User Guide

Wi-Fi 4G/4G+ LTE Router

4G09/4G07/4G06/4G03

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with product models. The actual product prevails.

www.tendacn.com

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

Thank you for choosing Tenda! This guide is a complement to Quick Installation Guide. The Quick Installation Guide provides instructions for quick internet setup, while this guide contains details of each function and demonstrates how to configure them.

Applicable product

This user guide walks you through all functions of the Wi-Fi 4G/4G+ LTE products (4G09 used for illustration). All the screenshots herein, unless otherwise specified, are taken from 4G09.

Conventions

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions supported by different models or different versions of the same model may differ. The actual product prevails.

The product figures and screenshots in this guide are for examples only. They may be different from the actual products you purchased, but do not affect the normal use.

If the function or parameter is displayed in gray on the product web interface, the product model is not supported or cannot be modified.

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.

Symbol	Meaning
TIP	This format is used to supplement or explain relevant operations.

For more documents

If you want to get more documents of the device, visit www.tendacn.com and search for the corresponding product model.

Technical Support

Contact us if you need more help. We will be glad to assist you as soon as possible.

Email address: support@tenda.cn

Website: www.tendacn.com

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
V2.0	2024-07-10	- Deleted description about Wireless repeating, AP mode, IPv6, IPTV and TR069. - Added description about ISP update. - Optimized description about Operating mode, Get to know your device, View internet status, Internet settings, Tenda WiFi App and Antennas settings. - Optimized sentence expression.
V1.1	2022-08-31	History version
V1.0	2022-07-23	

Contents

1 Get to know your device

1.1 Introduction

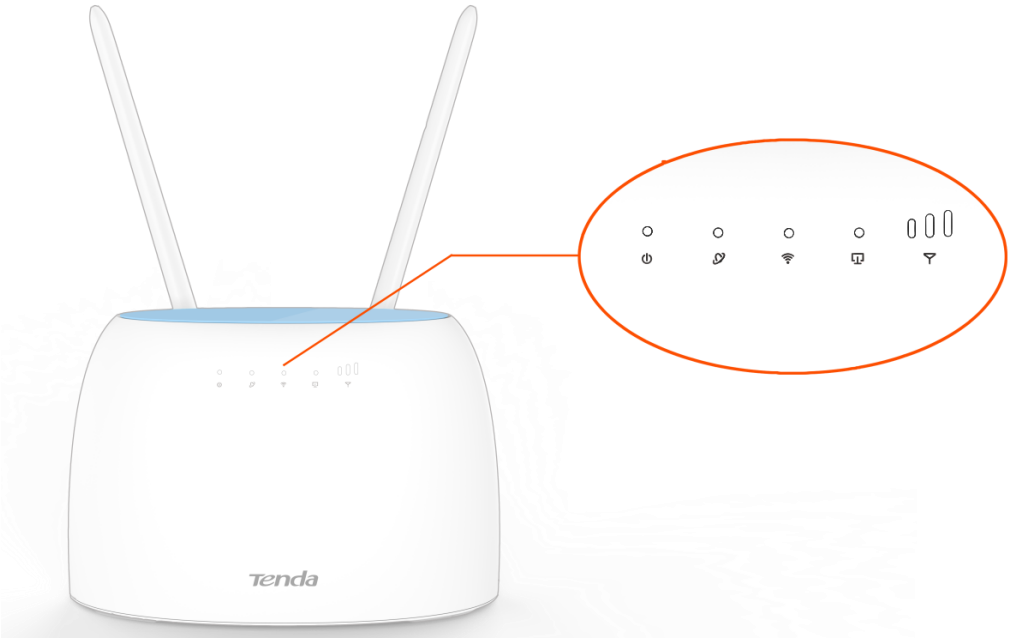
The Wi-Fi 4G/4G+ router series, powered by built-in 4G module, provides fast 4G LTE internet access. It realizes instant internet access with just a SIM card and achieves simultaneous communication with multiple devices. Different models feature varied performance and functions.

Feature \ Model	4G03	4G06	4G07	4G09
4G LTE category	CAT4	CAT4	CAT4	CAT6
Wi-Fi network	2.4 GHz	2.4 GHz	2.4 GHz & 5GHz	2.4 GHz & 5GHz
Wireless rate	2.4 GHz: 300 Mbps	2.4 GHz: 300 Mbps	2.4 GHz: 300 Mbps 5 GHz: 867 Mbps	2.4 GHz: 300 Mbps 5 GHz: 867 Mbps
4G antennas	Internal antennas	Two 5 dBi external antennas	Two 5 dBi external antennas	Two 5 dBi external antennas
Ethernet port	2*FE	2*FE	2*FE	2*GE
App management	√	√	√	√
Telephone port	-	√	-	-

1.2 Indicators

The indicators may vary with device models. Please refer to the product you purchased.

4G09 is used for illustration here.

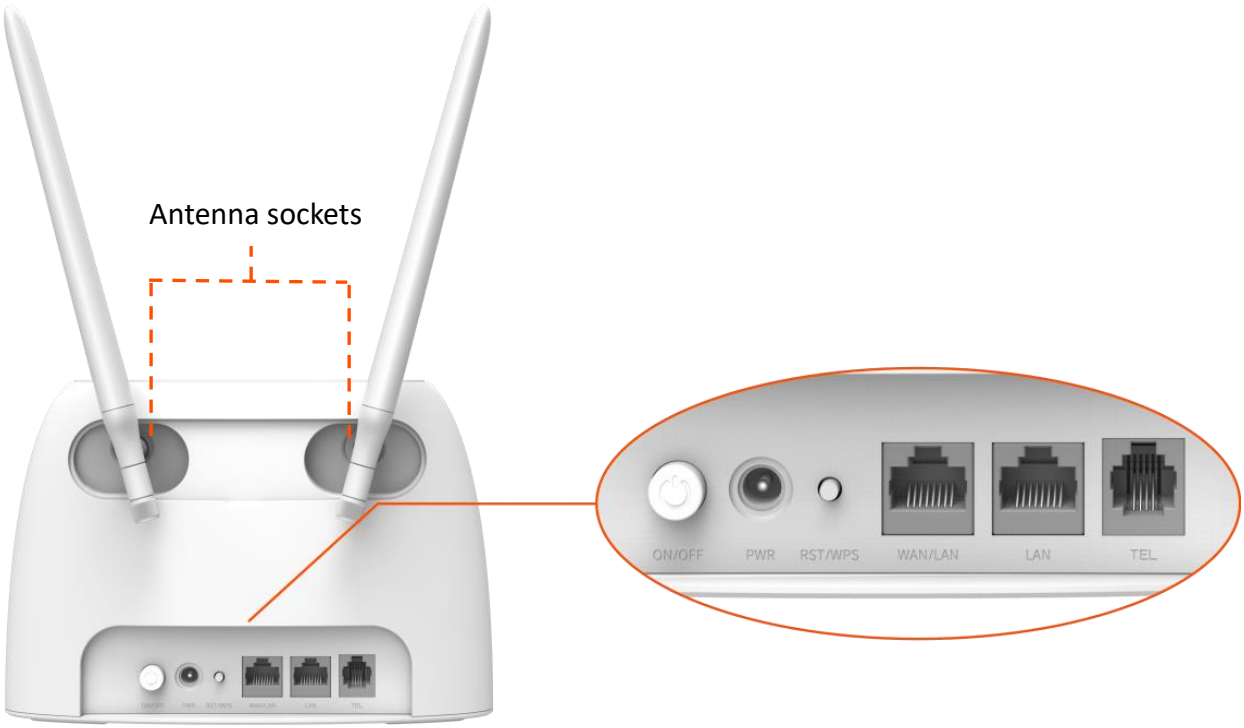


Indicator	Status	Description
(Power indicator)	Solid on	The router is powered on.
	Off	The router is powered off.
(Internet indicator)	Solid on	The router is connected to the internet.
	Off	The router fails to connect to the internet.
(Wi-Fi indicator)	Solid on	The Wi-Fi network of the router is enabled.
	Blinking	The router is performing WPS negotiation.
	Off	The Wi-Fi network is disabled.
(Ethernet port indicator)	Solid on	At least one device is connected to the Ethernet port of the router.
	Off	No device is connected to the Ethernet port of the router.
(Signal indicator)	3 bars	Excellent signal.
	2 bars	Good signal.
	1 bar	Fair signal.
	Off	No 4G/3G signal.

1.3 Ports and buttons

The ports and buttons may vary with device models. Please refer to the product you purchased.

4G06 is used for illustration here.

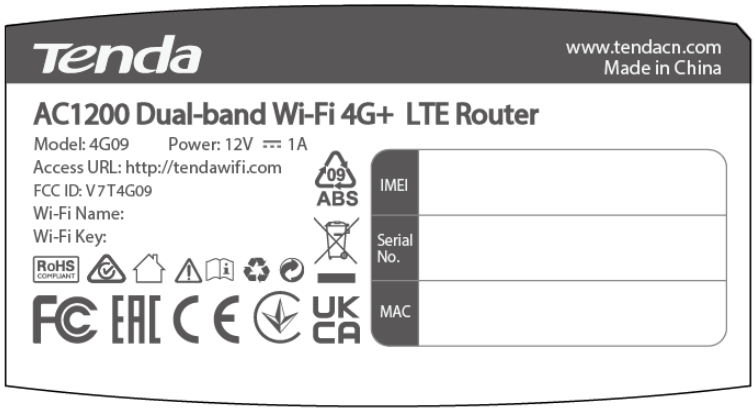


Port/Button	Description
ON/OFF	Power button. It is used to power on or power off the router.
PWR	Power jack. It is used to connect to the included power adapter.
RST/WPS	It serves as both reset and WPS button. - Reset: When the router is working properly, hold down the button for about 8 seconds and release it when all indicators light off and then light up. The router is restored to factory settings. - WPS: Press the button and release it, the (Wi-Fi) indicator blinks. The router gets ready for WPS negotiation. Configure WPS-enabled wireless devices within 2 minutes to start WPS negotiation with the router.
WAN/LAN	It is a fast Ethernet port, which can serve as a WAN port or a LAN port. By default, it is a LAN port.

Port/Button	Description
LAN	It is a LAN port used to connect wired devices, such as a computer. When the IPTV function is enabled, it serves as the IPTV port to be connected to the set-top box.
TEL	Telephone port. It is used to connect to a landline telephone using the included telephone cable for voice service. TIP - Voice service is only available with a SIM card inserted. Ensure that the mobile data is enabled and the router can access the internet before using the voice service. - Internet access is unavailable when you are making phone calls through 3G network.
Antenna sockets	They are used to connect to the detachable antennas.

1.4 Label

The bottom label shows the Model, Power, Access URL, FCC ID, Wi-Fi Name, Wi-Fi Key, IMEI, Serial No. and MAC address of the router. The following figure is for reference only.



Model: Specifies the model of the router.

Power: Specifies the power supply for the router.

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

FCC ID: Specifies the Federal Communications Commission Identification number of the router.

Wi-Fi Name: Specifies the default Wi-Fi name of the router.

Wi-Fi Key: Specifies the default Wi-Fi password of the router.

IMEI: It is the unique mobile device identification code of the router.

Serial No.: It is required if you need technical assistance to repair your router.

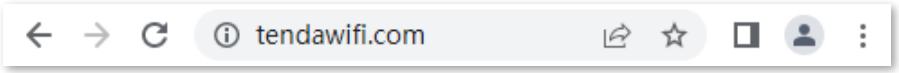
MAC: Specifies the MAC address of the router.

2 Web UI

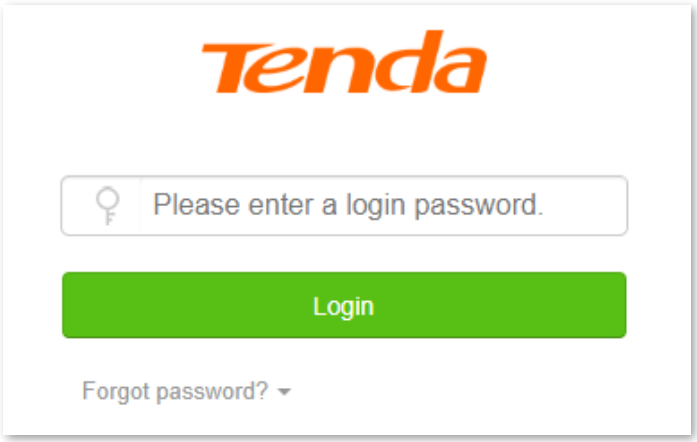
2.1 Log in to the web UI

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

Step 2 Start a web browser on the device connected to the router, and visit **tendawifi.com**.



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



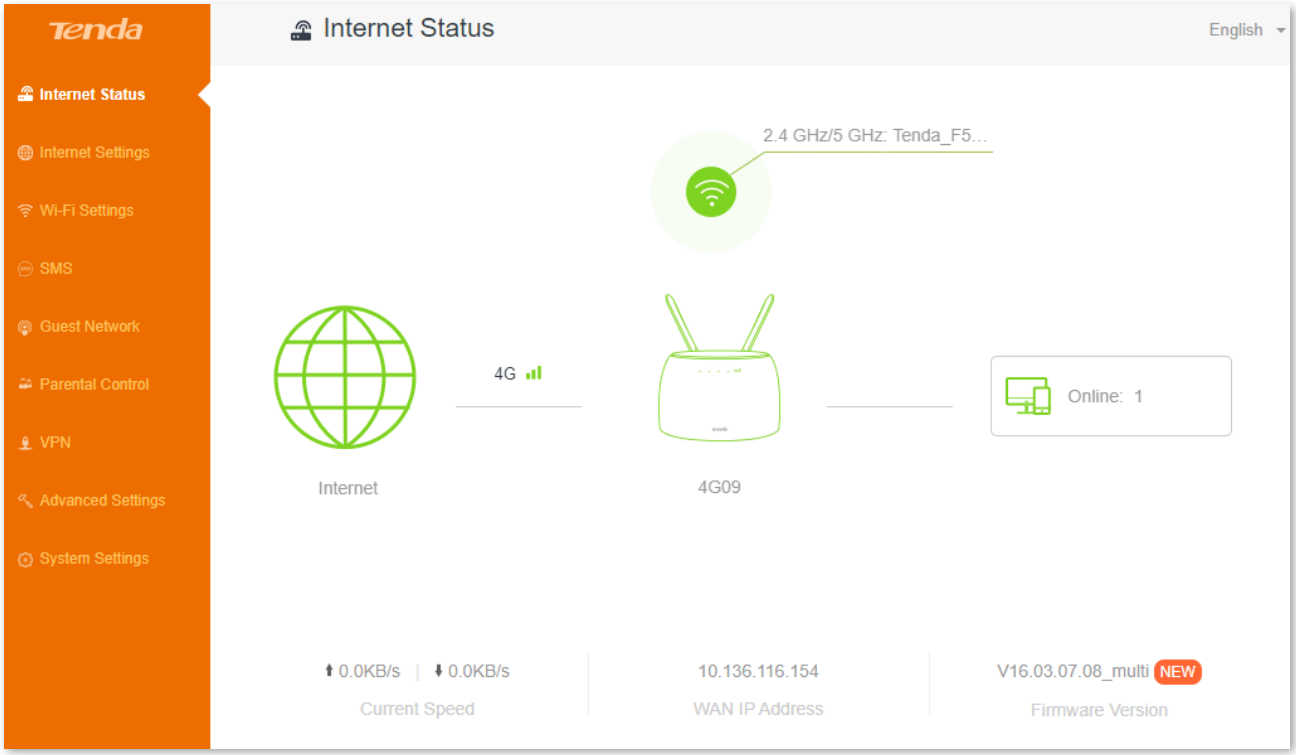
---End

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, and Configure the computer to obtain an IP address automatically.
- Restore the router to factory settings and try again.

Successfully logged in to the web UI of the router. The following figure is for reference only.

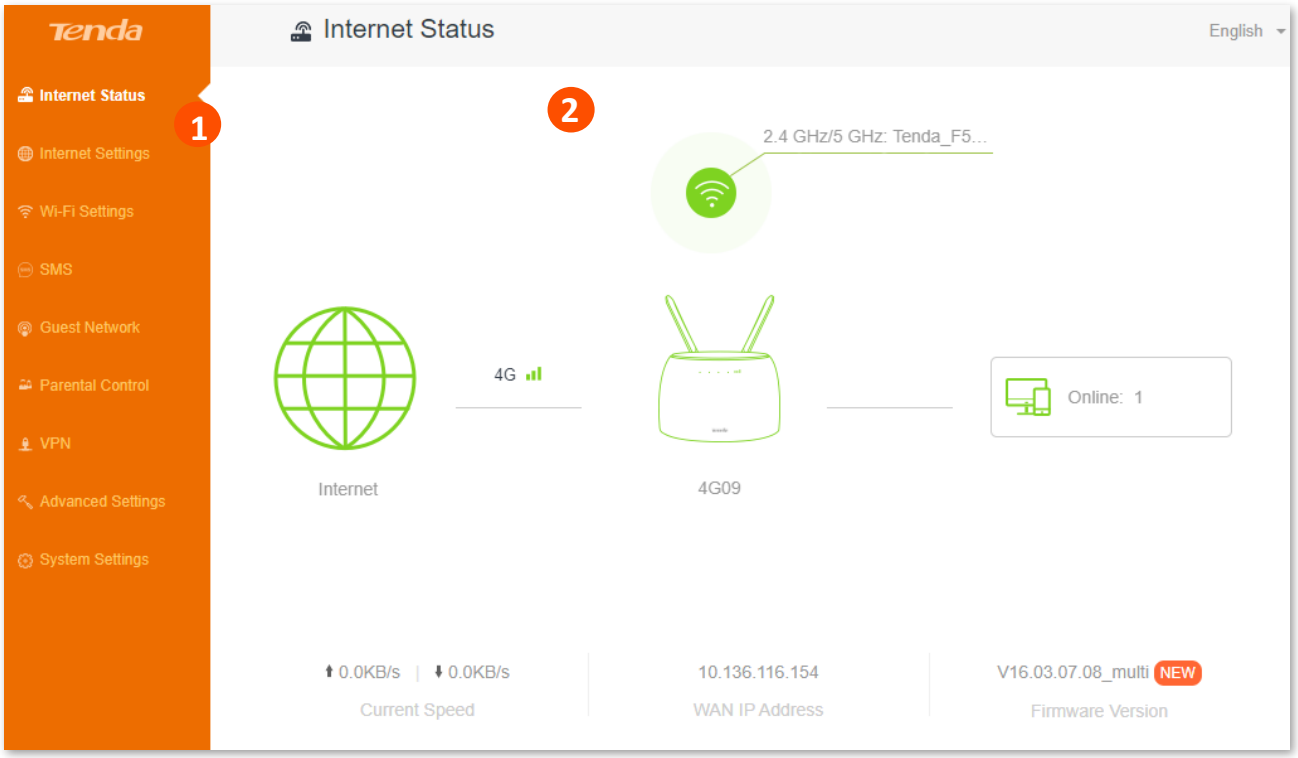


2.2 Log out of the web UI

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

2.3 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.



SN	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.

3 Internet status

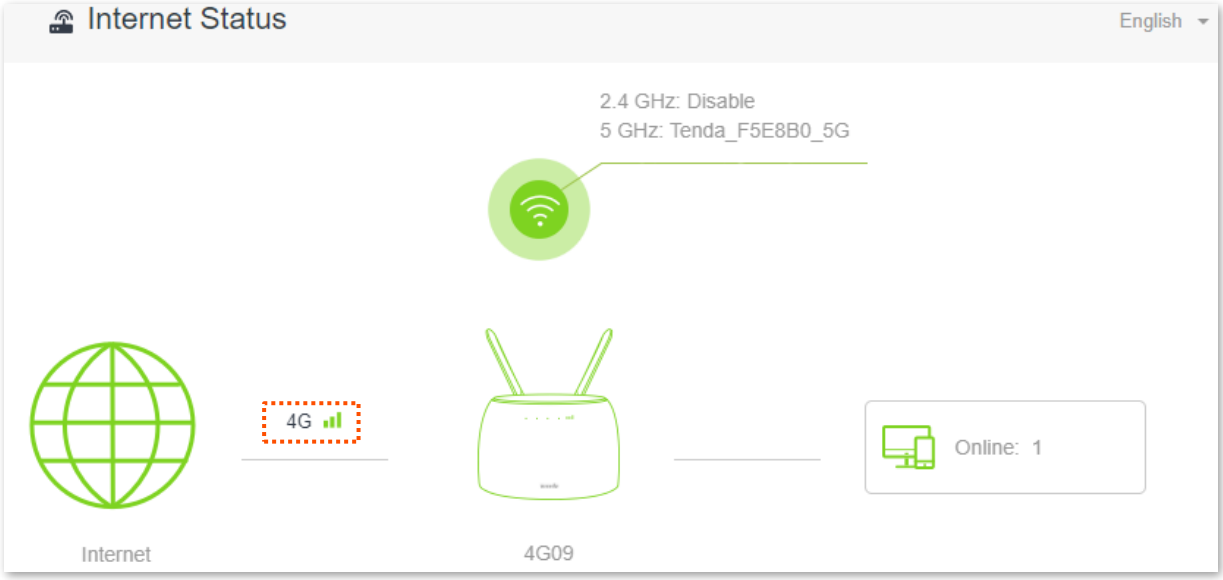
This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with product models. The actual product prevails.

3.1 View internet status

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

3.1.1 Normal connection

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



3.1.2 Abnormal connection

Connection failed

When “Connection failed” is shown between the internet and the router, it indicates that the internet connection is abnormal. The following figure is for reference only.

Firstly, try the following solutions:

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

If the problem persists, try the following solutions:

- Ensure that the Ethernet cable is connected properly.
- Ensure that you choose the proper connection type. If you are unclear, contact your ISP about the connection type.
- Contact our technical support for help.

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 in the web UI.

No SIM card inserted

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

Monthly data limit reached

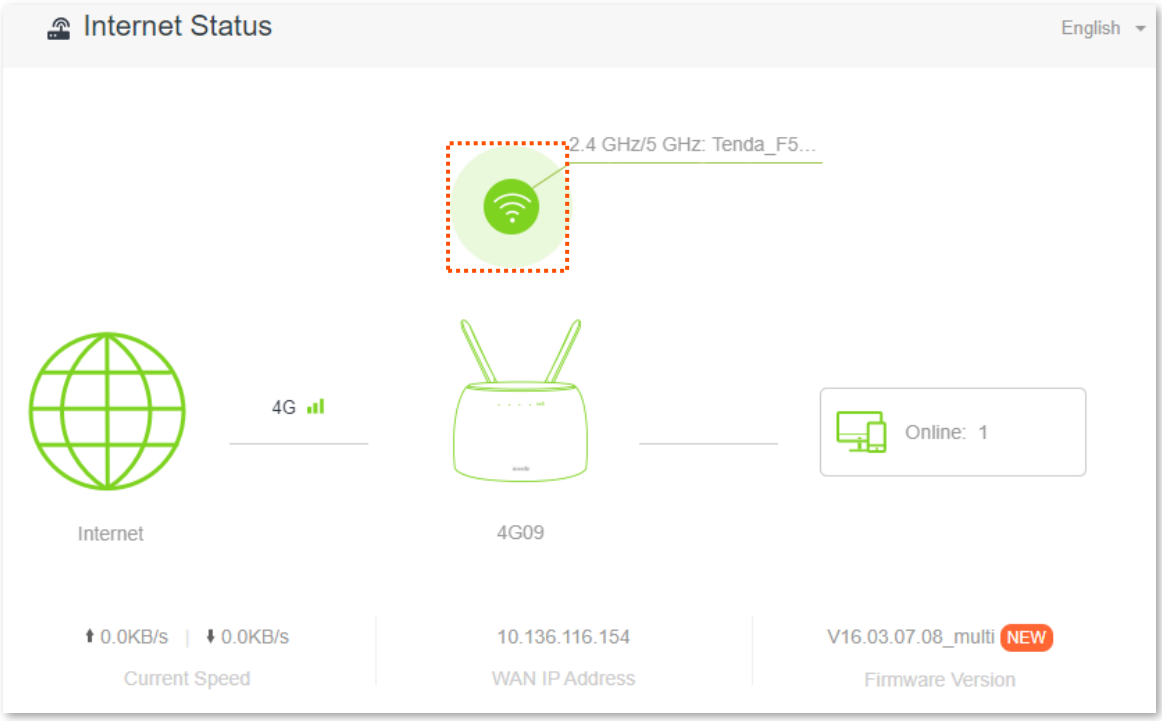
When “The monthly data limit is reached.” is shown between the internet and the router, it indicates that the router will disconnect from the internet automatically when the limit is reached. Refer to Mobile Data to modify the related parameters.

3.2 View wireless information

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

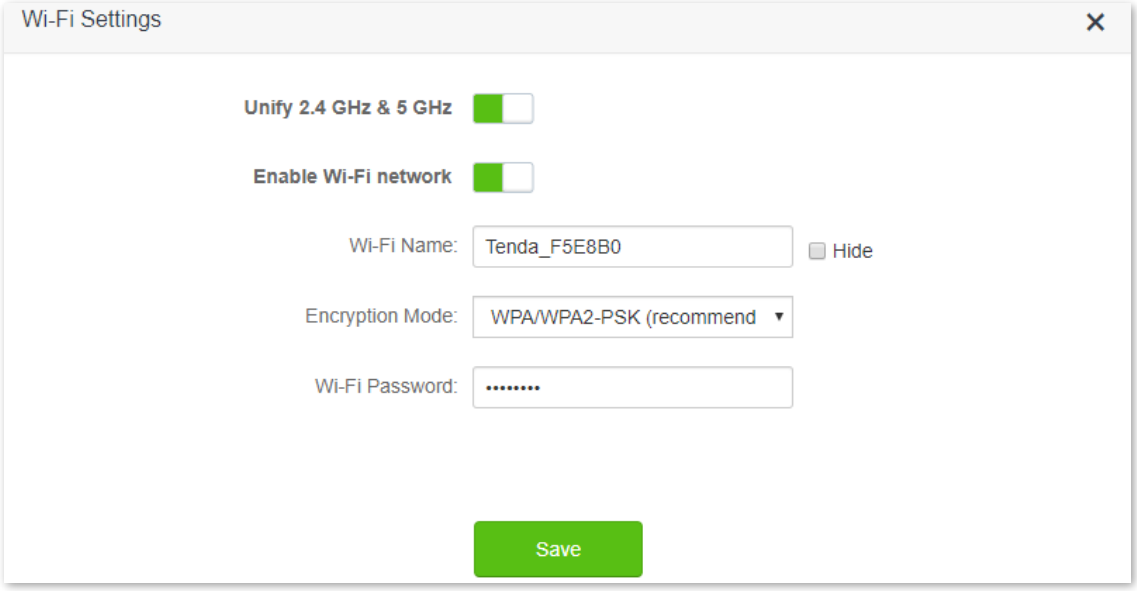
Step 2 Navigate to **Internet Status**.

Step 3 Click .



---End

You can change wireless parameters as required.

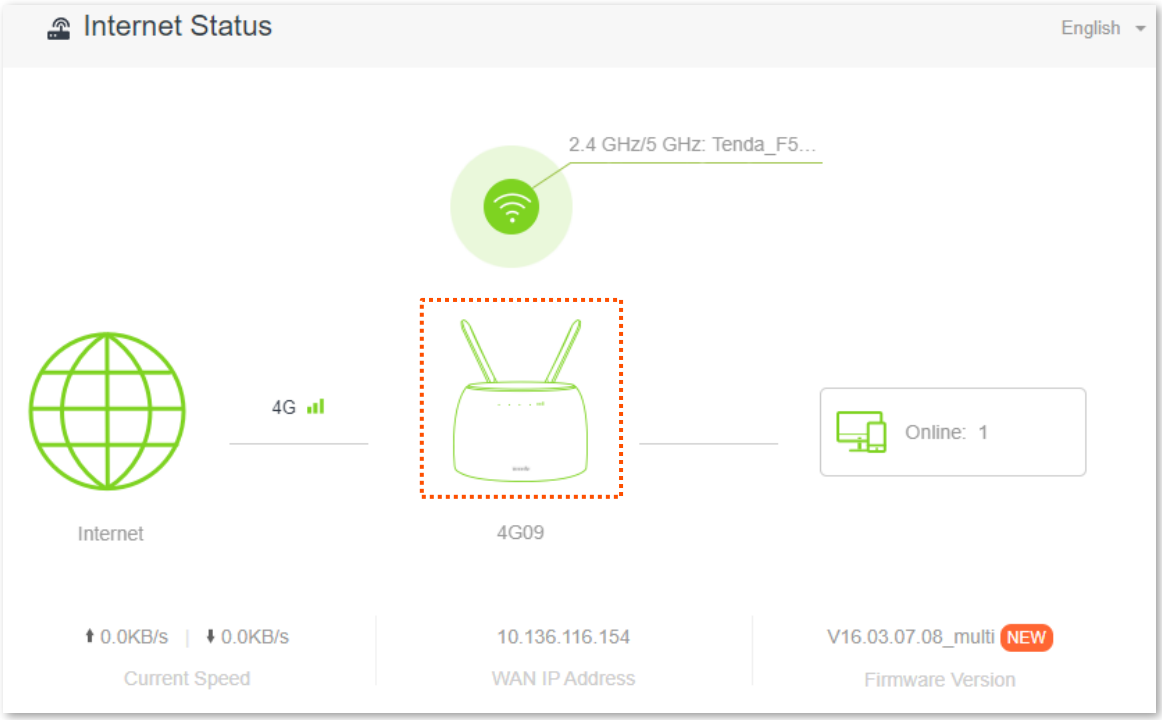


3.3 View system information

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

Step 2 Navigate to **Internet Status**.

Step 3 Click .



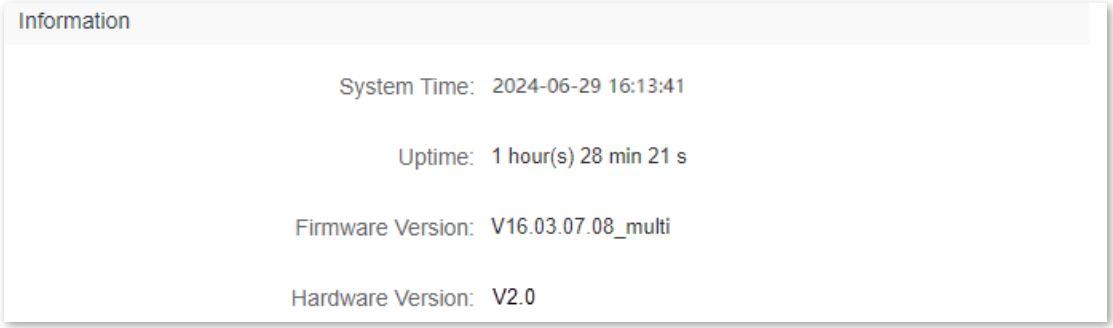
---End

TIP

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

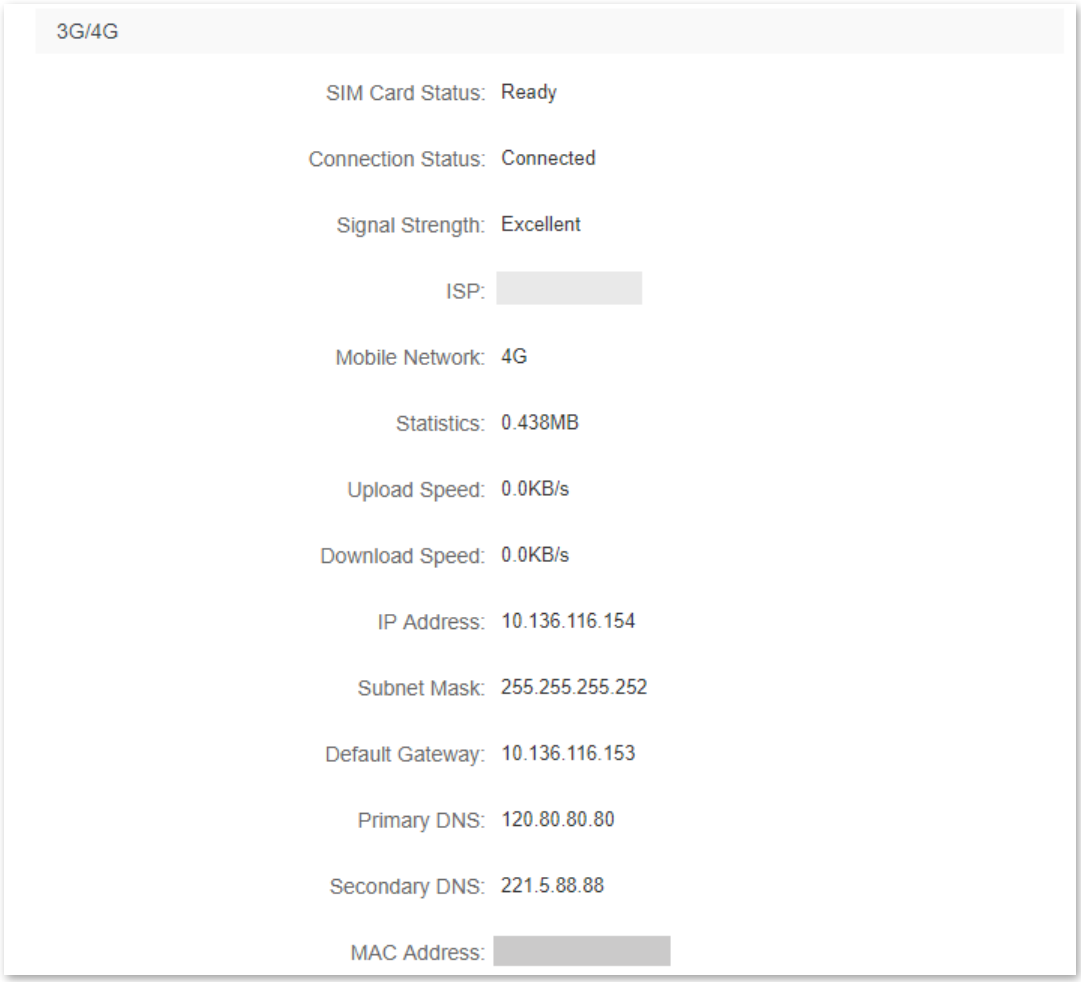
3.3.1 Basic information

In this part, you can view the basic information of the router, such as system time, uptime and firmware version and hardware version. The following figure is for reference only.



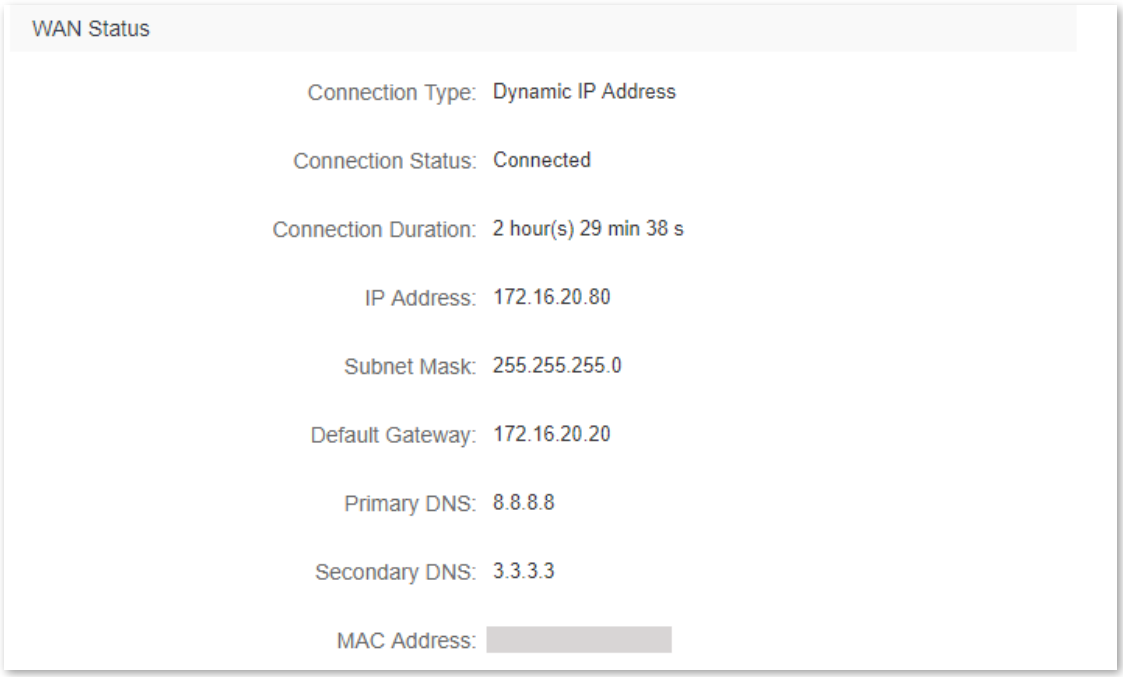
3.3.2 3G/4G status

On this page, you can view the information of the SIM card and 3G/4G network in this part. The following figure is for reference only.



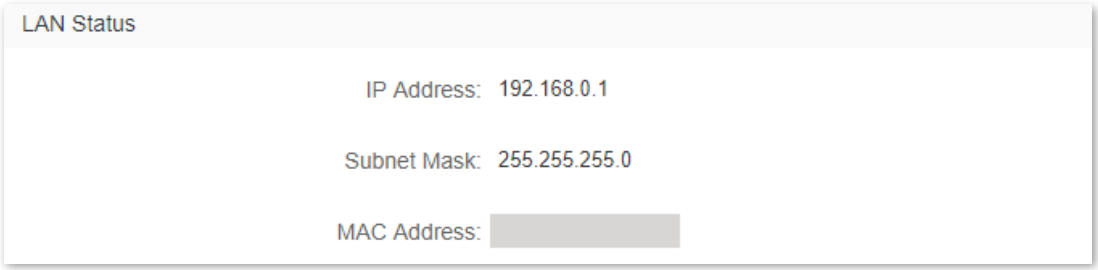
3.3.3 WAN status

In this part, you can view the information of the WAN port, including connection type, connection status and connection duration. The following figure is for reference only.



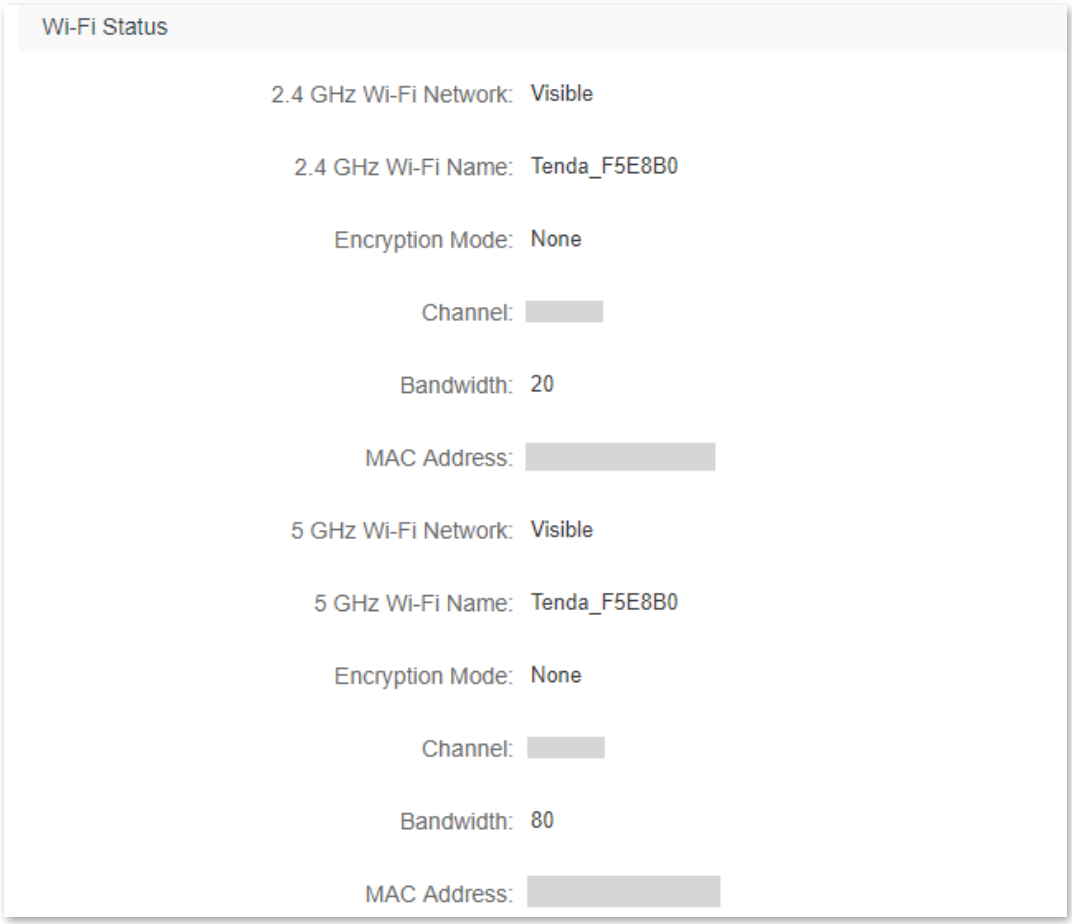
3.3.4 LAN status

In this part, you can view the LAN information, such as LAN IPv4 address, subnet mask and MAC address. The following figure is for reference only.



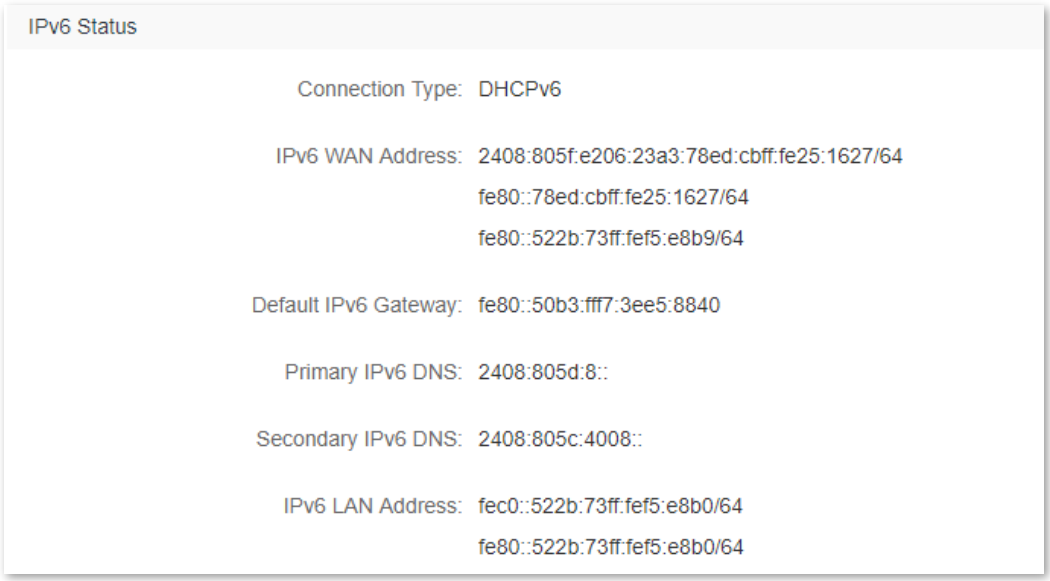
3.3.5 Wi-Fi status

In this part, you can view the information of 2.4 GHz and 5 GHz Wi-Fi network, including the connection status, visibility, hotspot name and encryption mode, and so on. The following figure is for reference only.



3.3.6 IPv6 status

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



3.4 View online device information

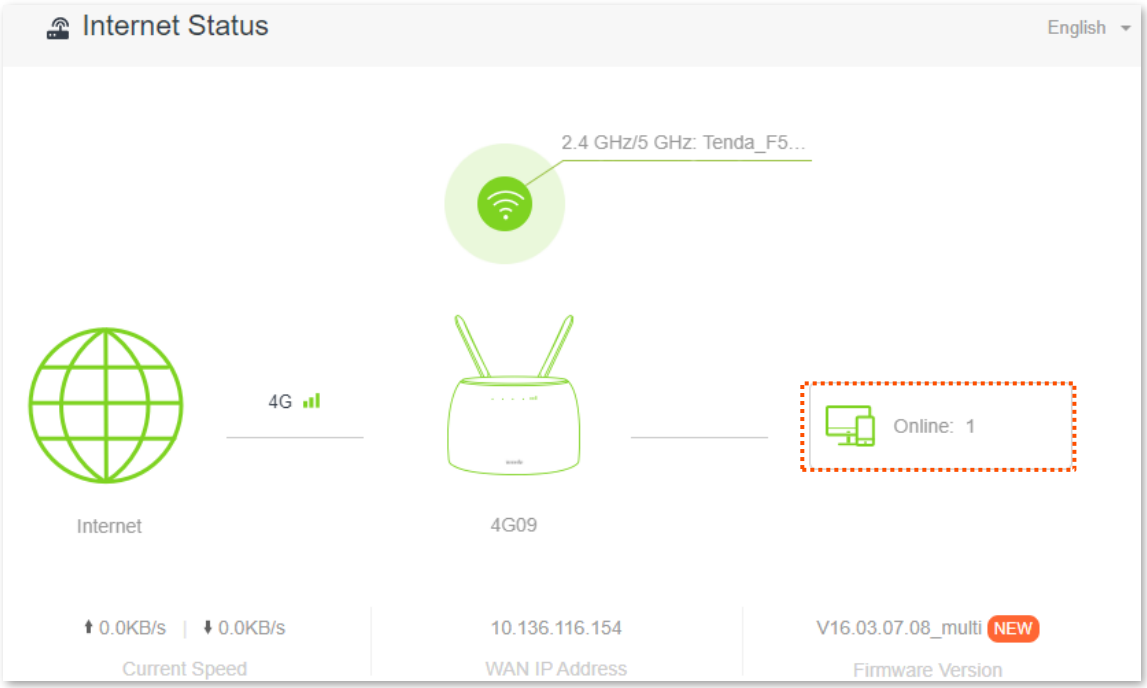
On this page, you can view the information of devices connected to the router, including the upload speed, download speed and access type. You can also view and add devices to the blacklist.

To access the page:

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

Step 2 Navigate to **Internet Status**.

Step 3 Click Online: .

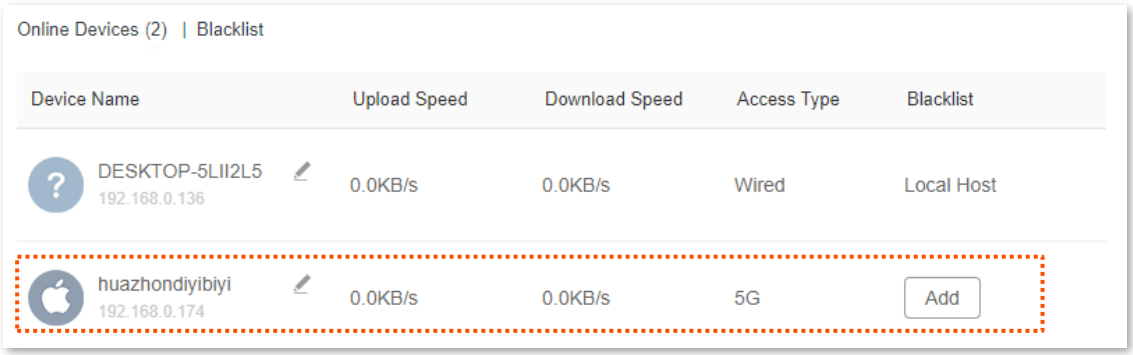


---End

3.4.1 Add devices to the blacklist

Adding devices to the blacklist to block the internet access:

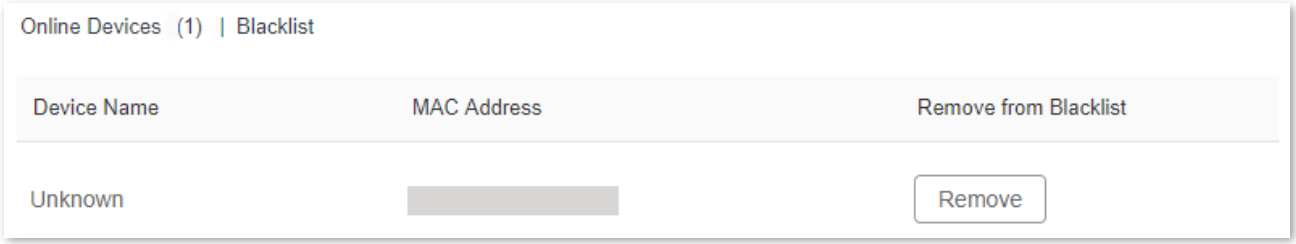
Step 1 Navigate to **Online Devices**, and locate the device to be added.



Step 2 Click **Add**.

---End

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

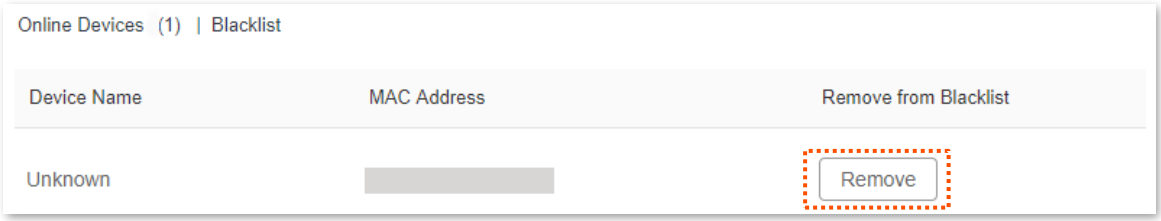


3.4.2 Remove devices from the blacklist

To remove devices from the blacklist as required:

Step 1 Navigate to **Blacklist**, and locate the device to be removed from the blacklist.

Step 2 Click **Remove**.



---End

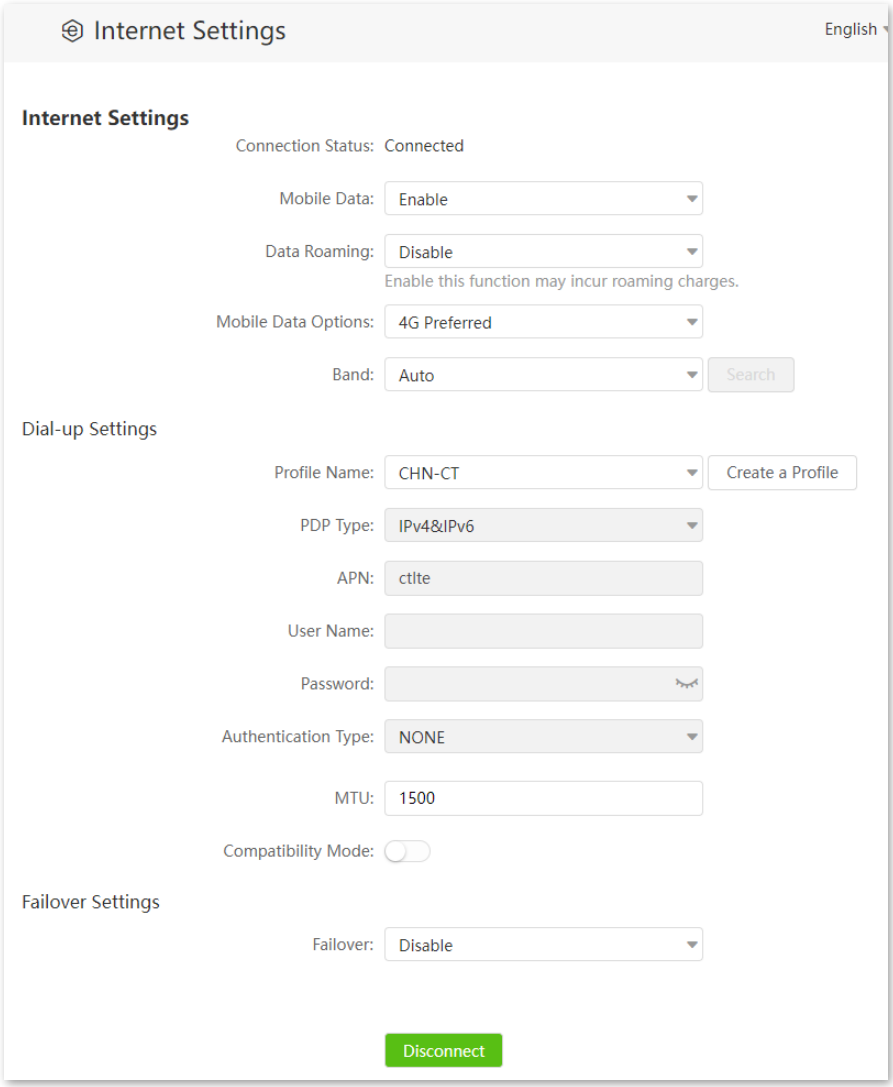
4 Internet settings

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with product models. The actual product prevails.

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



Parameter description

Parameter	Description
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.
Band	Specifies the Lock Band function of the router, which can improve the internet experience. - **Auto**: It will automatically scan and match the band supported by the SIM card and ISP according to the surrounding network environment. - **Manual**: You can manually scan and match the band supported by the SIM card and ISP.
Profile Name	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.
PDP Type	
APN	
User Name	
Password	
Authentication Type	
Create a Profile	Used to create an APN dial-up profile when the router fails to identify these parameters automatically.
MTU	Maximum Transmission Unit (MTU) is the largest data packet transmitted by a network device. The default MTU value is 1500. Do not change the value unless necessary.

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

4.1.1 Change mobile network preference

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

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

Configuring procedure:

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

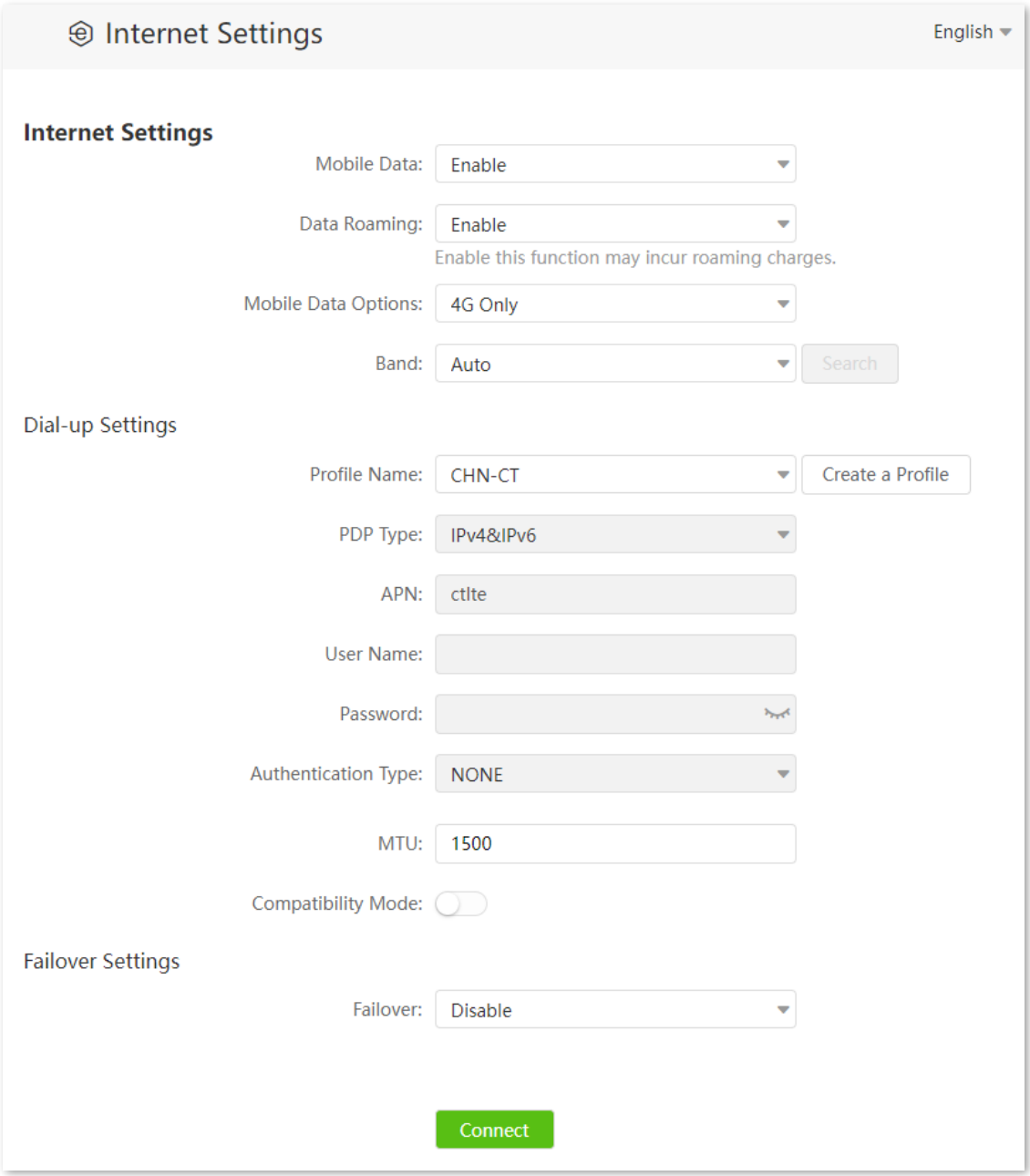
Step 2 Navigate to **Internet Settings**.

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

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

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

Step 6 Click **Connect**.



---End

After the configuration is completed, 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.

4.1.2 Create an APN profile manually to access the internet

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

Configuring procedure:

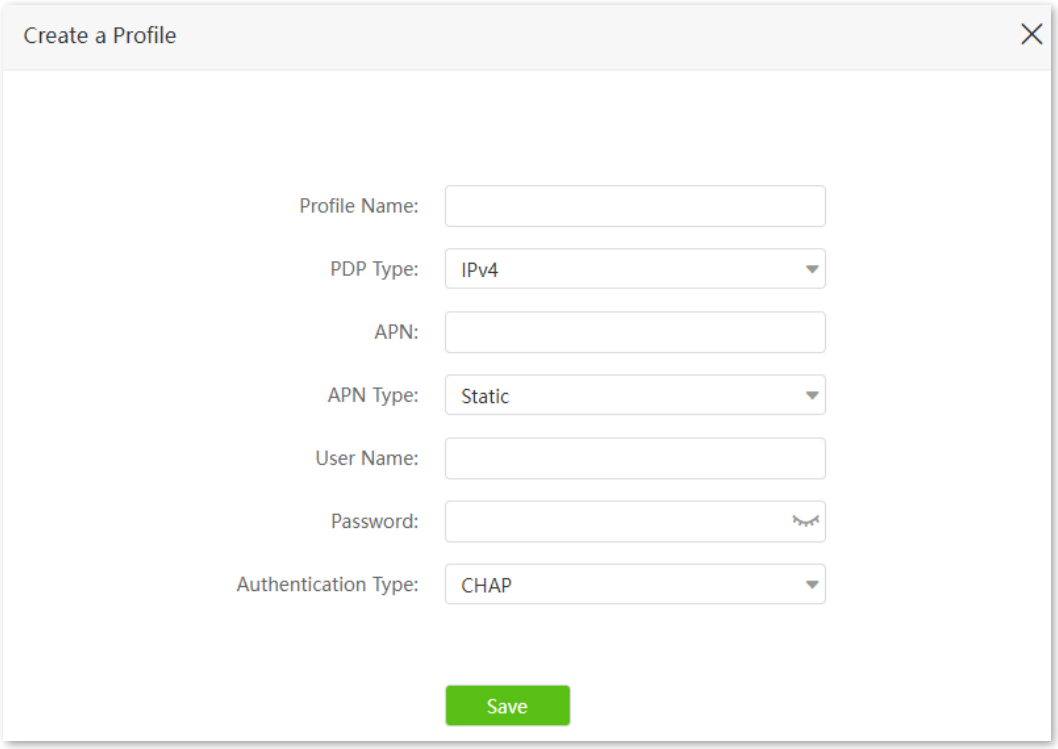
Step 1 Log in to the web UI of the router.

Step 2 Navigate to **Internet Settings**.

Step 3 Click **Create a Profile**.

Step 4 Enter required parameters from your ISP.

Step 5 Click **Save**.



---End

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

4.2 Access the internet through the WAN port

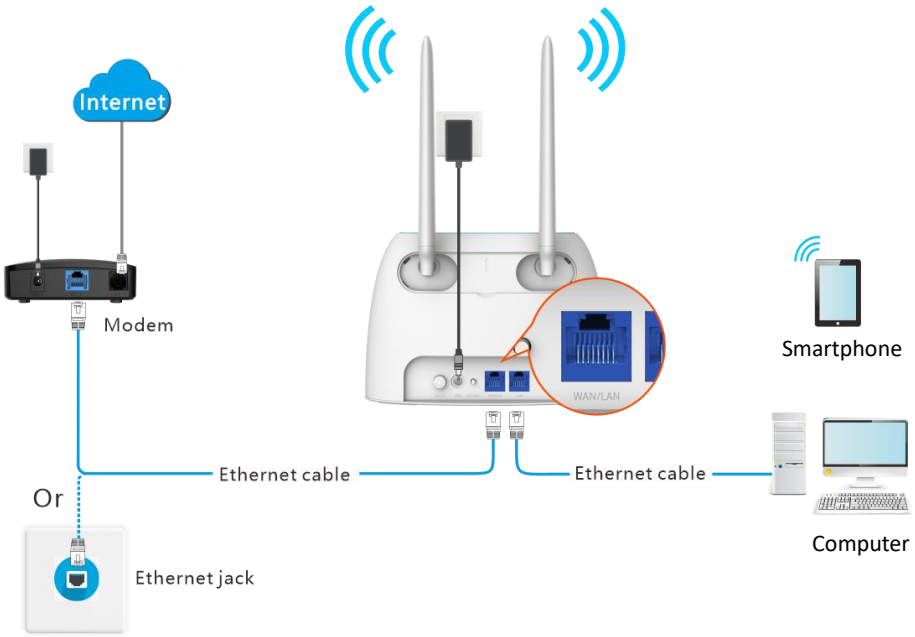
If you want to connect your broadband to the router to access the internet, you can access the internet through the WAN port.

TIP

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

4.2.1 Access the internet with a PPPoE account

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



Configuring procedure:

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

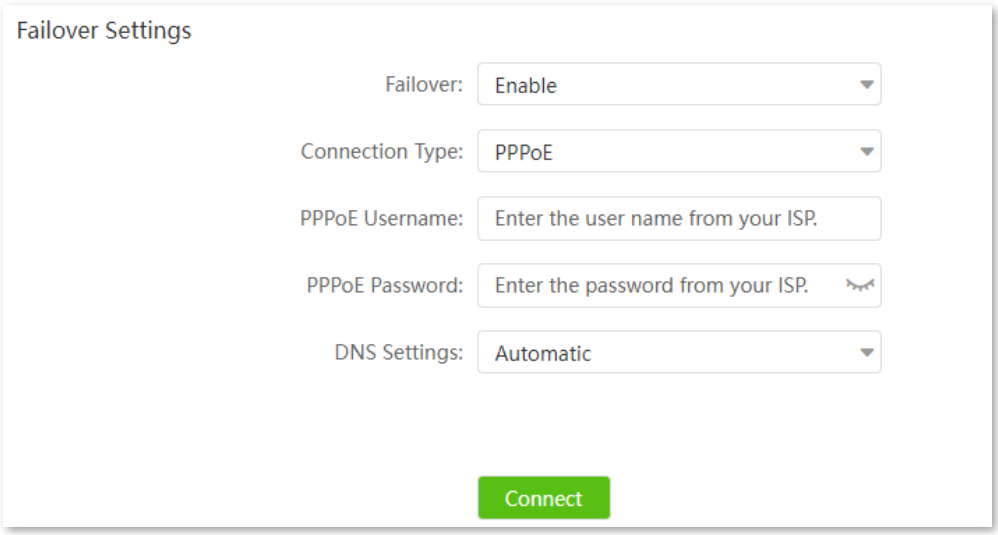
Step 2 Navigate to **Internet Settings**.

Step 3 Enable the **Failover** function.

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

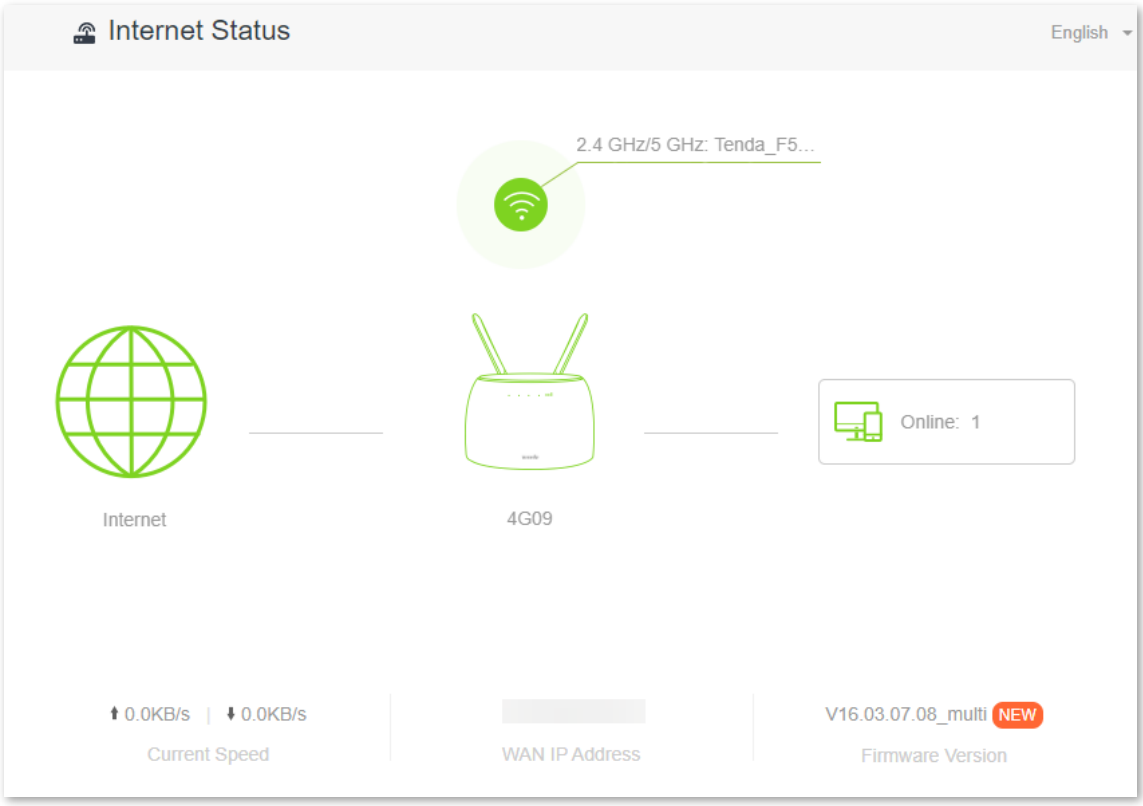
Step 5 Enter the **PPPoE UserName** and **PPPoE Password**.

Step 6 Click **Connect**.



---End

After the configuration is completed, you can access the internet with a PPPoE account. The following figure is for reference only.



Parameter description

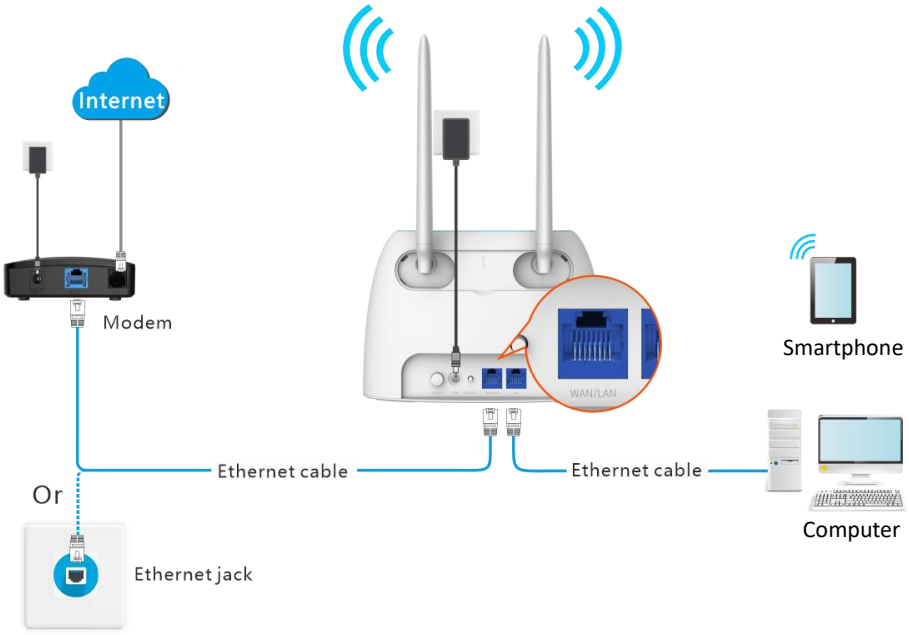
Parameter	Description
PPPoE Username	When PPPoE is chosen as the connection type, you need to enter the user name and password provided by your ISP to access the internet.
PPPoE Password	
DNS Settings	Specifies the obtaining method of WAN port DNS address, which is **Automatic** by default. - **Automatic**: The router obtains a DNS server address from the DHCP server of the upstream network automatically. - **Manual**: The DNS server address is configured manually.

4.2.2 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 4G09 as the other one.

The application scenario is shown below.



Configuring procedure:

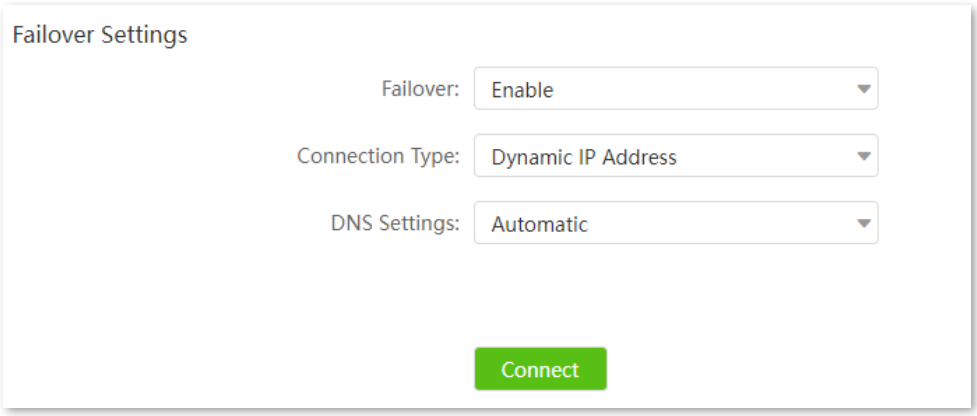
Step 1 Log in to the web UI of the router.

Step 2 Navigate to **Internet Settings**.

Step 3 Enable the **Failover** function.

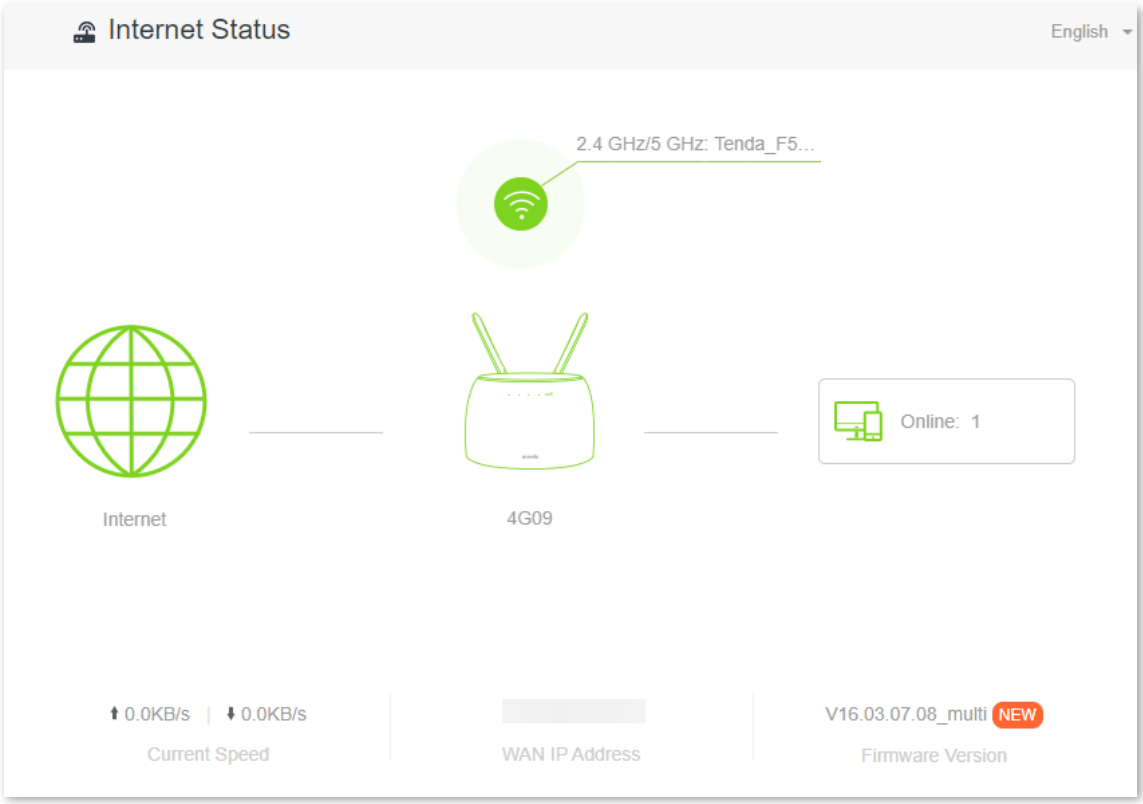
Step 4 Set **Connection Type** to **Dynamic IP Address**.

Step 5 Click **Connect.**



---End

After the configuration is completed, you can access the internet through dynamic IP address. The following figure is for reference only.



Parameter description

Parameter	Description
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.

4.2.3 Access the internet with static IP address information

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

Configuring procedure:

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

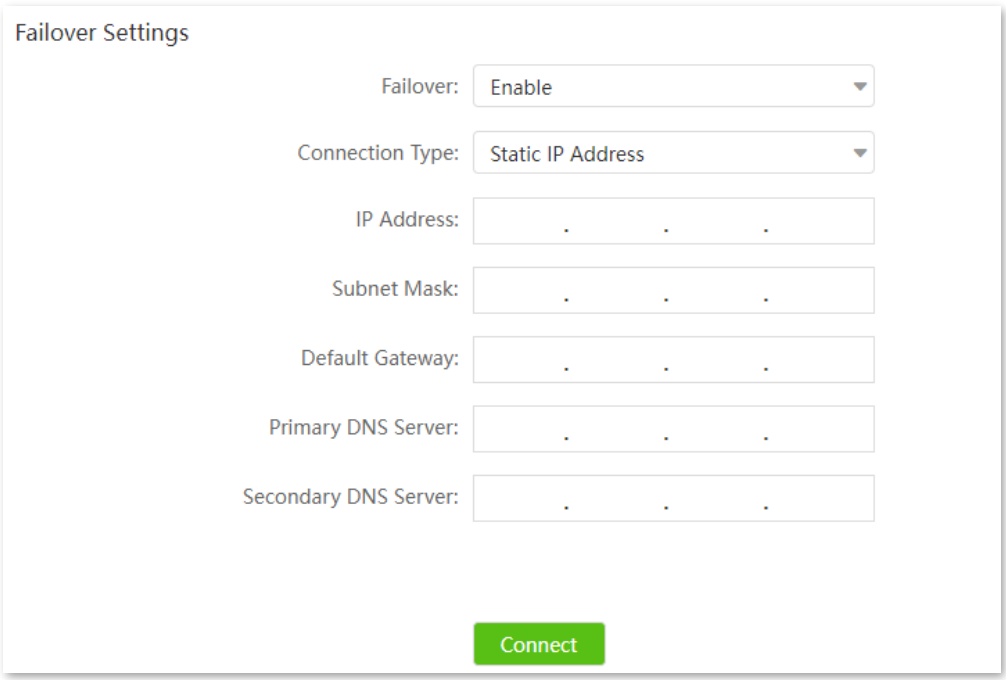
Step 2 Navigate to **Internet Settings**.

Step 3 Enable the **Failover** function.

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

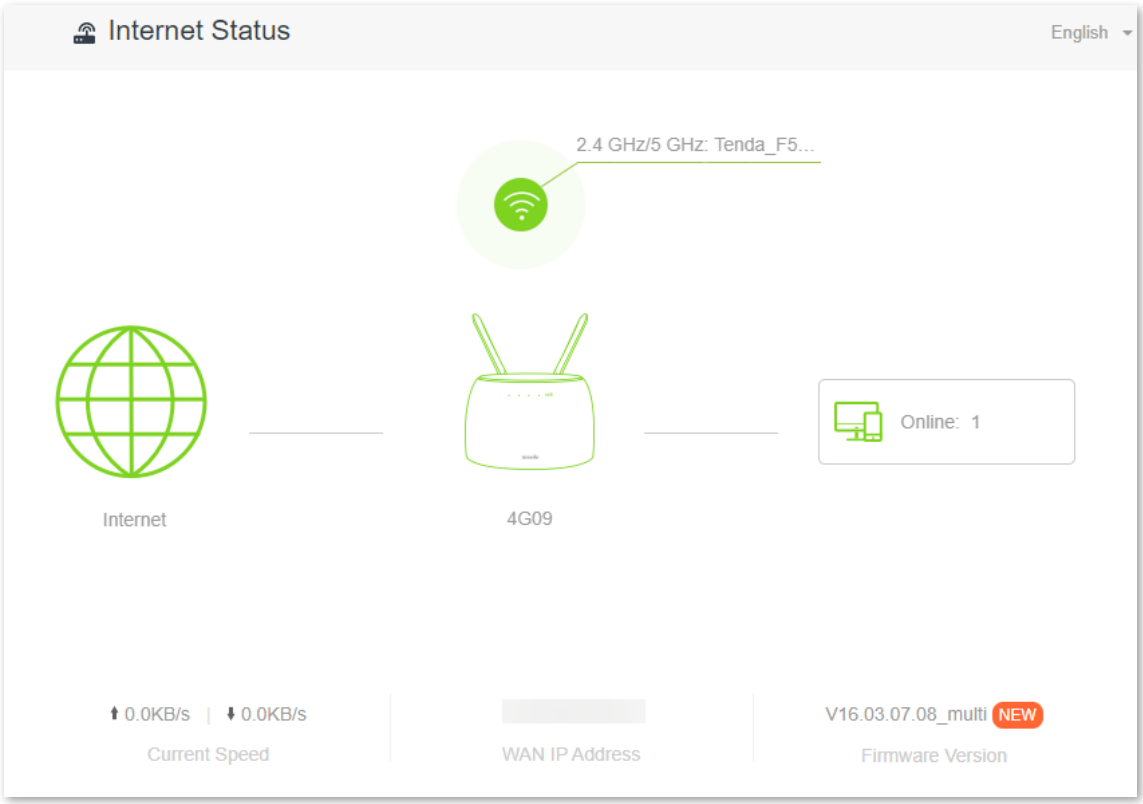
Step 5 Enter **IP Address**, **Subnet Mask**, **Default Gateway** and **Primary/Secondary DNS server**.

Step 6 Click **Connect**.



---End

After the configuration is completed, you can access the internet with static IP address information. The following figure is for reference only.



Parameter description

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

4.3 Set Failover connection

4.3.1 Overview

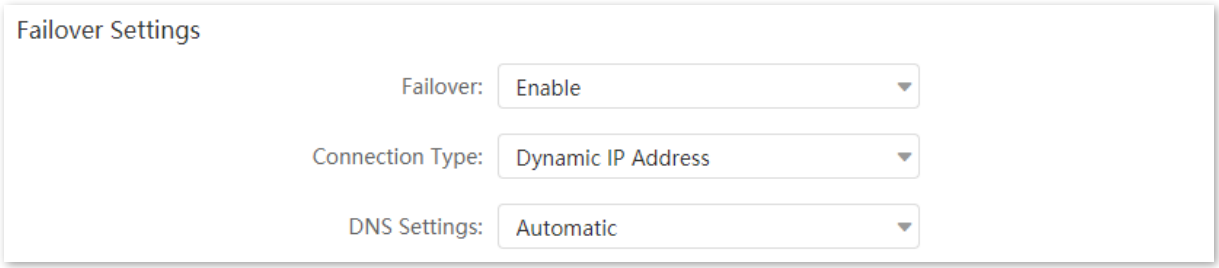
By configuring the Failover function, you can set parameters of the internet connection mode other than the current one. If the internet access under the current internet connection mode fails, the router switches to the other mode automatically, therefore ensuring an uninterrupted internet access for 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 configuration page, log in to the web UI of the router, and 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.



4.3.2 Example of setting up Failover connection

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

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

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

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

Configuring procedures:

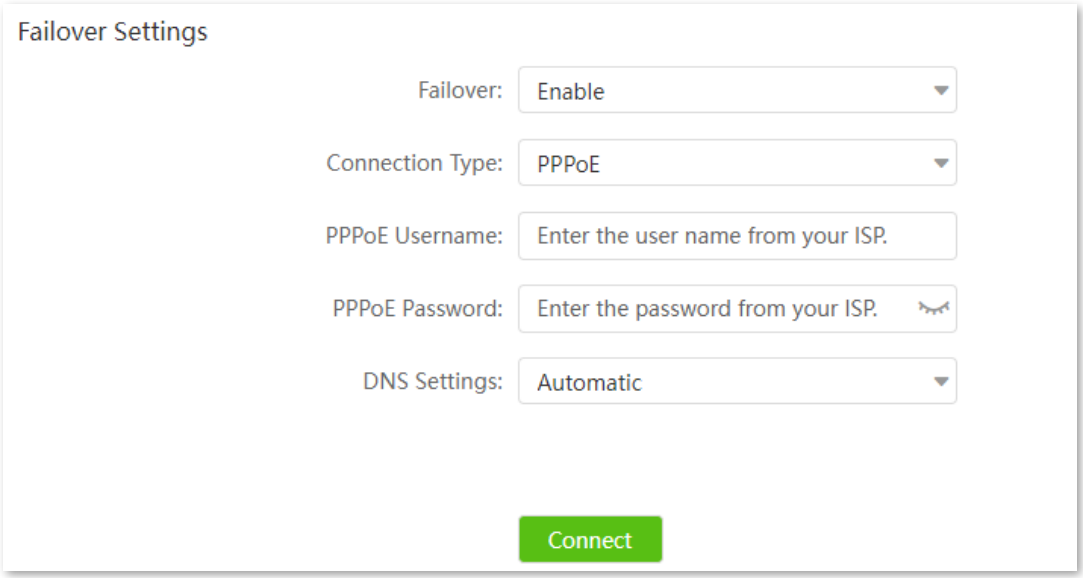
Step 1 Connect the **WAN/LAN** port of the router to the LAN port of your smart home gateway.

Step 2 Log in to the web UI of the router, and navigate to **Internet Settings**.

Step 3 Enable the **Failover** function.

Step 4 Set **Connection Type** to **PPPoE**, and enter the **PPPoE Username** and **PPPoE Password** provided by your ISP.

Step 5 Click **Connect**.



---End

When the configuration is completed, the router is connected to the internet successfully and you can enjoy uninterrupted internet access guaranteed by both the broadband and SIM card.

5 Wi-Fi settings

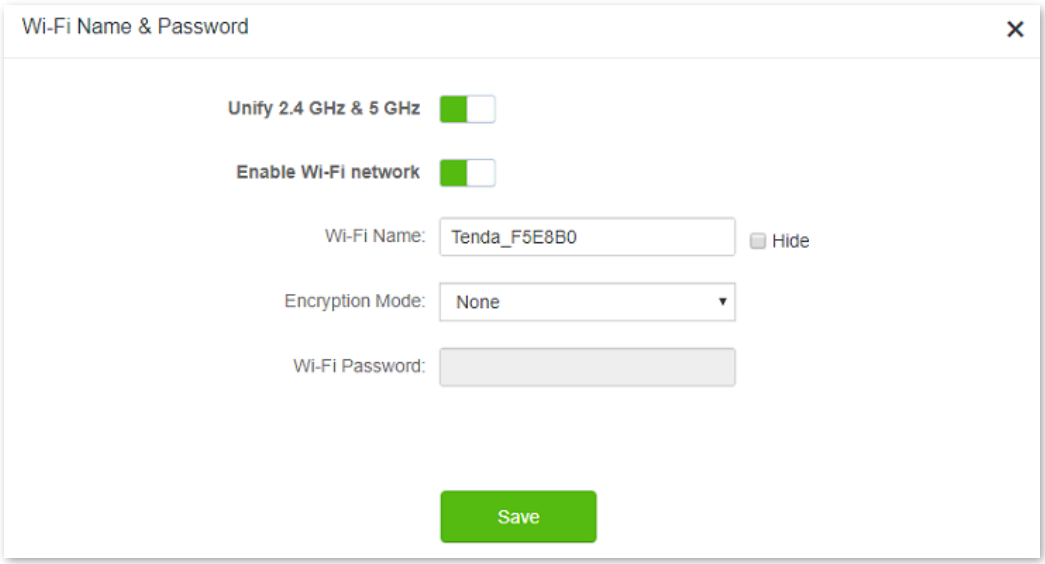
This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with product models. The actual product prevails.

5.1 Wi-Fi name & password

5.1.1 Overview

To access the configuration 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 and password.



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 enabled by default. When this function is enabled, the 2.4 GHz and 5 GHz Wi-Fi networks share the same SSID and password. Devices connected to the Wi-Fi network will use the network with better connection quality automatically.

Parameter	Description
Enable Wi-Fi Network	Used to enable or disable the Wi-Fi networks of the router.
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 (SSID) 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, including: - **None**: It indicates that the Wi-Fi network is not encrypted and any clients can access the network without a password. This option is not recommended as it leads to low network security. - **WPA-PSK**: The network is encrypted with WPA-PSK/AES, which has a better compatibility than WPA2-PSK. - **WPA2-PSK**: The network is encrypted with WPA2-PSK/AES, which has a higher security level than WPA-PSK. - **WPA/WPA2-PSK (recommended):** It indicates that WPA-PSK and WPA2-PSK are adopted to encrypt the network, providing both security and compatibility.
Wi-Fi Password	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.

5.1.2 Set separate names for 2.4 GHz and 5 GHz Wi-Fi

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

Configuring procedure:

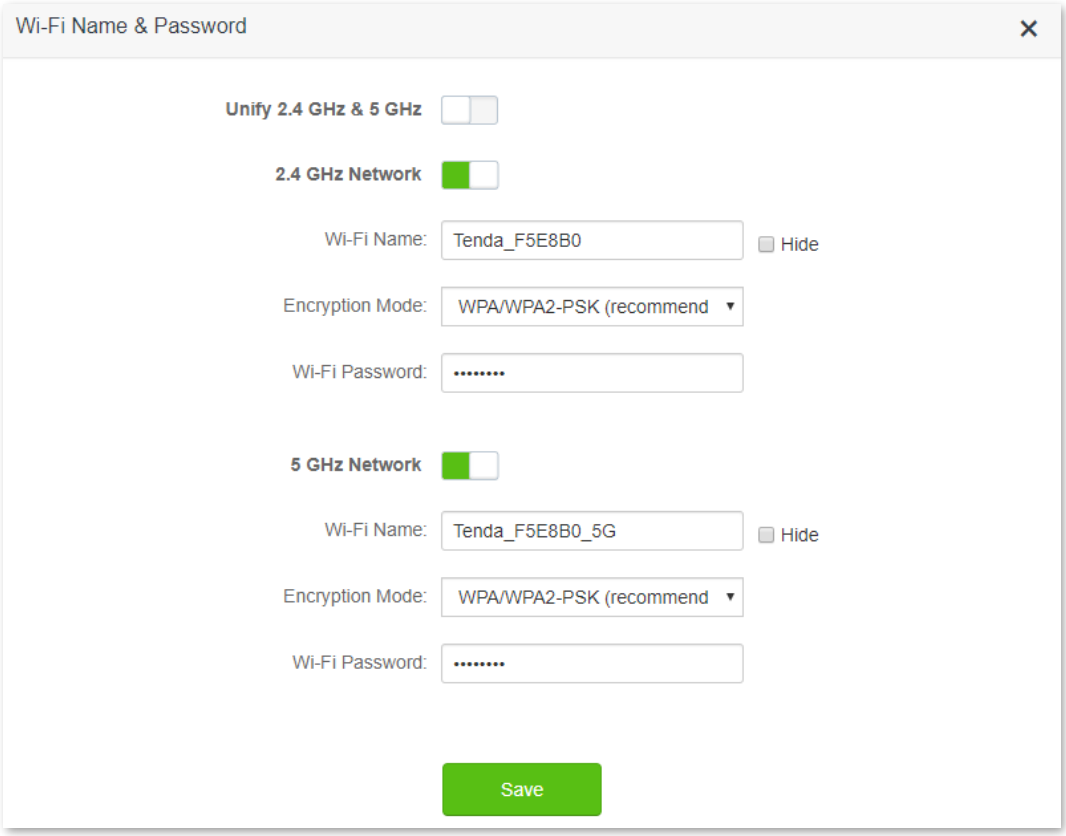
Step 1 Log in to the web UI of the router.

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

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

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

Step 5 Click **Save**.



---End

When the configuration is completed, you can connect to the Wi-Fi networks of the router to access the internet.

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

Assume that you want to change the 2.4 GHz Wi-Fi name and password to **John_Doe_2.4GHz** and **Tenda+Wireless24,** and the 5 GHz Wi-Fi name and password to **John_Doe_5GHz** and **Tenda+Wireless5**. Both networks adopt **WPA/WPA2-PSK (recommended)** as the encryption type.

Configuring procedure:

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

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

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

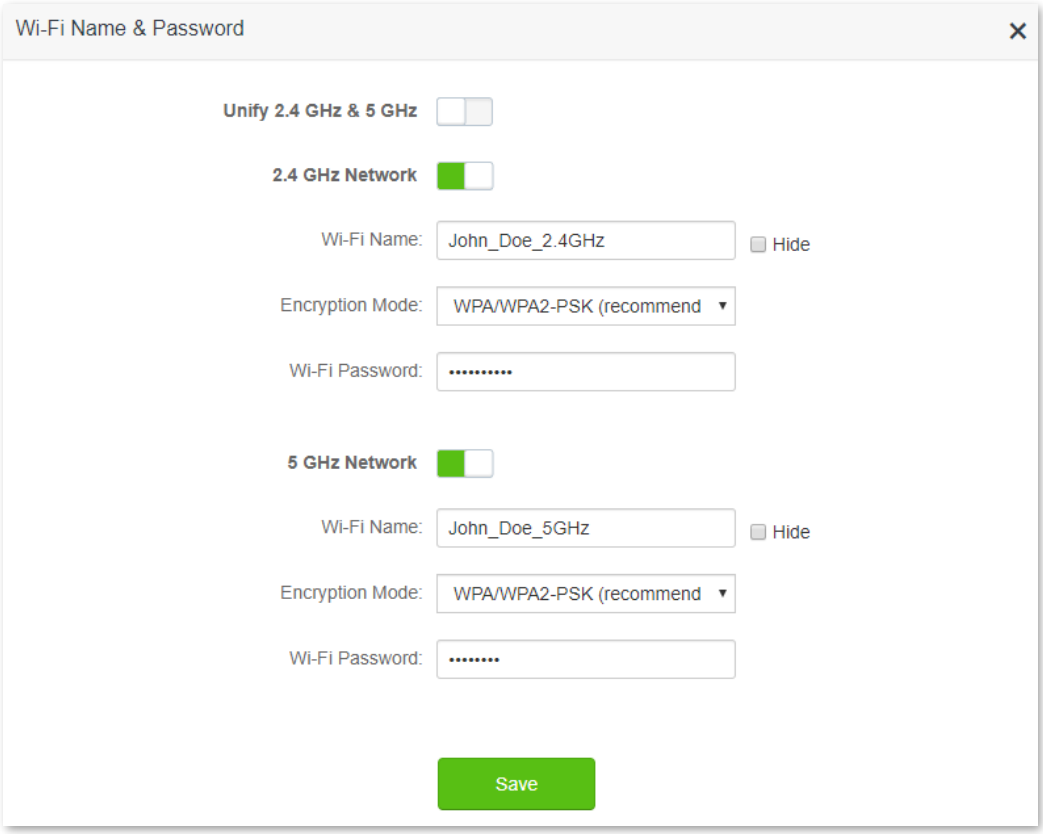
Step 4 Change the parameters of the 2.4 GHz network.

1. Change the **Wi-Fi Name** of the 2.4 GHz network, which is **John_Doe_2.4GHz** in this example.
2. Choose an **Encryption Mode**, which is **WPA/WPA2-PSK (recommended)** in this example.
3. Change the **Wi-Fi Password** of the 2.4 GHz network, which is **Tenda+Wireless24** in this example.

Step 5 Change the parameters of the 5 GHz network.

1. Change the **Wi-Fi Name** of the 5 GHz network, which is **John_Doe_5GHz** in this example.
2. Choose an **Encryption Mode**, which is **WPA/WPA2-PSK (recommended)** in this example.
3. Change the **Wi-Fi Password** of the 5 GHz network, which is **Tenda+Wireless5** in this example.

Step 6 Click **Save**.



---End

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

5.1.4 Hide the Wi-Fi network

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

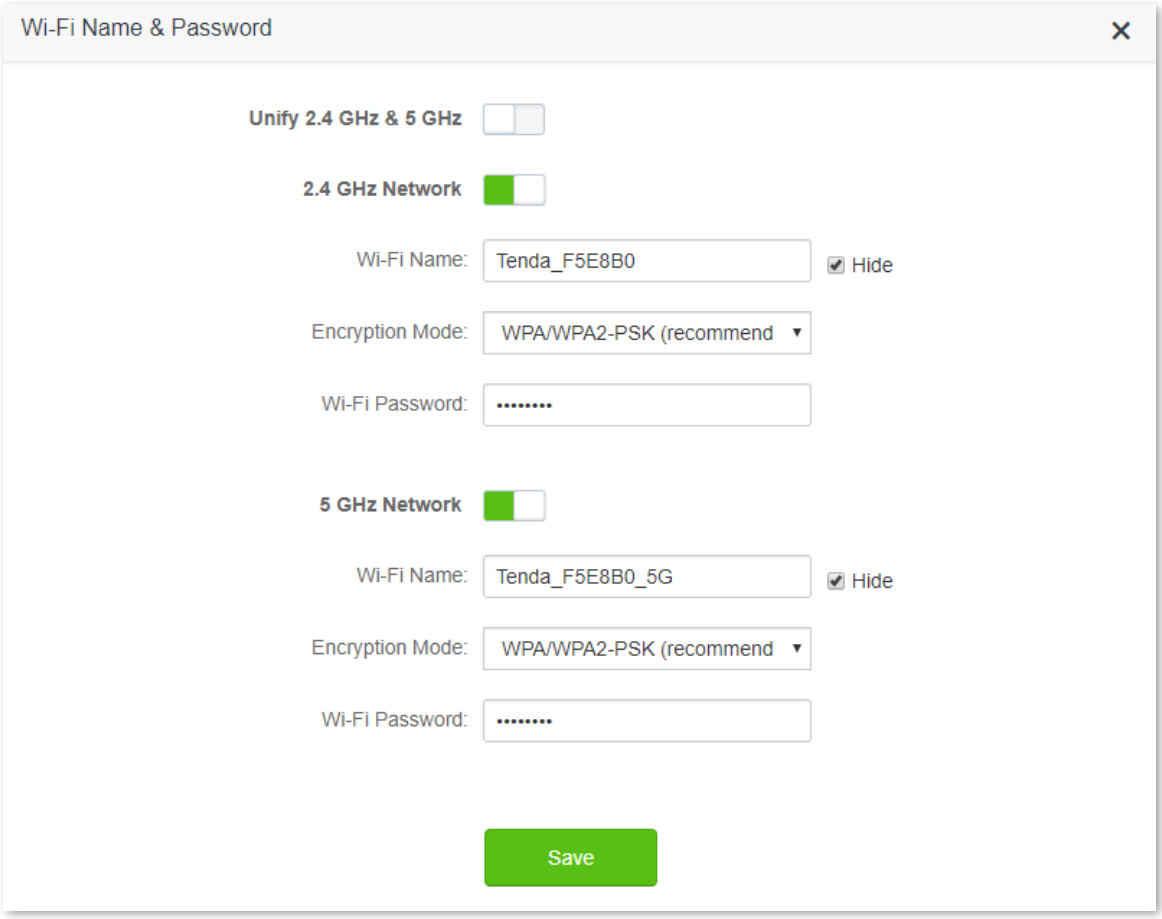
Configuring procedure:

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

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

Step 3 Tick **Hide** of the target network.

Step 4 Click **Save**.



---End

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

5.1.5 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.

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

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

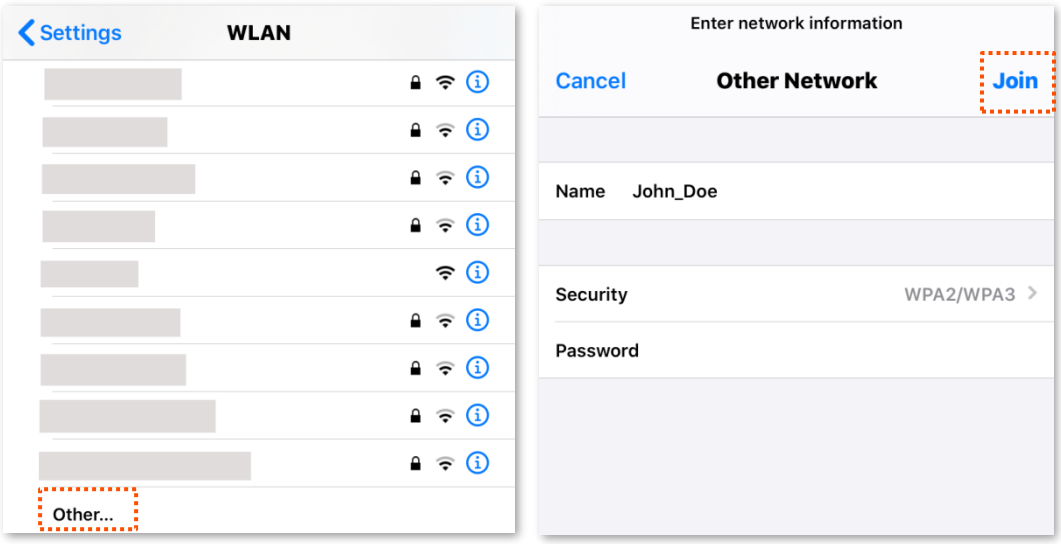
Step 2 Enable **WLAN**.

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

Step 4 Enter the Wi-Fi name and password, which are **John_Doe** and **Tenda+Wireless245** in this example.

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

Step 6 Tap **Join**.



---End

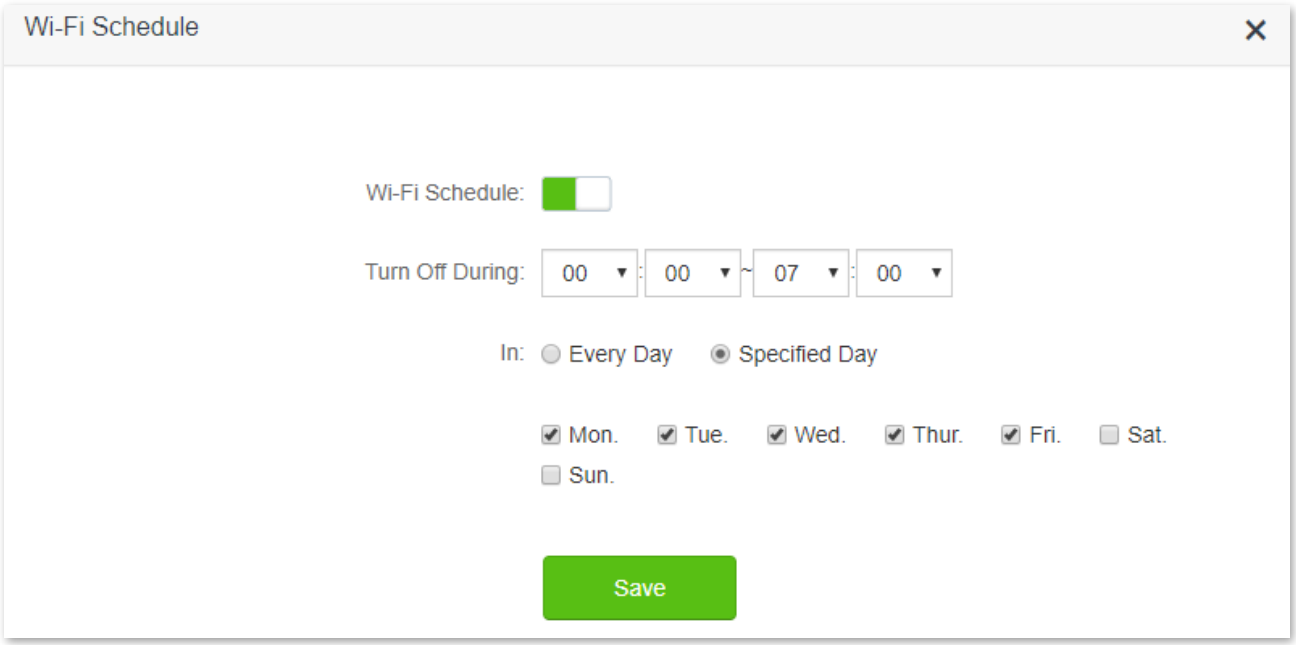
When the configuration is completed, you can connect to the hidden Wi-Fi network to access the internet.

5.2 Wi-Fi schedule

5.2.1 Overview

This Wi-Fi Schedule function allows you to disable the Wi-Fi networks of the router at specified period. By default, this function is disabled.

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



NOTE

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

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.
In	Specifies the day(s) on which the Wi-Fi networks are disabled during the specified period.

5.2.2 Example of configuring Wi-Fi schedule

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

Configuring procedure:

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

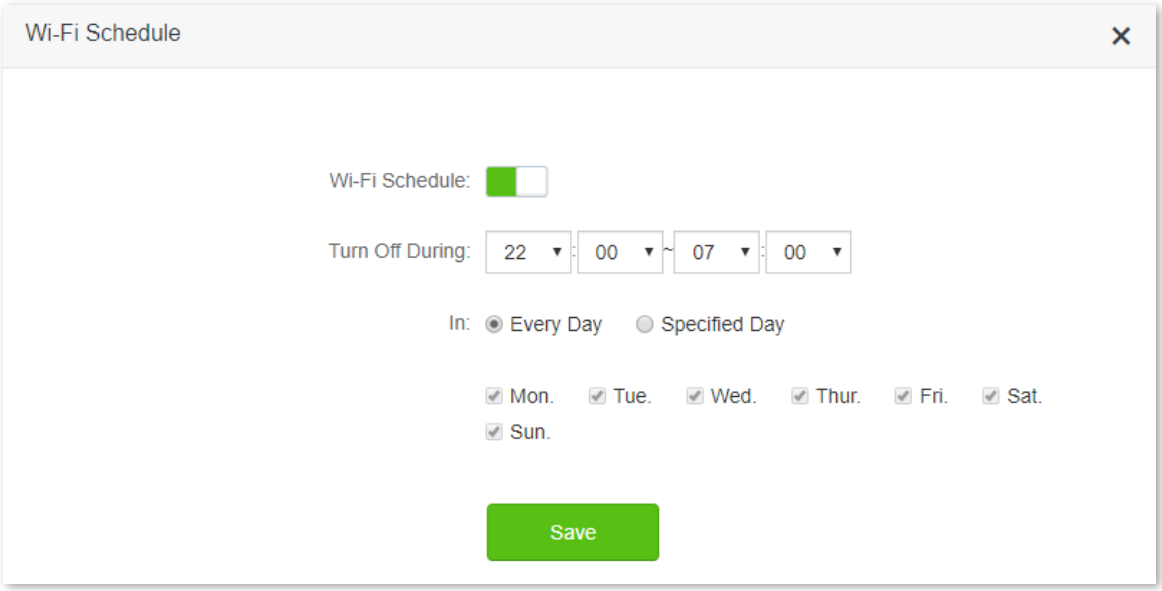
Step 2 Navigate to **Wi-Fi Settings** > **Wi-Fi Schedule.**

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

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

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

Step 6 Click **Save**.



---End

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

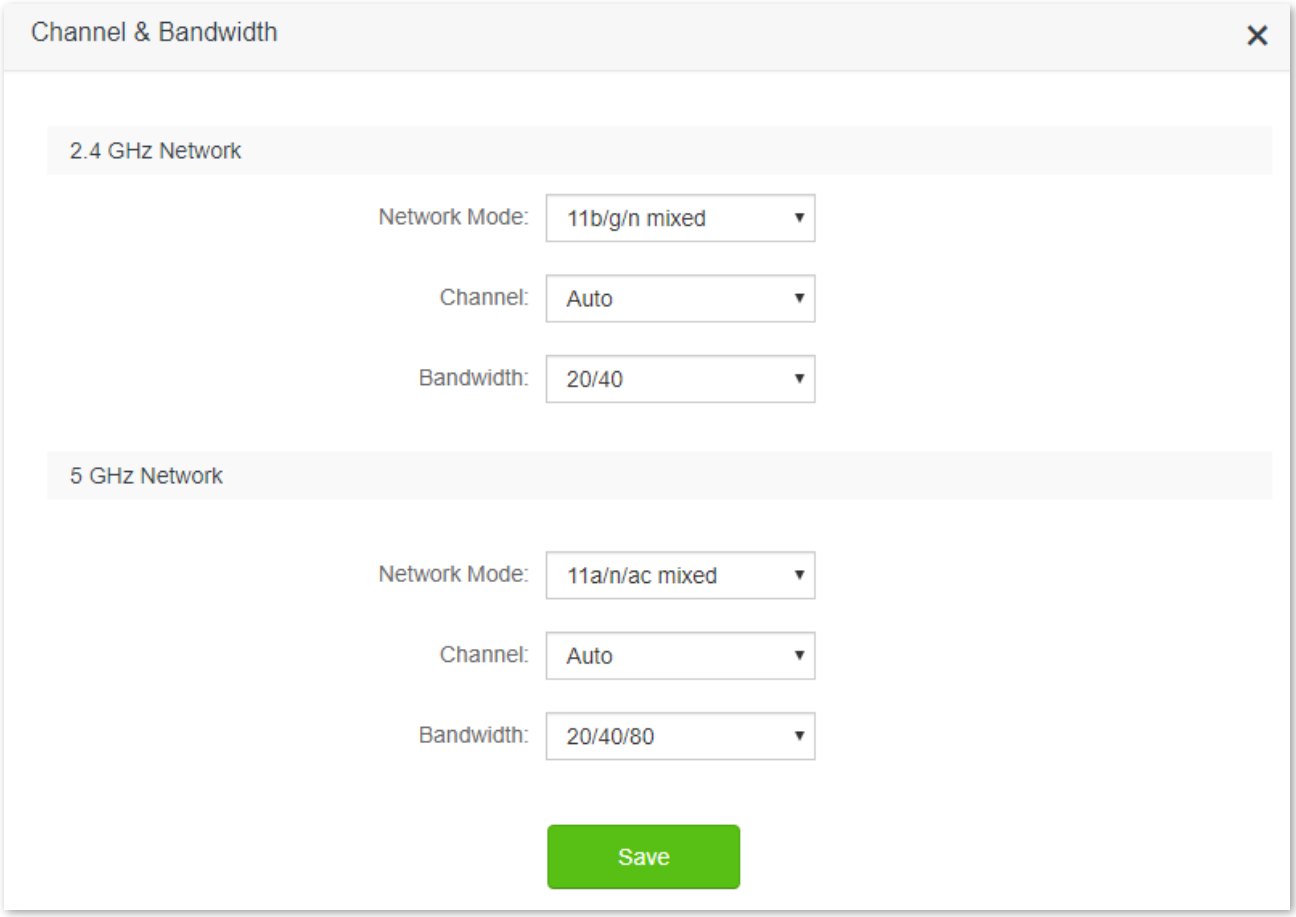
5.3 Channel & bandwidth

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

To access the configuration page, log in to the web UI of the router, and 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.



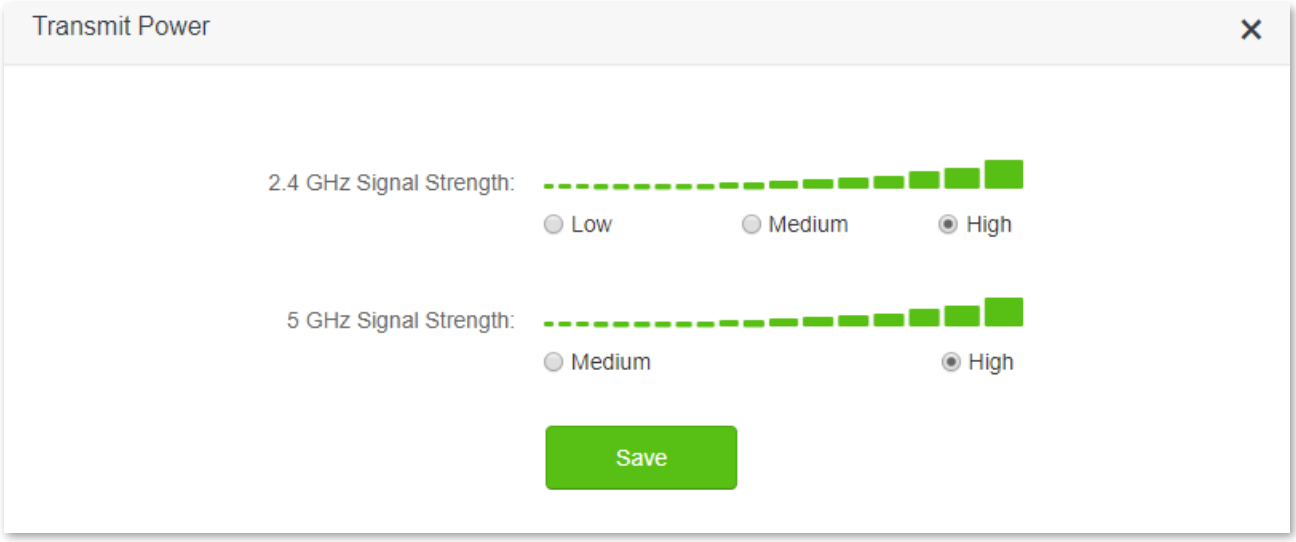
Parameter description

Parameter	Description
Network Mode	Specifies various protocols adopted for wireless transmission. 2.4 GHz Wi-Fi network includes11n, 11b/g mixed and 11b/g/n mixed modes. - **11n**: It indicates that devices compliant with IEEE 802.11n protocol can connect to the 2.4 GHz Wi-Fi network of the router. - **11b/g mixed**: It indicates that devices compliant with IEEE 802.11b or IEEE 802.11g protocol can connect to the 2.4 GHz Wi-Fi network of the router. - **11b/g/n mixed**: It indicates that all devices can connect to the router if they are compliant with IEEE 802.11b or IEEE 802.11g protocol, or work at 2.4 GHz with IEEE 802.11n protocol. 5 GHz Wi-Fi network includes11ac, 11a/n/ac mixed modes. - **11ac**: It indicates that devices complaint with IEEE 802.11ac protocol can connect to the router. - **11a/n/ac mixed**: It indicates that all devices that are compliant with IEEE 802.11a or IEEE 802.11ac protocol, or work at 5 GHz with IEEE 802.11n protocol can connect to the router.
Channel	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.

5.4 Transmit power

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

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



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

5.5 WPS

5.5.1 Overview

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

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

NOTE

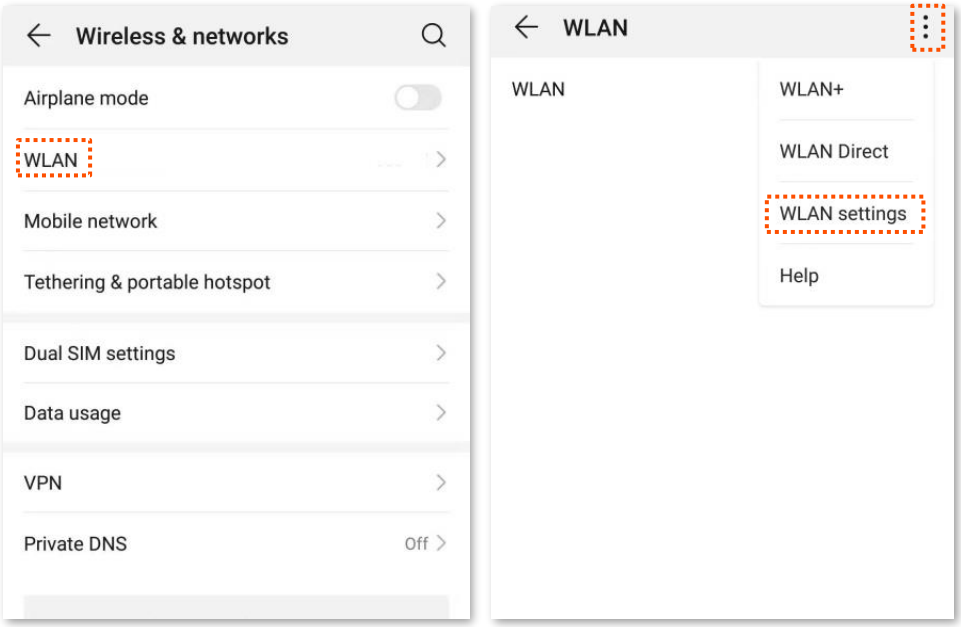
This function is only applicable to WPS-enabled wireless devices.

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

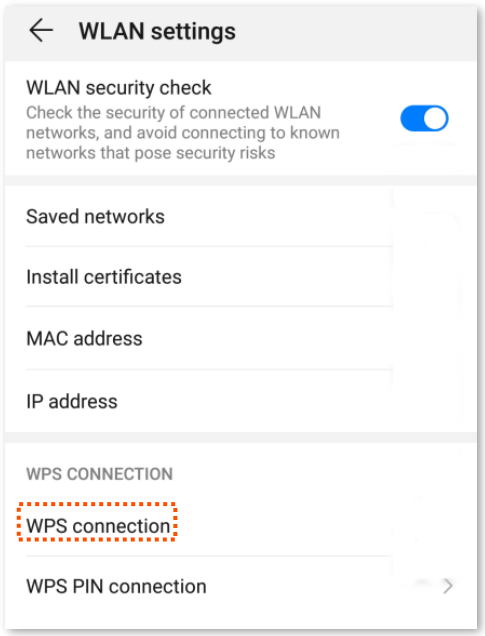
Step 1 Find the **RST/WPS** button on the rear panel of the router, and hold it down for 1 to 3 seconds. The Wi-Fi indicator blinks slow.

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

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

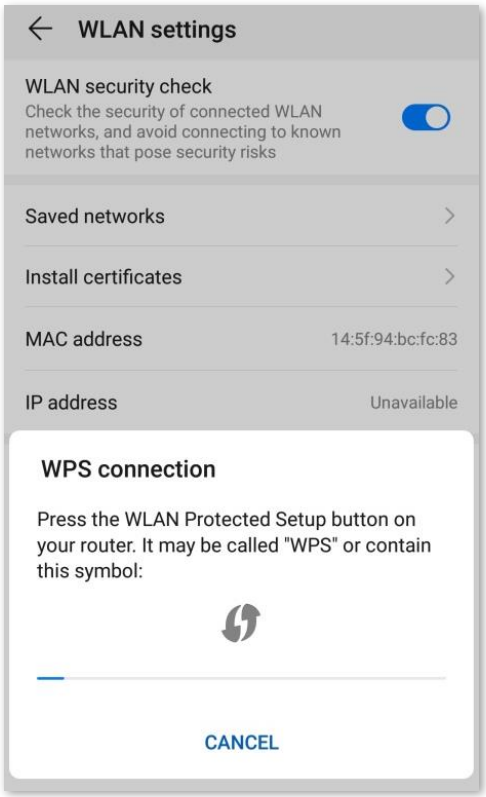


4. Choose **WPS connection**.



---End

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



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

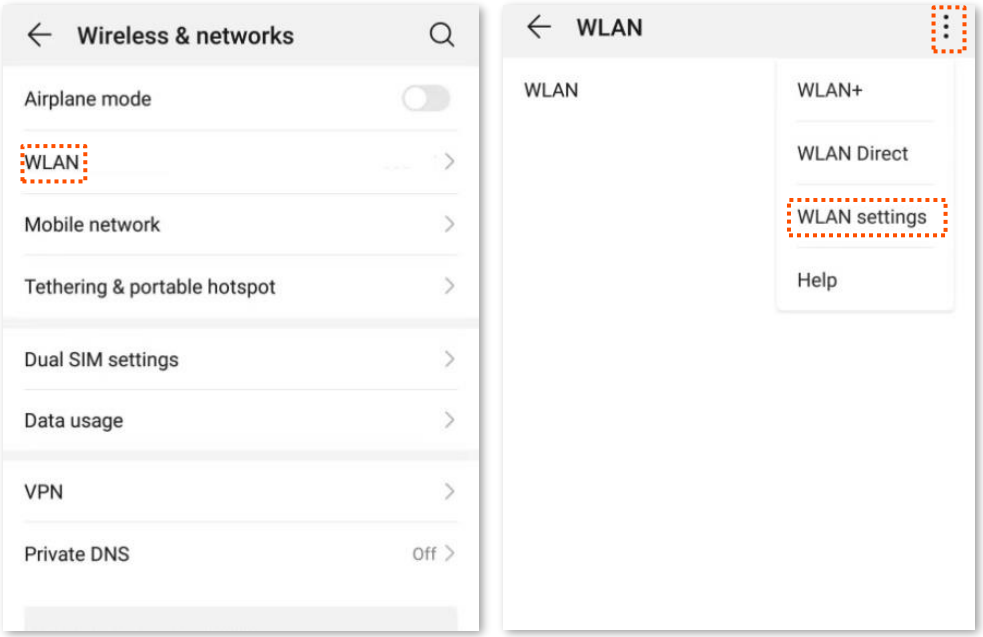
Step 1 Log in to the web UI of the router.

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

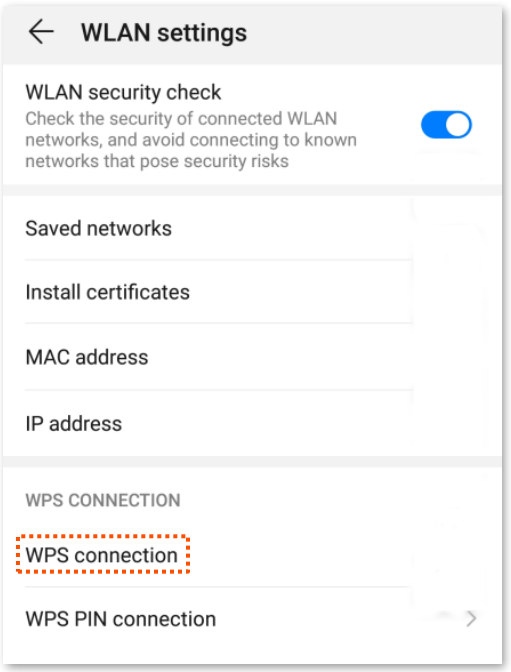
Step 3 Click Click Here below **Method 1**.

Step 4 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**.

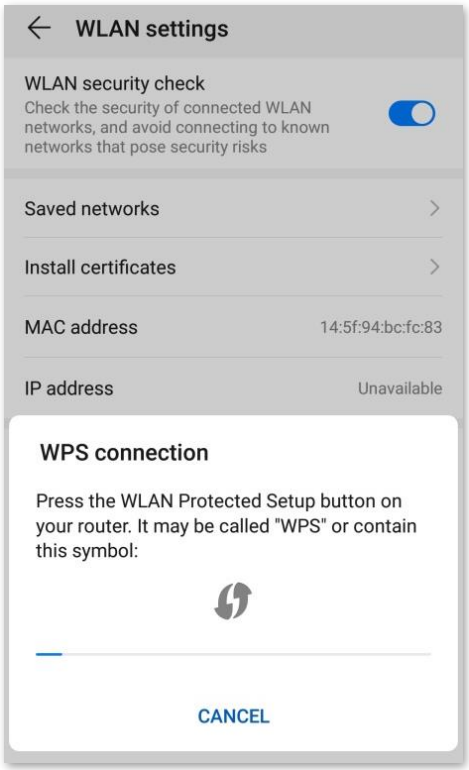


3. Choose **WPS connection**.



---End

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



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

NOTE

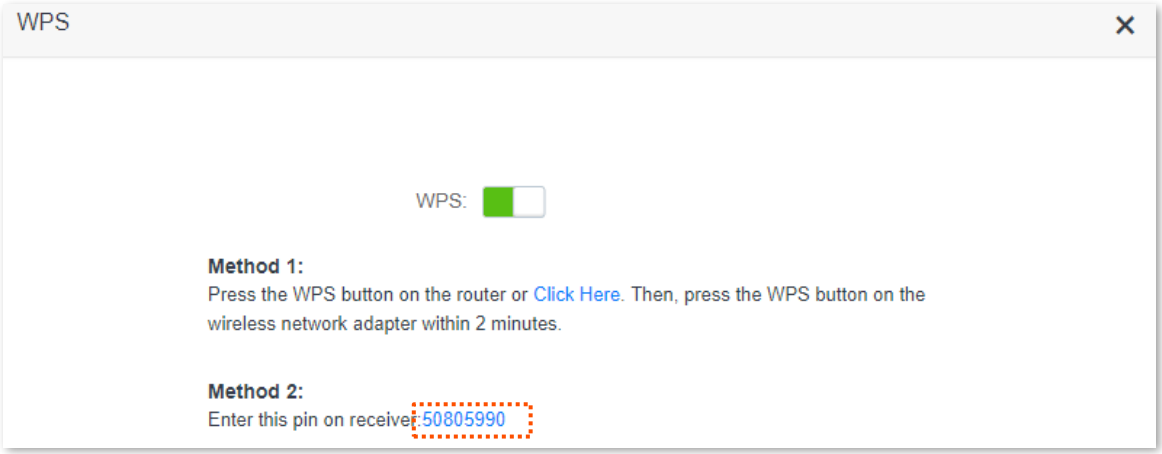
It is available only when wireless devices such as Wi-Fi network adapters can perform WPS negotiation by entering the PIN code. Please refer to the user guide of the Wi-Fi network adapter for configuration details.

Configuring procedure:

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

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

Step 3 Find the PIN code of the router. The PIN code is shown under **Method 2**.



Step 4 Enter the PIN code on the wireless device that can perform WPS negotiation using the PIN code.

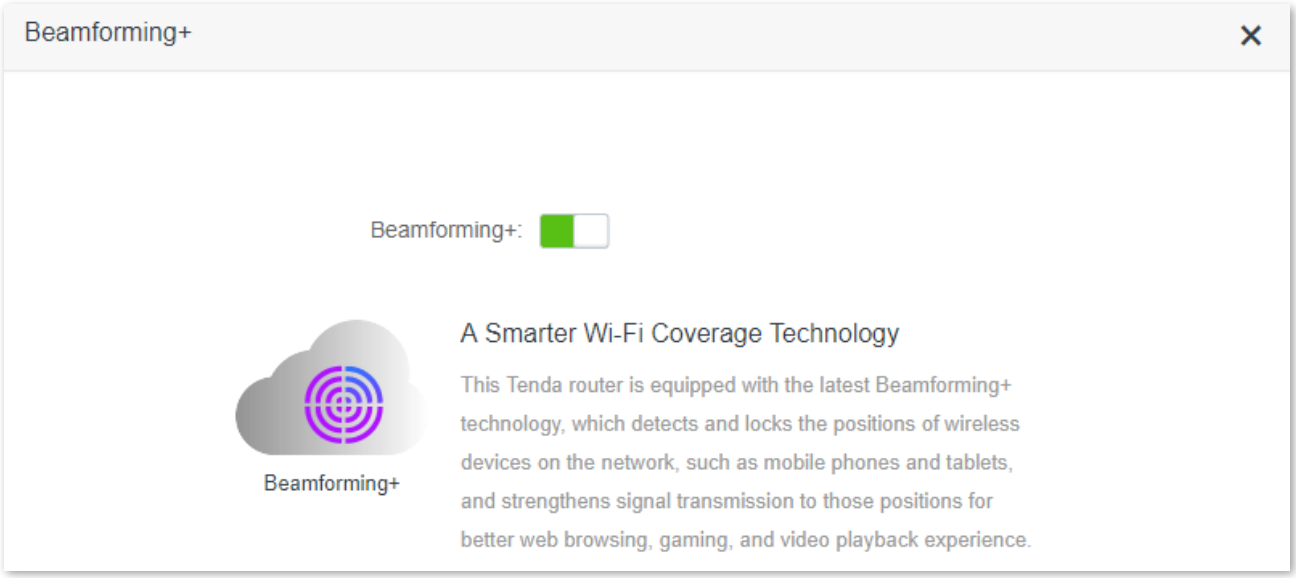
---End

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

5.6 Beamforming+

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

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



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

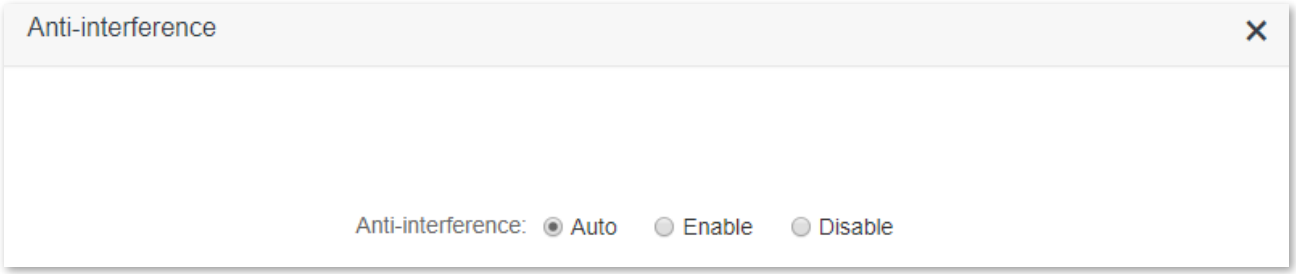
The following figure shows the wireless transmission when Beamforming+ is disabled.

5.7 Anti-interference

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

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

The default setting is **Auto**.



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

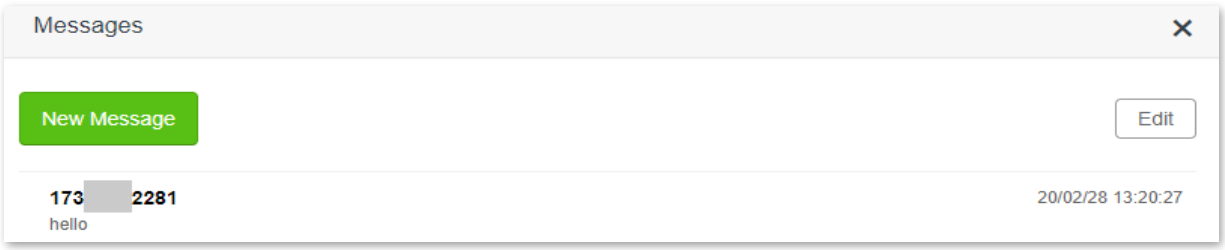
6 SMS

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with product models. The actual product prevails.

6.1 Manage SMS messages

On this page, you can send, receive, and delete SMS messages in the web UI of the router.

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



6.1.1 Send SMS messages

Send SMS messages to a new smartphone number

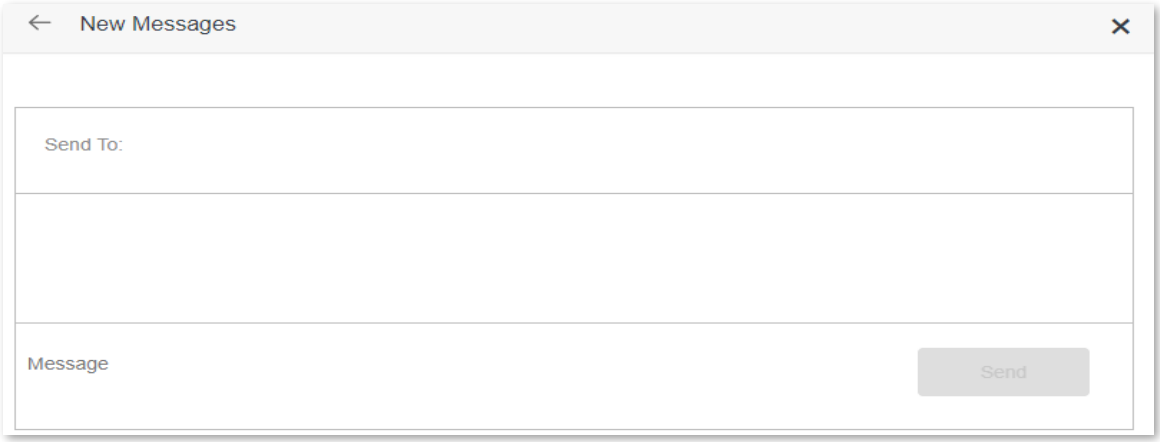
Step 1 Log in to the web UI of the router.

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

Step 3 Click **New Message**.

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

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



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

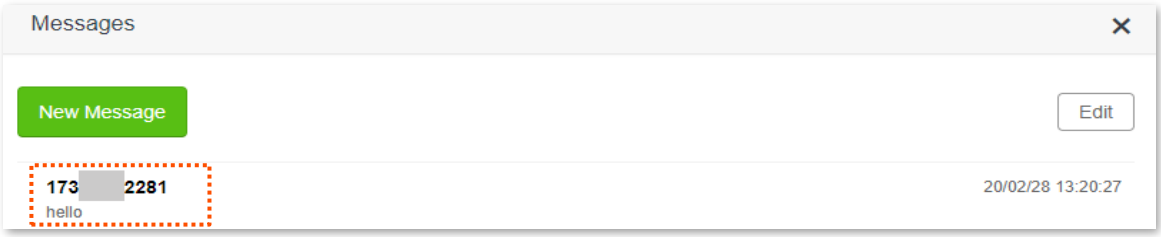
---End

Send messages to an existing smartphone number

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

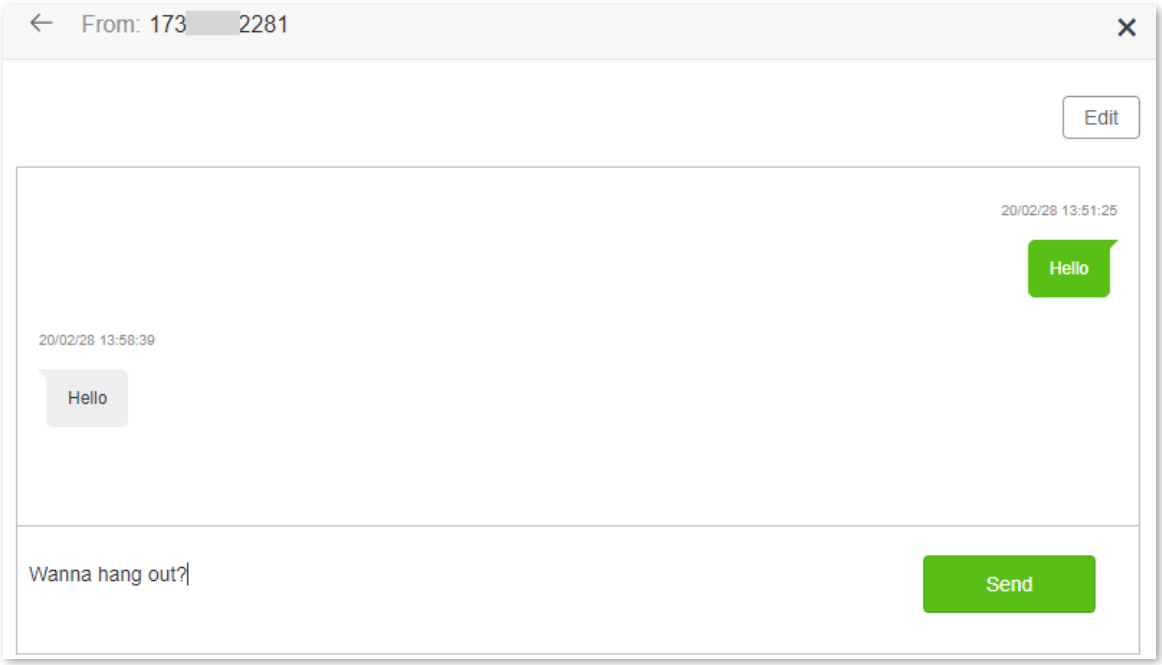
Step 2 Navigate to **SMS** > **Messages.**

Step 3 Click the targeted smartphone number.



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

Step 5 Click **Send**.



---End

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

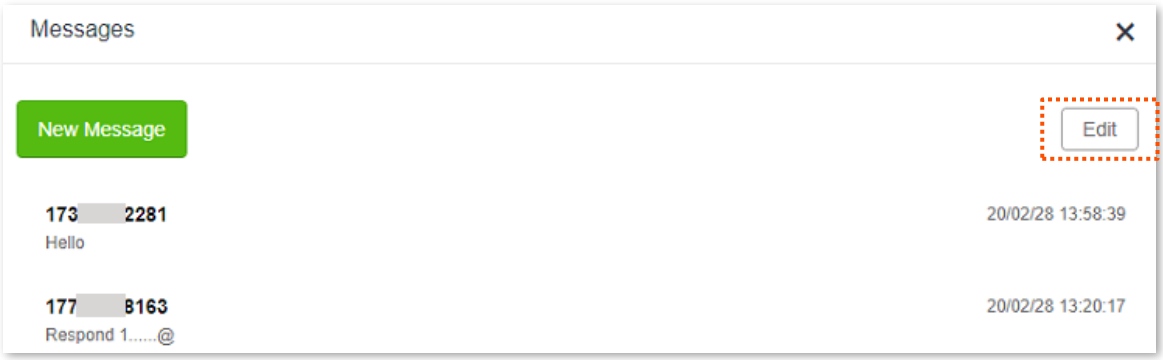
6.1.2 Delete SMS messages

Delete all messages of the same smartphone numbers

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

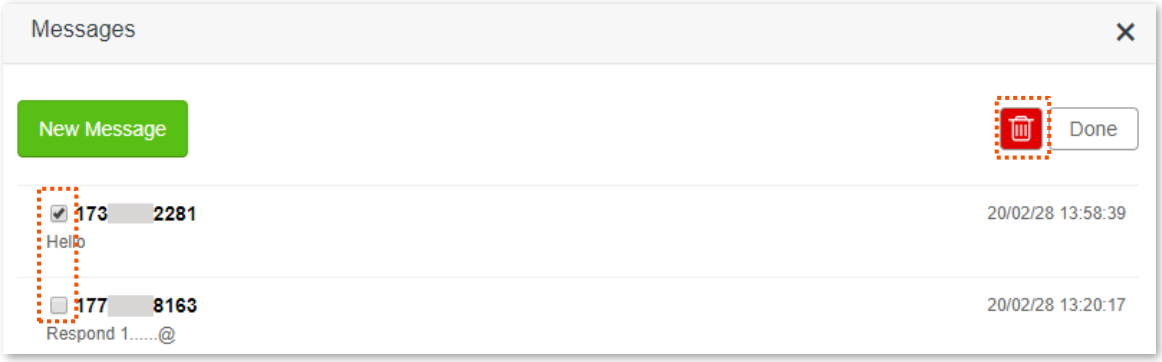
Step 2 Navigate to **SMS** > **Messages.**

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



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

Step 5 Click .



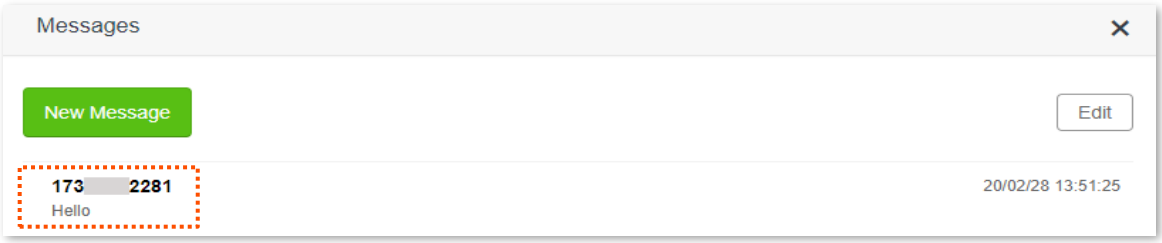
---End

Delete certain messages of the same smartphone number

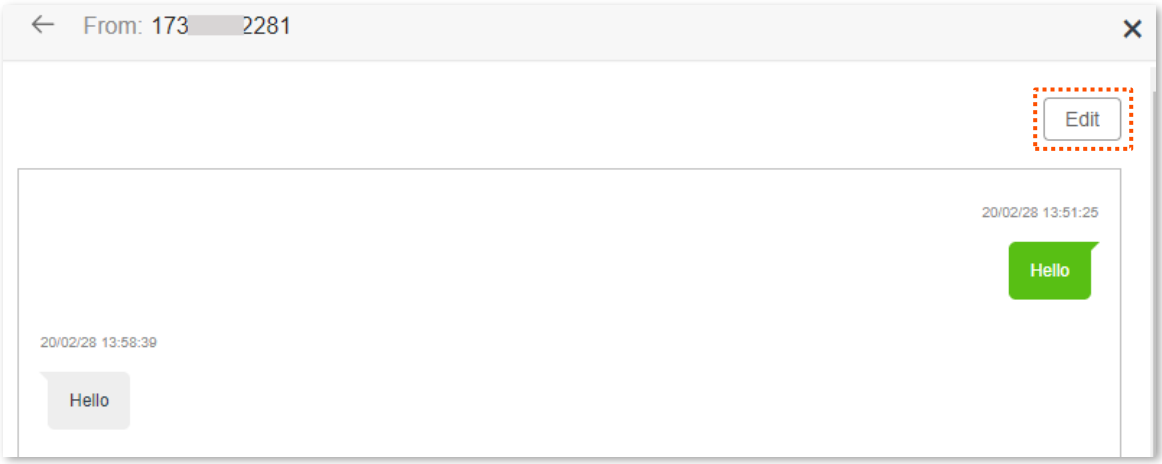
Step 1 Log in to the web UI of the router.

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

Step 3 Click the targeted smartphone number.

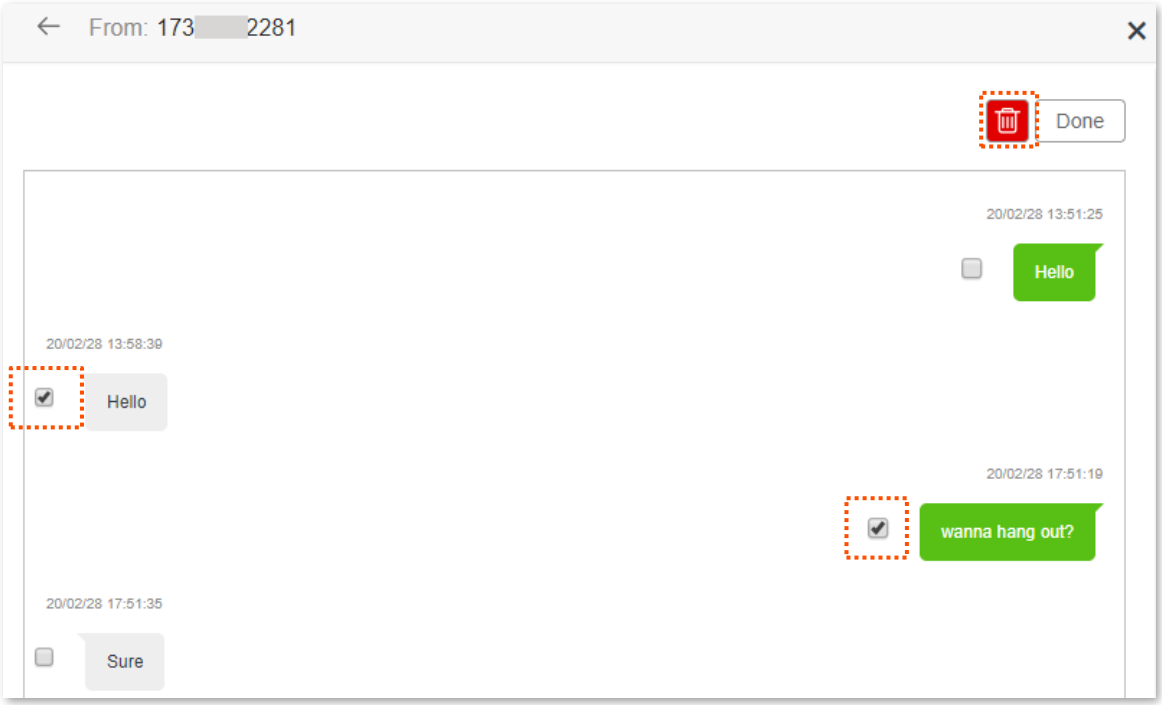


Step 4 Click **Edit**.



Step 5 Select the messages to be deleted.

Step 6 Click  .



---End

6.2 Set the message center number

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

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

Configuring procedure:

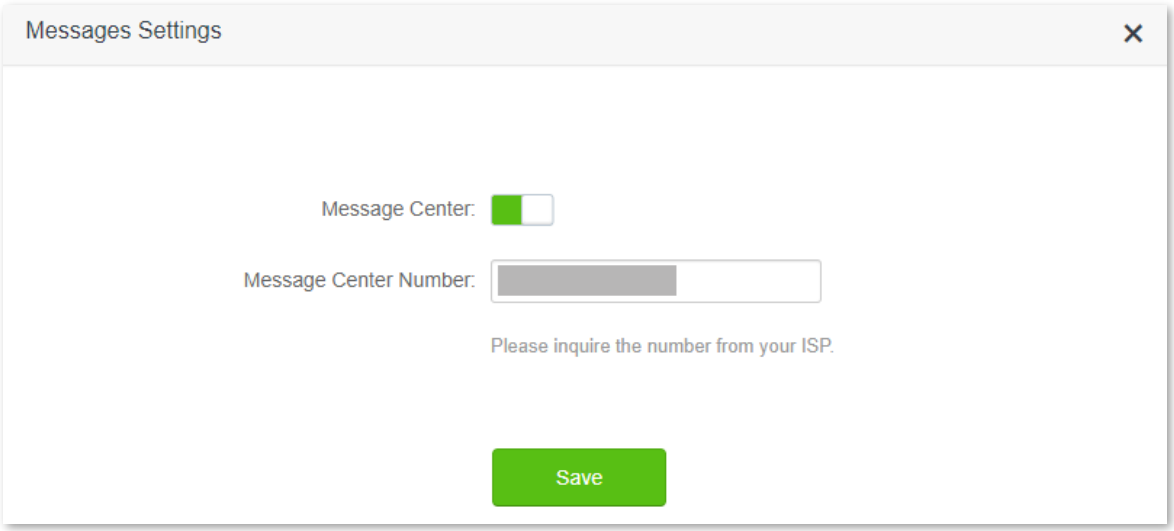
Step 1 Log in to the web UI of the router.

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

Step 3 Enable **Message Center**. The following figure is for reference only.

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

Step 5 Click **Save**.



---End

NOTE

Contact your ISP for correct message center number.

6.3 Inquire information by sending USSD commands

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

NOTE

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

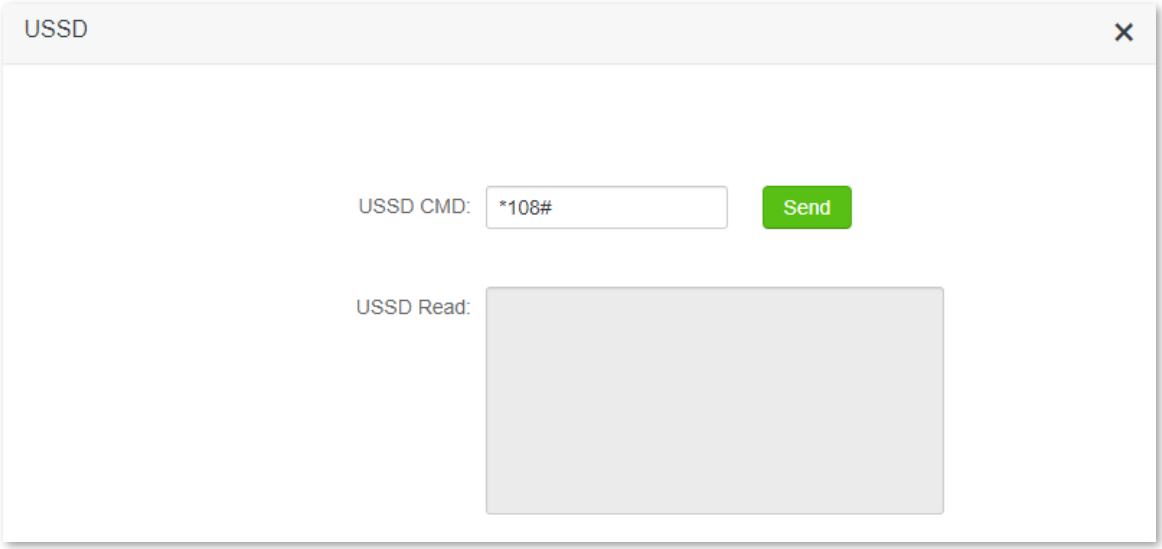
Configuring procedure:

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

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

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

Step 4 Click **Send**.



---End

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

7 Guest network

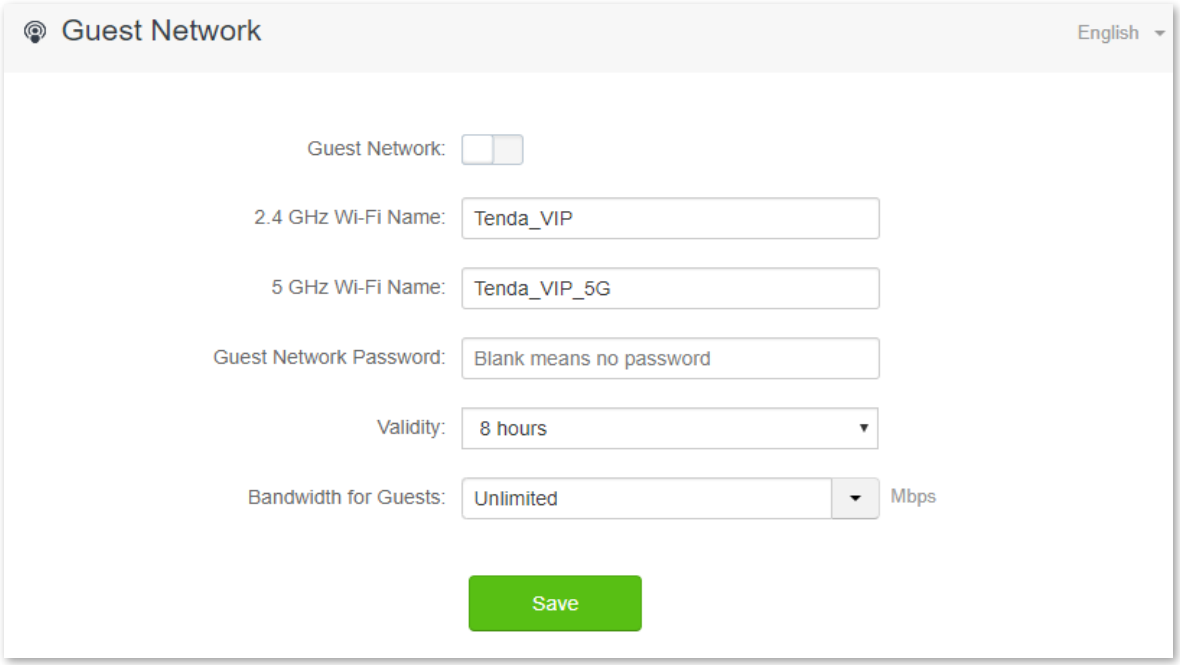
This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with product models. The actual product prevails.

7.1 Overview

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

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

To access the configuration page, log in to the web UI of the router, and navigate to the **Guest Network**. This function is disabled by default.



Parameter description

Parameter	Description
Guest Network	Used to enable or disable the guest network function.
2.4 GHz Wi-Fi Name	Specify the Wi-Fi name of the router's guest network. By default, **Tenda_VIP** is for the 2.4 GHz Wi-Fi network and **Tenda_VIP_5G** for the 5 GHz Wi-Fi network. You can change the SSIDs (Wi-Fi names) as required. To distinguish the guest network from the main network, you are recommended to set different Wi-Fi network names.
5 GHz Wi-Fi Name	
Guest Network Password	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.

7.2 Example of configuring the guest network

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

Requirements: 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

Configuring procedure:

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

Step 2 Navigate to **Guest Network**.

Step 3 Enable the **Guest Network**.

Step 4 Set the **2.4 GHz Wi-Fi Name**, which is **John_Doe** in this example.

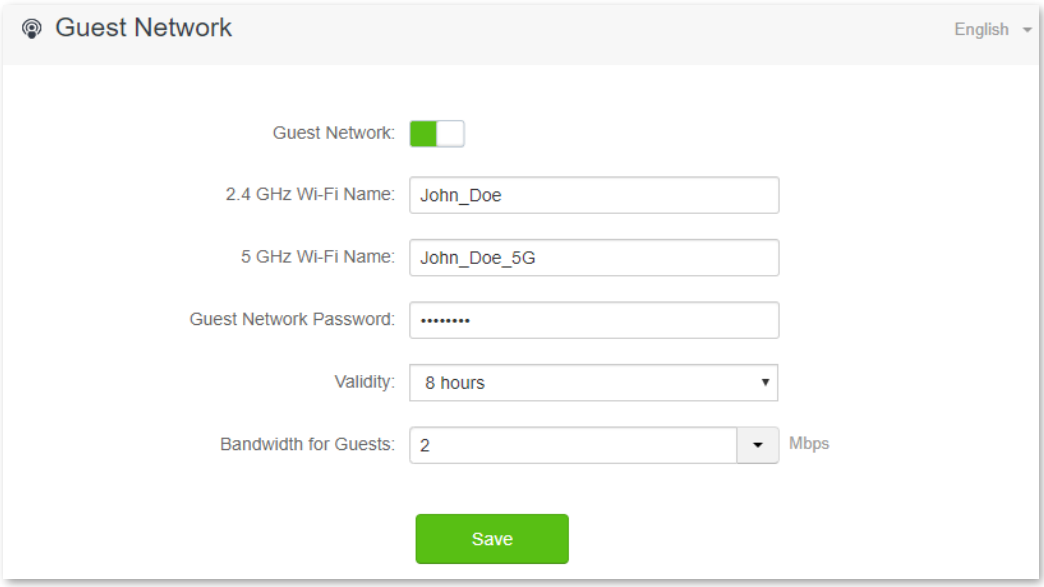
Step 5 Set the **5 GHz Wi-Fi Name**, which is **John_Doe_5G** in this example.

Step 6 Set the **Guest Network Password**, which is **Tenda_12345** in this example.

Step 7 Select a validity time from the **Validity** drop-down box, which is **8 hours** in this example.

Step 8 Set the bandwidth in the **Bandwidth for Guests** drop-down box, which is **2** in this example.

Step 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.

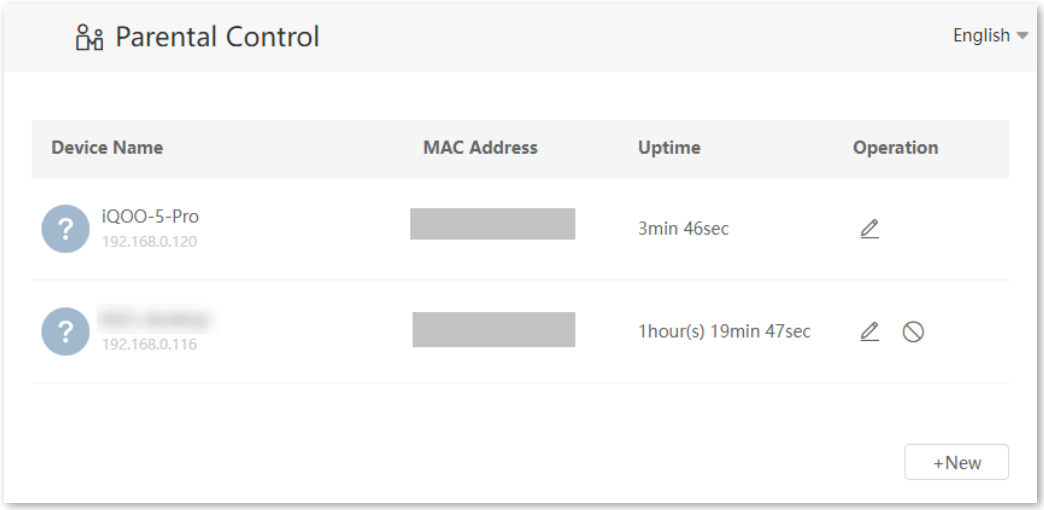
8 Parental control

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with product models. The actual product prevails.

8.1 Overview

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

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

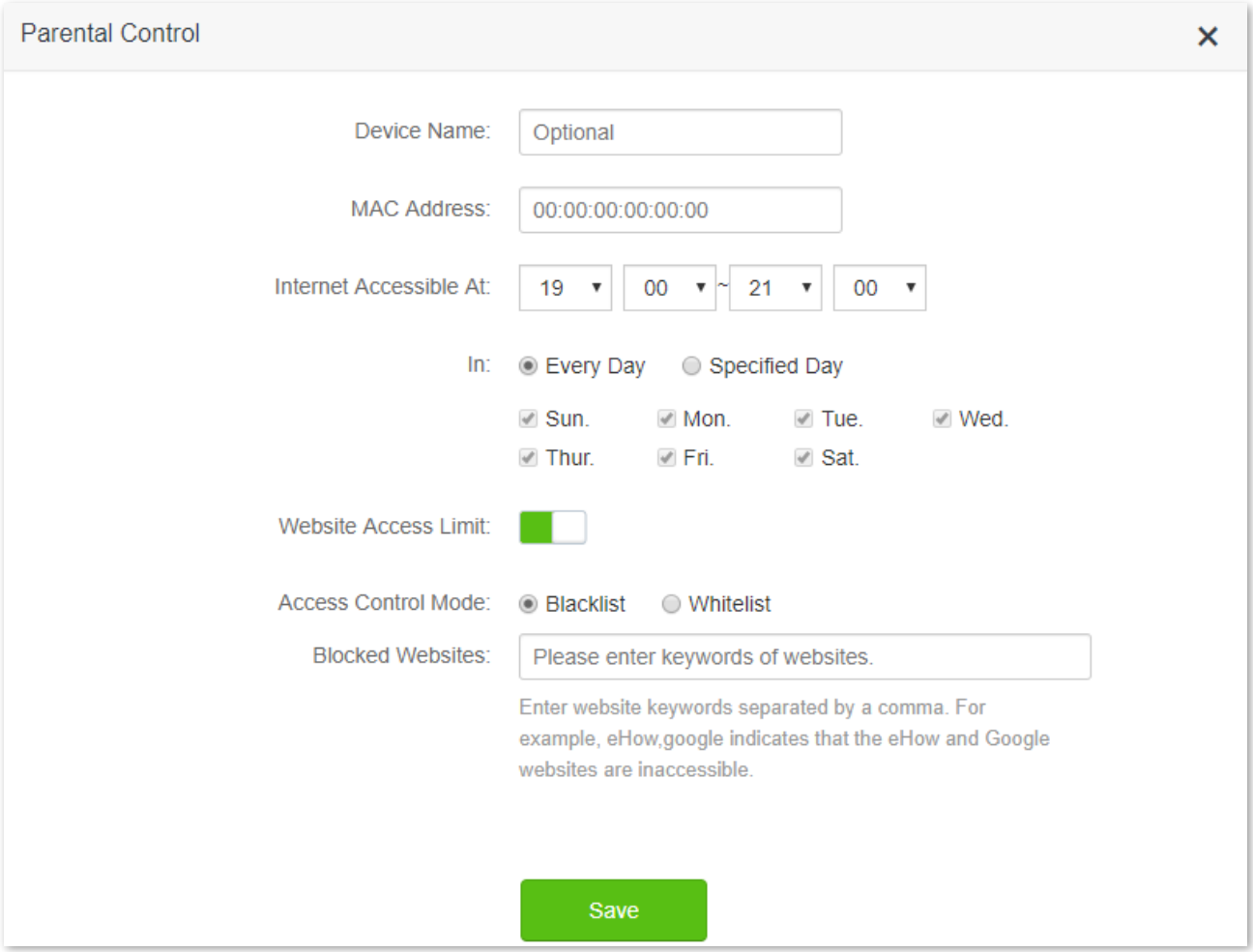


Parameter description

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.

8.2 Configure the parental control rule

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



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.
In	Specifies the days when the rule takes effect.
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	

8.3 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.

Requirements: Websites, such as Facebook, Twitter, Youtube and Instagram, are inaccessible during 8:00 to 22:00 on weekends using the computer in her room, and no internet access is available from 22:00 to 8:00.

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

Configuring procedure:

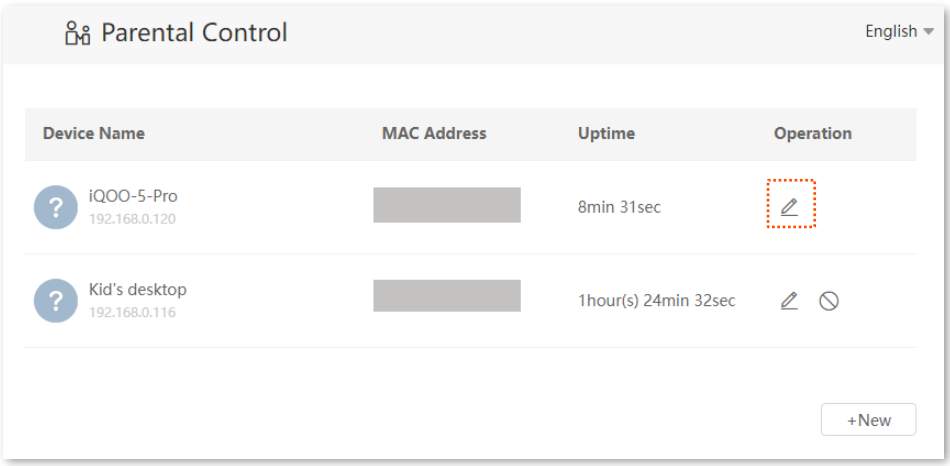
Step 1 Log in to the web UI of the router.

Step 2 Navigate to **Parental Control**.

Step 3 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.



Step 4 Specify the period when the target websites cannot be accessed, which is **8:00 ~ 22:00** in this example.

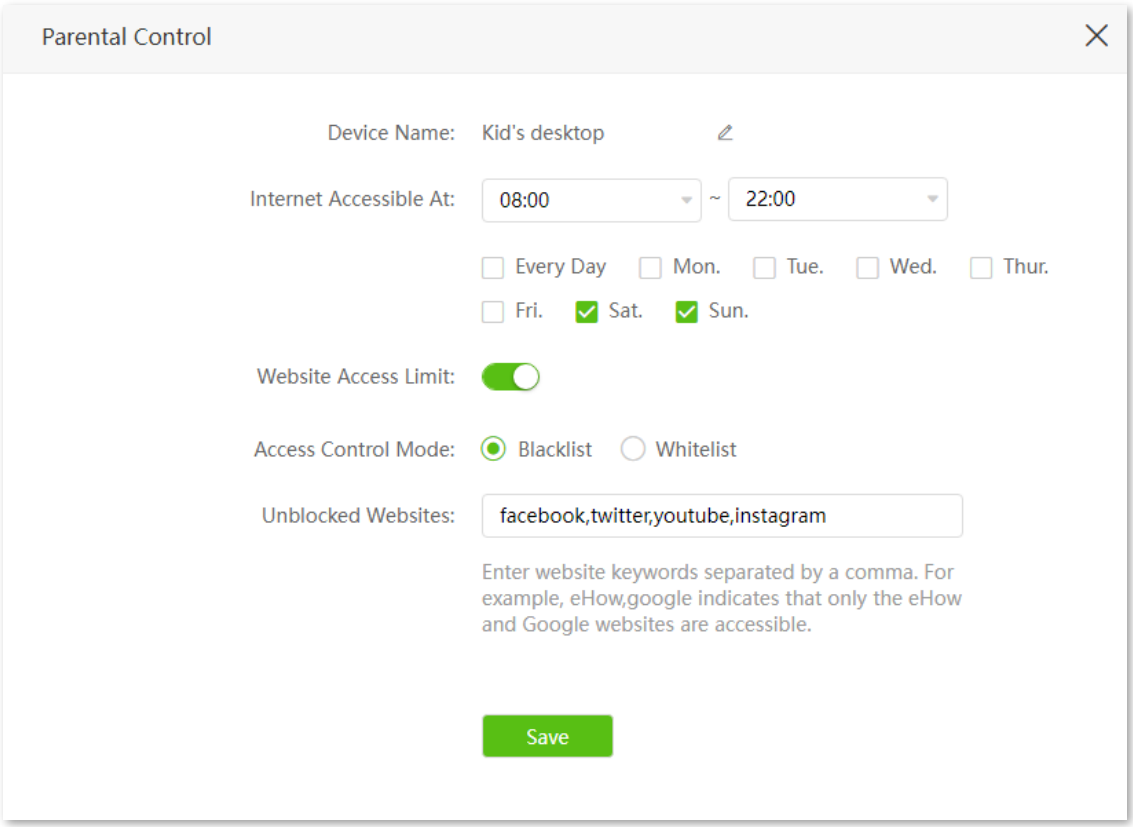
Step 5 Navigate to **Specified Day**, and tick the days when the rule is applied, which are **Sun.** and **Sat.** in this example.

Step 6 Enable **Website Access Limit**.

Step 7 Choose **Blacklist**.

Step 8 Set **Blocked Websites**, which is **facebook,twitter,youtube,instagram** in this example.

Step 9 Click **Save**.



---End

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

9 VPN

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with product models. The actual product prevails.

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.

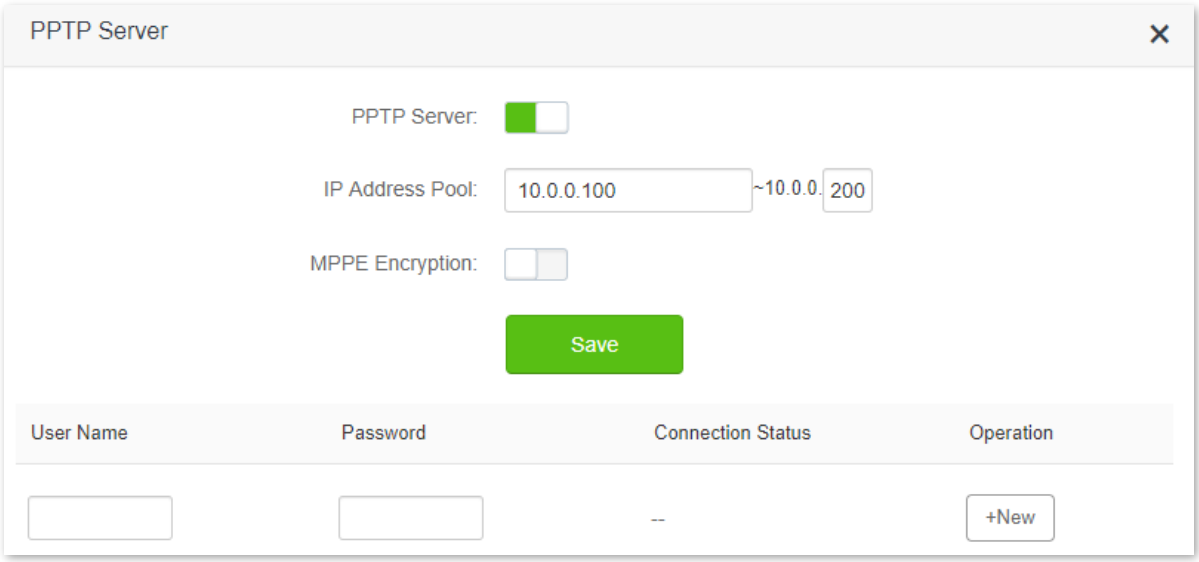
The typology of a VPN network is shown below.

9.1 PPTP server

9.1.1 Overview

This series of routers can function as a PPTP server and accept connections from PPTP clients.

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



Parameter description

Parameter	Description
PPTP Server	Used to enable or disable the PPTP server. When it is enabled, the router functions as a PPTP server, which can accept the connections from PPTP clients.
IP Address Pool	Specifies the range of IP address range within which the PPTP server can assign to PPTP clients. It is recommended to keep the default settings.
MPPE Encryption	Used to enable or disable 128-bit data encryption. The encryption settings should be the same between the PPTP server and PPTP clients. Otherwise, the communication cannot be achieved normally.
User Name Password	Specify the VPN user name and password, which the VPN user needs to enter when making PPTP dial-ups (VPN connections).
Connection Status	Specifies the connection status of the VPN connection.
Operation	The available operations include: +New : Used to add new PPTP user accounts. : Used to disable the PPTP user account. : Used to enable the PPTP user account. : Used to delete the PPTP user account.

9.1.2 Enable internet users to access resources of the LAN

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

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

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

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

TIP

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

Configuring procedure:

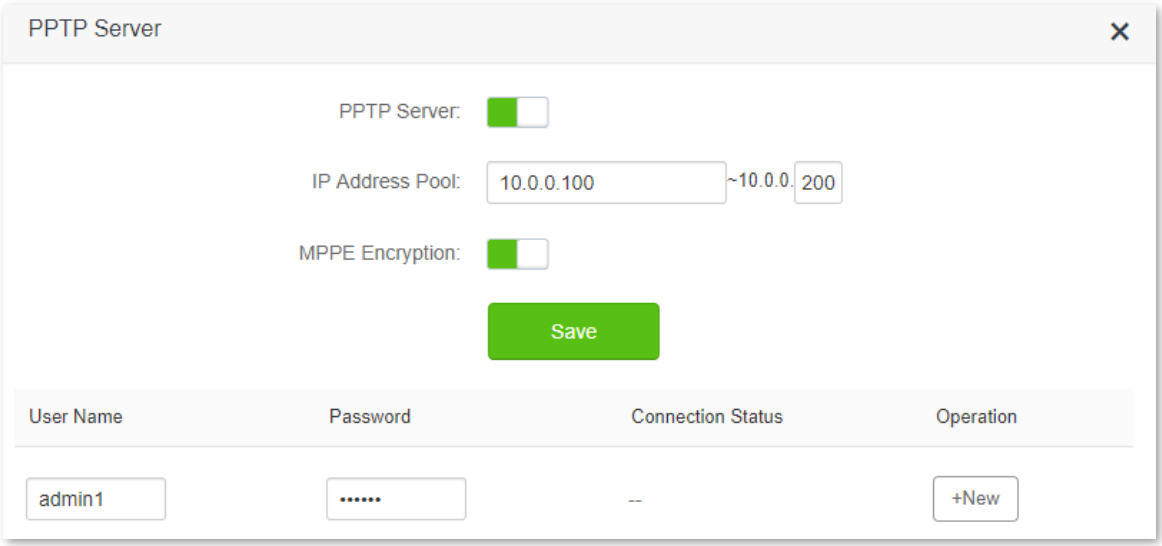
Step 1 Log in to the web UI of the router.

Step 2 Enable the PPTP server function.

1. Navigate to **VPN** > **PPTP Server**.
2. Enable the **PPTP Server**.
3. Enable the **MPPE Encryption**, which means that the encryption digit remains the default value “128”.
4. Click **Save**.

Step 3 Add PPTP user name and password.

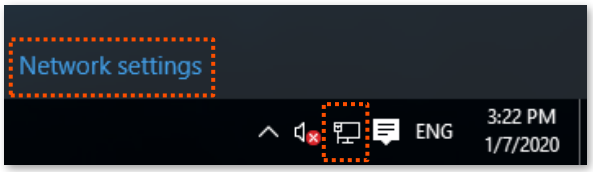
1. Set the **User Name** and **Password** of the PPTP server, which are **admin1** in this example.
2. Click **+New**.



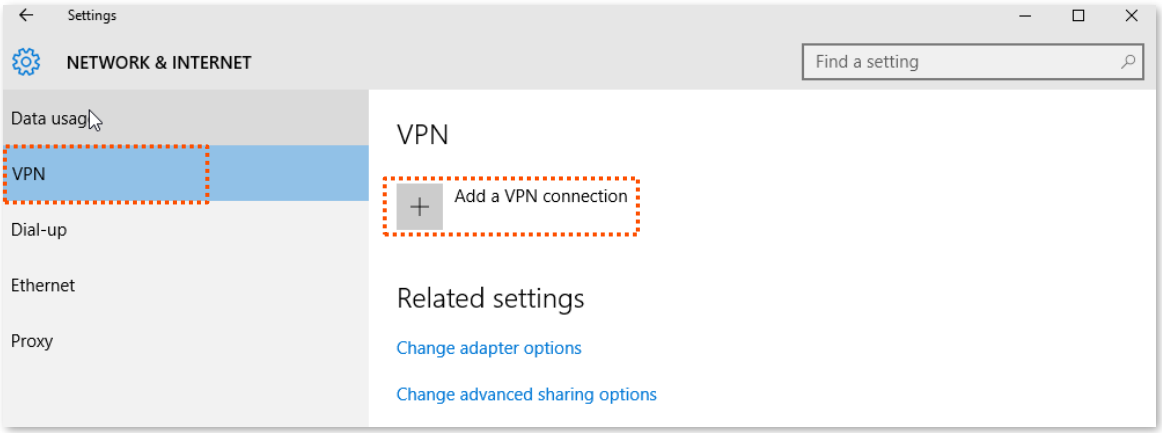
---End

When the configuration is completed, internet users can access the FTP server by following these steps:

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



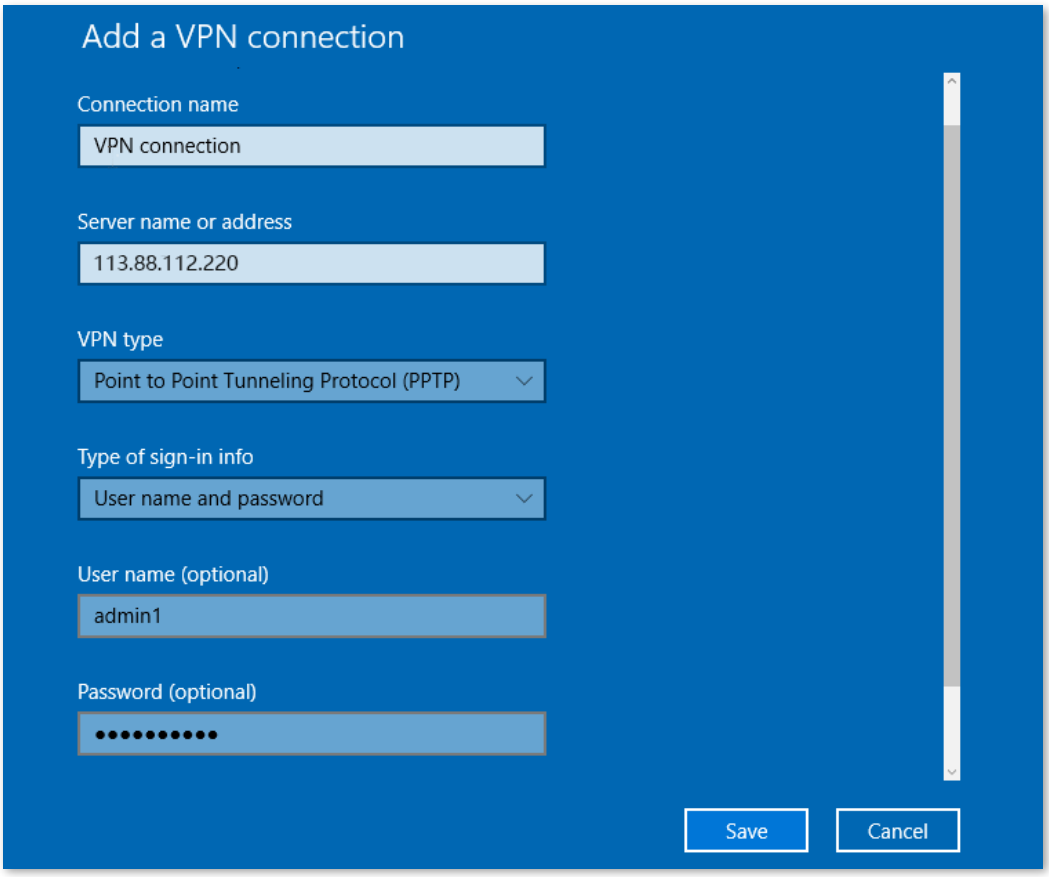
Step 2 Choose **VPN** on the left side, and click **Add a VPN connection**.



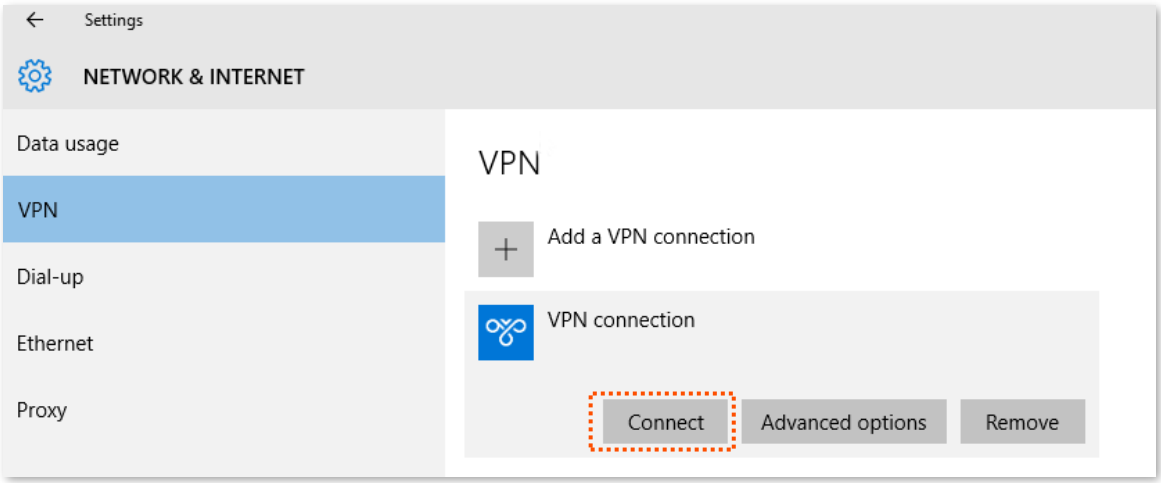
Step 3 Configure the VPN parameters.

1. Enter a connection name, such as **VPN connection**.
2. Enter the server address, which is **113.88.112.220** in this example.

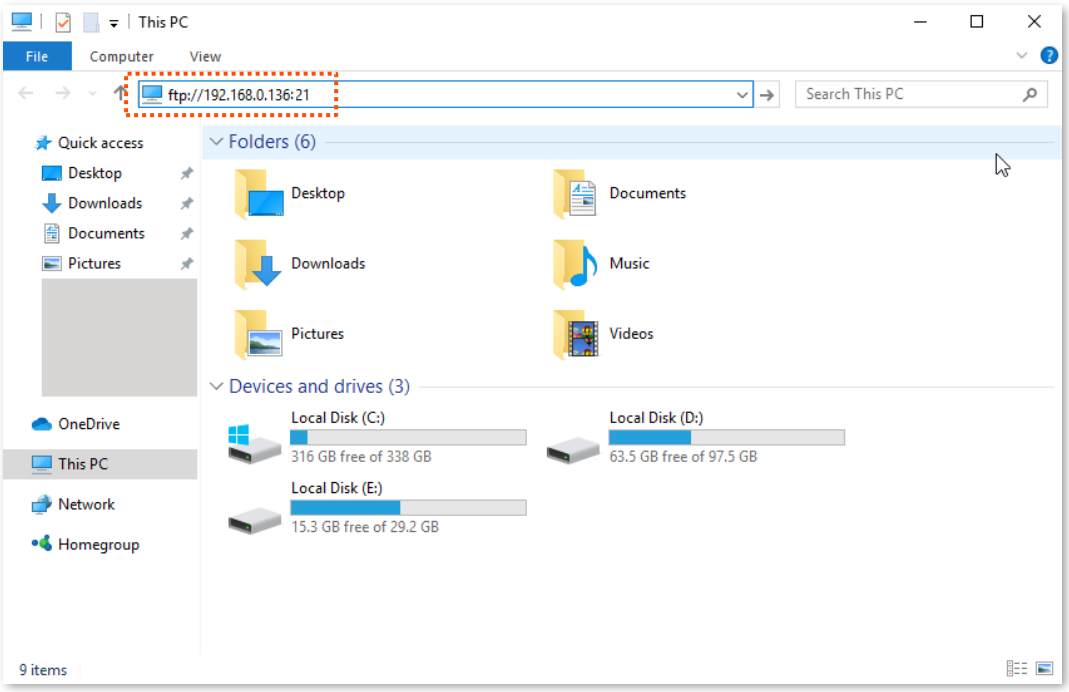
3. Select a VPN type, which is **Point to Point Tunneling Protocol (PPTP)** in this example.
4. Select a type of sign-in info, which is **User name and password** in this example.
5. Enter the user name and password, which are both **admin1** in this example.
6. Click **Save**.



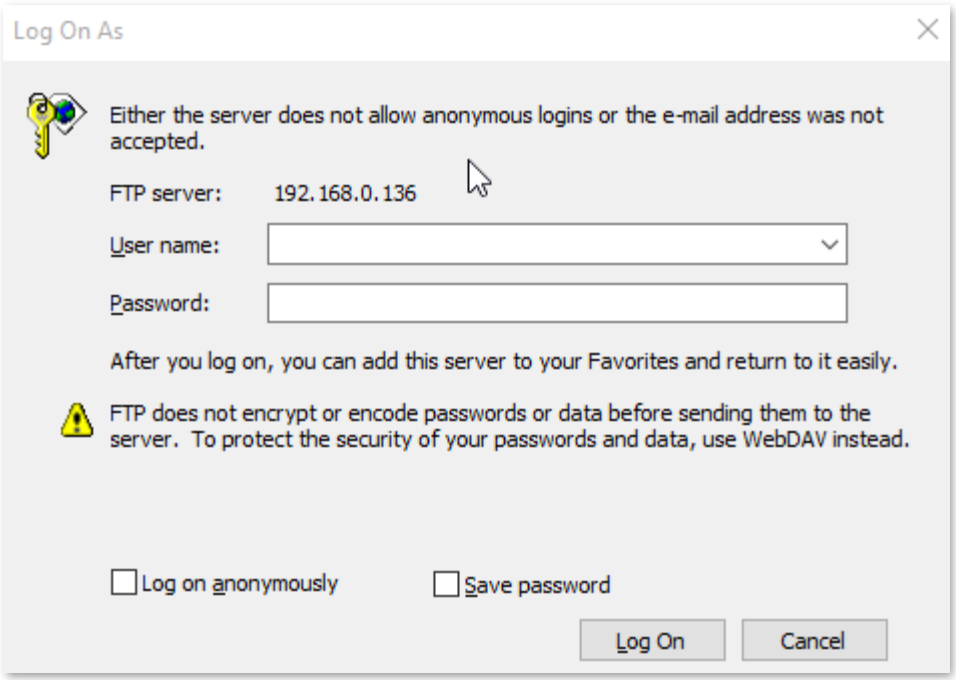
Step 4 Locate the VPN connection added, and click **Connect**.



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



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



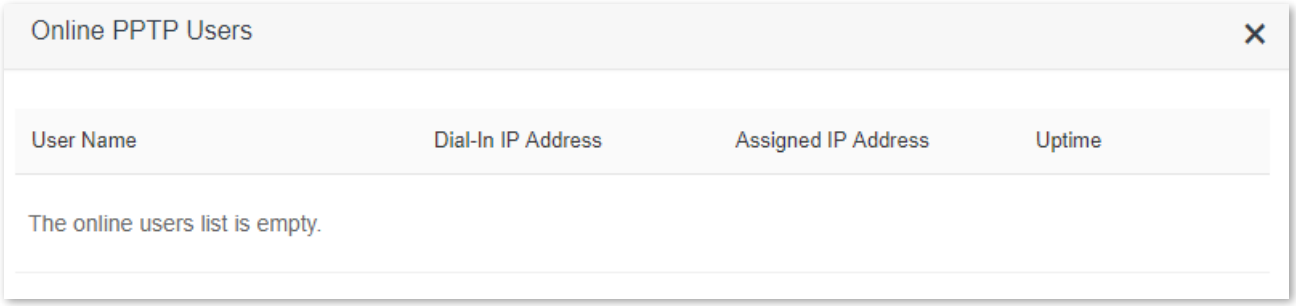
---End

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

9.2 Online PPTP users

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

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



Parameter description

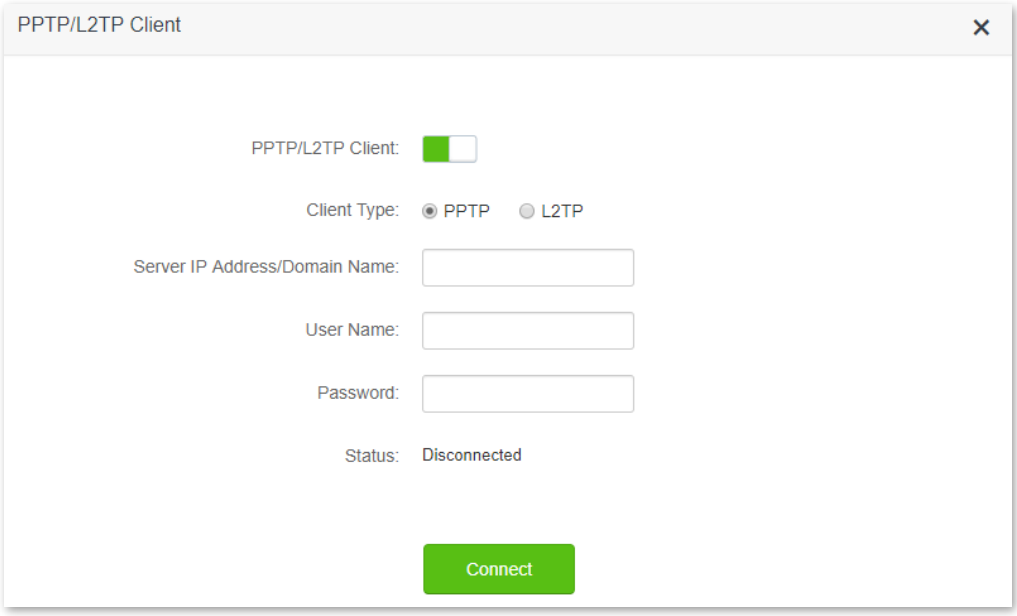
Parameter	Description
User Name	Specifies the VPN user name, which the VPN user uses when making PPTP dial-ups (VPN connection).
Dial-In IP Address	Specifies the IP address of the PPTP client. If the client is a router, it will be the IP address of the WAN port whose VPN function is enabled.
Assigned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

9.3 PPTP/L2TP client

9.3.1 Overview

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

The PPTP/L2TP client function is disabled by default. When it is enabled, the page is show 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, either PPTP or L2TP. - PPTP: When the router is connecting to a PPTP server, choose this option. - L2TP: When the router is connecting to a L2TP server, choose this option.
Server IP Address/Domain Name	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.

9.3.2 Access VPN resources with the router

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

Requirements: Access the VPN resources of your ISP.

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

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

Configuring procedure:

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

Step 2 Navigate to **VPN** > **PPTP/L2TP Client**.

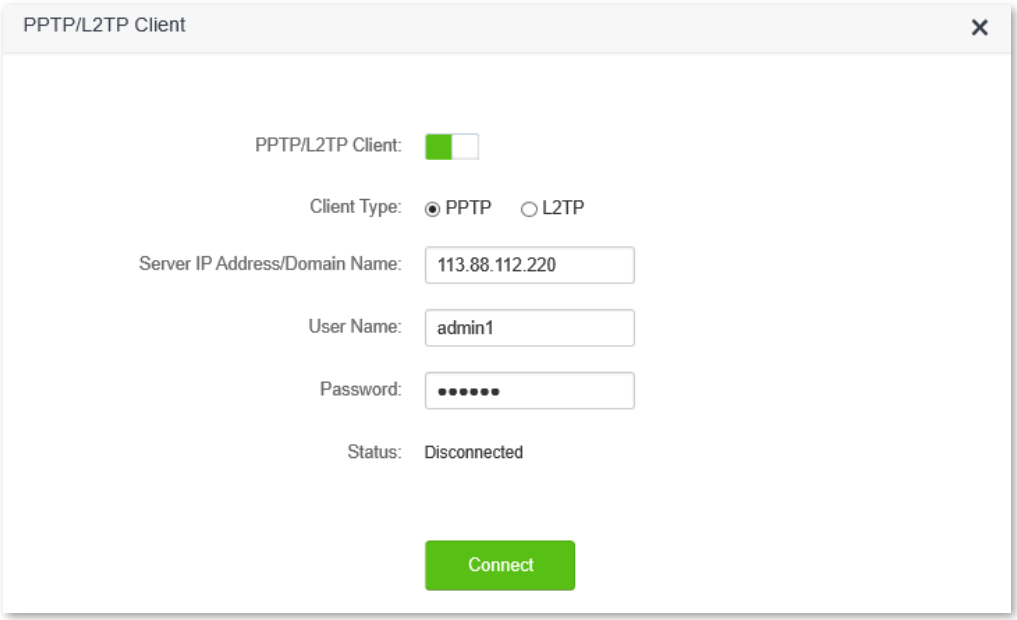
Step 3 Enable the **PPTP/L2TP Client**

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

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

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

Step 7 Click **Connect**.



---End

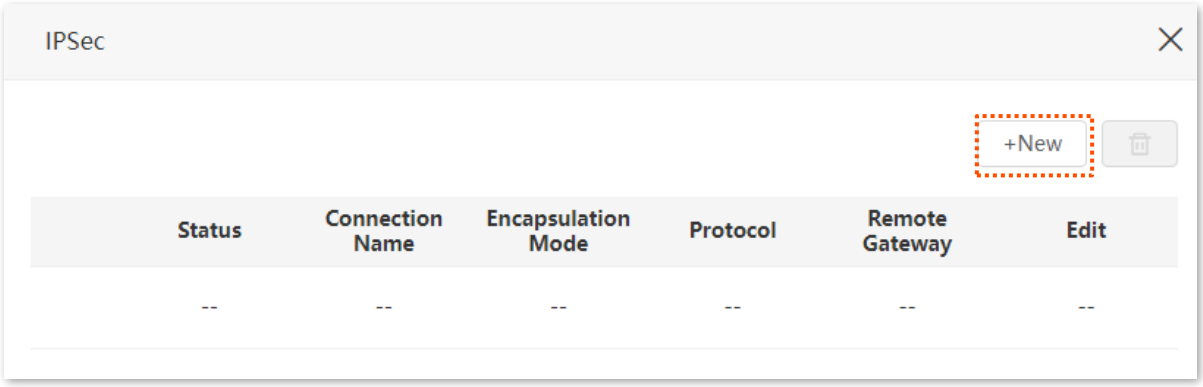
When Connected is shown in **Status**, you can access the VPN resources of your ISP.

9.4 IPSec (Example: 4G06)

9.4.1 Overview

This router can function IPSec VPN.

To access the configuration page, log in to the web UI of the router, and navigate to **VPN** > **IPSec**. This function is disabled by default. Click **+New** to configure the IPSec function.



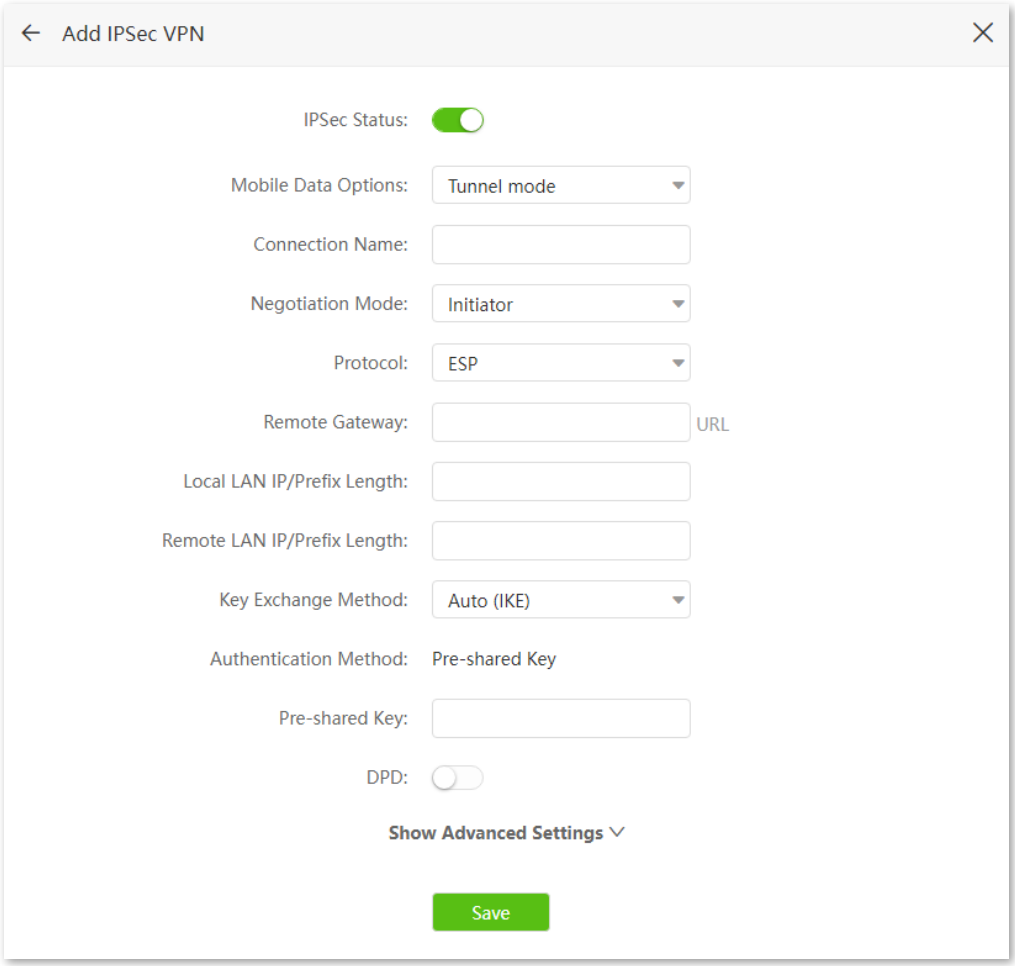
Parameter description

Parameter	Description
Status	Specifies the status of IPSec function.
Connection Name	Specifies the name of the IPSec connection.
Encapsulation Mode	Specifies the IPSec data encapsulation mode. - **Tunnel**: This mode is generally used between two security getaways. - **Transport**: This mode is generally used between hosts or host and gateway.
Protocol	Specifies the protocol which offers the security service for IPSec. - **AH**: It is abbreviated for Authentication Header. This protocol is used for verifying data integrity. If a packet is tampered during transmission, the receiver discards it during data integrity verification. - **ESP**: It is abbreviated for Encapsulating Security Payload. This protocol is used for verifying data integrity and encrypting data. If a packet processed using this protocol is intercepted during transmission, it is difficult for the intercepting party to obtain the real information contained in the packet. This compatible protocol is widely used in gateway products. - **AH+ESP**: It indicates that the function features both AH and ESP.
Remote Gateway	Specifies the IP address or domain name of the peer gateway of the IPSec tunnel.

Parameter	Description
Operation	The available operations include: +New : Used to add a new IPSec VPN. : Used to delete the IPSec VPN.

9.4.2 Configure IPSec connection

When it is enabled, the page is shown as below.



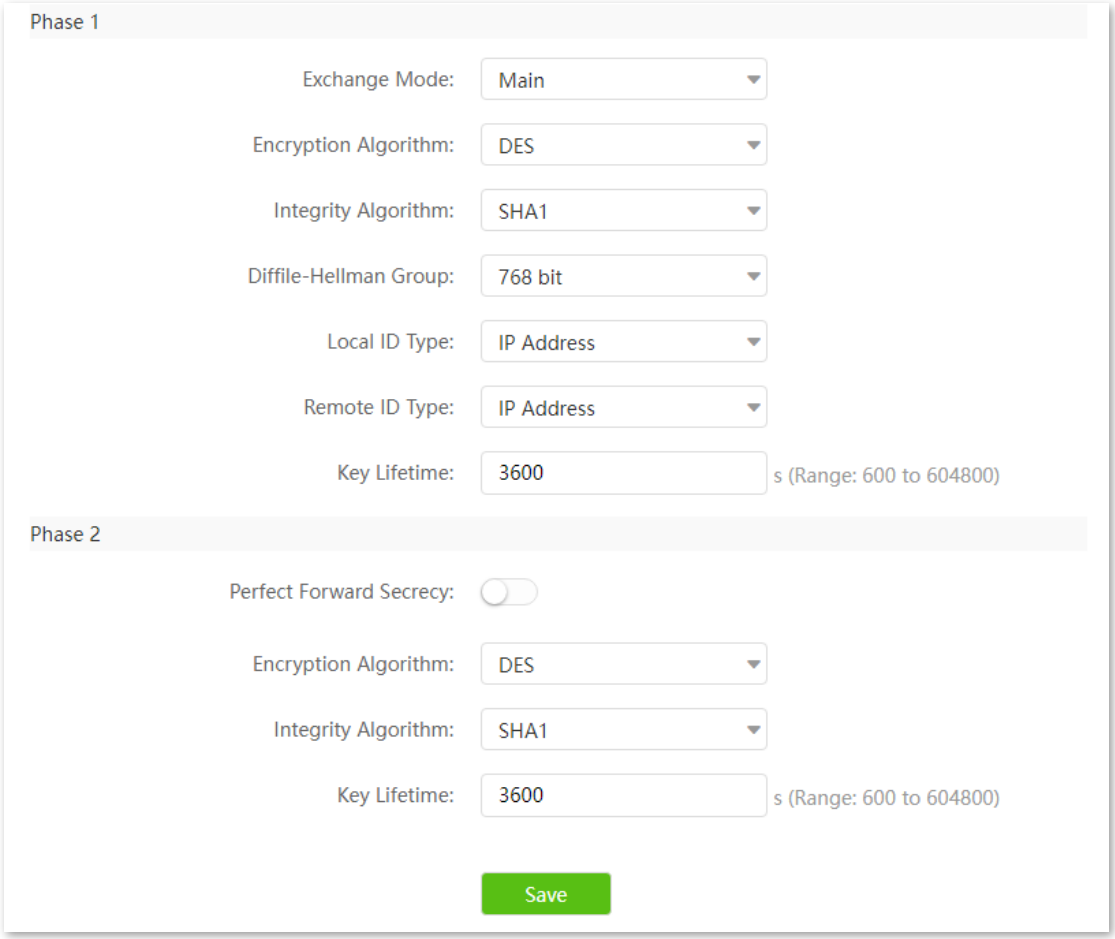
Parameter description

Parameter	Description
IPSec Status	Used to enable or disable the IPSec function.
Mobile Data Options	Specifies the IPSec mobile data options. - **Tunnel**: This mode is generally used between two security gateways. - **Transport:** This mode is generally used between hosts or host and gateway.

Parameter	Description
Connection Name	Specifies the name of the IPSec connection.
Negotiation Mode	Specifies the negotiation mode of the IPSec tunnel. - **Initiator**: The device sends a connection request to the peer device. - **Responder**: The device waits for the peer device to send a connection request. TIP Do not set both ends of the IPSec tunnel as **Responder**. Otherwise, the IPSec tunnel setup fails.
Protocol	Specifies the protocol which offers the security service for IPSec. - **AH**: It is abbreviated for Authentication Header. This protocol is used for verifying data integrity. If a packet is tampered during transmission, the receiver discards it during data integrity verification. - **ESP**: It is abbreviated for Encapsulating Security Payload. This protocol is used for verifying data integrity and encrypting data. If a packet processed using this protocol is intercepted during transmission, it is difficult for the intercepting party to obtain the real information contained in the packet. This compatible protocol is widely used in gateway products. - **AH+ESP**: It indicates that the function features both AH and ESP.
Remote Gateway	Specifies the IP address or domain name of the peer gateway of the IPSec tunnel.
Local LAN IP/Prefix Length	Specifies the network segment/prefix length of the LAN of the device. For example, if the IP address of the LAN port of the device is 192.168.5.1 and the subnet mask is 255.255.255.0, the local LAN/prefix length can be 192.168.5.0/24.
Remote LAN IP/Prefix Length	Specifies the network segment/prefix length of the LAN of the peer gateway of the IPSec tunnel. If the peer device is a host, this parameter can be set as “the IP address of the device/32”.
Key Exchange Method	Specifies the key exchange method of the IPSec security tunnel. By default, **Auto (IKE)** is selected. - **Auto (IKE)**: It indicates that an SA is set up, maintained, and deleted automatically using IKE (Internet Key Exchange). This reduces configuration complexity and simplifies IPSec usage and management. Such an SA (Security Association) has a life cycle and is updated regularly, leading to higher security. - **Manual**: It indicates that an SA is set up by manually specifying encryption and authentication algorithms and keys. Such an SA does not have a life cycle, and therefore it remains valid unless being manually deleted, leading to security risks. Generally, this mode is used only for commissioning.

Parameter	Description
Authentication Method	Specifies the shared key mode, which indicates a shared key string negotiated by IPSec parties with some way in advance.
Pre-shared Key	Specifies the pre-shared key used during negotiation. This parameter must be the same with that of the peer gateway. A maximum of 128 characters are allowed.
DPD	Specifies whether to enable the DPD Detection. This function can detect whether the remote tunnel site is valid.

Click **Advanced** to display the advanced parameters of auto negotiation. The following displays the page when the advanced parameters are displayed.



Parameter description

Parameter	Description
Exchange Mode	Specifies the exchange mode in IKE **Phase 1**, which should be the same as that of peer gateway. - **Main**: This mode is the primary mode. In this mode, exchanged packets are huge to offer identity protection, which is applicable to scenarios where identity protection is rigorous. - **Aggressive**: This mode does not offer identity protection. In this mode, the exchanged packets are few in number and negotiation rate is high, which is applicable to scenarios where identity protection is loose.
Encryption Algorithm	Specifies the IKE session encryption algorithm. - **DES** (Data Encryption Standard): A 56-bit key is used to encrypt 64-bit data. The last 8 bits of the 64-bit data are used for parity check. 3DES indicates that three 56-bit keys are used for encryption. - **AES** (Advanced Encryption Standard): AES 128/192/256 indicates that 128/192/256-bit keys are used for encryption respectively.
Integrity Algorithm	Specifies the IKE session verification algorithm. - **MD5** (Message Digest Algorithm): A 128-bit message digest is generated to prevent message tampering. - **SHA1** (Secure Hash Algorithm): A 160-bit message digest is generated to prevent message tampering, leading to higher security than MD5.
Diffie-Hellman Group	Specifies the group information for the Diffie-Hellman algorithm for generating a session key used to encrypt an IKE tunnel. The information should be the same as that of the remote gateway.
Local ID Type	Specifies the ID of the local gateway. - **IP Address**: The router uses the IP address of the specified WAN port for negotiation with the remote gateway. - **FQDN**: Fully Qualified Domain Name. If you select FQDN, you need to manually set a string of characters, which should be identical with the remote ID. TIP **Local ID Type** and **Remote ID Type** should be the same. Under such circumstances, you are recommended to modify the **Mode** to **Aggressive**.

Parameter	Description
Remote ID Type	Specifies the ID of the remote gateway. - **IP Address**: By default, the remote gateway uses the WAN IP address of the router for negotiation. - **FQDN**: Fully Qualified Domain Name. If you select FQDN, you need to manually set a string of characters, which should be identical with the local ID. TIP **Local ID Type** and **Remote ID Type** should be the same. Under such circumstances, you are recommended to modify the **Mode** to **Aggressive**.
Key Lifetime	Specifies the life cycle of IPSec SA.
Perfect Forward Secrecy	This feature generates a new key in IKE Phase II, which is unrelated to the key generated in IKE Phase I, ensuring that the key generated in Phase II is secure even if the key generated in IKE1 **Phase 2** is cracked. With the **Perfect Forward Secrecy** disabled, generation of the new key in IKE Phase II depends on the key in Phase I. Once the key generated in IKE Phase I is cracked, the key generated in Phase II will suffer threats, and further threatens the communication security.

10 Advanced settings

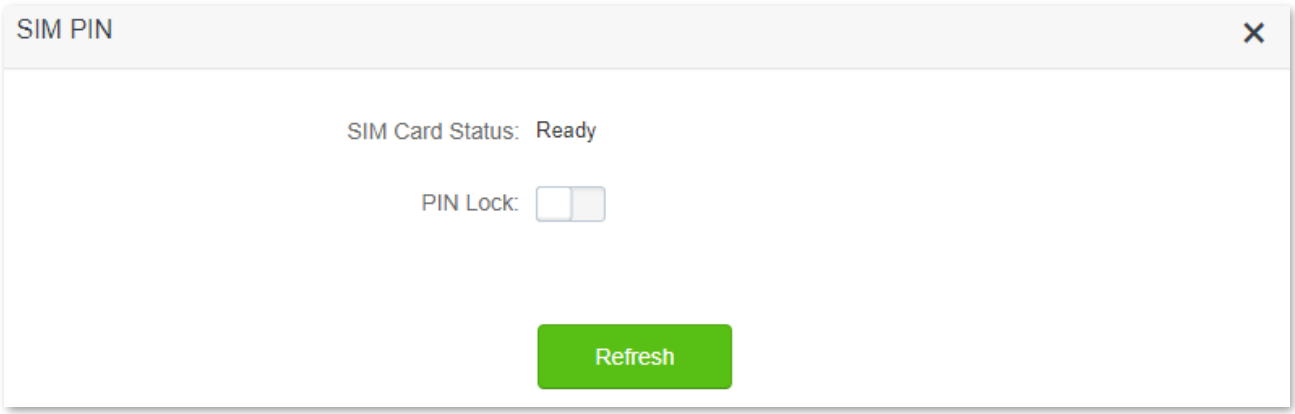
This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with product models. The actual product prevails.

10.1 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 SIM PIN setting 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.



10.1.1 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

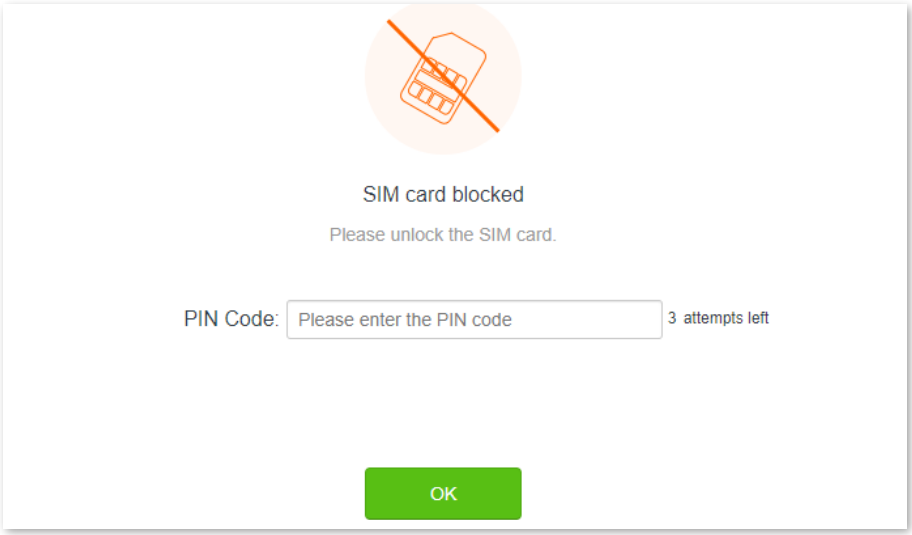
When you use the router for the first time or the router is reset, you are required to unlock the SIM card in the quick setup wizard.

Configuring procedure:

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

Step 2 Click **Start**.

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



NOTE

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

Step 4 Follow the steps to complete the setup process.

---End

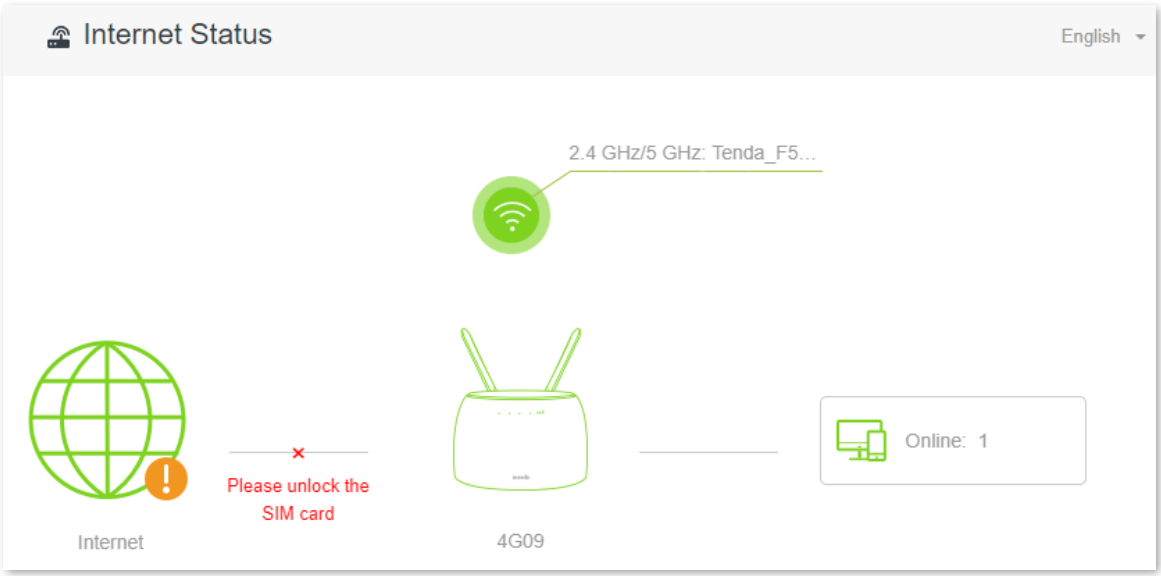
Unlock the SIM card in the web UI

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

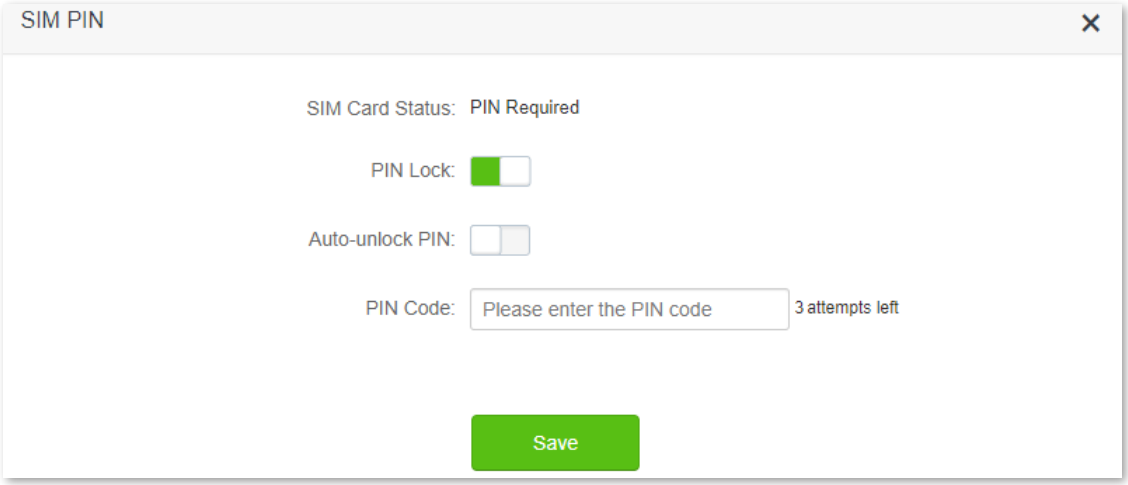
Configuring procedure:

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

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



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



NOTE

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

---End

10.1.2 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.

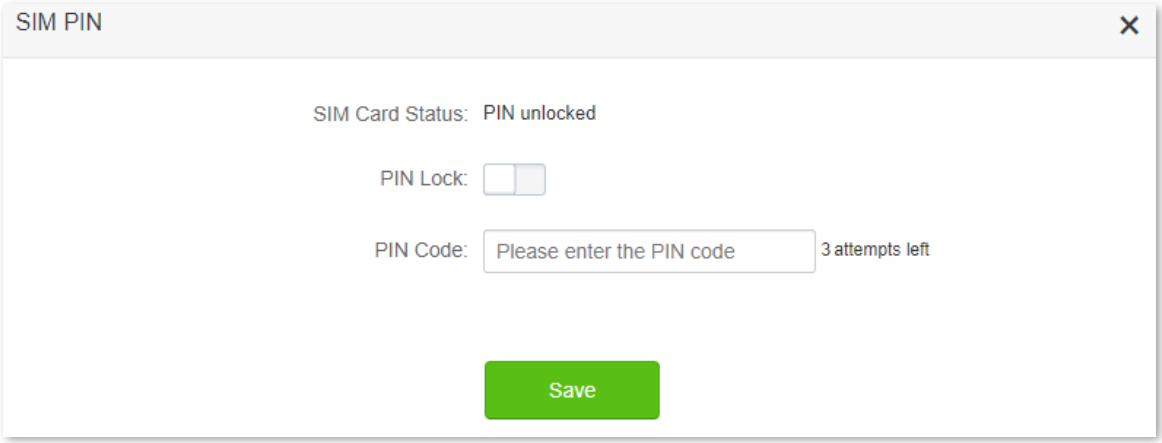
Configuring procedure:

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

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

Step 3 Disable **PIN Lock**.

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



---End

NOTE

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

10.1.3 Enable PIN lock for the SIM card

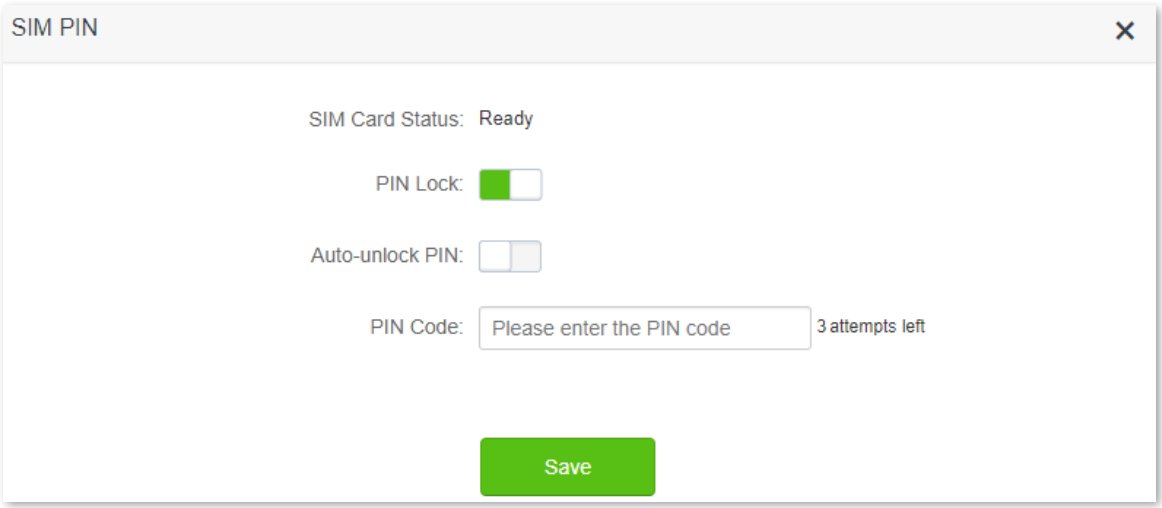
You can set a PIN lock for a SIM card. SIM PIN is a protective measure to prevent your SIM card from misuse

Configuring procedure:

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

Step 2 Enable **PIN Lock**.

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



TIP

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

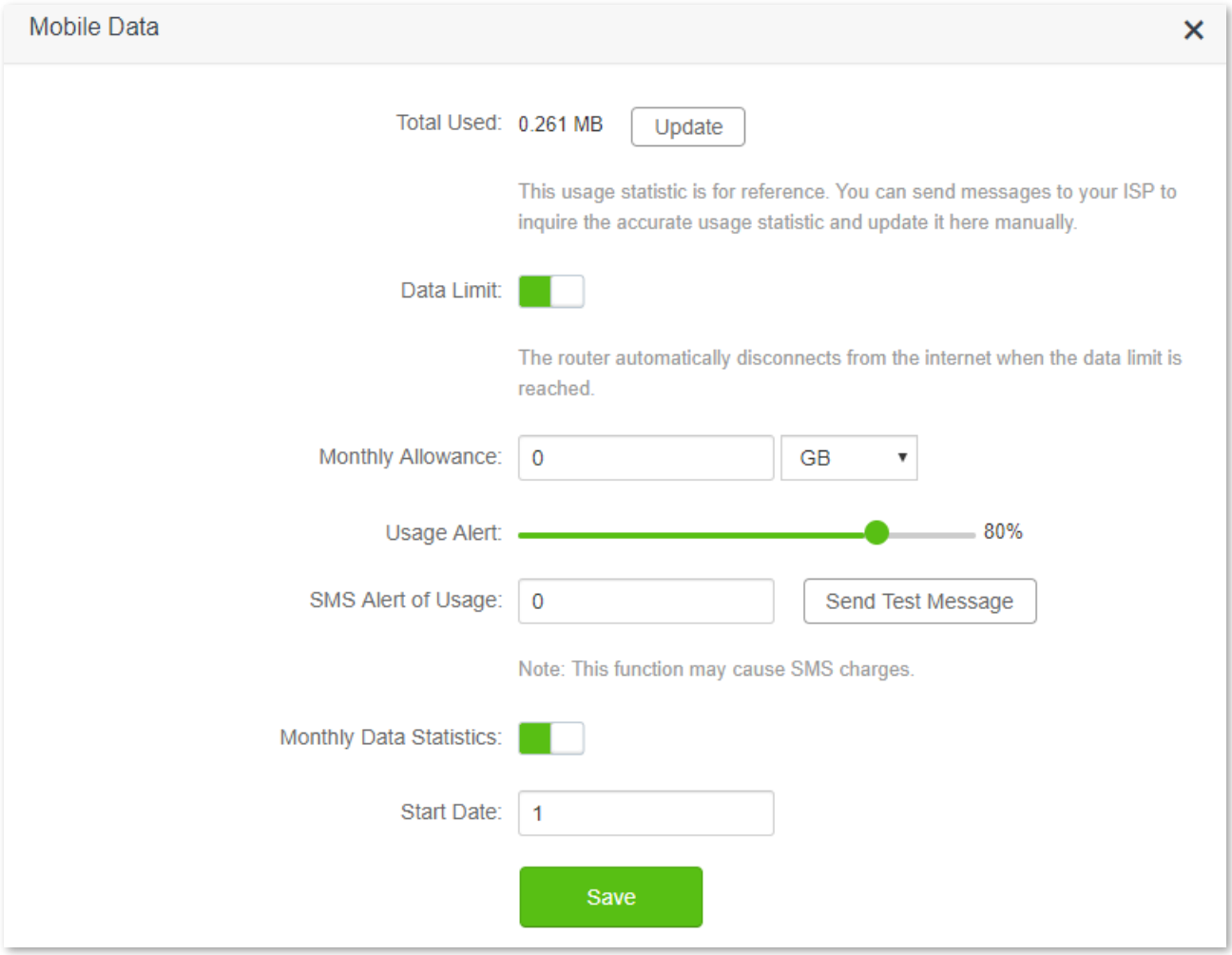
---End

10.2 Mobile data

10.2.1 Overview

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

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



Parameter description

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

10.2.2 Example of mobile data configurations

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

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

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

Assume that:

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

Configuring procedure:

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

Step 2 Navigate to **Advanced Settings** > **Mobile Data**.

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

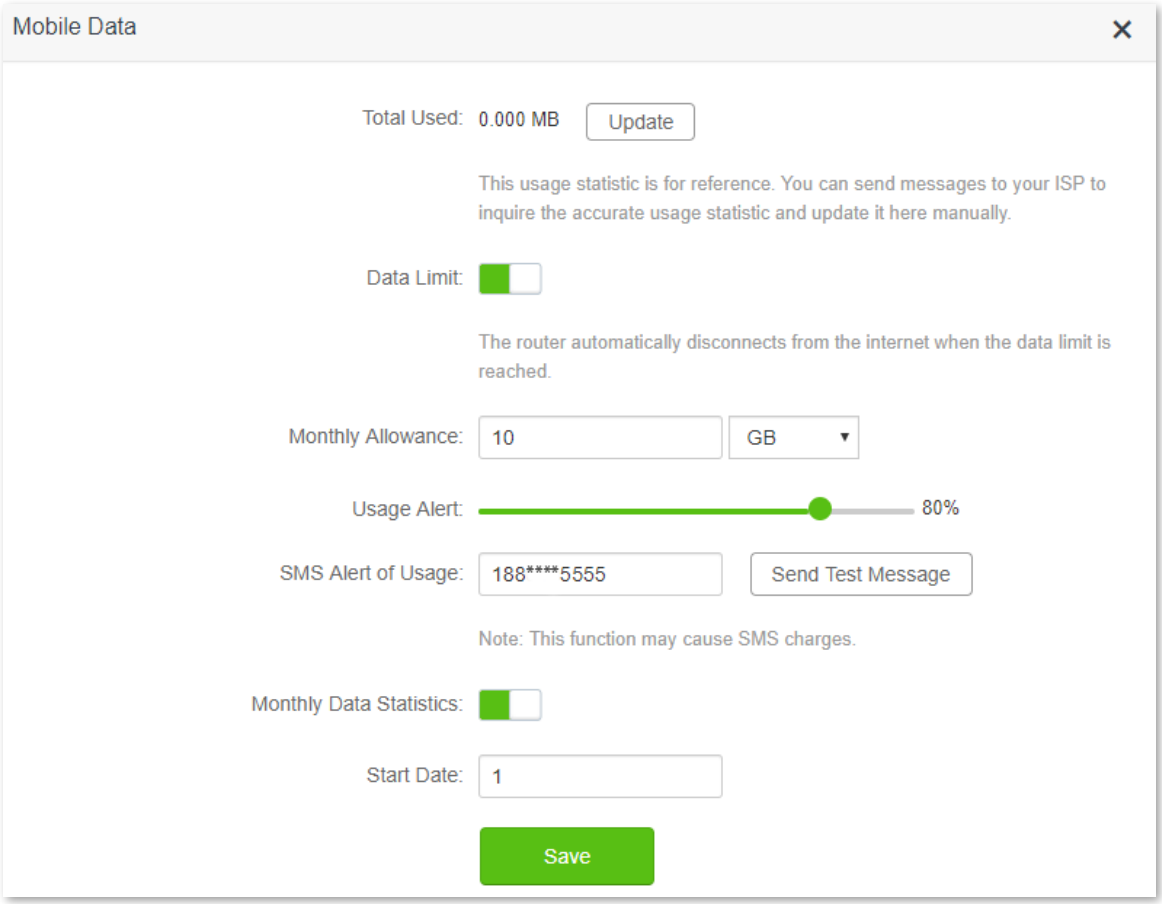
Step 4 Enable **Data Limit**, enter **10** in Monthly Allowance, and choose **GB** in the drop-down box.

Step 5 Set **Usage Alert** to **80%**.

Step 6 Enter **188****5555** in **SMS Alert of Usage**.

Step 7 Enable **Monthly Data Statistics**.

Step 8 Enter **1** in Start Date, 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:

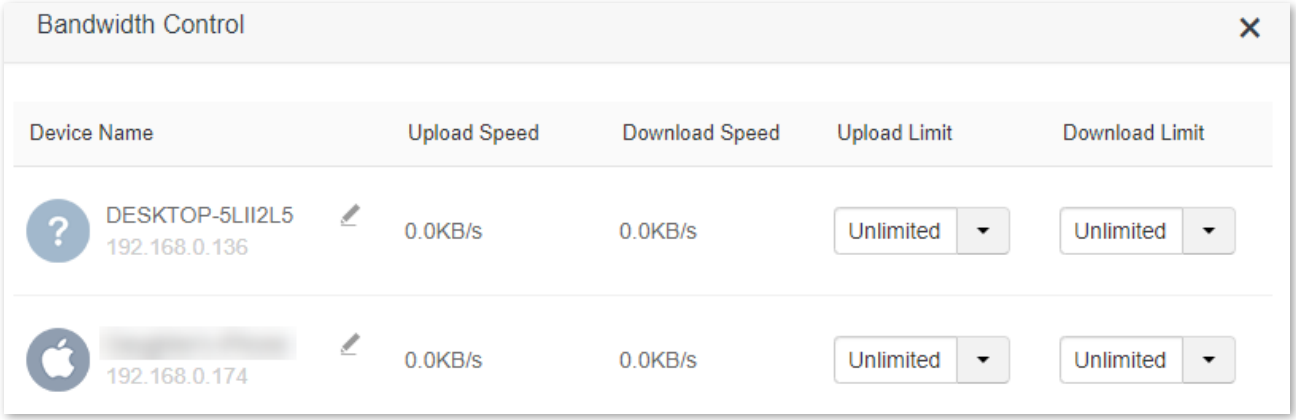
- Change the **Total Usage** by clicking **Update**.
- Disable **Data Limit**.
- Navigate to **Internet Settings**, and click **Connect** at the bottom of the page.

10.3 Bandwidth control

10.3.1 Overview

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

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



Parameter description

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

10.3.2 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 meet the requirement.

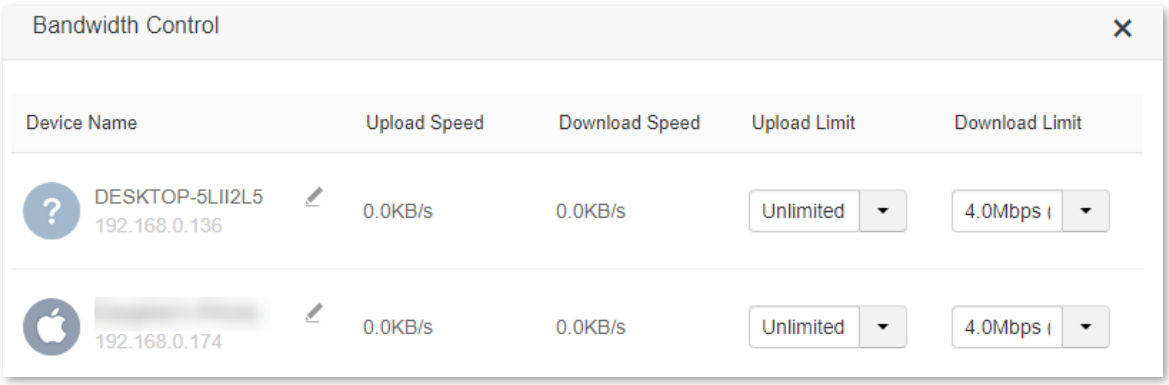
Configuring procedure:

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

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

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

Step 4 Click **Save**.



---End

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

10.4 Tenda WiFi App

The router can be managed by the Tenda WiFi App. With the App, you can:

- Manage your router within the LAN.
- Manage your router through the internet.

To manage the router with Tenda WiFi App, follow the steps below (Example: iPhone).

TIP

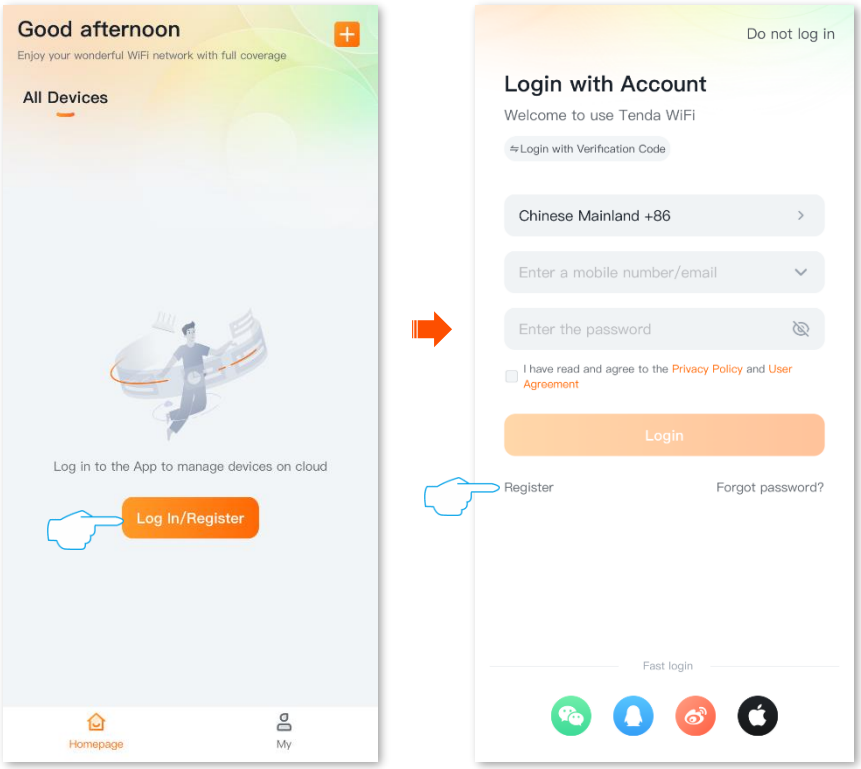
The Tenda WiFi App V4.0.1 is taken as an example here.

Configuring procedure:

Step 1 Connect your smartphone to the internet, and download the **Tenda WiFi App** onto your mobile device by scanning the **QR code** or searching for **Tenda WiFi** in the **Google Play** or **App Store**.

Or

Step 2 (Optional) Run the **Tenda WiFi App**, and click **Log In/Register**. Click **Register**, and then enter the related-parameters to register.

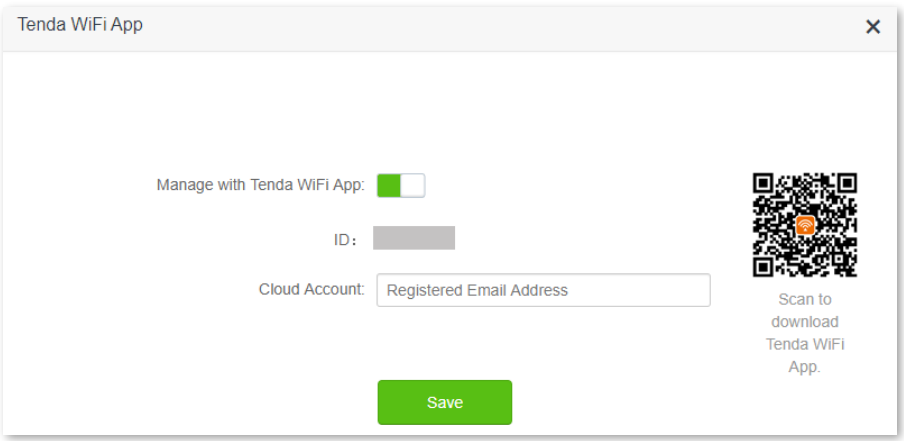


Step 3 Log in with a registered account.

Follow the instructions on the home page of the Tenda WiFi App to add the router.

Step 4 Bind your router with your smartphone.

1. Start a web browser on the smartphone connected to the router and visit **tendawifi.com** to log in to the web UI of the router.
2. Navigate to **Advanced Settings** > **Tenda WiFi App**.
3. Enable **Manage with Tenda WiFi App**.
4. Enter an account registered in the Tenda WiFi App in **Cloud Account**.
5. Click **Save**.



---End

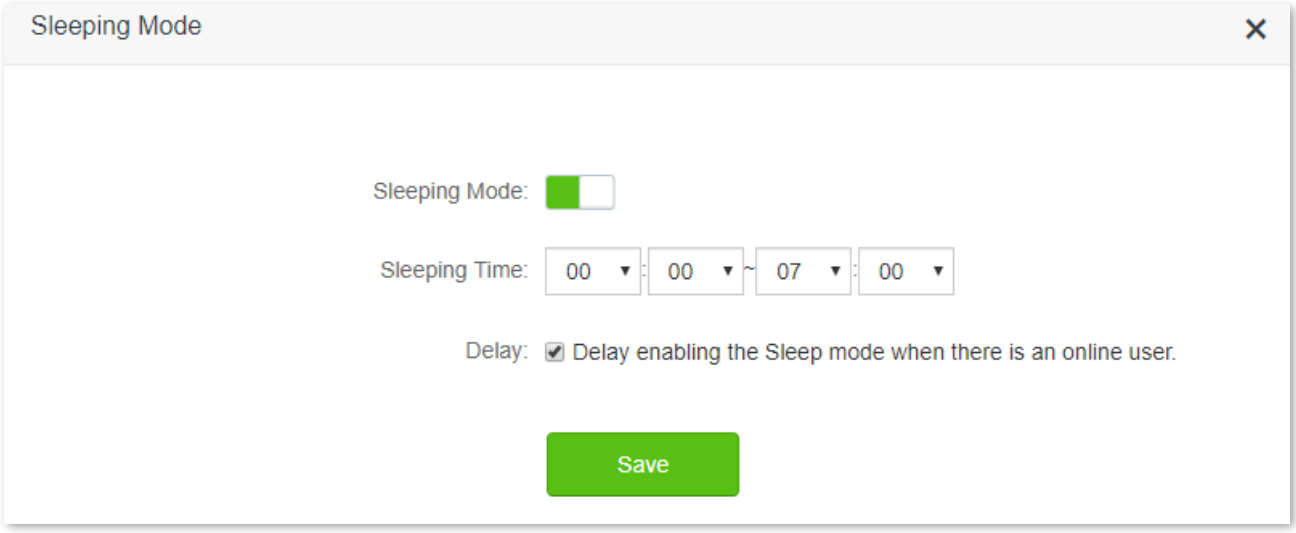
When the configuration is completed, you can manage your router with Tenda WiFi App on your smartphone anywhere and anytime through the internet.

10.5 Sleeping mode

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

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

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



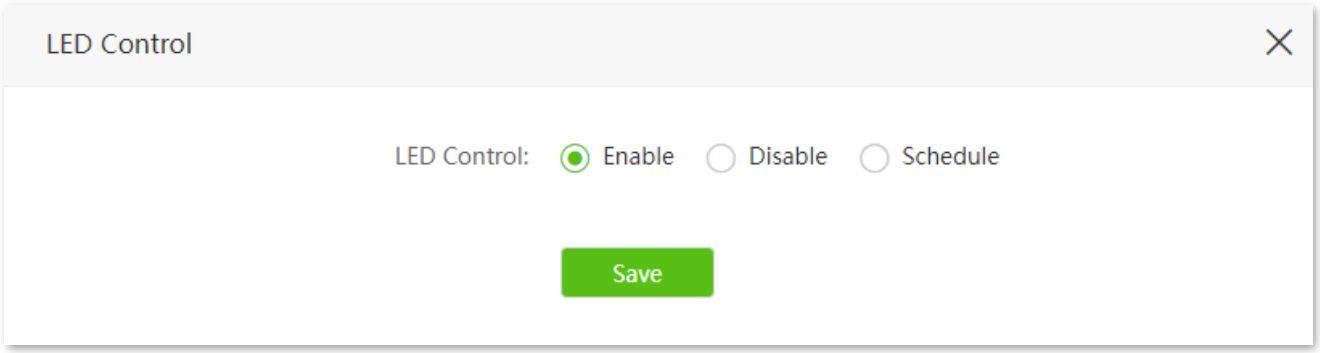
Parameter description

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

10.6 LED control

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

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



Parameter description

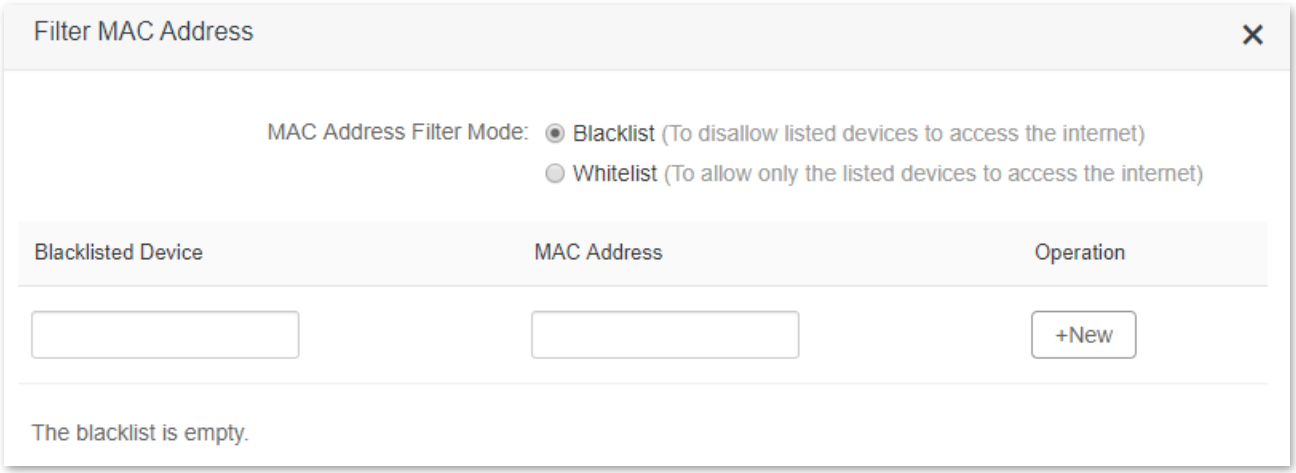
Parameter	Description
Enable	All indicators stay in their normal status.
Disable	All indicators are turned off.
Schedule	Indicators are only turned off during the specified period.
Turn Off During	It is required only when **Schedule** is selected. Specifies the period during which the indicators are turned off. TIP If the start time you set is greater than the end time, the schedule starts from the start time to the end time on second day. For example, if you set **Turn Off During** to **08:00~06:25**, it indicates that the schedule starts from 08:00 to 06:25 on the second day.

10.7 Filter MAC address

10.7.1 Overview

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

To access the configuration page, log in to the web UI of the router, and navigate to **Advanced Settings** > **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	+New : 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.

10.7.2 Only allow specified device to access the internet

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

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

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

Assume that:

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

Configuring procedure:

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

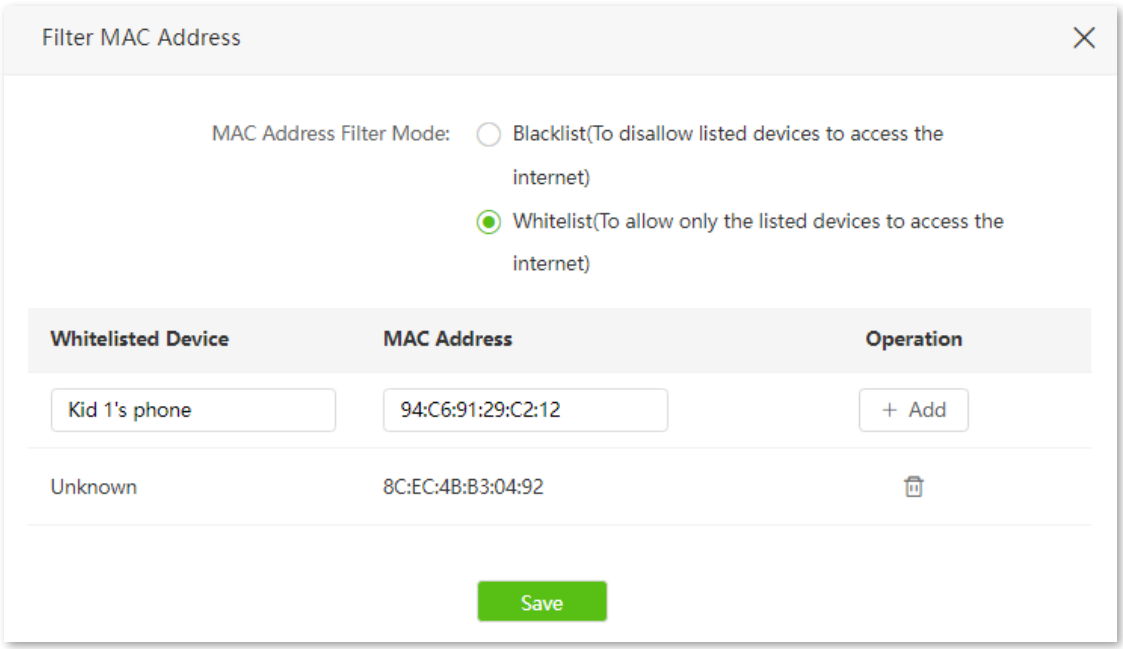
Step 2 Navigate to **Advanced Settings** > **Filter MAC Address**.

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

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

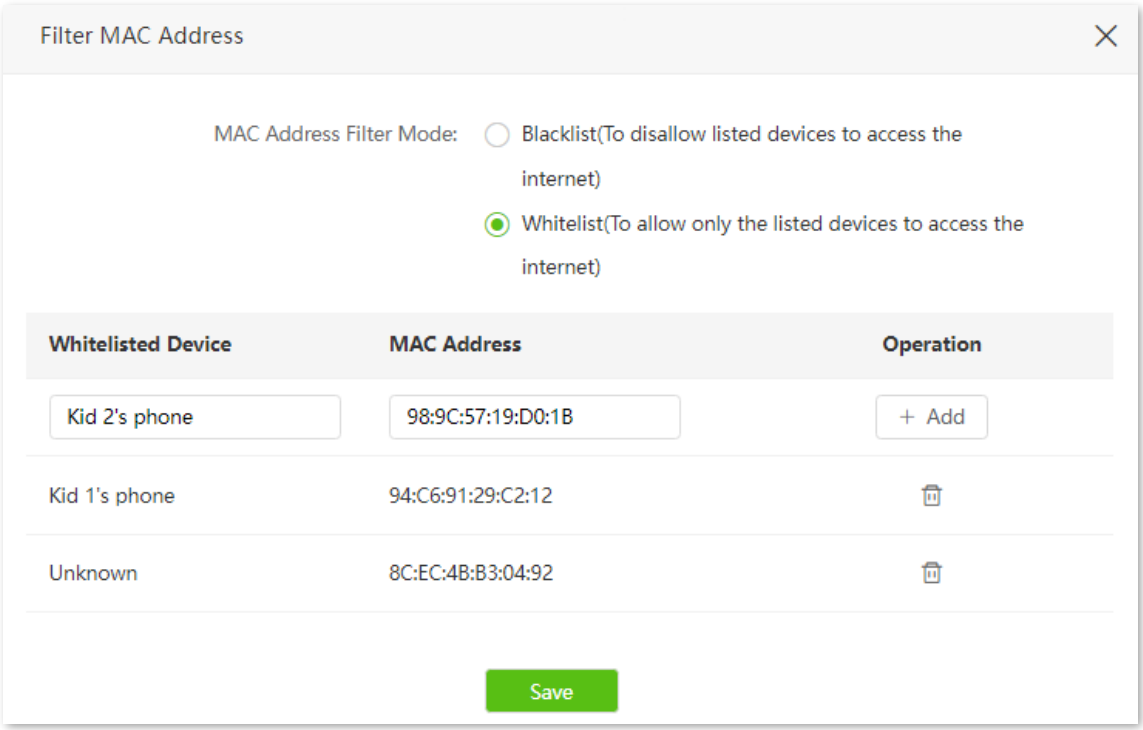
Step 5 Enter the **MAC Address** of the device, which is **94:C6:91:29:C2:12** in this example.

Click **+Add**.



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

Step 7 Click **Save**.



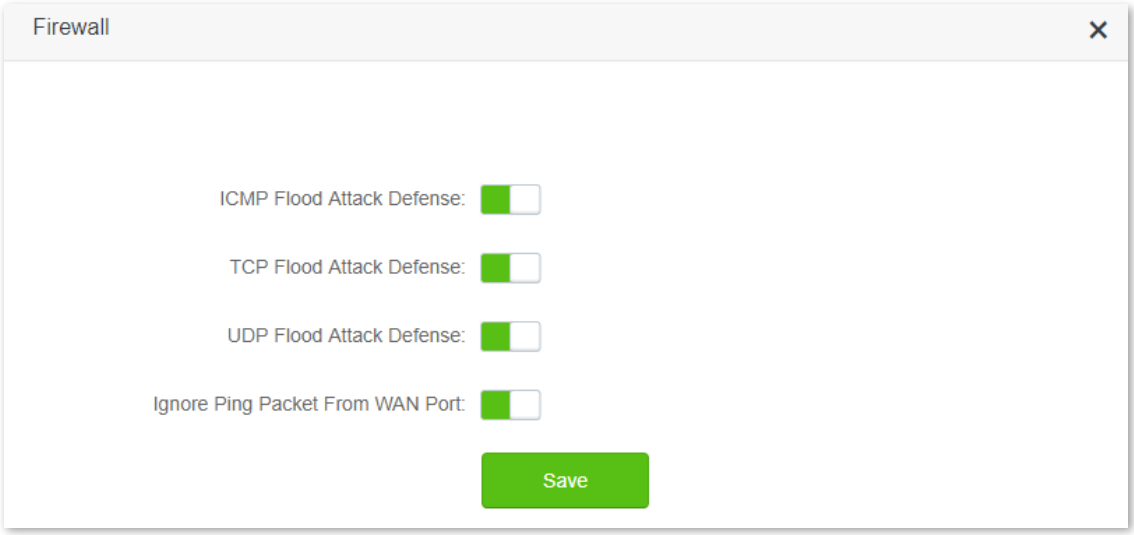
---End

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

10.8 Firewall

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

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

Parameter	Description
Ignore Ping Packet From WAN Port	Used to enable or disable the Ignore Ping packet from WAN Port function. When it is enabled, the router automatically ignores the ping to its WAN from hosts from the internet and prevent itself from being exposed, while preventing external ping attacks.

10.9 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.

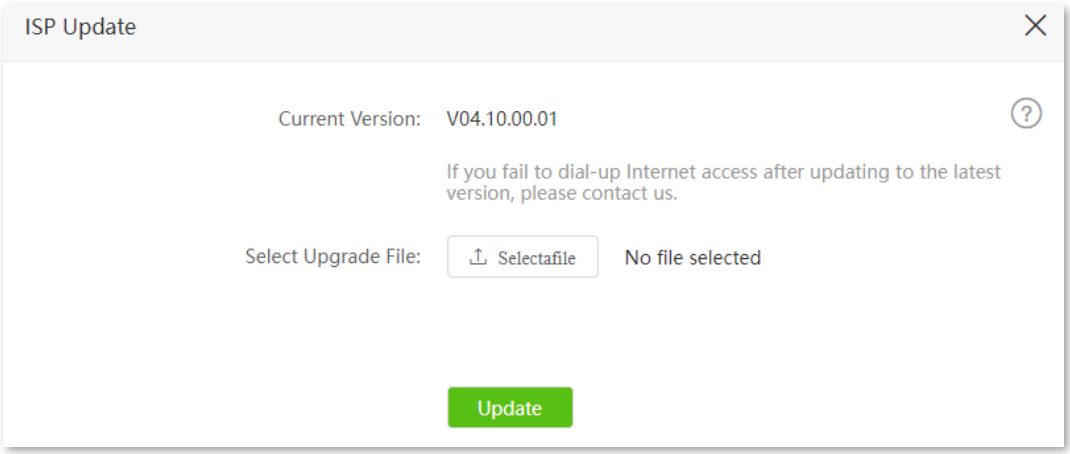
Procedure:

Step 1 Go to www.tendacn.com. Download an applicable ISP update file to your local computer and unzip it.

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

Step 3 Navigate to **Advanced Settings** > **ISP Update.**

Step 4 Click **Selectafile**. Select and upload the ISP update file that has been downloaded in Step 1, 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.

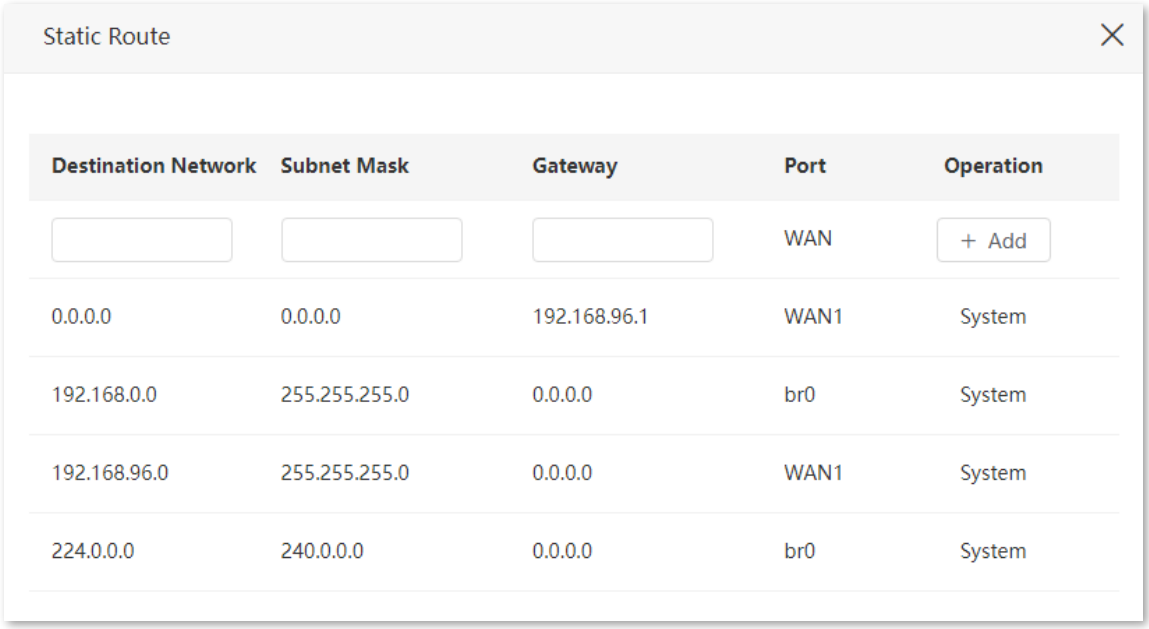
10.10 Static route

10.10.1 Overview

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

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

To access the configuration page, log in to the web UI of the router, and 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.
WAN	Specifies the interface that the packet exits from.
Operation	+ Add : Used to add a static route rule. : Used to delete a static route rule.

10.10.2 Add a static route rule

Scenario: You have a 4G09 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.

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

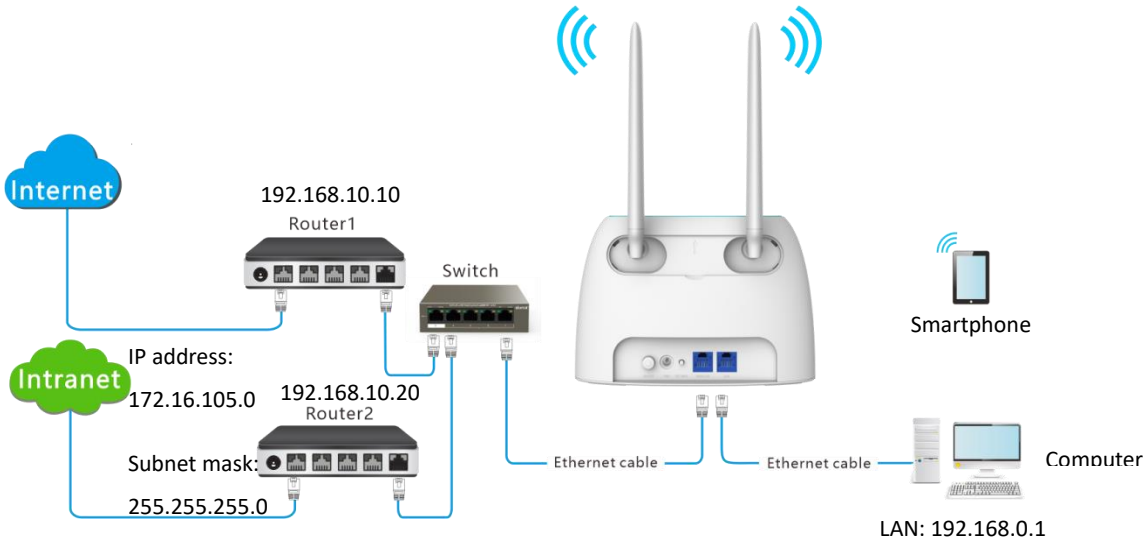
Solution: You can configure the static route function to reach the requirements.

Assume the LAN IP addresses of these devices are:

- 4G09: 192.168.0.1
- Router1: 192.168.10.10
- Router2: 192.168.10.20

The information about the intranet:

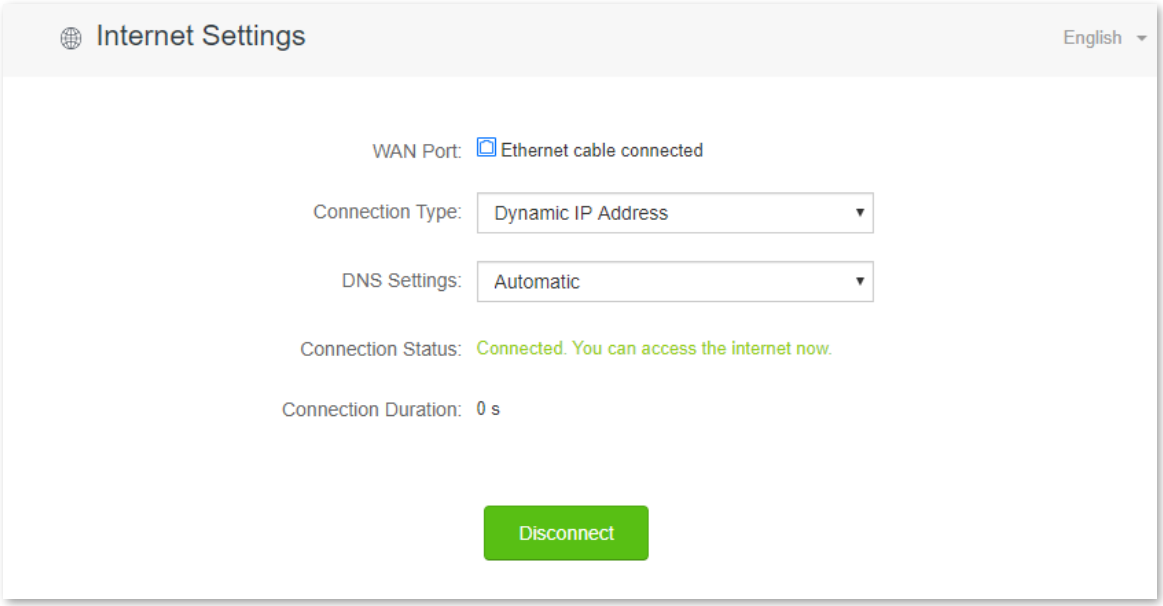
- IP address: 172.16.105.0
- Subnet mask: 255.255.255.0



Configuring procedure:

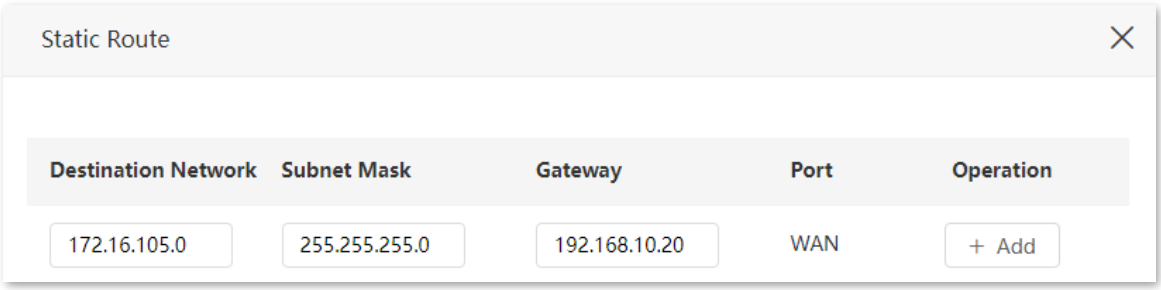
Step 1 Log in to the web UI of the router.

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



Step 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

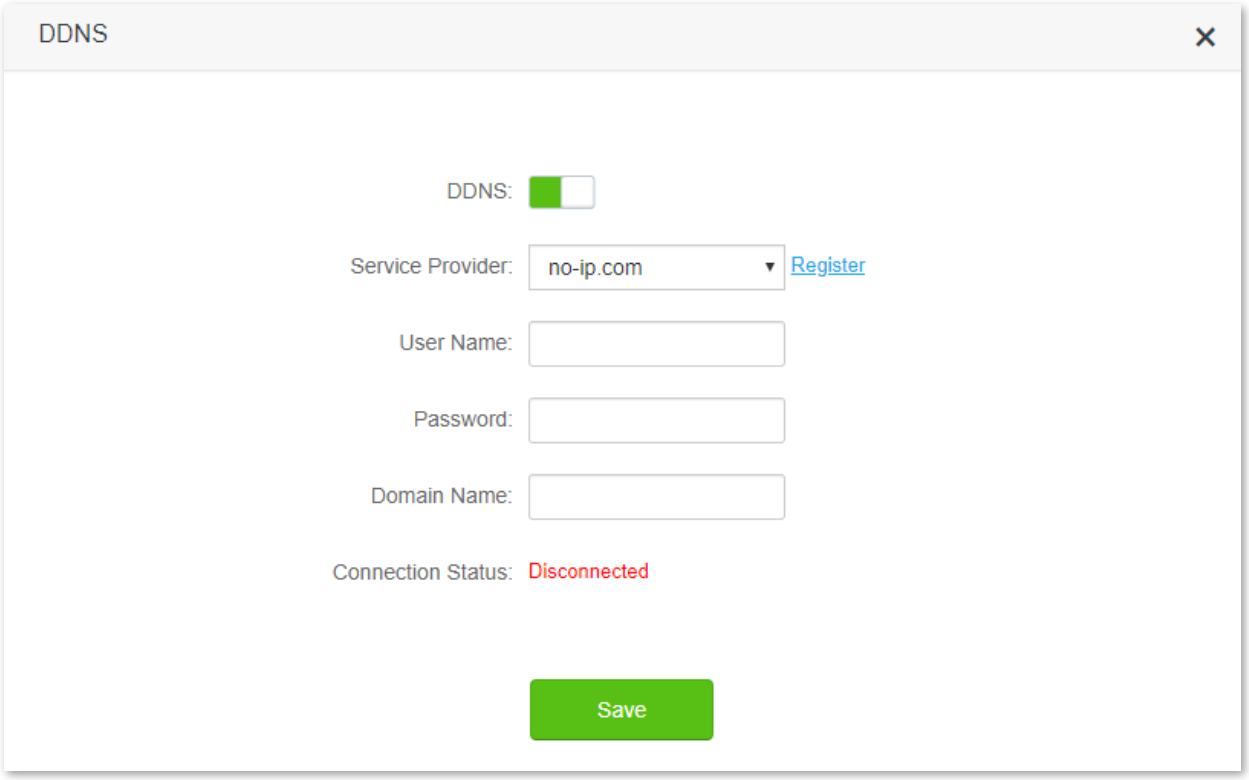
When the configuration is completed, you can access both the internet and intranet through 4G09 at the same time.

10.11 DDNS

10.11.1 Overview

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

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



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.

Parameter	Description
Connection Status	Specifies the current connection status of the DDNS service.

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

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

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

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

Assume that the information of the FTP server includes:

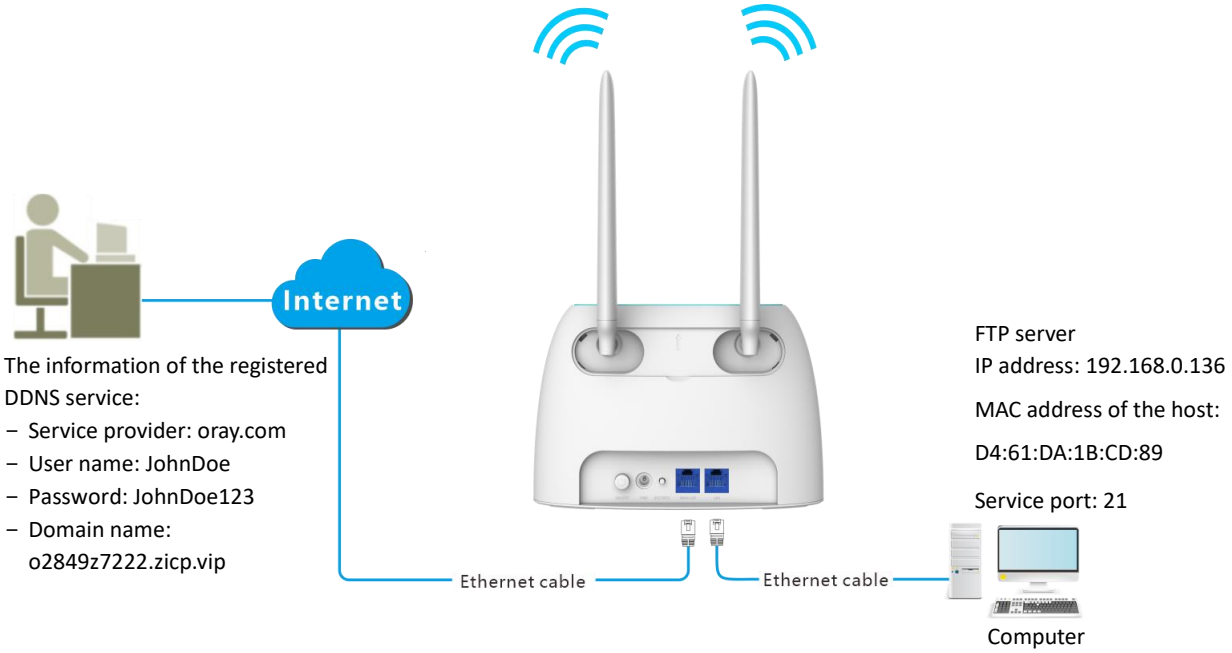
- IP address: 192.168.0.136
- MAC address of the host: D4:61:DA:1B:CD:89
- Service port: 21

The information of the registered DDNS service:

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

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.

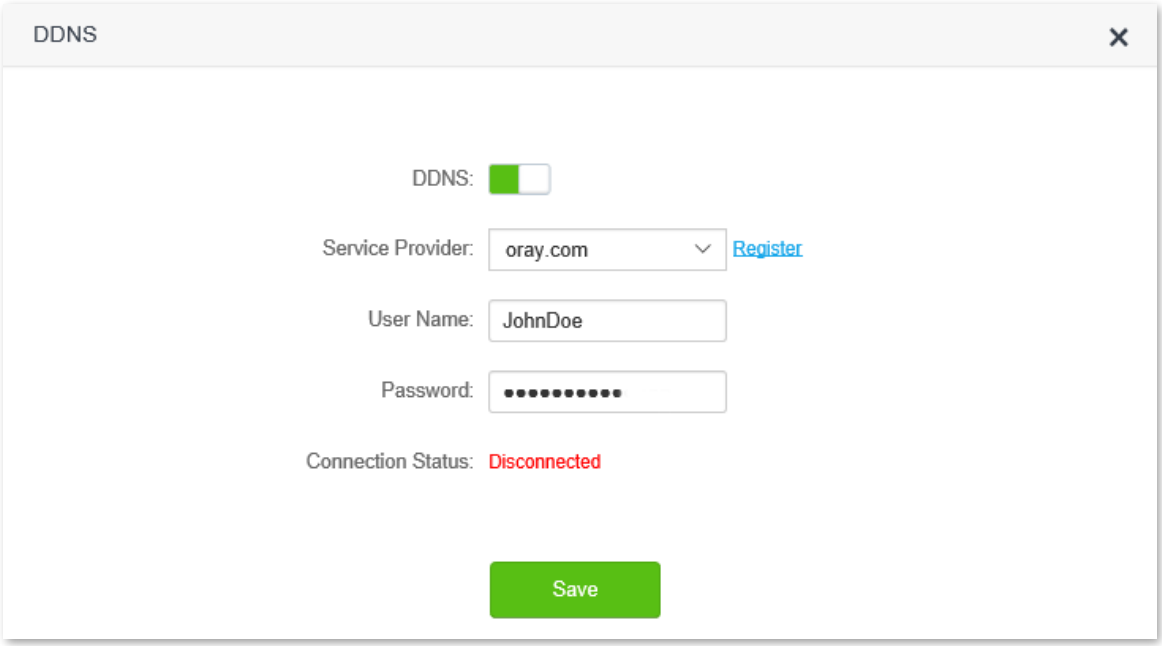


Configuration procedure:

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

Step 2 Configure the DDNS function.

1. Navigate to **Advanced Settings** > **DDNS**.
2. 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**.

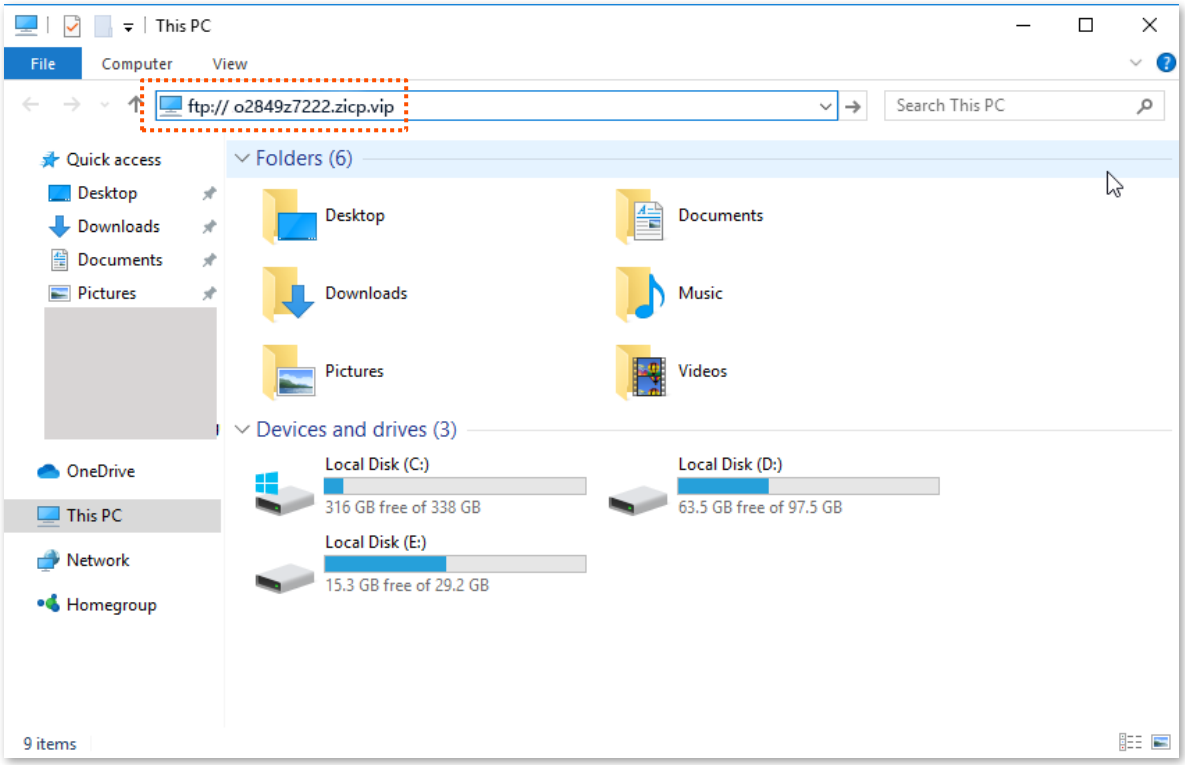


Wait a moment, when the Connection Status turns Connected, the configurations succeed.

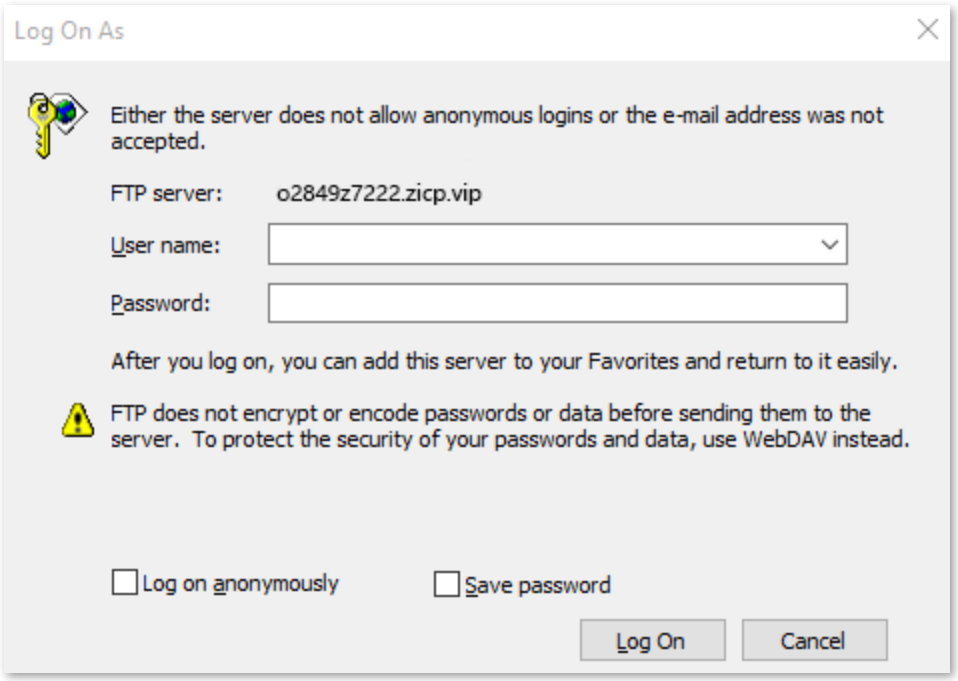
Step 5 Configure the virtual server function (refer to Virtual server)

---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.

10.12 Virtual server

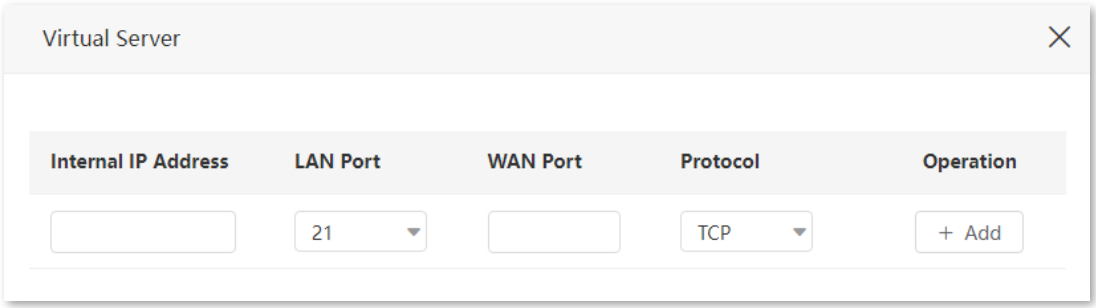
10.12.1 Overview

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

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

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

To access the configuration page, log in to the web UI of the router, and navigate to **Advanced Settings** > **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. You can either choose a service port number in the drop-down box, or enter a service port number manually.
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.
Operation	Available operations include: + Add : Used to add a new virtual server rule. : Used to delete existing virtual server rules.

10.12.2 Enable internet users to access LAN resources

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

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

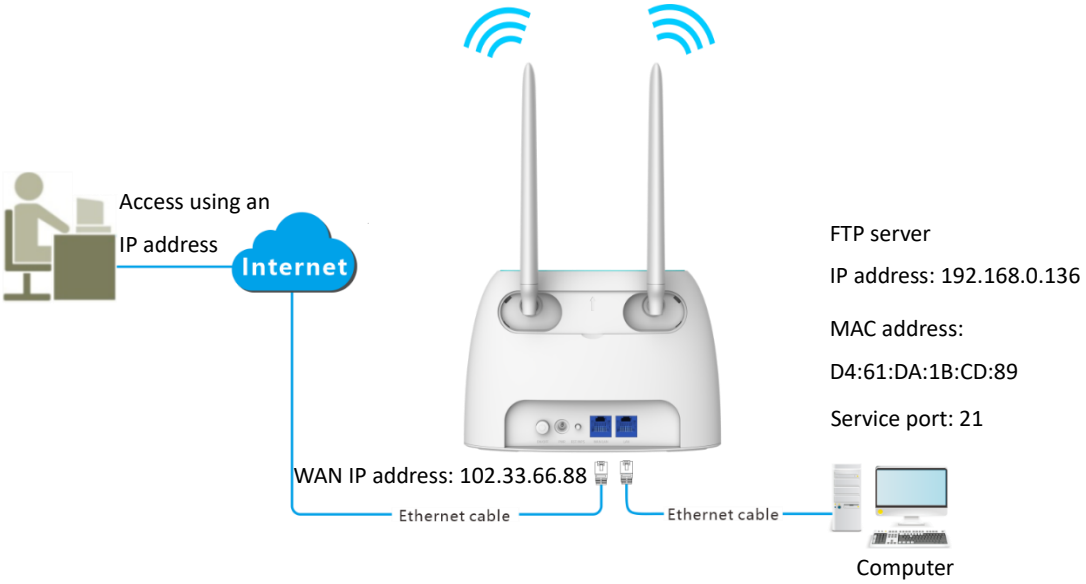
Solution: You can configure the virtual server function to reach the requirements.

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.

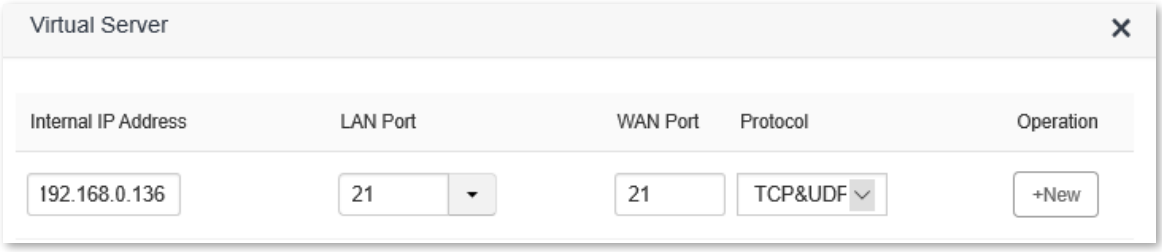


Configuration procedure:

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

Step 2 Add a virtual server rule.

1. Navigate to **Advanced Settings** > **Virtual Server**.
2. Enter the **Internal IP Address**, which is **192.168.0.136** in this example.
3. Choose a **LAN Port** in the drop-down box, which is **21** in this example.
4. Choose a protocol, which is **TCP&UDP** in this example.
5. Click **+New**.

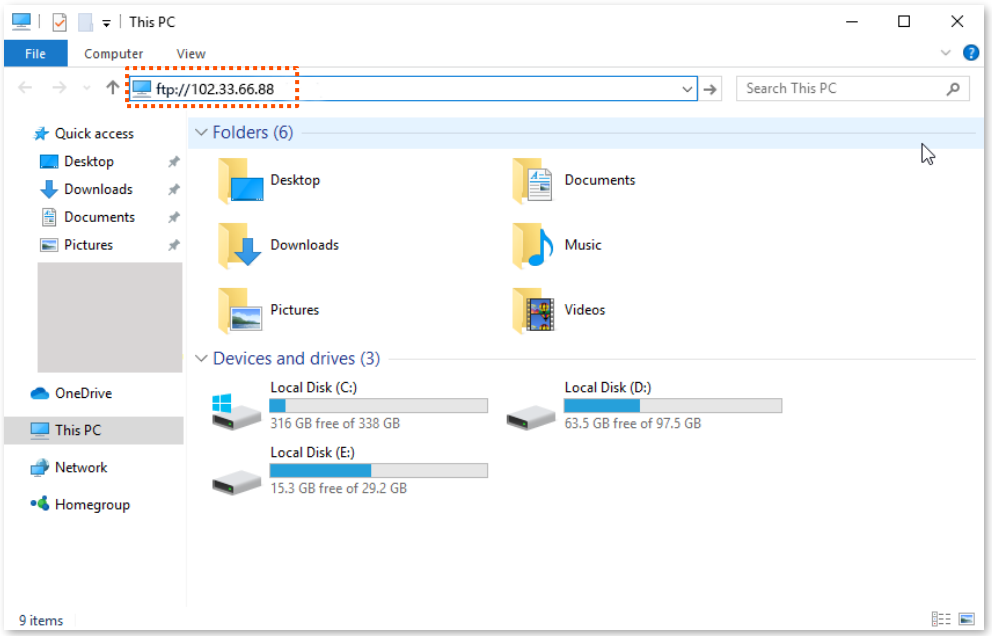


Step 6 Assign a fixed IP address to the host where the server locates.

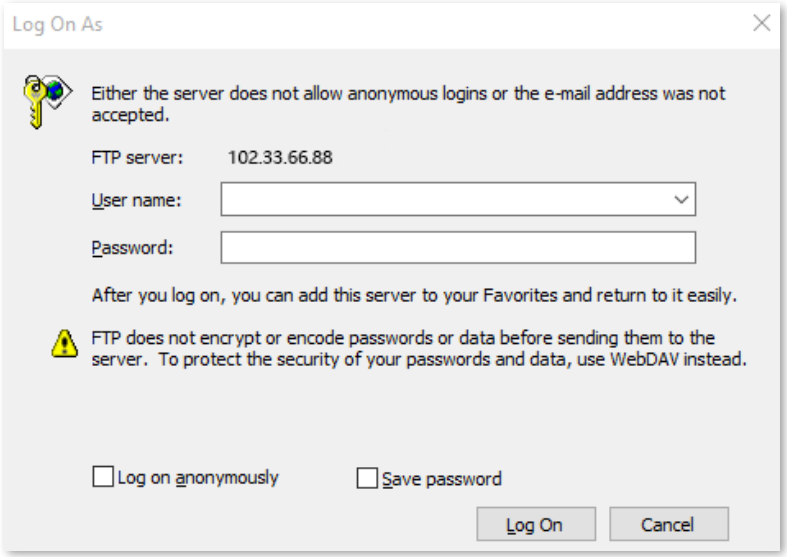
1. Navigate to **System Settings** > **DHCP Reservation**.
2. Specifies a **Device Name** for the host of the server, which is **FTP server** in this example.
3. Enter the **MAC Address** of the host of the server, which is **D4:61:DA:1B:CD:89** in this example.
4. Enter the **IP Address** of host of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

---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.

10.13 DMZ host

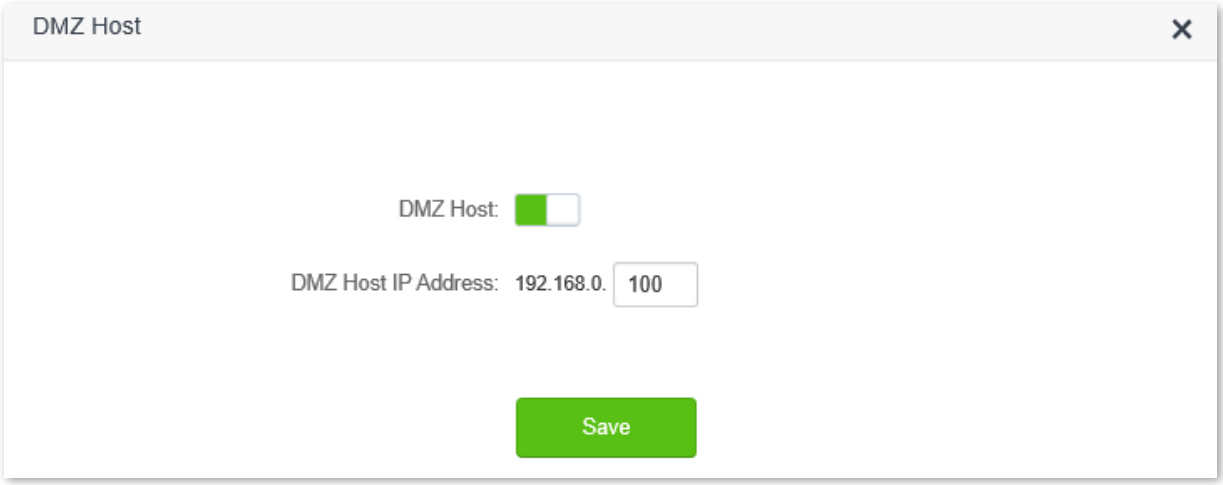
10.13.1 Overview

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 configuration page, log in to the web UI of the router, and navigate to **Advanced Settings** > **DMZ Host**.



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.

10.13.2 Enable internet users to access LAN resources

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

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

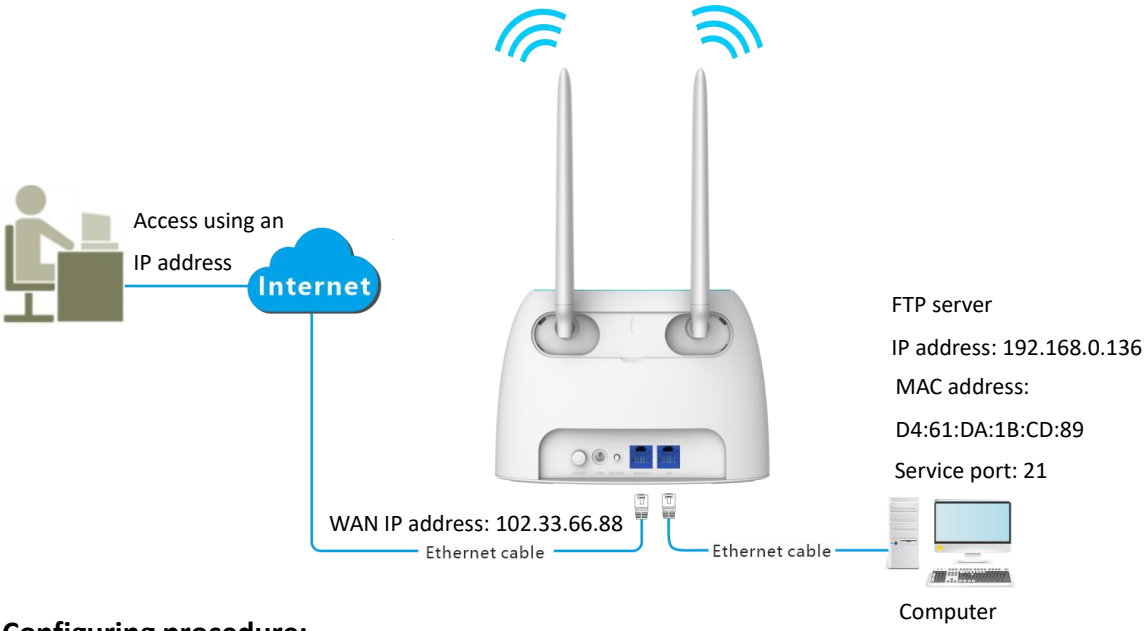
Solution: You can configure the DMZ host function to reach the requirements.

Assume that the information of the FTP server includes:

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

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.



Configuring procedure:

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

Step 2 Set the server host as the DMZ host.

1. Navigate to **Advanced Settings** > **DMZ Host**.
2. Enable **DMZ Host**.
3. Enter the IP address of the host, which is **192.168.0.136** in this example.

4. Click **Save**.

Step 7 Assign a fixed IP address to the host where the server locates.

1. Navigate to **System Settings** > **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. Enter the reserved IP Address for the server host, which is **192.168.0.136** in this example.
5. Click **+New**.

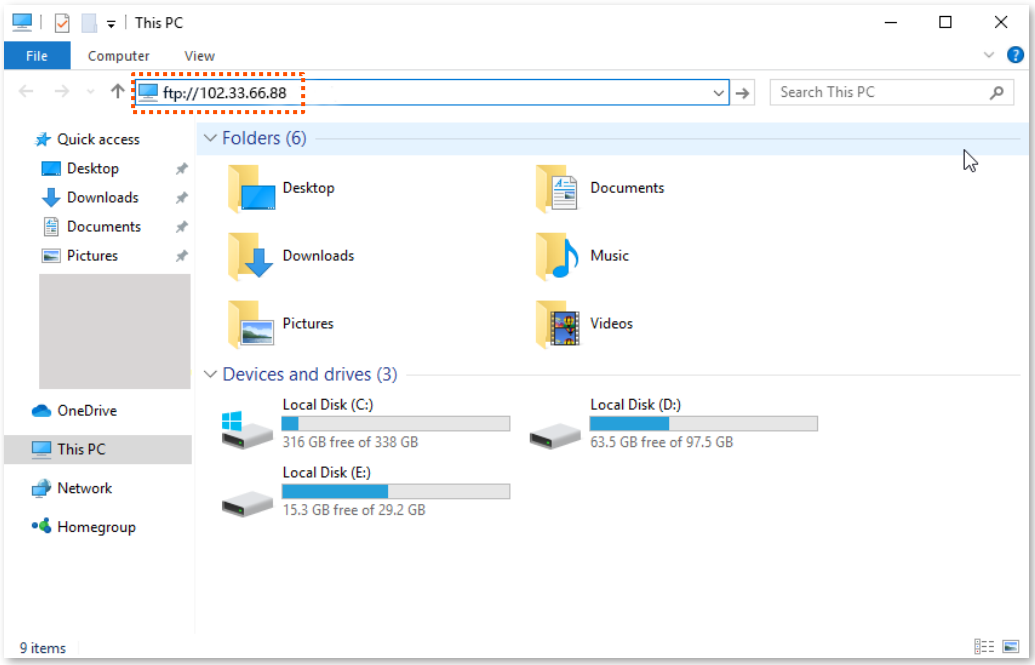
----End

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*".

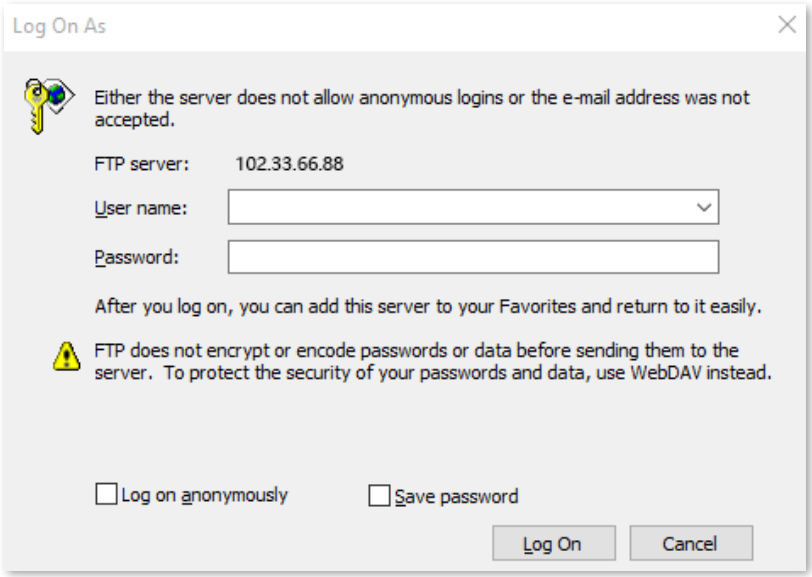
In this example, the address is "**ftp://102.33.66.88**". You can find the WAN IP address of the router in View system information.

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

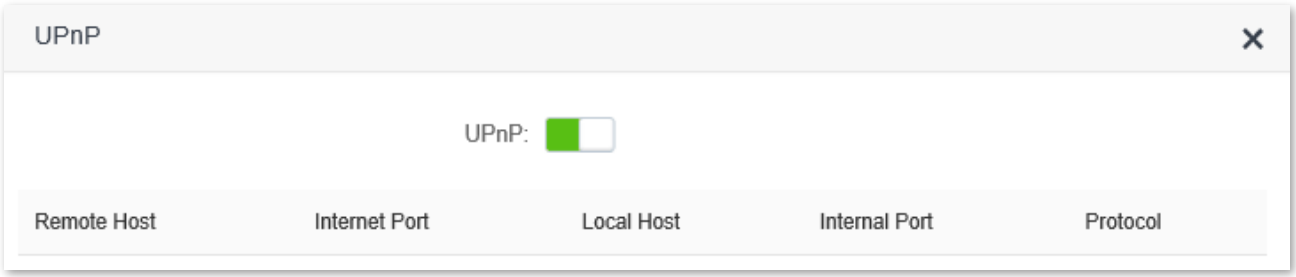
After the configurations, if internet users still cannot access the FTP server, close the firewall, antivirus software and security guards on the host of the FTP server and try again.

10.14 UPnP

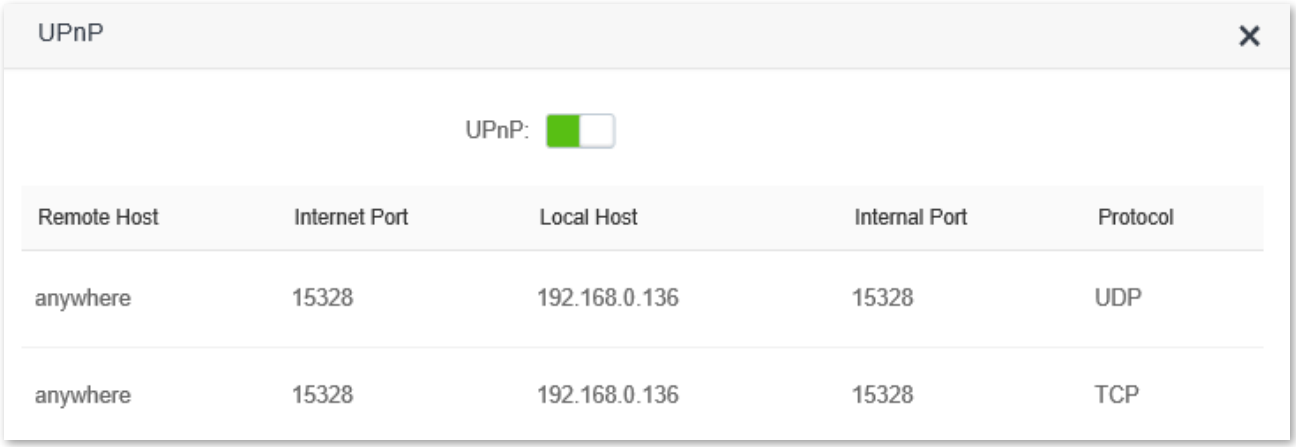
UPnP is short for Universal Plug and Play. This function enables the router open port automatically for UPnP-based programs. It is generally used for P2P programs, such as BitComet and AnyChat, and helps increase the download speed.

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

This function is enabled by default.



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



10.15 Antenna settings

This function is only available for 4G03 that supports external antenna installation (See figure 2). For details, check the antenna port of the router.

The antenna port of the router is shown as follows.

Not supported:	Supported:

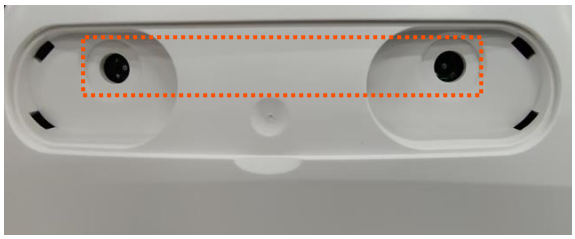
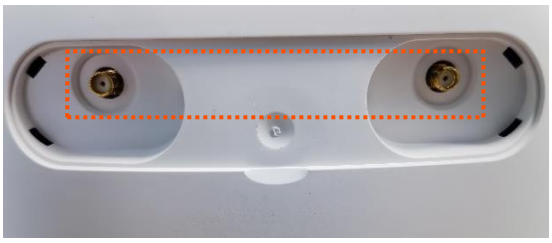

	

Figure 1	Figure 2

NOTE

Please gently remove the cover of antenna to avoid damaging the router. Contact our technical support if you still have questions about the installation of external antennas.

If the router supports external antenna installation and antenna setting function, see the following content.

TIP

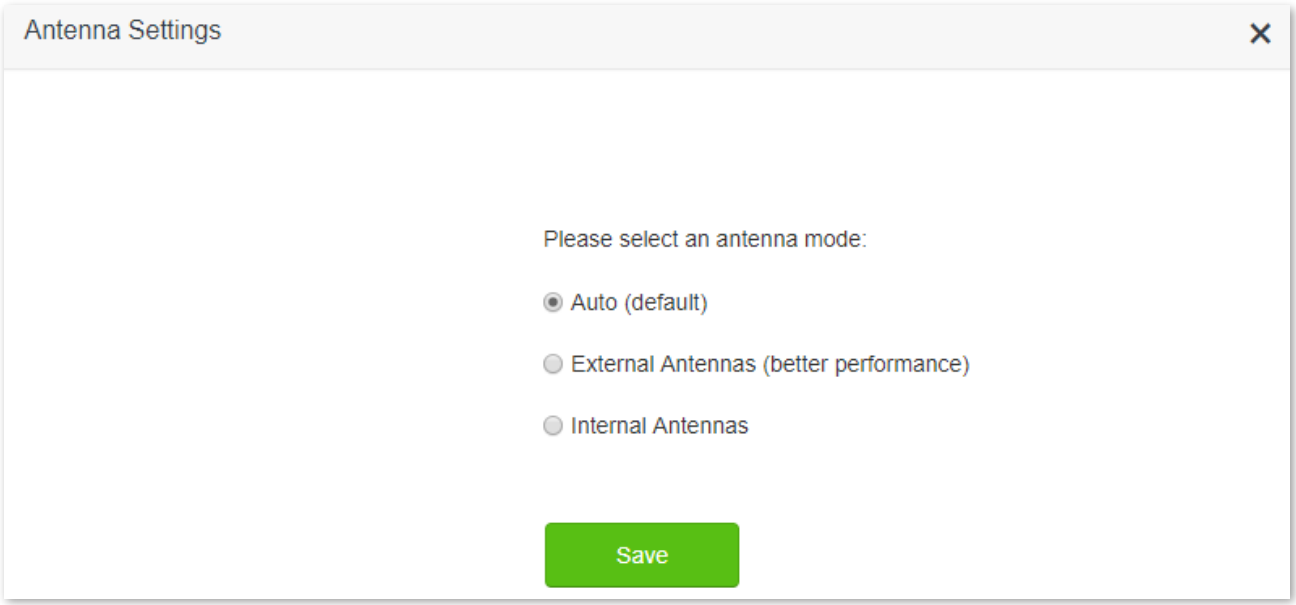
- The external antennas are not included in the package of 4G03, and you need to purchase separately.
- The external antennas can only enable the router to receive 3G/4G signal at a greater distance from the ISP.

Antenna settings enable you to choose the antennas used for receiving 3G/4G signal from the ISP. Compatible external antennas enable the router to receive3G/4G signal at a greater distance from the ISP.

Three modes are available for the router.

- **Auto (default)**: The router switches between internal and external antennas automatically based on whether external antennas are installed. When external antennas are installed, the router gives priority to external antennas.
- **External Antennas (better performance)**: The router receives and transmits 4G signal through external antennas. Under the wireless router mode, the setting does not work.
- **Internal Antennas**: The router receives and transmits 4G signal, or provides Wi-Fi network through internal antennas.

To access the configuration page, log in to the web UI of the router, and navigate to **Advanced Settings** > **Antennas Settings**. Choose the suitable mode as required.



11 System settings

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with product models. The actual product prevails.

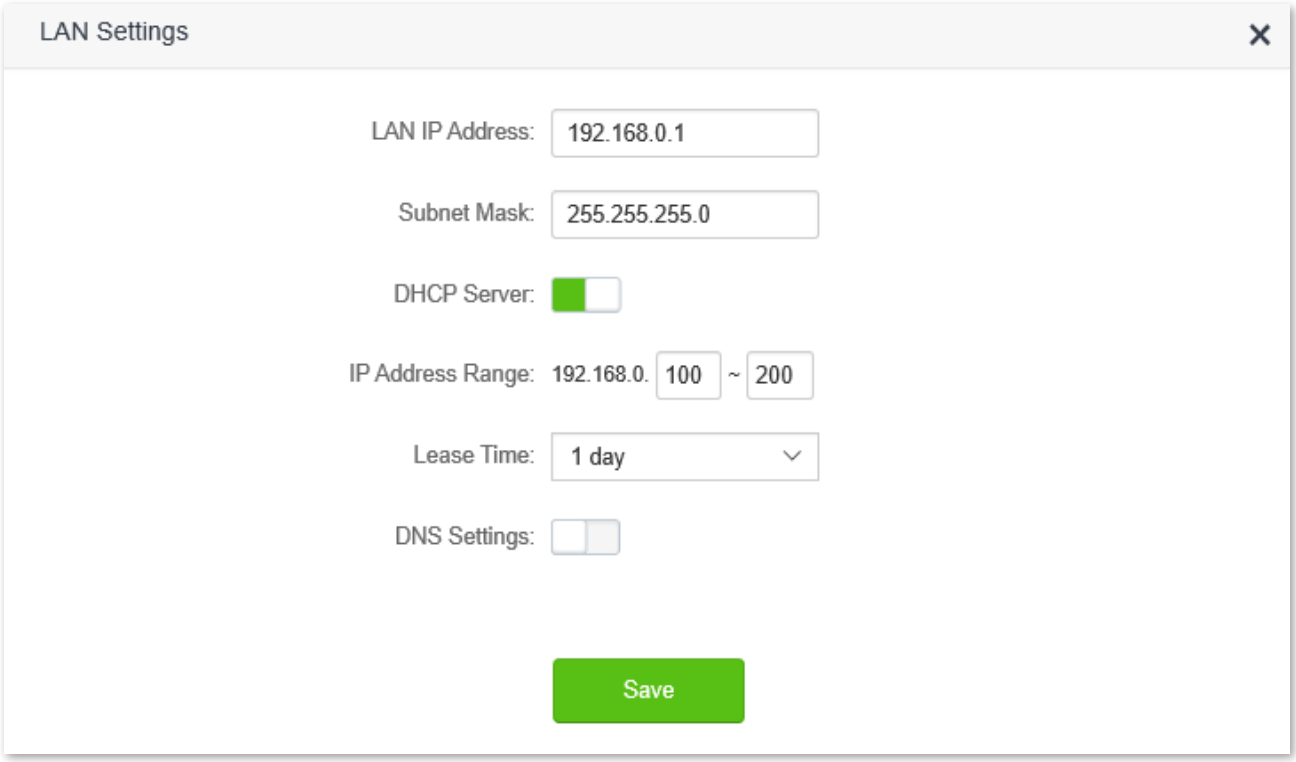
11.1 LAN settings

To access the configuration 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

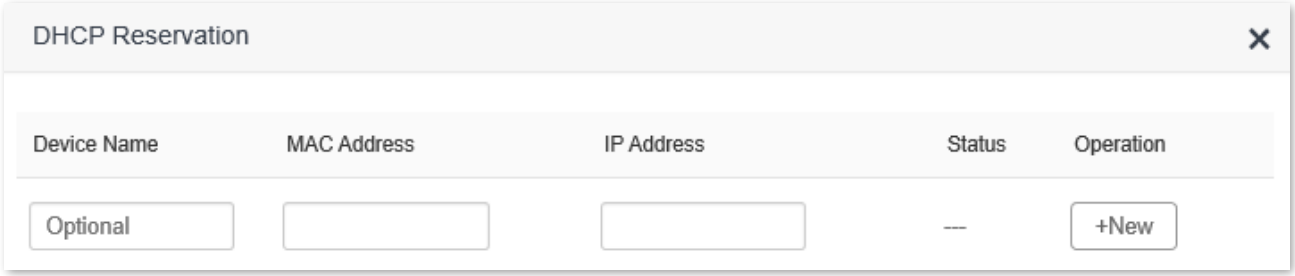
Parameter	Description
LAN IP Address	Specifies the LAN IP address of the router, which is also the management IP address for logging in to the web UI of the router.
Subnet Mask	Specifies the subnet mask of the LAN port, used to identify the IP address range of the local area network.
DHCP Server	Used 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 terminal device. This function is recommended to be enabled.
IP Address Range	Specifies the range of IP addresses that can be assigned to devices connected to the router. The default range is 192.168.0.100 to 192.168.0.200. It is required only when **DHCP Server** is enabled.
Lease Time	Specifies the valid duration of the IP address that is assigned to a client. It is required only when **DHCP Server** is enabled. 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.
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** must be set and **Secondary DNS** is optional. It is required only when **DHCP Server** is enabled. TIP 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. It is required only when **DNS Settings** is enabled. TIP Make sure that the primary DNS server is the IP address of the correct DNS server or DNS proxy. Otherwise, you may fail to access the internet.
Secondary DNS Server	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.

11.2 DHCP reservation

11.2.1 Overview

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

To access the configuration page, log in to the web UI of the router, and navigate to **System Settings** > **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	The available options include: +New : Used to add a new DHCP reservation rule. : Used to bind the MAC address to the reserved IP address. : Used to unbind the MAC address from the reserved IP address. : Used to delete the DHCP reservation rule.

11.2.2 Assign static IP addresses to LAN clients

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

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

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

Assume that the information of the FTP server includes:

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

Configuring procedure:

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

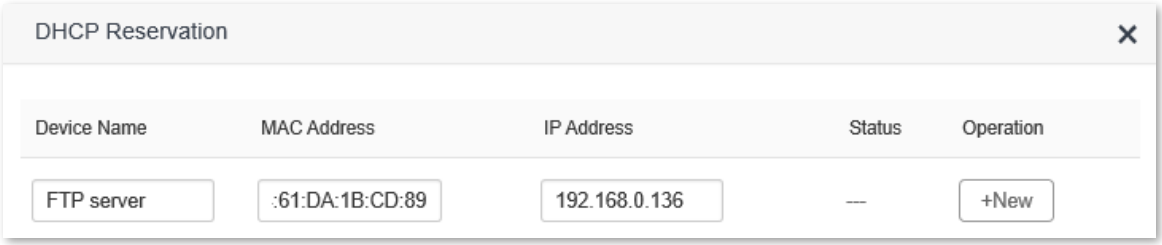
Step 2 Navigate to **System Settings** > **DHCP Reservation**.

Step 3 (Optional) Enter the **Device Name** for the host.

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

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

Step 6 Click **+New**.



---End

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

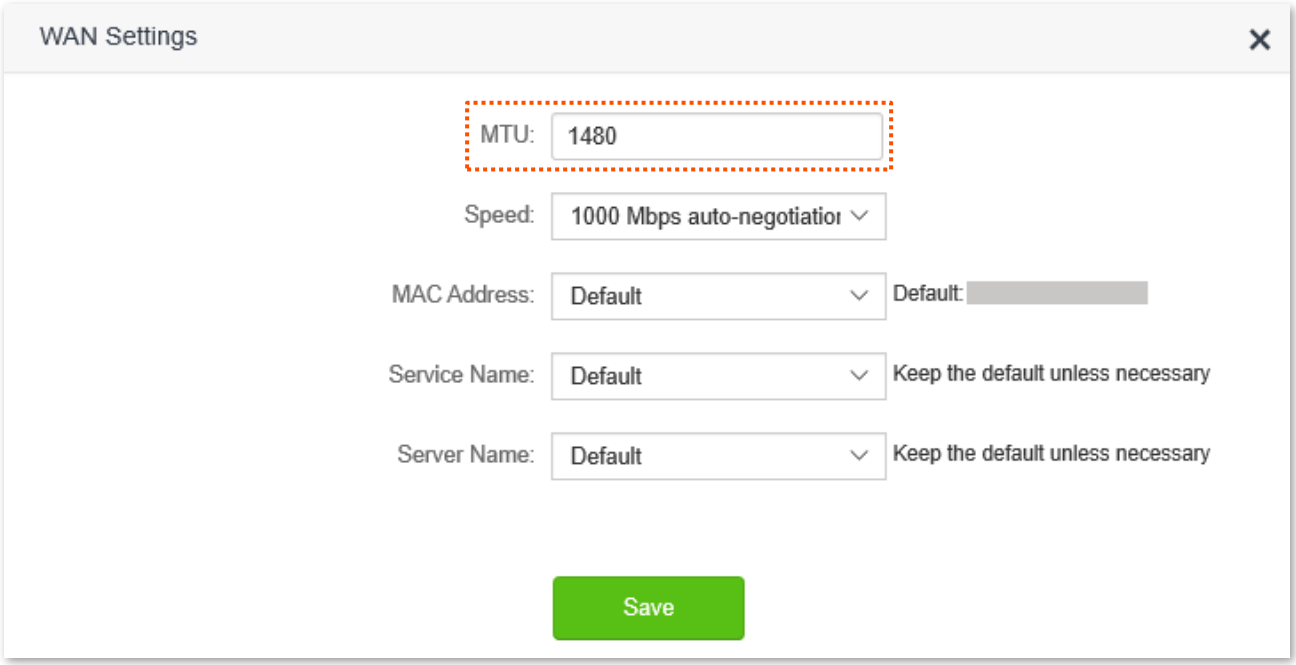
11.3 WAN settings

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

11.3.1 Change MTU value

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

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



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

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

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

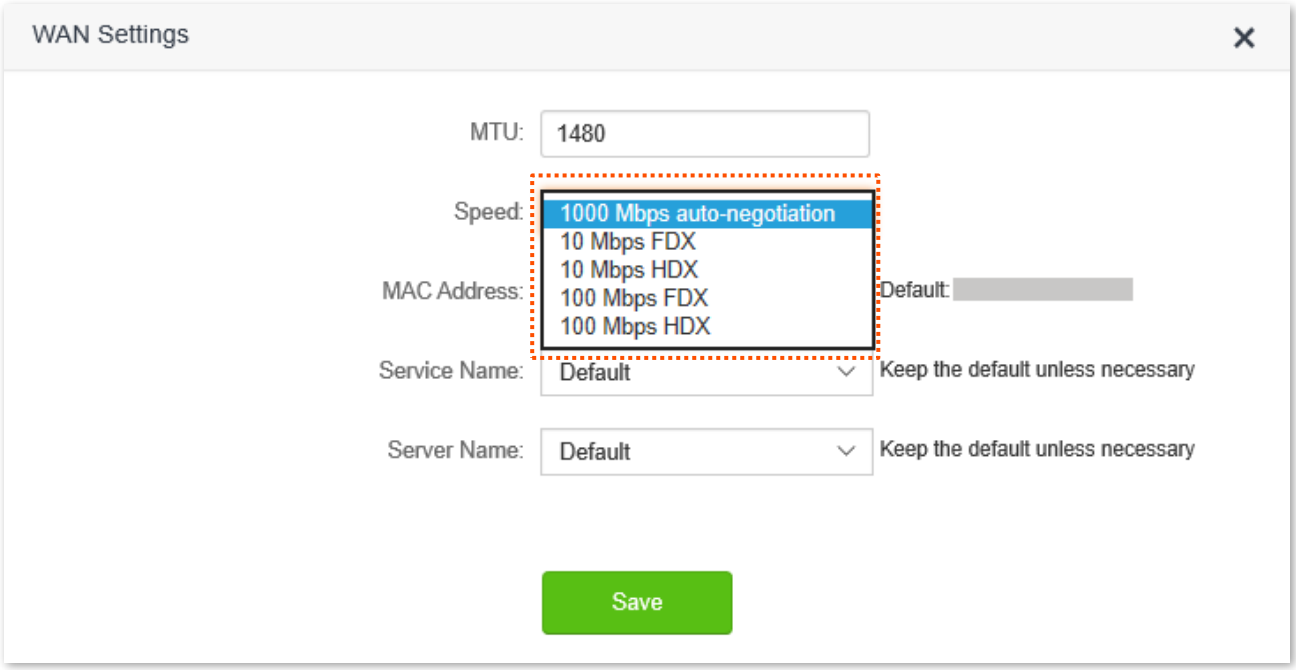
MTU application description

MTU	Application
1500	It is commonly used for non-ADSL and non-VPN dial-up connections.
1492, 1480	It is used for ADSL dial-up connections.
1472	It is the maximum value for the ping command. A packet with a larger size is fragmented.
1468	It is used for DHCP connections.
1436	It is used for VPN or PPTP connections.

11.3.2 Change the WAN speed and duplex mode

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

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



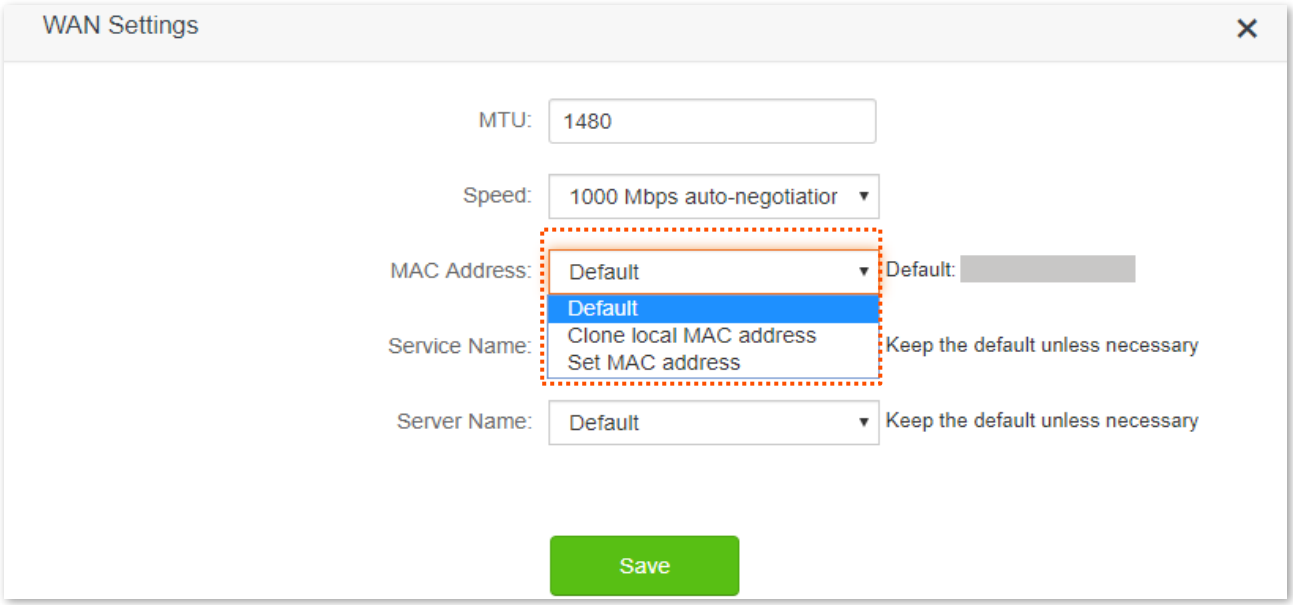
MTU parameter description

MTU	Application
1000 Mbps auto-negotiation	It indicates that the speed and duplex mode are determined through the negotiation with the peer port.
10 Mbps FDX	10 Mbps Full Duplex. It indicates that the WAN port is working at the speed of 10 Mbps, and the port can receive and send data packets at the same time.
10 Mbps HDX	10 Mbps Half Duplex. It indicates that the WAN port is working at the speed of 10 Mbps, but the port can only receive or send data packets alternately.
100 Mbps FDX	100 Mbps Full Duplex. It indicates that the WAN port is working at the speed of 100 Mbps, and the port can receive and send data packets at the same time.
100 Mbps HDX	100 Mbps Half Duplex. It indicates that the WAN port is working at the speed of 100 Mbps, but the port can only receive or send data packets alternately.

11.3.3 Change the MAC address of the WAN port

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

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



- **Default**: Keep the factory setting of MAC address.

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

NOTE

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

Configuration procedure:

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

Step 2 Navigate to **System Settings** > **WAN Settings.**

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

Step 4 Click **Save**.

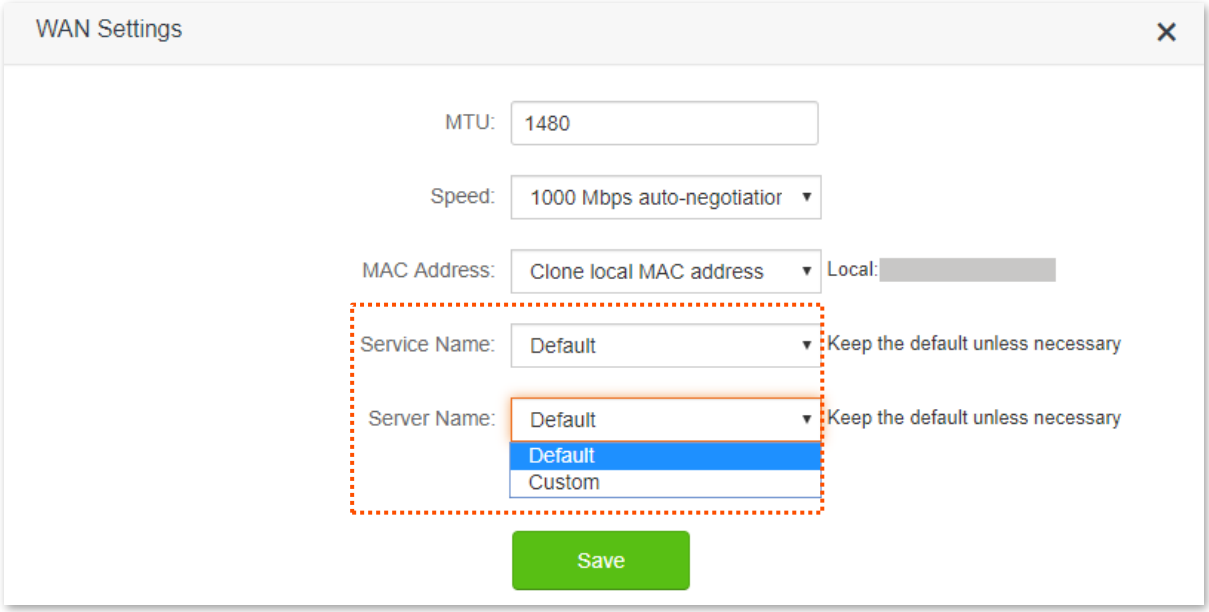
---End

11.3.4 Change the service name and server name

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

You may need to change the service name and server name of the broadband service only when the connection type is PPPoE.

If you obtain the service name and server name from your ISP when purchasing the broadband service, you can change them on this page after completing the internet settings. Otherwise, keep the default settings.



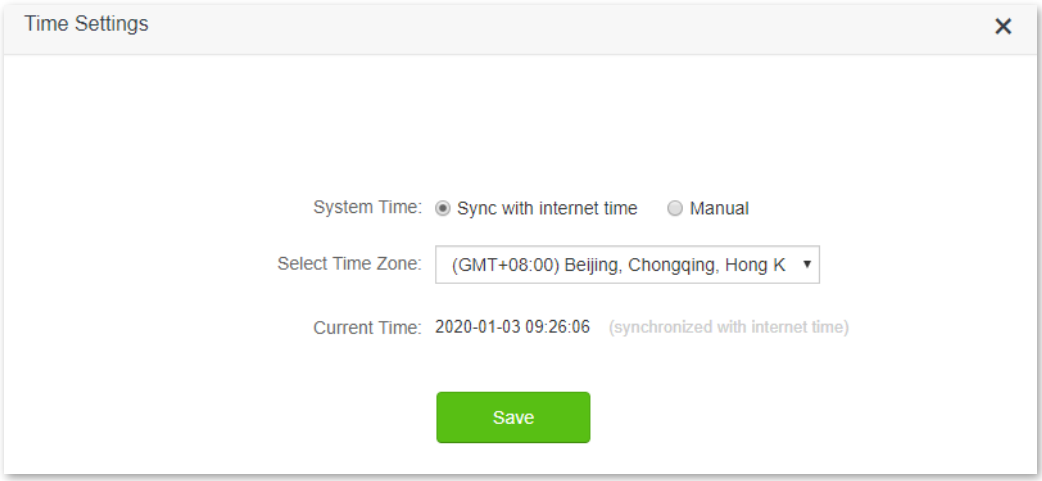
11.4 Time settings

To access the configuration 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 functioning of functions based on time requires an accurate system time. The system time of the router can be synchronized with the internet or set manually. By default, it is synchronized with the internet.

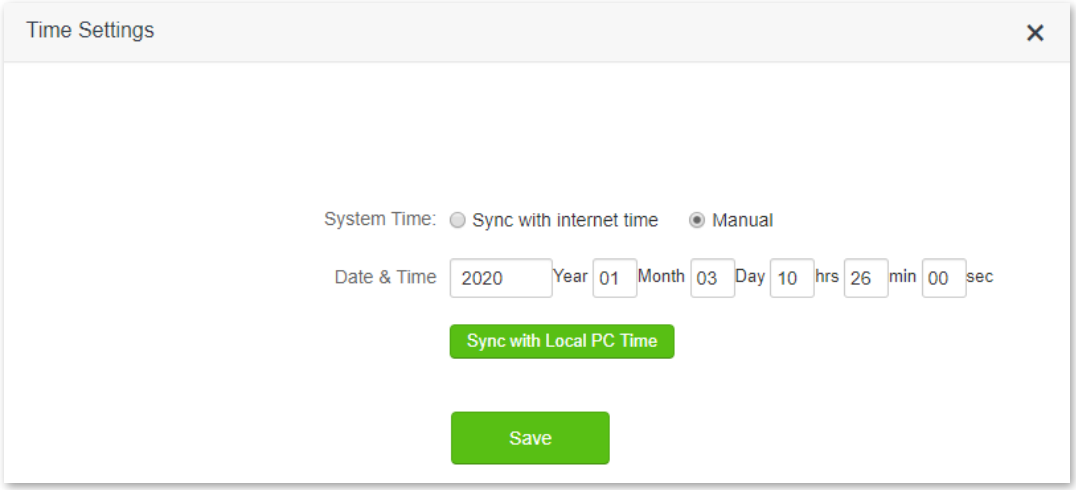
11.4.1 Sync system time with the internet time

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



11.4.2 Set the time manually

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

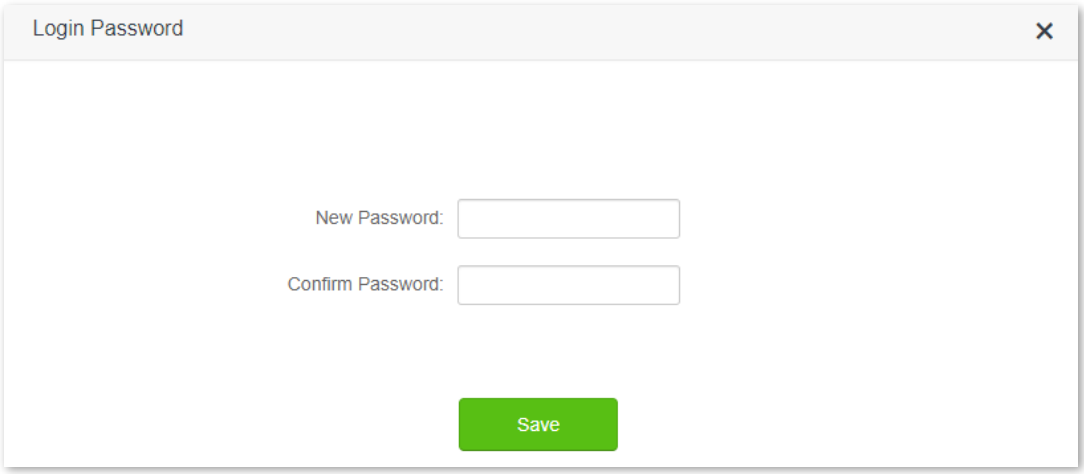


11.5 Login password

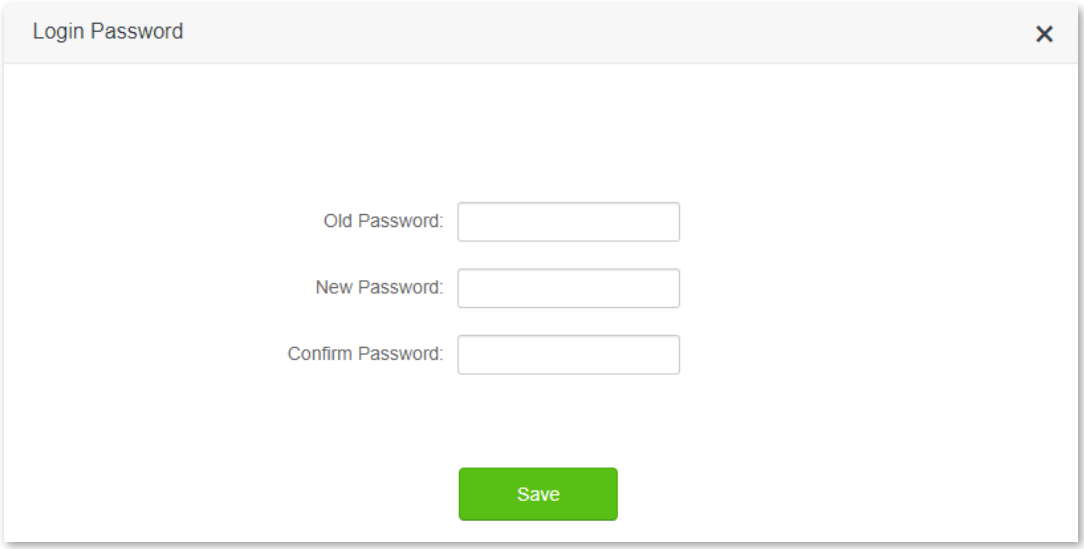
To ensure network security, a login password is recommended. A login password consisting of more types of characters, such as uppercase letters and lowercase letters, brings higher security.

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

When you use the router for the first time, no password is required to log in to the web UI of the router and 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 old password is required.



TIP

If you forget your login password and cannot log in to the web UI of the router, refer to reset the router to restore the router to factory settings and log in to the web UI without password.

11.6 Reboot and reset

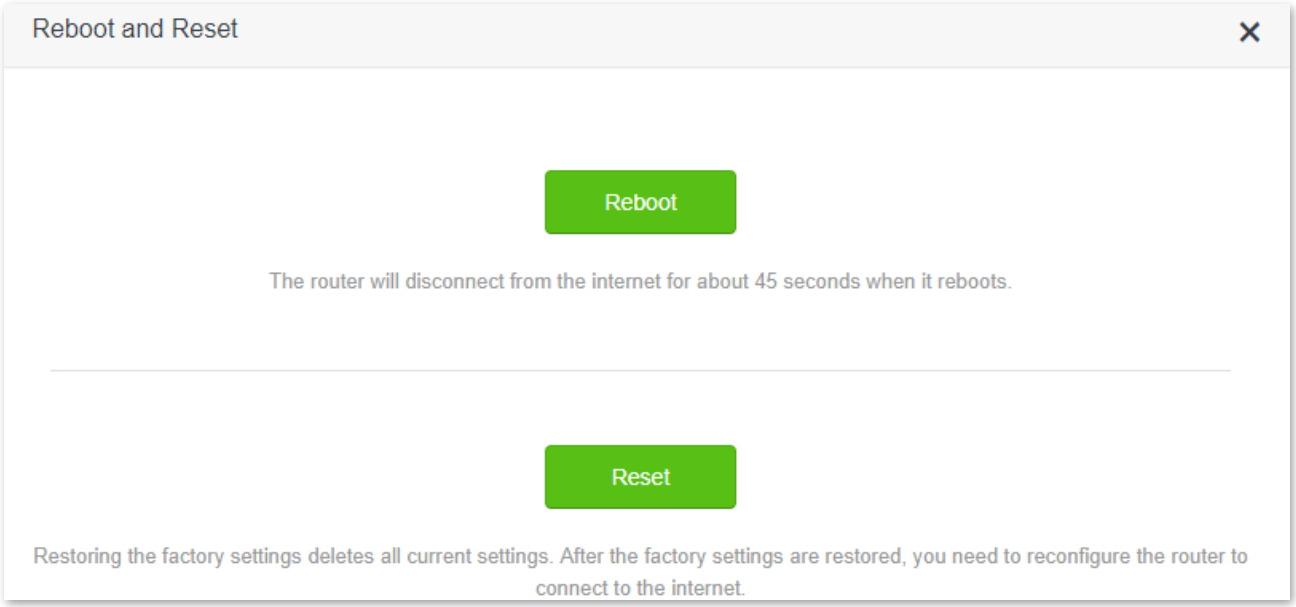
11.6.1 Reboot the router

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

TIP

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

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



Wait for a moment until the ongoing process finishes.

11.6.2 Reset the router

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

NOTE

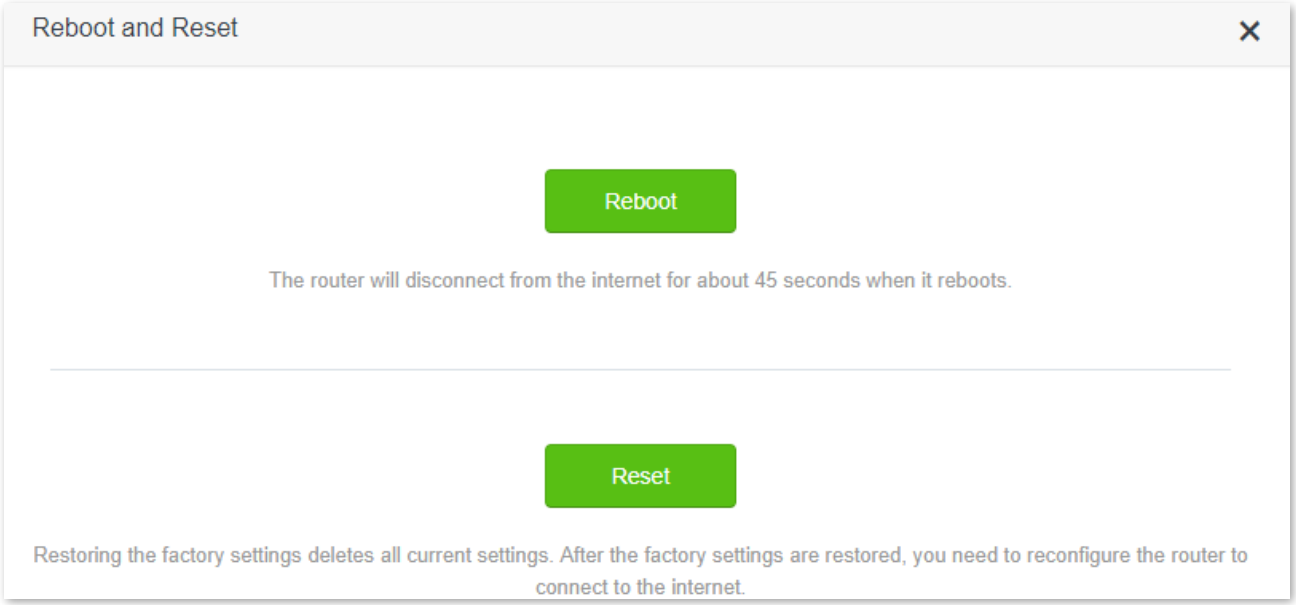
- Resetting the router is not recommended unless you cannot find a solution for the current problem anyway. You need to reconfigure the router after it is reset.
- Ensure that the power supply of the router is normal when the router is reset. Otherwise the router could be damaged.
- The default login IP address is 192.168.0.1 after resetting, and no password is required.

Reset the router using the reset button

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

Reset the router on the web UI

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



Wait for a moment until the ongoing process finishes.

11.7 Upgrade firmware

This function enables the router to obtain the latest functions and more stable performance. It is recommended that the router uses the latest firmware version. On this page, you can configure the online firmware upgrade and local firmware upgrade.

11.7.1 Online upgrade

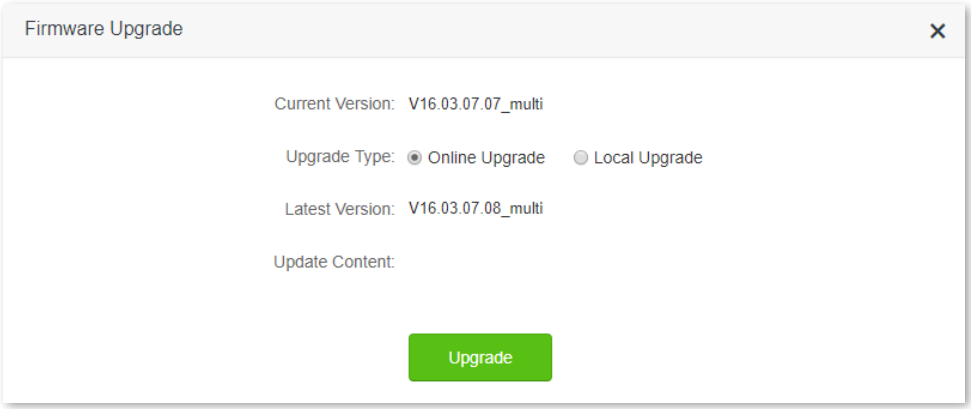
When the router is connected to the internet, it auto-detects whether there is a new firmware and displays the detected information on the page. You can choose whether to upgrade to the latest firmware.

Configuration procedure:

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

Step 1 Navigate to **System Settings** > **Firmware Upgrade**.

Step 2 Wait until a new firmware version is detected.



Step 3 Click **Update**.

---End

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

11.7.2 Local upgrade

NOTE

To prevent the router from being damaged:

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

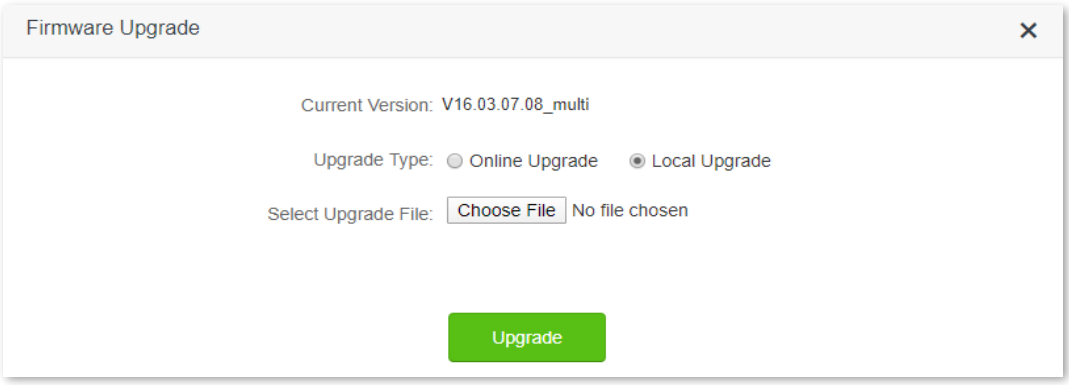
Step 1 Go to www.tendacn.com. Download an applicable firmware of the router to your local computer and unzip it.

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

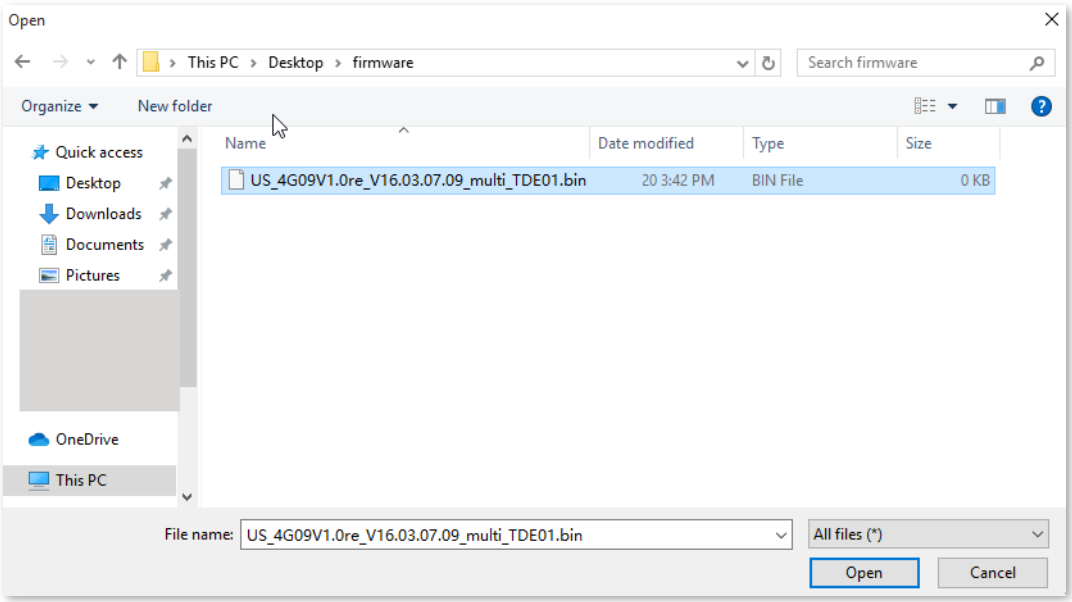
Step 3 Navigate to **System Settings** > **Firmware Upgrade.**

Step 4 Choose **Local Upgrade**.

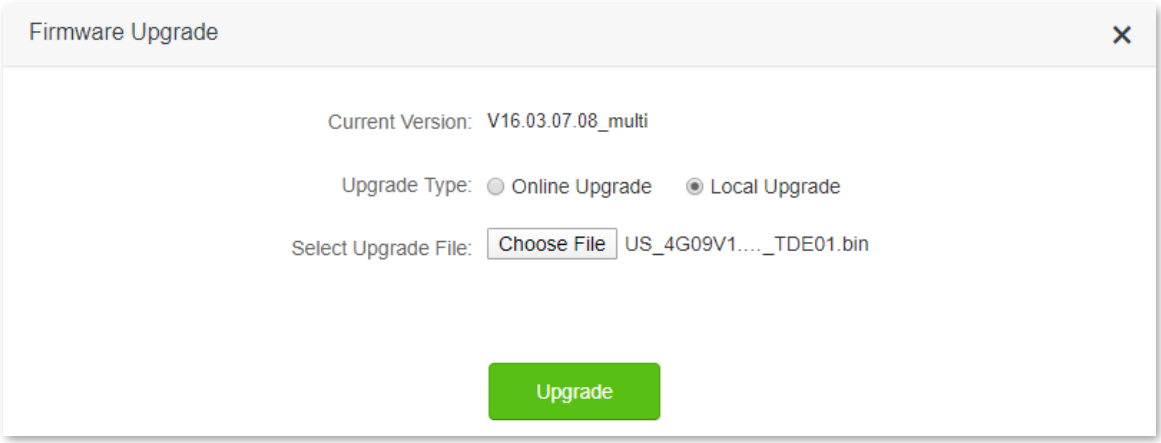
Step 5 Click **Choose File**.



Step 6 Locate the firmware file downloaded previously (extension: bin), and click **Open.**



Step 7 Click **Upgrade**.



---End

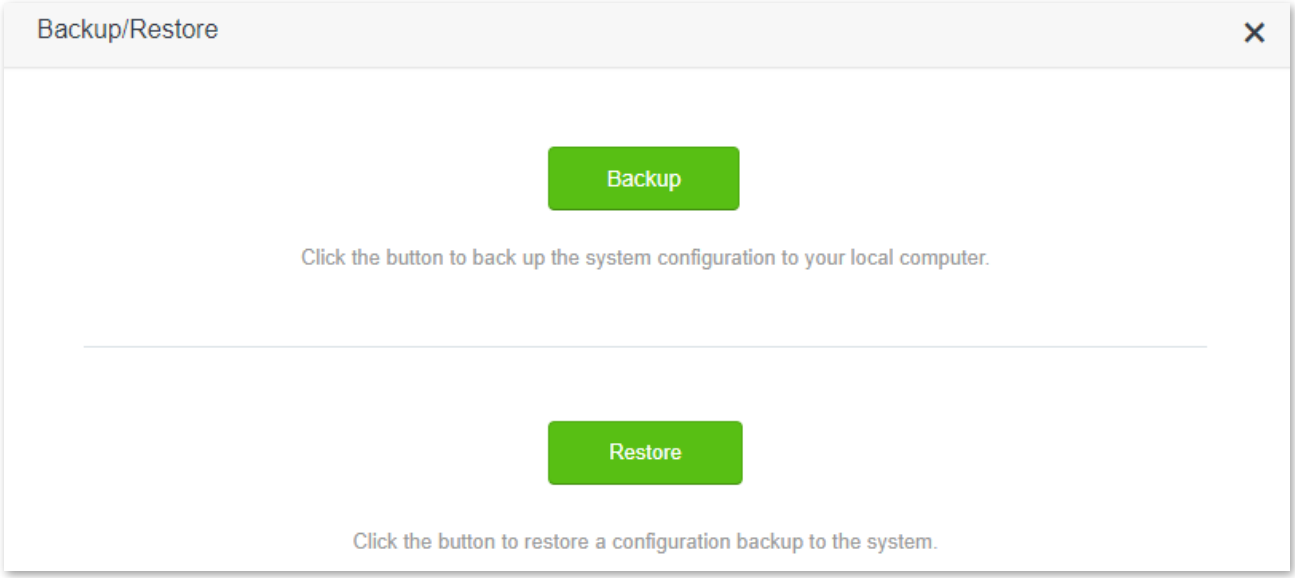
Wait for a moment until the ongoing process finishes. Log in to the web UI of the router again. Navigate to **System Settings** > **System Status** and check whether the upgrade is successful based on the **Firmware Version**.

11.8 Backup/Restore

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

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

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



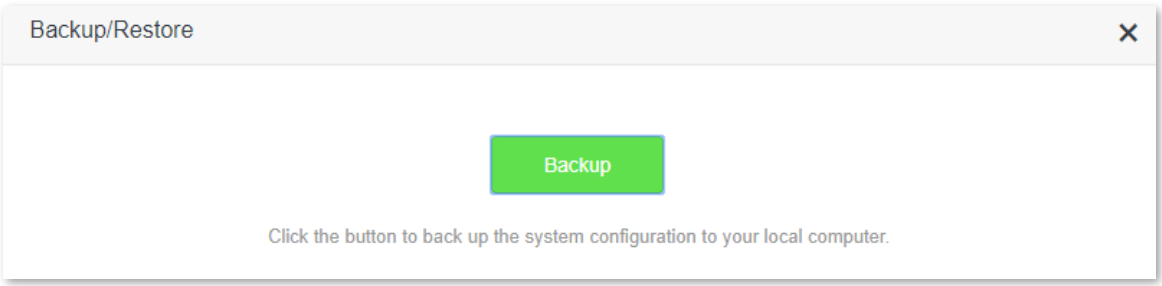
11.8.1 Back up the configurations of the router

To back up the configurations of the router:

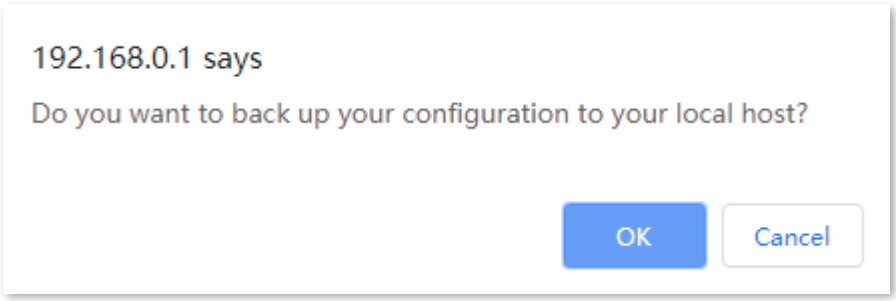
Step 1 Log in to the web UI of the router.

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

Step 3 Click **Backup**.



Step 4 Click **OK** in the pop-up window.



---End

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

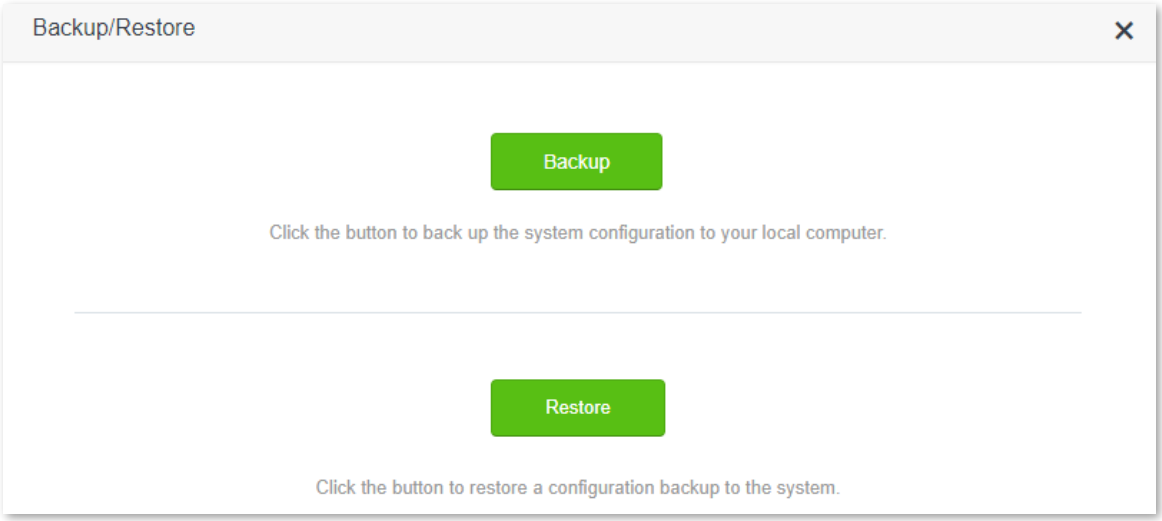
11.8.2 Restore previous configurations of the router

To restore the previous configurations of the router:

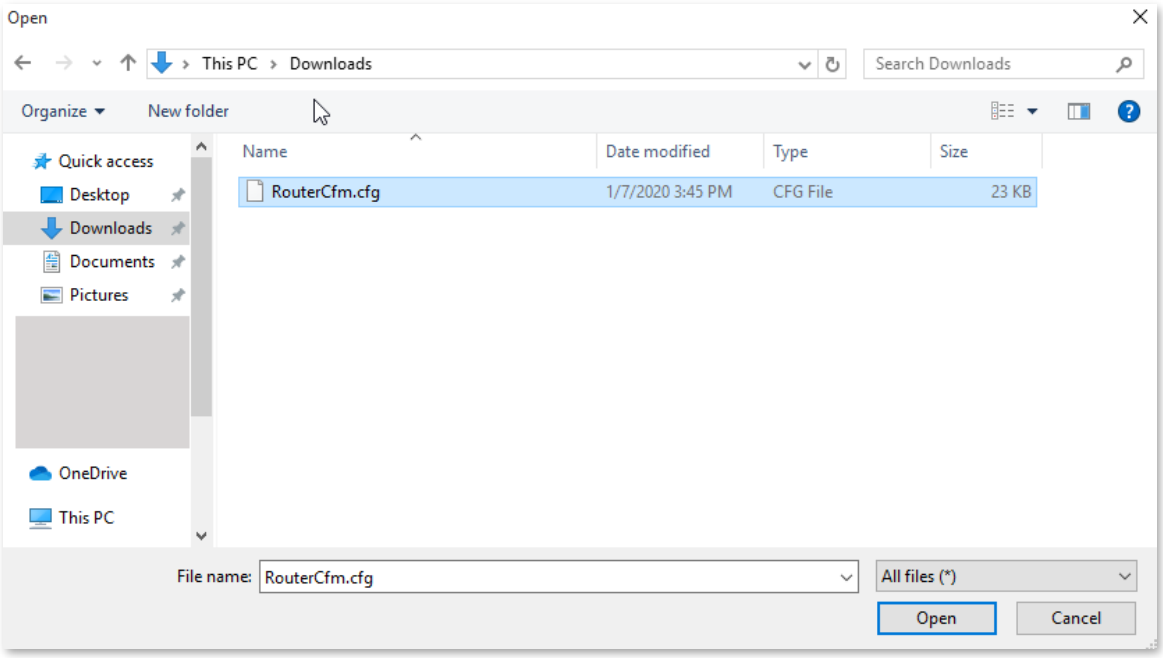
Step 1 Log in to the web UI of the router.

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

Step 3 Click **Restore**.



Step 4 Choose the configuration file (extension: cfg) to be restored, and click **Open**.



---End

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

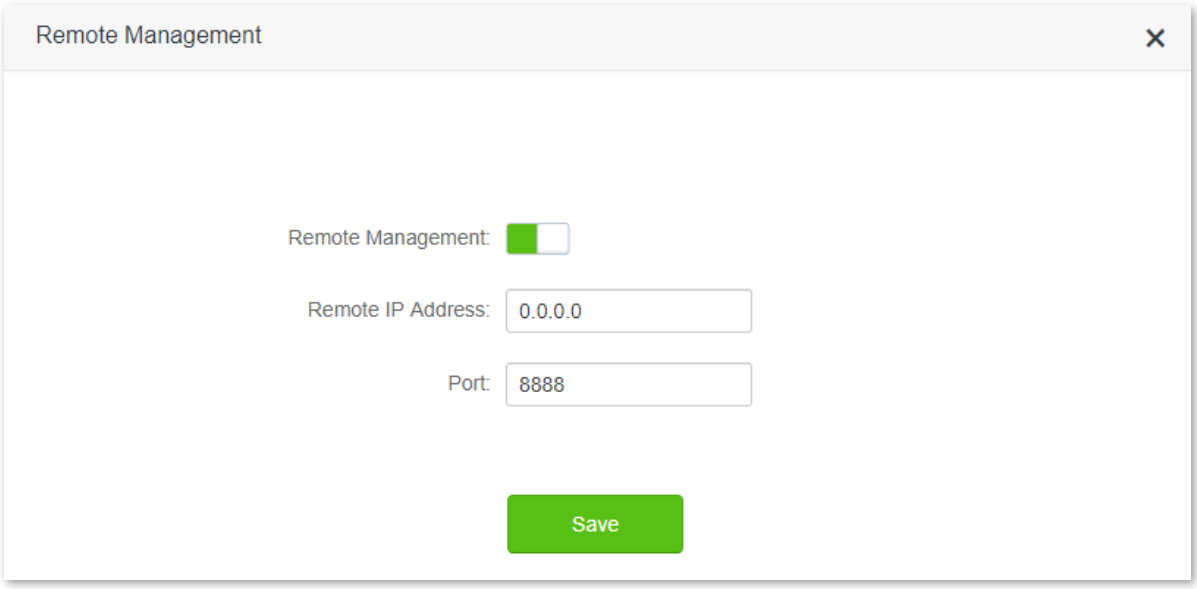
11.9 Remote management

11.9.1 Overview

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

To access the configuration page, log in to the web UI of the router, and 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”.

11.9.2 Enable Tenda technical support to access and manage the web UI

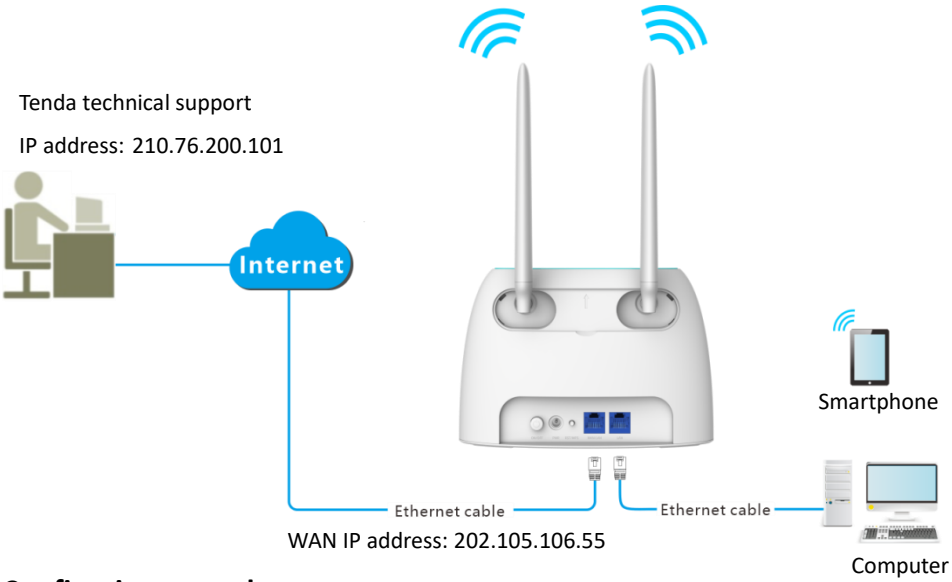
Scenario: You encounter a problem in configuring the router, and the router can access internet access.

Requirements: 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



Configuring procedure:

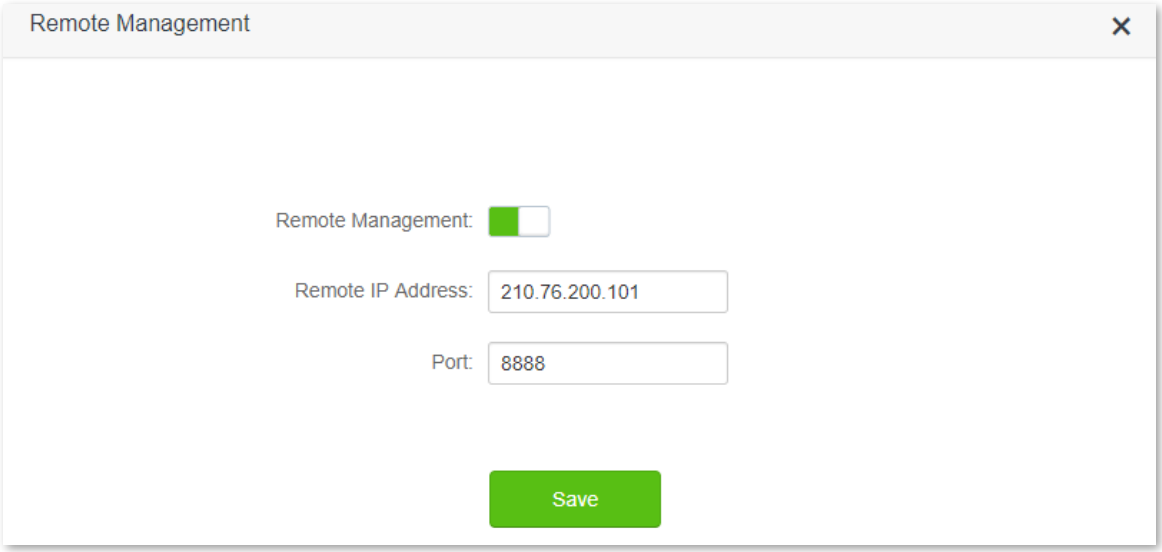
Step 1 Log in to the web UI of the router.

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

Step 3 Enable the **Remote Management**.

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

Step 5 Click **Save**.



---End

When the configurations are 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.

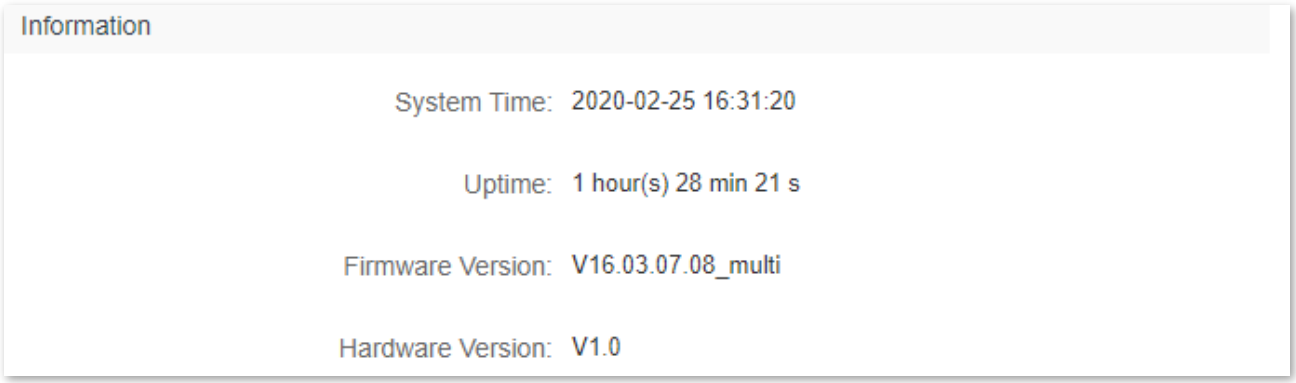
11.10 System status

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

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

11.10.1 Basic information

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



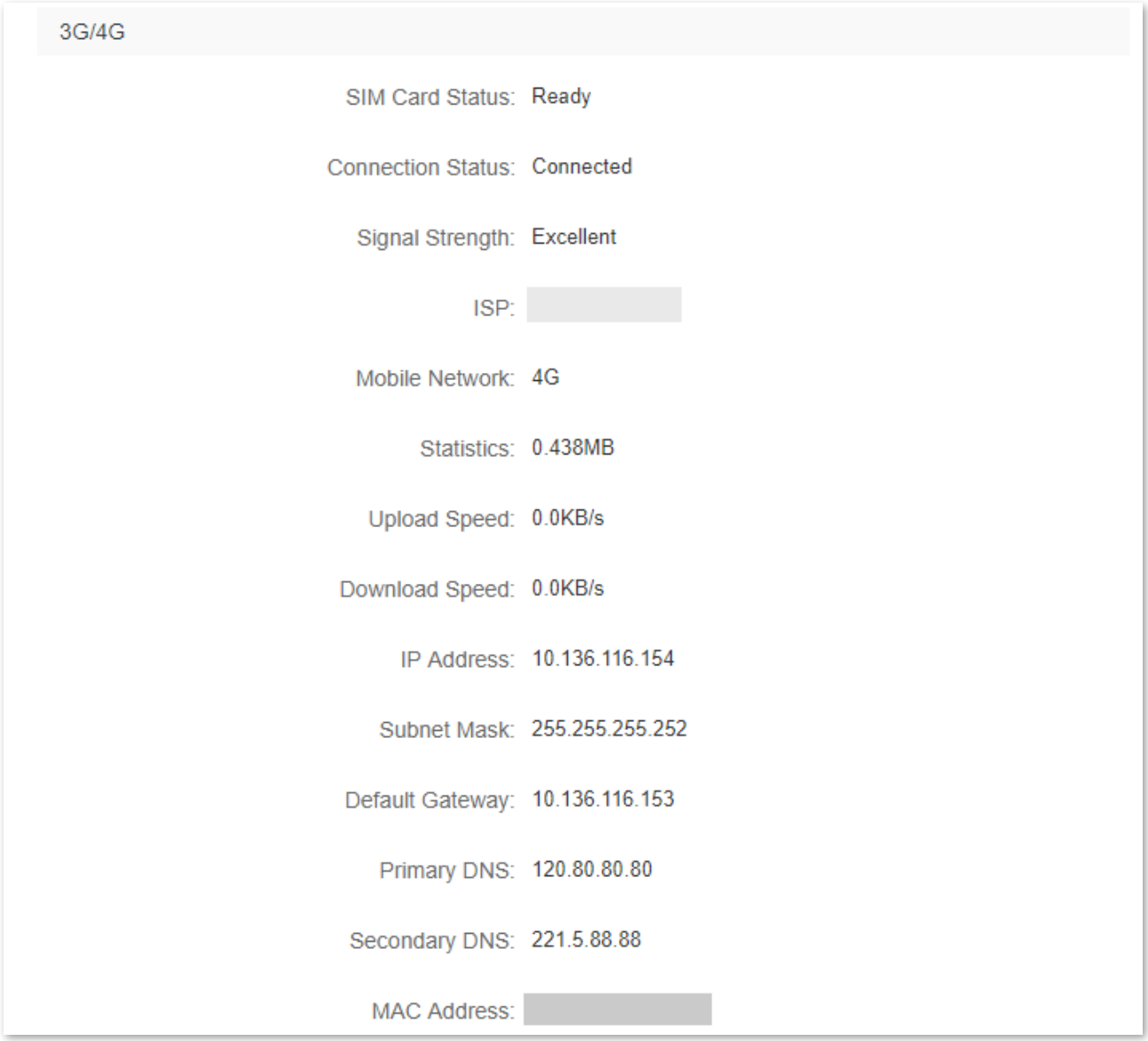
Parameter description

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.

11.10.2 Connection status

3G/4G

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



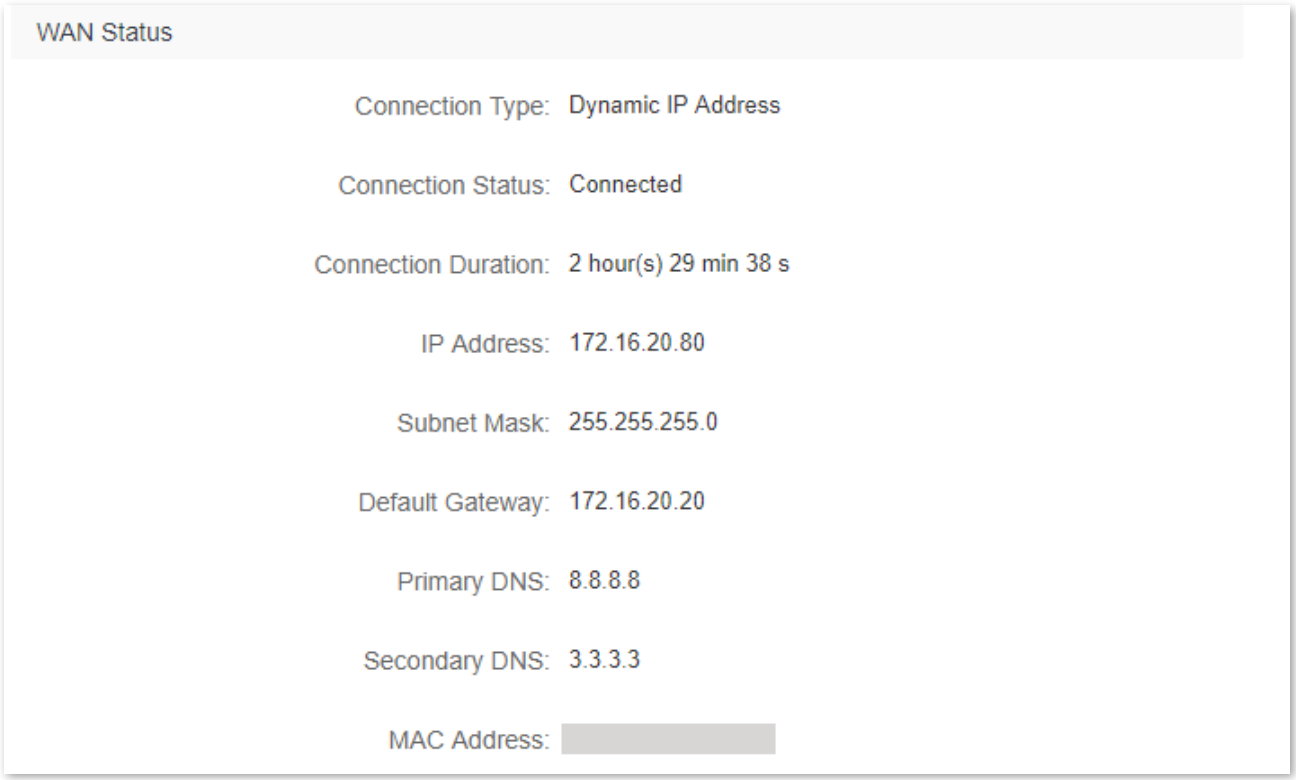
Parameter description

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

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

WAN status

On this page, you can view the information of the WAN port, including connection type, connection status and connection duration, and so on.

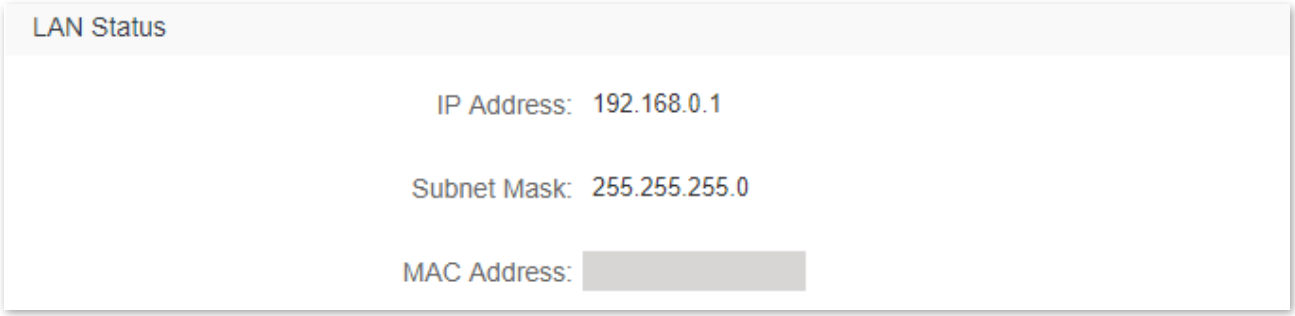


Parameter description

Parameter	Description
Connection Type	Specifies the IPv4 connection type of the WAN port.
Connection Status	Specifies internet connection status of the WAN port.
Connection Duratoin	Specifies the duration since the router is connected to the internet.
IP address	Specifies the WAN IP address of the router.
Subnet Mask	Specifies the WAN subnet mask of the router.
Default Gateway	Specifies the gateway IP address of the router.
Primary DNS	Specify the IP address of primary and secondary DNS servers of the router.
Secondary DNS	
MAC Address	Specifies the WAN MAC address of the router.

11.10.3 LAN status

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

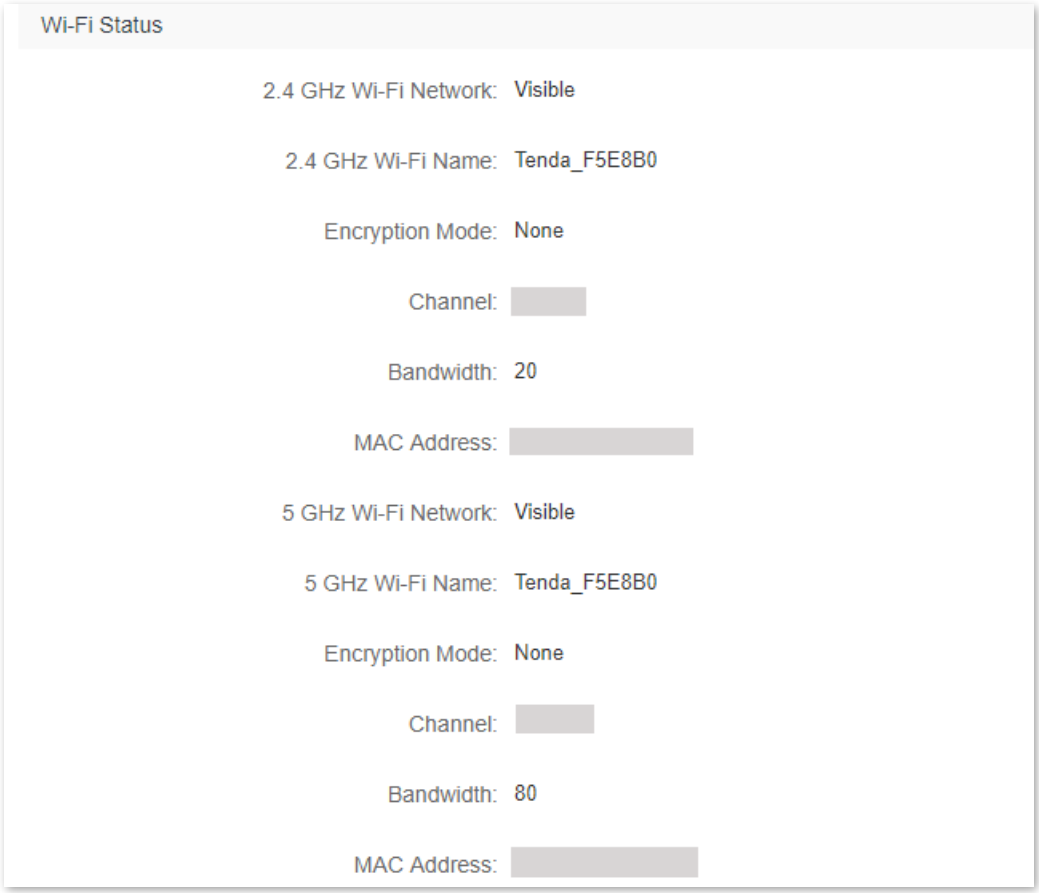


Parameter description

Parameter	Description
IP Address	Specifies the LAN IP address of the router, and the IP address for logging in to the web UI of the router.
Subnet Mask	Specifies the LAN subnet mask of the router.
MAC Address	Specifies the LAN MAC address of the router.

11.10.4 Wi-Fi status

In this part, you can view the information of 2.4 GHz and 5 GHz Wi-Fi network, including the connection status, visibility, hotspot name and encryption mode, and so on.

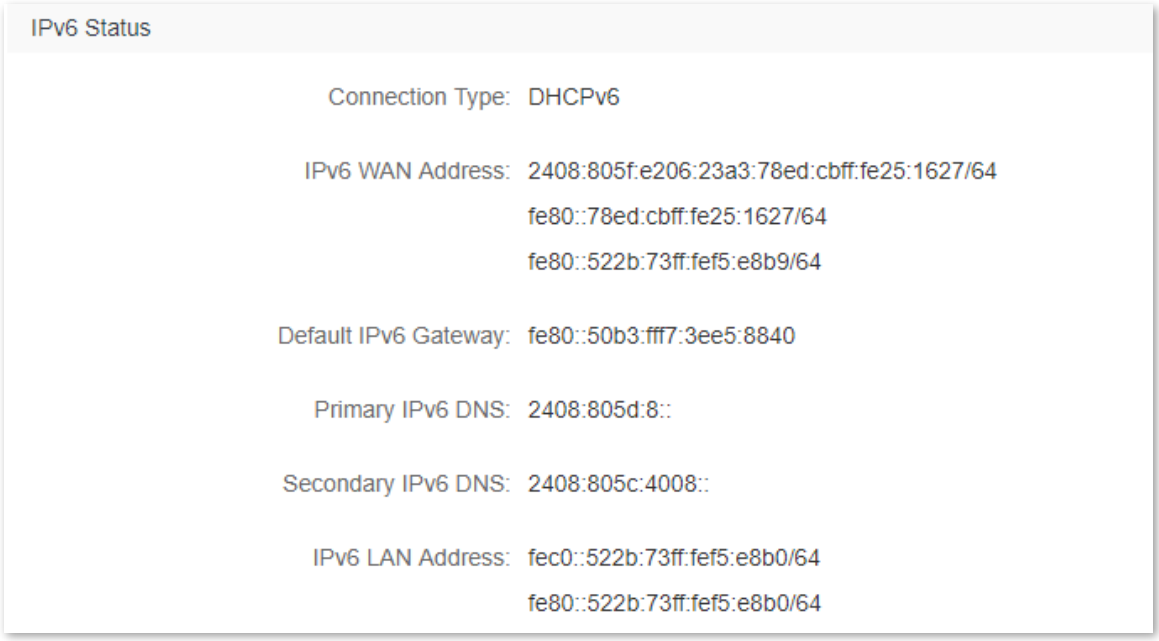


Parameter description

Parameter	Description
2.4 GHz Wi-Fi Network	Specify whether the corresponding Wi-Fi network is enabled or disabled, and the visibility of the Wi-Fi network.
5 GHz Wi-Fi Network	
2.4 GHz Wi-Fi Name	Specify the 2.4 GHz Wi-Fi and 5 GHz Wi-Fi name of the router.
5 GHz Wi-Fi Name	
Encryption Mode	Specifies the encryption mode of the respective Wi-Fi network.
Channel	Specifies the channel that the respective Wi-Fi network works in.
Bandwidth	Specifies the bandwidth of the respective Wi-Fi network.
MAC Address	Specifies the MAC address of the respective Wi-Fi network.

11.10.5 IPv6 status

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



Parameter description

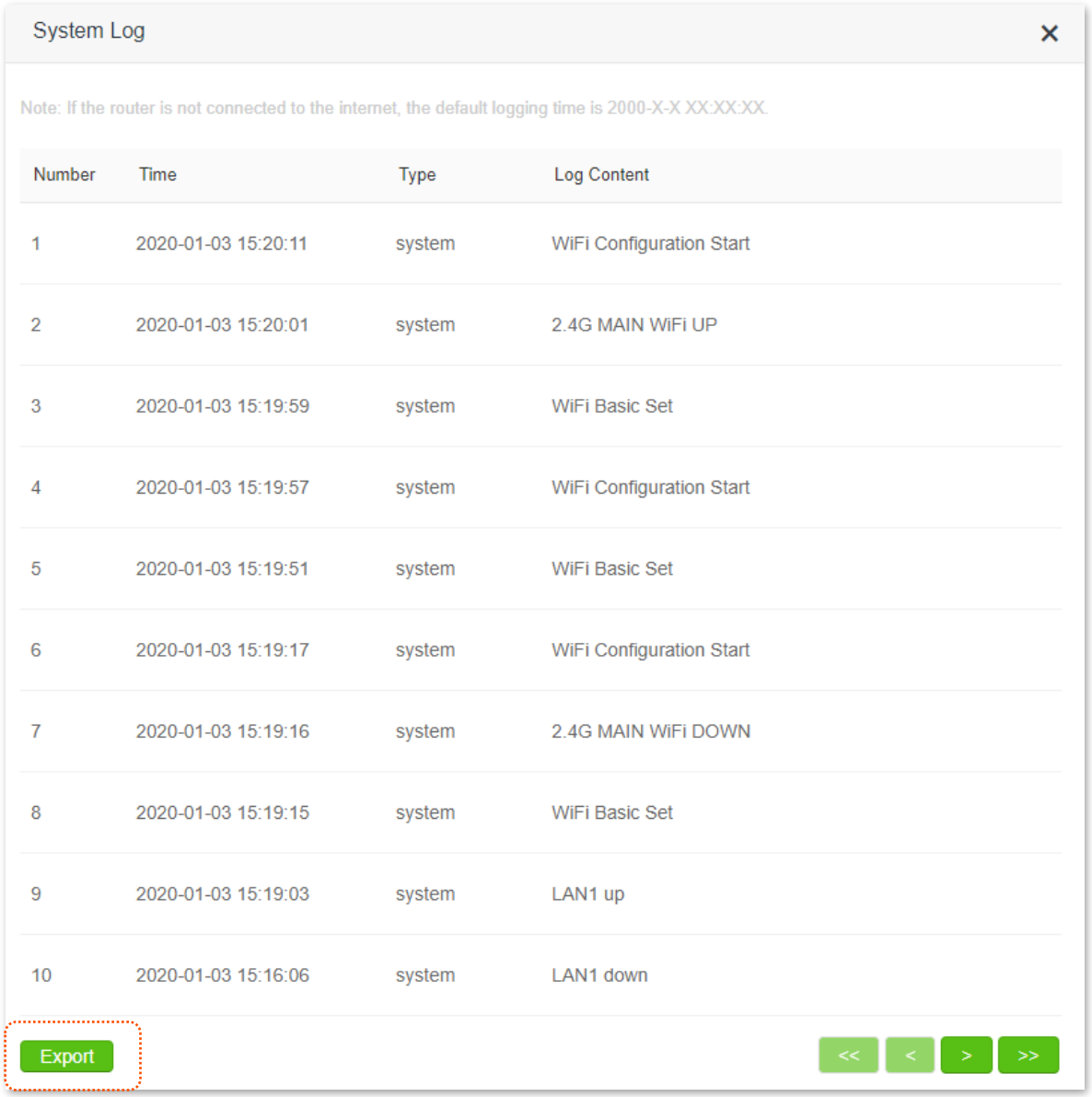
Parameter	Description
Connection Type	Specifies the IPv6 connection type of the router.
IPv6 WAN Address	Specifies the WAN IPv6 address of the router. After the IPv6 function is configured, the WAN port of the router obtains a global unicast IPv6 address or a tunnel address.
Default IPv6 Gateway	Specifies the primary DNS server address of IPv6 network.
Primary IPv6 DNS	Specify the primary and secondary DNS server address of IPv6 network.
Secondary IPv6 DNS	
IPv6 LAN Address	Specifies the LAN IPv6 address of the router. After the IPv6 function is configured, the LAN port of the router obtains a global unicast IPv6 address or a tunnel address, and a link local address.

11.11 System log

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

This function logs all key events that occur after the router is started. If you encounter a network fault, you can turn to system logs for fault rectification.

If necessary, you can also export the system logs to your local computer by clicking **Export**.



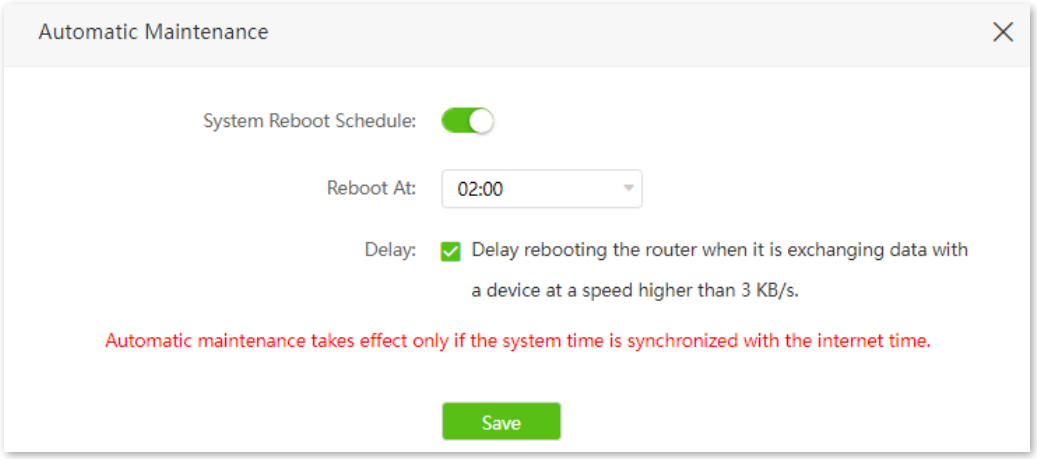
TIP

Rebooting the router will clear all previous system logs.

11.12 Automatic maintenance

Automatic maintenance enables you to make the router restart regularly. It helps improve the stability and service life of the router. This function is enabled by default.

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



Parameter description

Parameter	Description
System Reboot Schedule	Used to enable or disable the automatic reboot function.
Reboot At	Specifies the time when the router reboots automatically every day.
Delay	Used to enable or disable the delay function. - **Ticked**: The function is enabled. When the time for rebooting approaches, if there is any user connected to the router and the traffic over the router's WAN port exceeds 3 KB/s within 30 minutes, the router will delay rebooting. If there is any user connected to the router and the traffic over the WAN port does not exceed 3 KB/s within 30 minutes, or there is no user connected to the router and the traffic over the router's WAN port is slower than 3 KB/s within 3 minutes, the router will reboot automatically. - **Unticked**: The function is disabled. The router 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

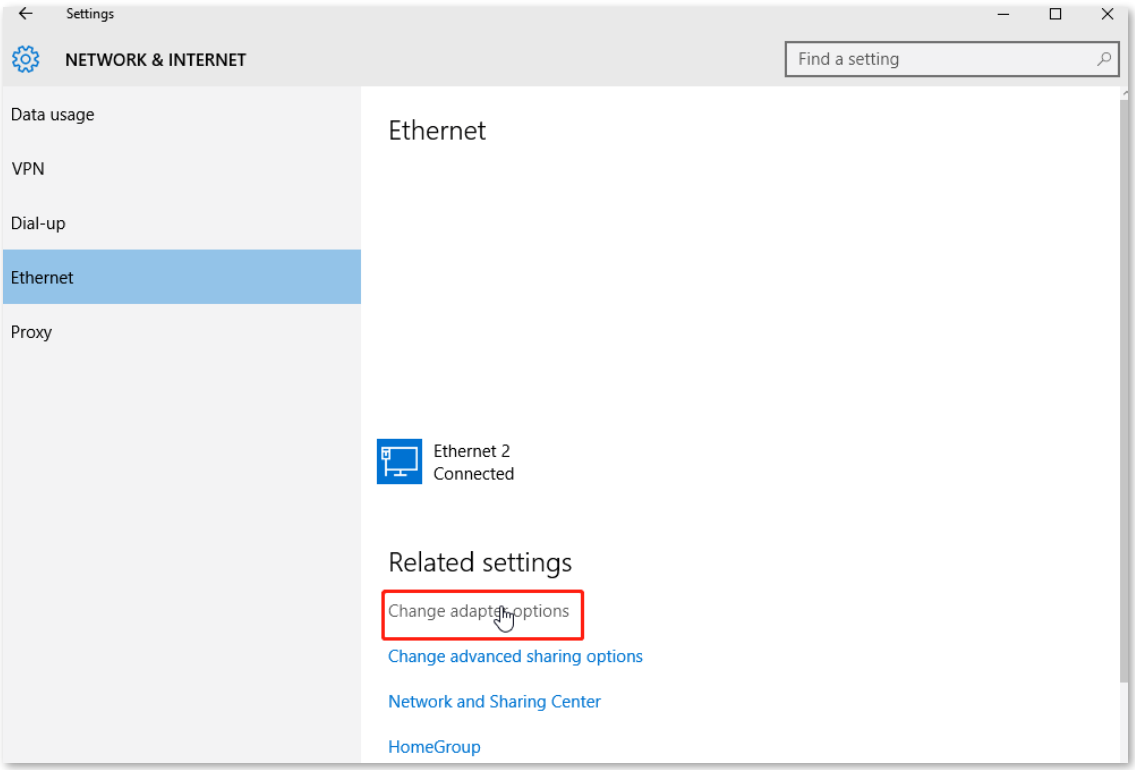
A.1 Configuring the computer to obtain an IPv4 address automatically

Perform the configuration procedures corresponding to Windows 10, Windows 8 and Windows 7 and as required. 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.

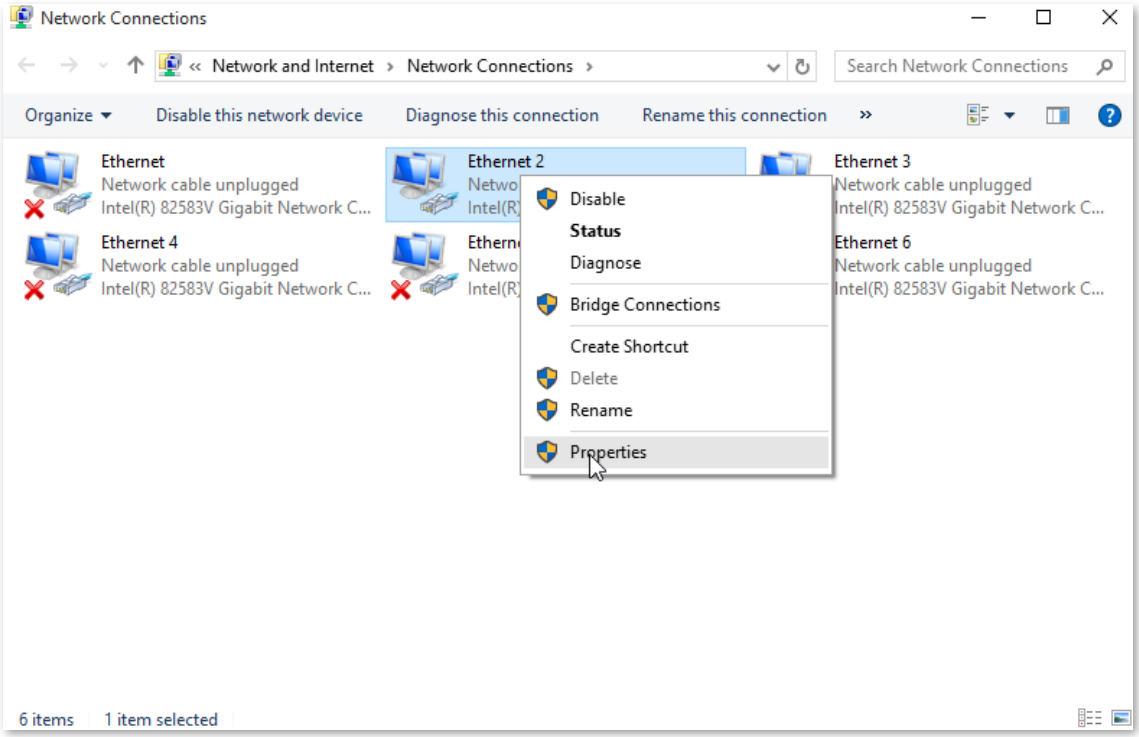
A.1.1 Windows 10

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

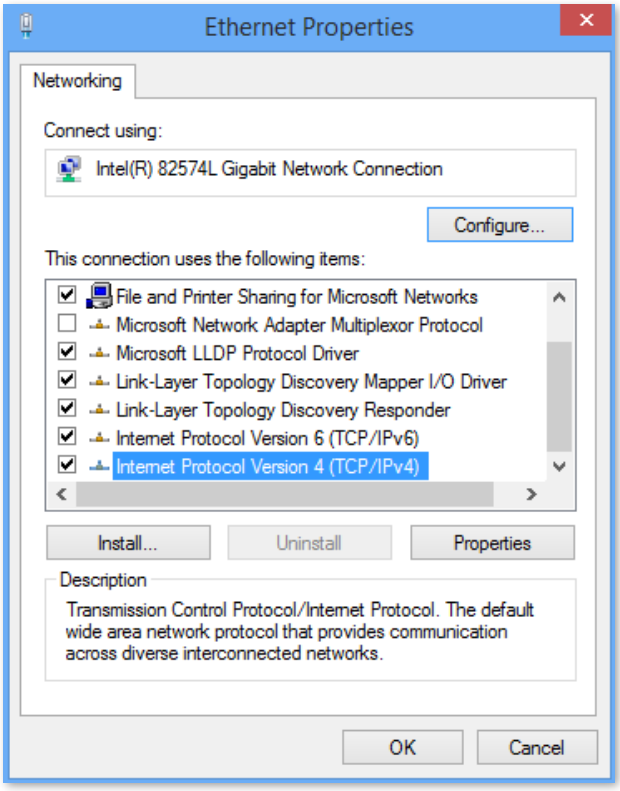
Step 2 Click **Change adapter options**.



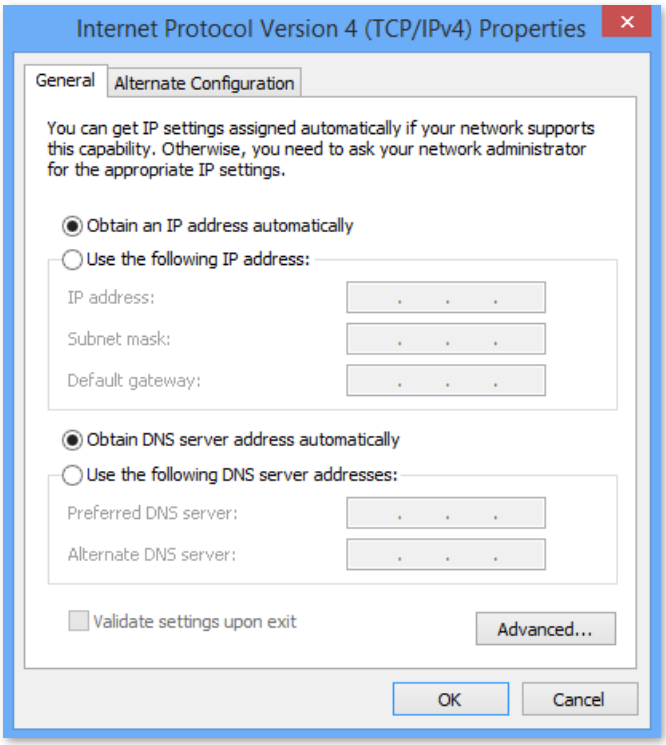
Step 3 Right click on the connection which is being connected, and then click **Properties**.



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



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

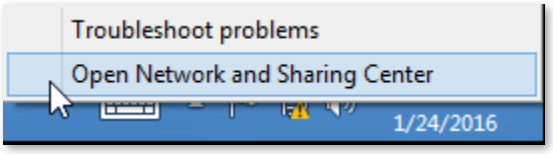


Step 6 Click **Close** in the **Ethernet Properties** window.

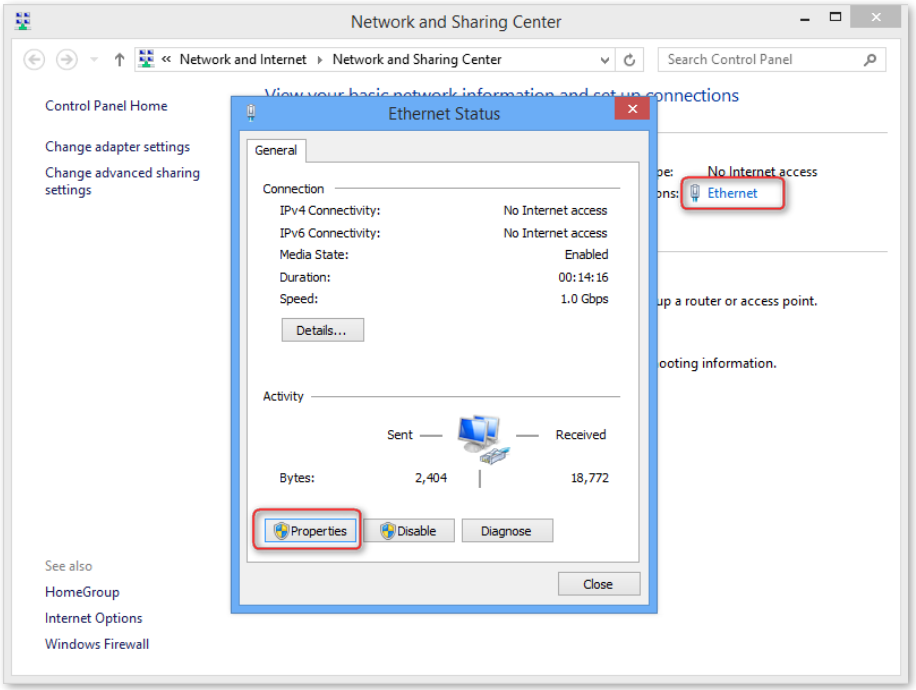
---End

A.1.2 Windows 8

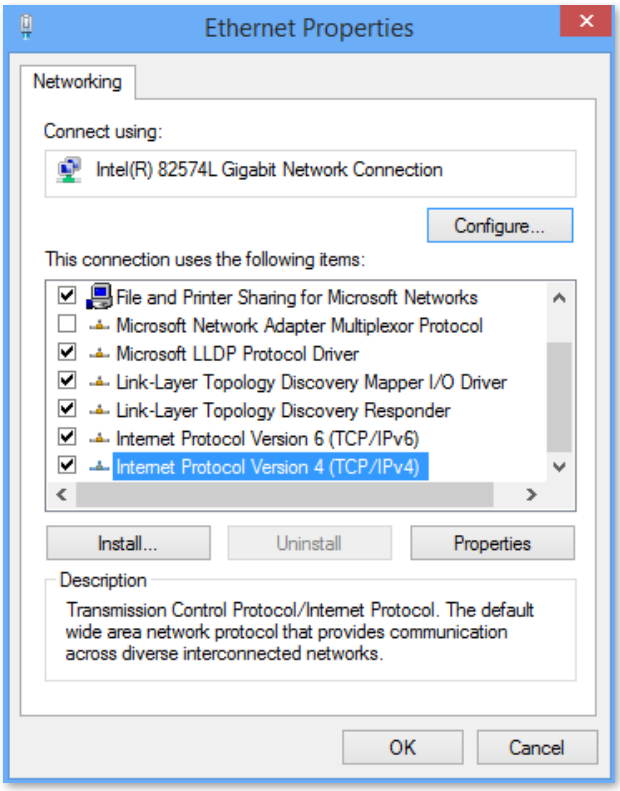
Step 1 Right-click in the bottom right corner of the desktop and choose **Open Network and Sharing Center**.



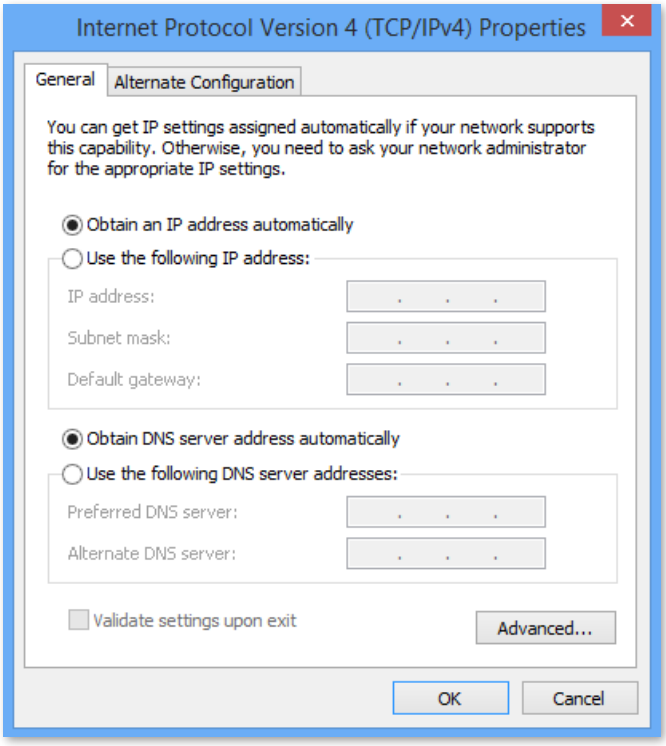
Step 2 Click **Ethernet** and then **Properties**.



Step 3 Double-click **Internet Protocol Version 4 (TCP/IPv4)**.



Step 4 Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**, and click **OK**.

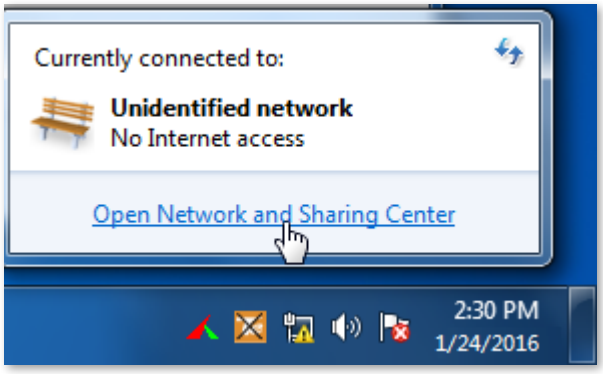


Step 5 Click **OK** in the **Ethernet Properties** window.

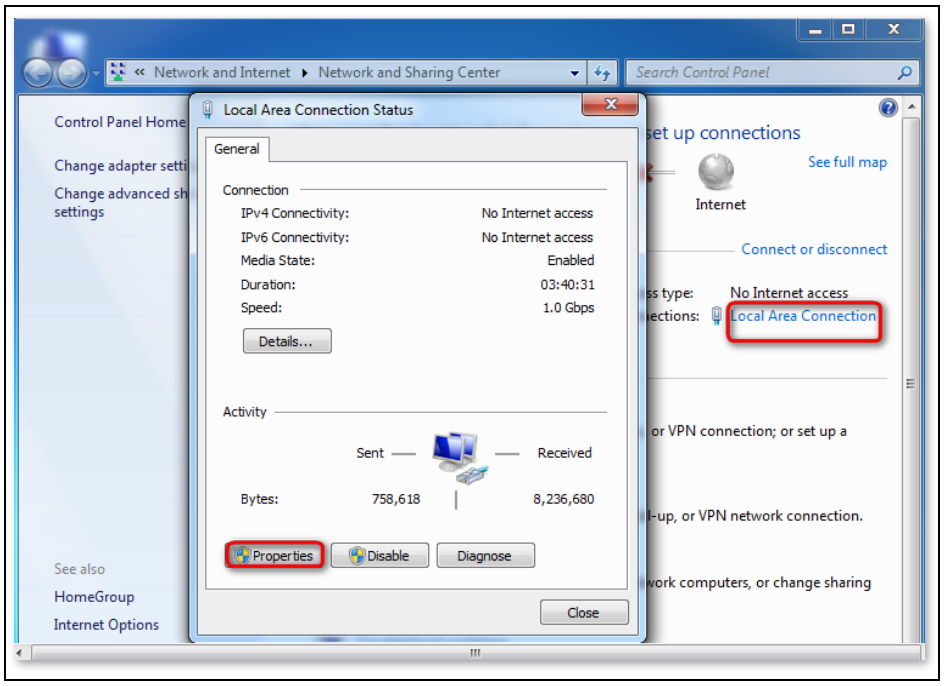
---End

A.1.3 Windows 7

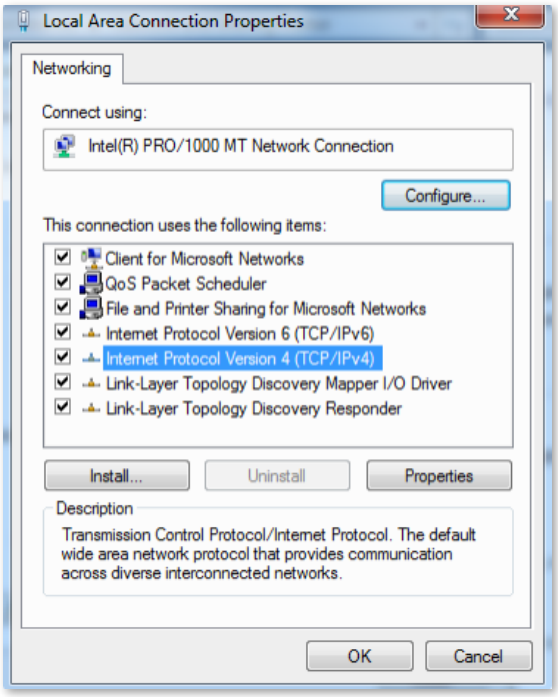
Step 1 Click in the bottom right corner of the desktop and choose **Open Network and Sharing Center**.



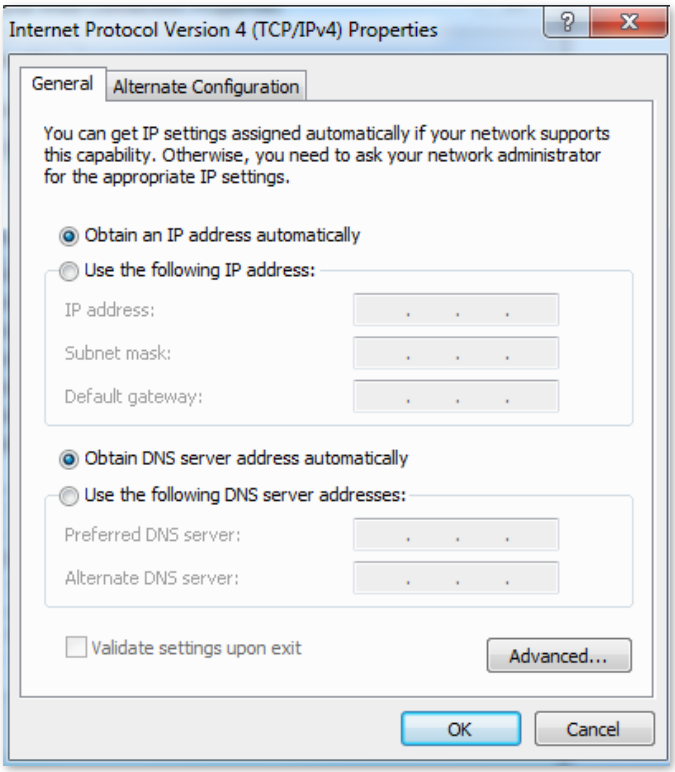
Step 2 Click **Local Area Connection** and then **Properties**.



Step 3 Double-click **Internet Protocol Version 4 (TCP/IPv4)**.



Step 4 Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**, and click **OK**.



Step 5 Click **OK** in the **Local Area Connection Properties** window.

---End

A.2 Acronyms and abbreviations

Acronym or Abbreviation	Full Spelling
AES	Advanced Encryption Standard
BR	Border Relay
CE	Customer Edge
DDNS	Dynamic Domain Name System
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
GMT	Greenwich Mean Time
IKE	Internet Key Exchange
IP	Internet Protocol
IPTV	Internet Protocol Television
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
MAC	Medium Access Control
MTU	Maximum Transmission Unit
PIN	Personal Identification Number
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point to Point Tunneling Protocol
PUK	Personal Identification Number Unlock Key
SIM	Subscriber Identity Module

Acronym or Abbreviation	Full Spelling
SMS	Short Message Service
SSID	Service Set Identifier
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
USSD	Unstructured Supplementary Service Data
WAN	Wide Area Network
WISP	Wireless Internet Service Provider
WPA-PSK	WPA-Pre-shared Key