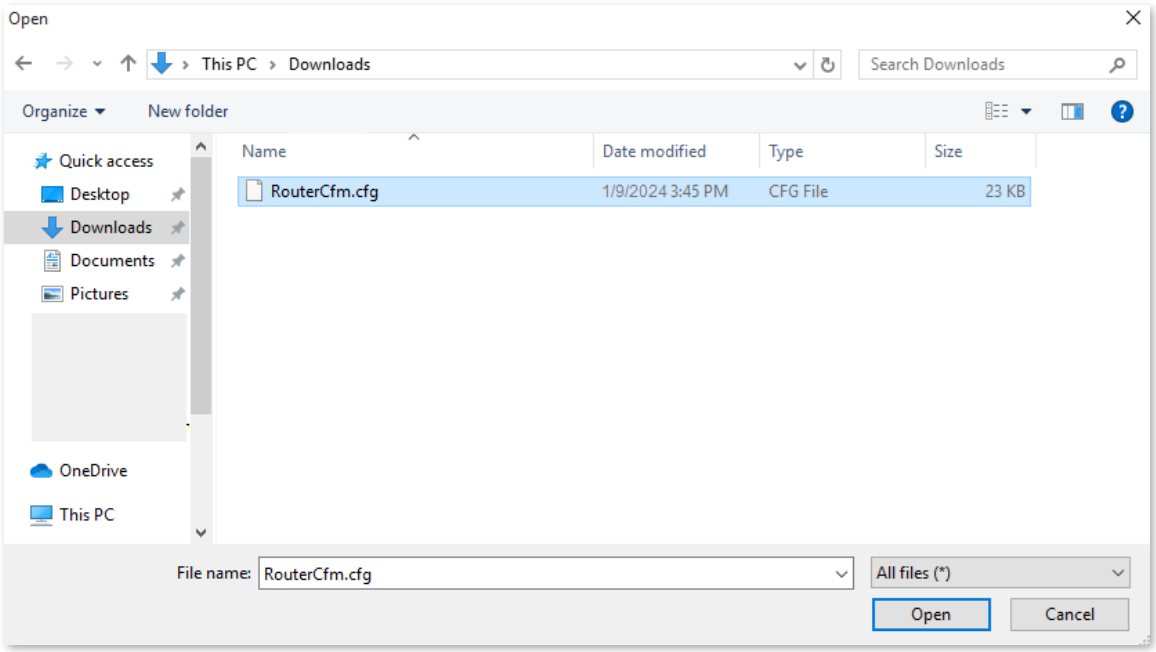
A file named **RouterCfm.cfg** will be downloaded to your local host.

15.6.2 Restore previous configurations of the router

1. Log in to the web UI of the router.
2. Navigate to **System Settings** > **Backup/Restore.**
3. Click **Restore**.



4. Select the configuration file (suffixed with **.cfg**) to be restored, and click **Open**.



---End

Wait until the ongoing process finishes, and the router restores previous settings.

15.7 ISP update

On this page, you can update the ISP information to obtain the better user experience. When the compatibility problem of the ISP or the APN mismatch appears, you can try to use this function to solve the problem.

NOTE

To prevent the router from being damaged:

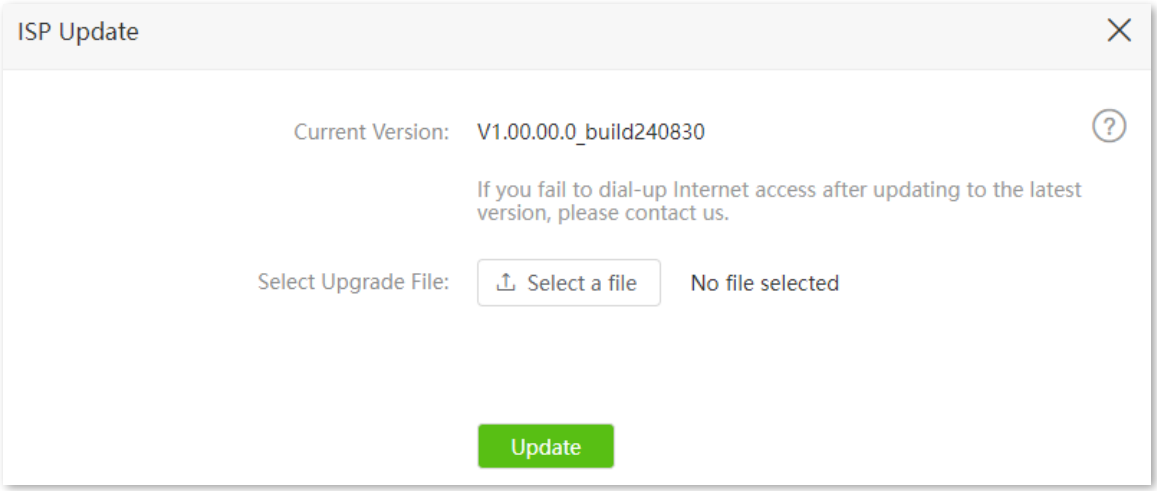
- Ensure that the update file is applicable to the router.
- When you are updating the ISP information, do not power off the router.

Procedure:

1. Log in to the web UI of the router.
2. Navigate to **System Settings** > **ISP Update.**
3. Click (?), and click **www.tendacn.com** on the **ISP Update Help** page. The following figure is for reference only.

   Download an applicable ISP update file to your local computer and unzip it.

4. Click **Select a file**. Select and upload the ISP update file that has been downloaded in step 3, and click **Update**.



---End

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 **Current Version** on the **ISP Update** page.

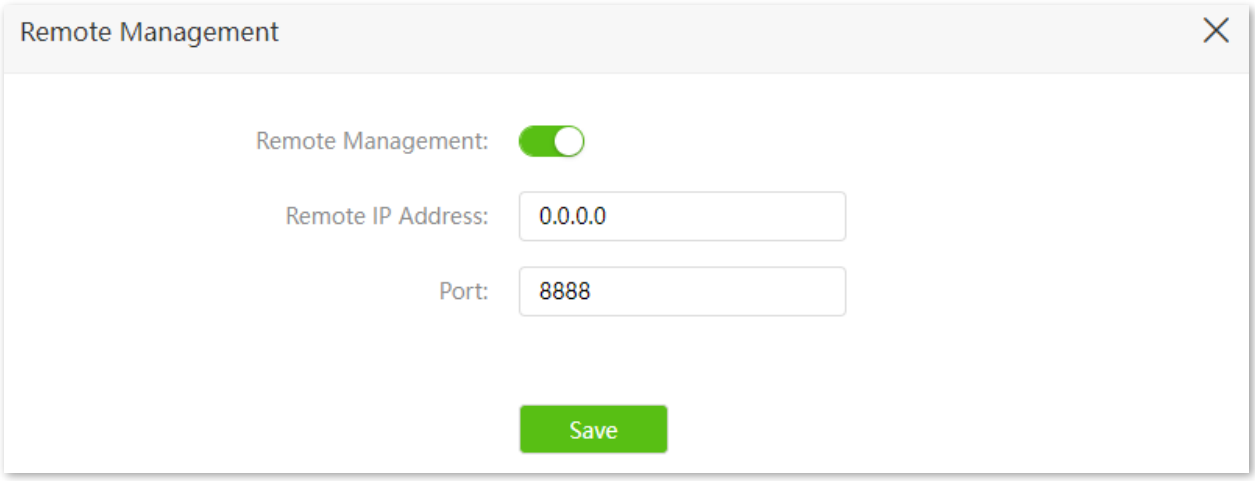
15.8 Remote management

15.8.1 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 access 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.



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. TIP - 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 confliction. - Remote management can be achieved by visiting “http://the WAN IP address of the router:port number”. If the DDNS host function is enabled, the web UI can also be accessed through “http://the domain name of the router’s WAN port:port number”.

15.8.2 Example of configuring remote management function

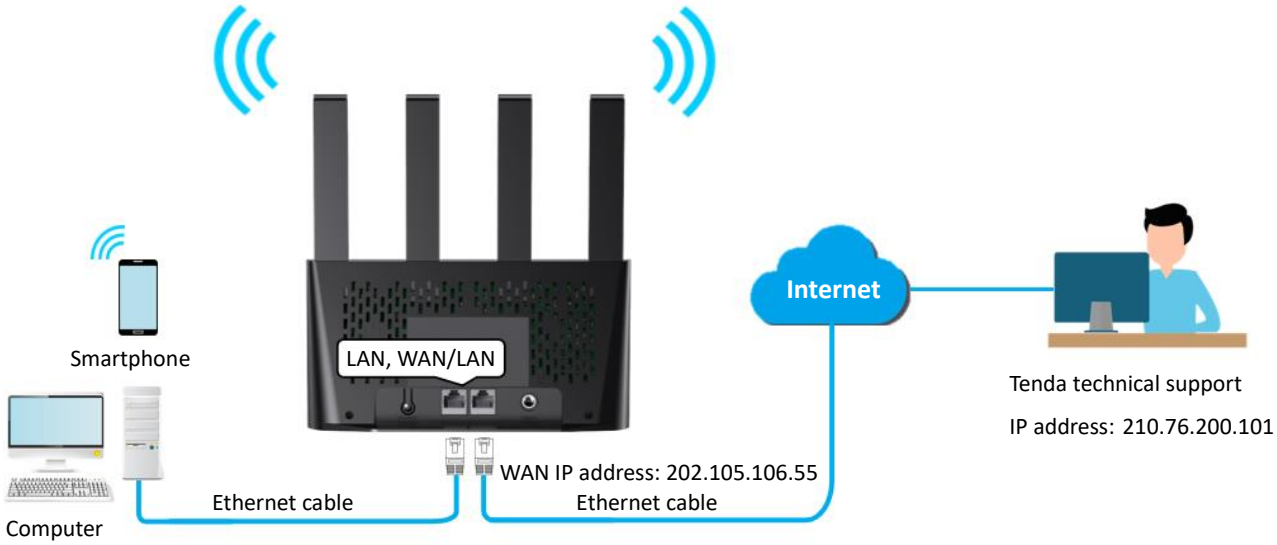
Scenario: You encounter a problem in configuring the router, and the router can access internet access.

Requirement: Ask the Tenda technical support to help you configure the router remotely.

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

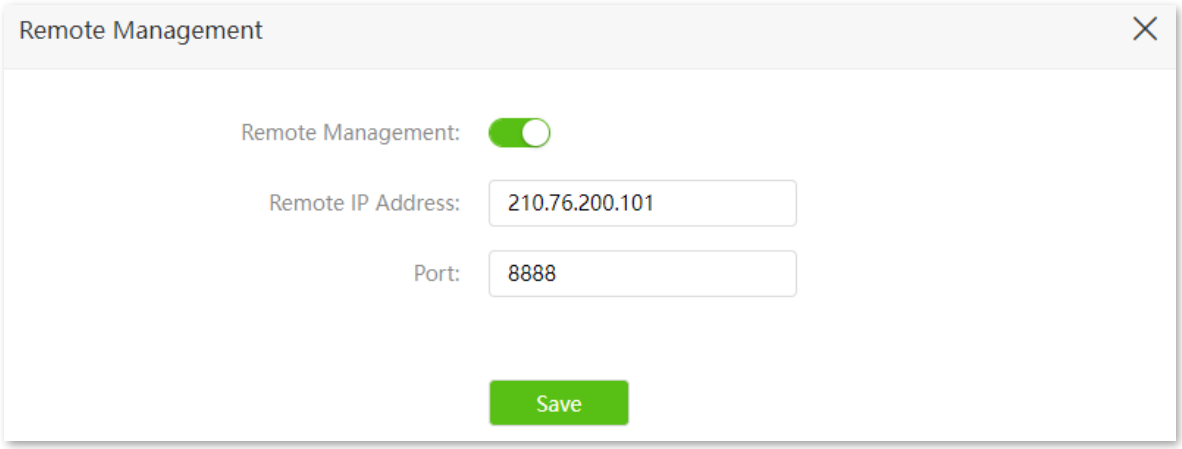
Assume that:

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



Procedure:

1. Log in to the web UI of the router.
2. Navigate to **System Settings** > **Remote Management**.
3. Enable the **Remote Management**.
4. Enter the IP address that can access the web UI remotely, which is **210.76.200.101** in this example.
5. Click **Save**.



---End

When the configuration is completed, the Tenda technical support can access and manage the web UI of the router by visiting “http://202.105.106.55:8888” on the computer.

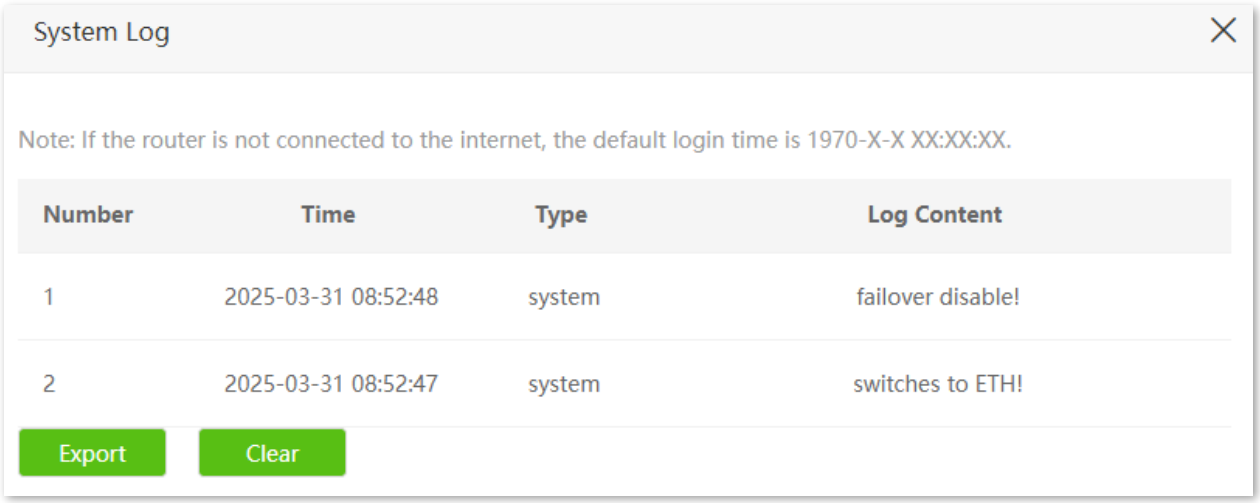
15.9 System log

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.

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

TIP

– Rebooting the router or clicking **Clear** will clear all previous system logs.
– Clicking **Export** will export the system logs to your local computer.

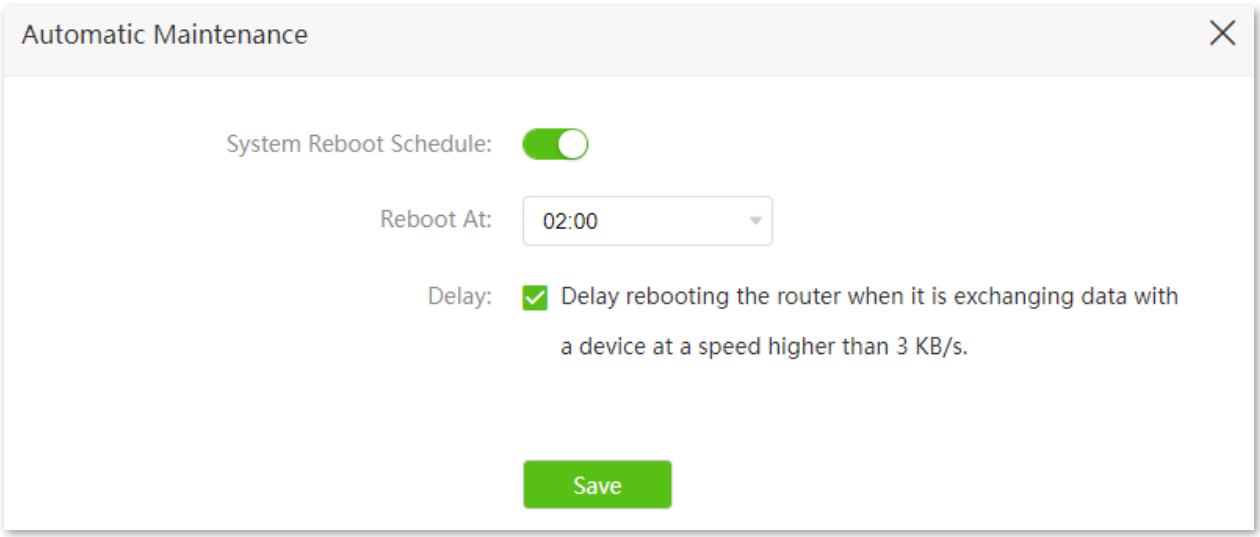


15.10 Automatic maintenance

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

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

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



Parameter description

Parameter	Description
System Reboot Schedule	Used to enable or disable the automatic maintenance function.

Parameter	Description
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 enters the sleeping mode during the sleeping time. TIP 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.

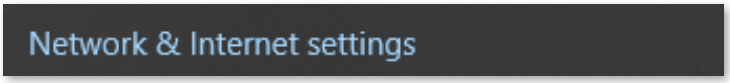
Appendix

A.1 Configuring the computer to obtain an IPv4 address automatically

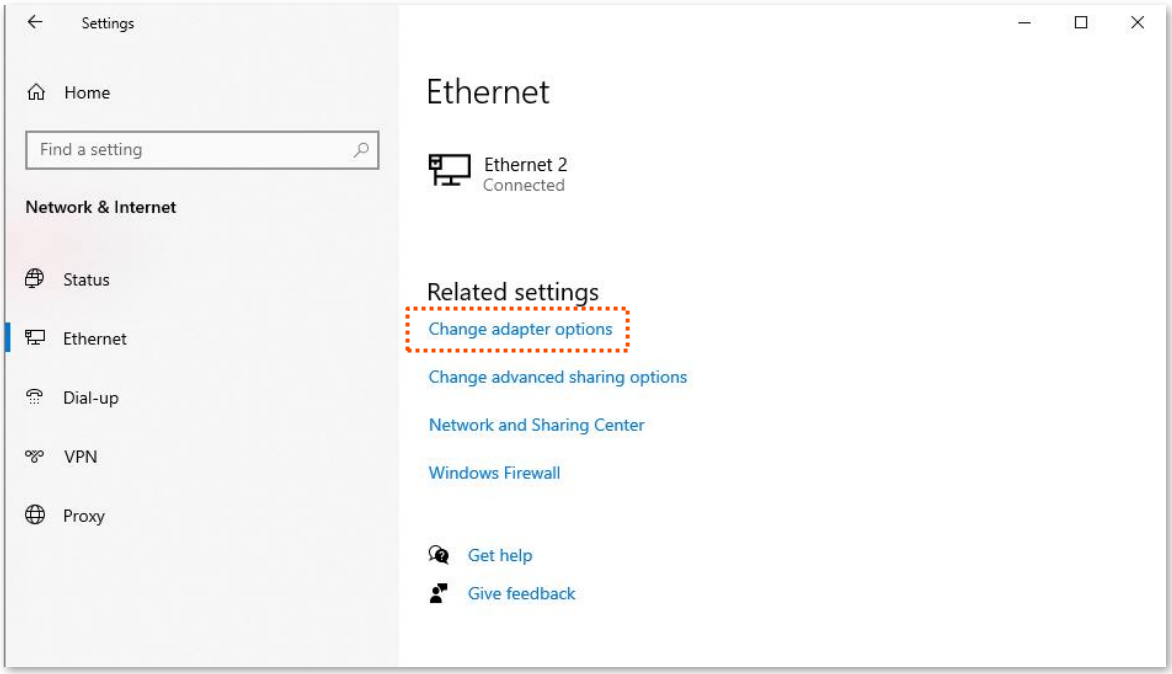
Windows 10 is used for illustration here.

A computer installed with a wired network adapter is used as an example to describe the procedures. The procedures for configuring computers installed with a Wi-Fi network adapter are similar.

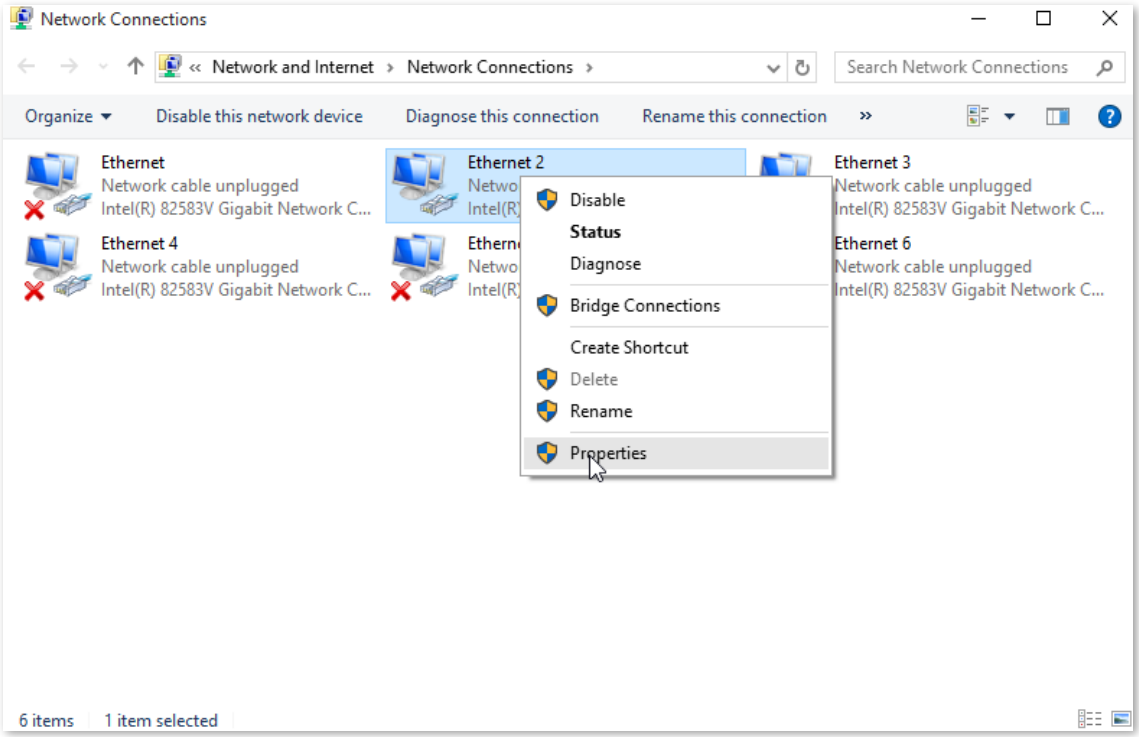
1. Click  in the bottom right corner of the desktop and choose **Network & Internet settings**.



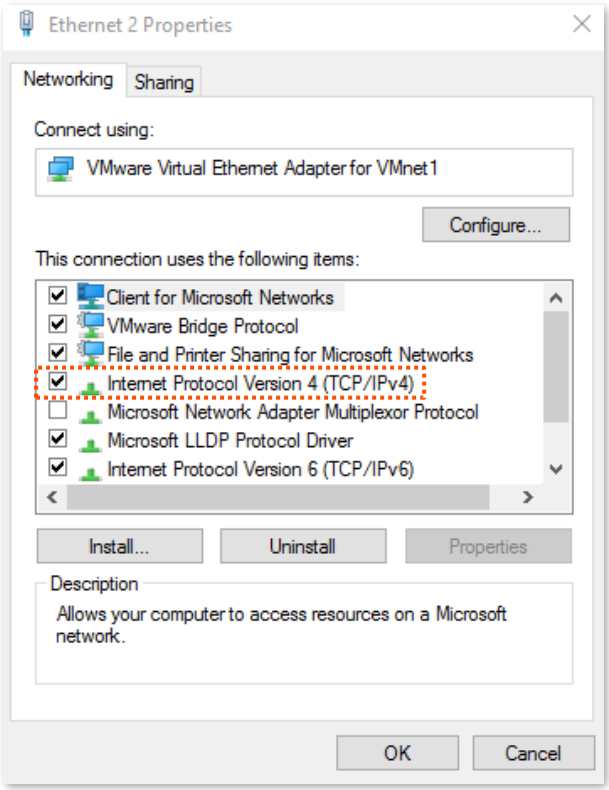
2. Click **Change adapter options**.



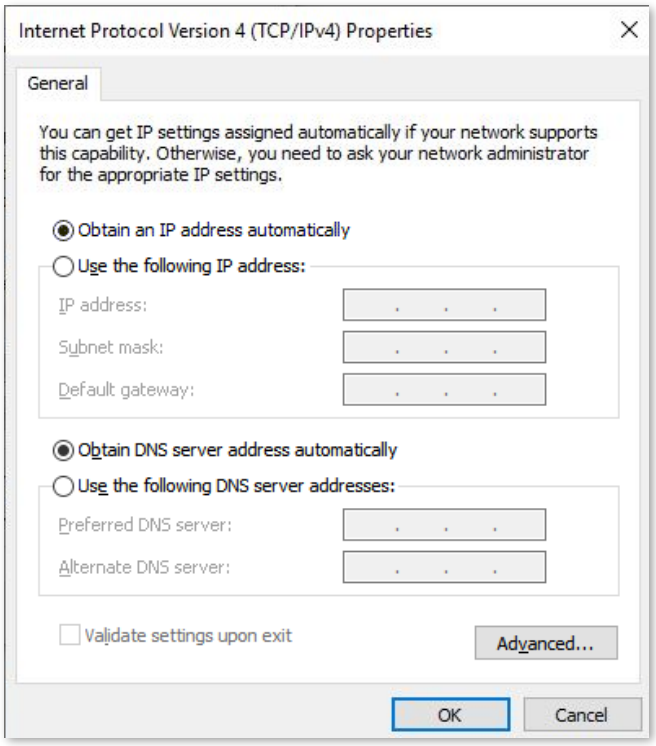
3. Right click on the connection which is being connected, and then click **Properties**.



4. Double-click **Internet Protocol Version 4 (TCP/IPv4)**.



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



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

---End

A.2 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
HL	Hop Limit
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
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TTL	Time to Live
UDP	User Datagram Protocol

Acronym or Abbreviation	Full Spelling
UPnP	Universal Plug and Play
USSD	Unstructured Supplementary Service Data
WAN	Wide Area Network
WPA-PSK	WPA-Pre-shared Key