

User Guide

AX3000 Wi-Fi 6 5G NR Router

5G06



Copyright statement

© 2025 Shenzhen Tenda Technology Co., Ltd. All rights reserved.

Tenda is a registered trademark legally held by Shenzhen Tenda Technology Co., Ltd. Other brand and product names mentioned herein are trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to Shenzhen Tenda Technology Co., Ltd. No part of this publication can be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the prior written permission of Shenzhen Tenda Technology Co., Ltd.

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 a warranty of any kind, express or implied.

Preface

This guide describes how to configure each feature of the AX3000 Wi-Fi 6 5G NR Router.



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

In this guide, unless otherwise specified, all screenshots are taken from 5G06 V1.0.

Conventions

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

Item	Presentation	Example
Cascading menus	>	System > Live Users
Parameter and value	Bold	Set User Name to Tom .
Variable	Italic	Format: <i>XX:XX:XX:XX:XX:XX</i>
UI control	Bold	On the Policy page, click the OK button.
Message	“ ”	The “Success” message appears.

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

Symbol	Meaning
	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.
	This format is used to highlight a procedure that will save time or resources.

More information and support

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

Revision history

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

Version	Date	Description
V1.0	2025-10-08	Original publication.

Contents

Getting started with the router	1
1.1 Connect the router to the network	1
1.2 Perform quick setup wizard	4
1.3 Expand existing network	7
Login and logout	11
2.1 Log in to the web UI	11
2.2 Log out of the web UI	12
2.3 Check web UI layout	12
Manage internet settings	14
3.1 Access internet through the SIM card	14
3.2 Access internet through the WAN port	18
3.3 Set Failover connection	25
Manage Wi-Fi settings	28
4.1 Change Wi-Fi name and password of main Wi-Fi	28
4.2 Hide the main Wi-Fi	31
4.3 Configure guest network	32
4.4 Configure Wi-Fi schedule	34
4.5 Change network mode, channel or bandwidth	35
4.6 Configure transmit power	37
4.7 Enable or disable beamforming+	37
Control internet access	40
5.1 Add a device to the blacklist	40
5.2 Remove a device from the blacklist	41
5.3 Add a parental control rule	41
5.4 Control internet access speed	44
5.5 Configure MAC address filter	45
Maintain and monitor network	49
6.1 Check internet status	49
6.2 Check WAN status	53

6.3 Check system information	57
6.4 Check or configure Wi-Fi information	60
6.5 Check online or blacklisted devices	61
6.6 Control indicators	63
6.7 TR069	64
6.8 Configure system time	65
6.9 Change login password	68
6.10 Reboot and reset	68
6.11 Upgrade firmware	70
6.12 Backup and Restore	72
6.13 Configure remote management	74
6.14 Check or export system logs	76
6.15 Configure automatic maintenance	77
Manage mobile settings	79
7.1 Configure SIM PIN	79
7.2 Configure mobile data	85
7.3 Configure PCI&Band lock	88
7.4 Perform ISP update	90
7.5 Manage SMS messages	91
7.6 Set the message center number	97
7.7 Inquire information by sending USSD commands	98
Use VPN to access network	100
8.1 Configure OpenVPN server	100
8.2 Configure L2TP client	106
8.3 Configure IPsec	108
8.4 Configure Wireguard client	114
Configure more settings	116
9.1 Manage LAN settings	116
9.2 Configure DHCP reservation	120
9.3 Configure static route	121
9.4 Configure virtual server	123
9.5 Configure DMZ host	127
9.6 ALG	131
9.7 Firewall	132
9.8 Improve network connections with UPnP	133
9.9 Configure DDNS	134
9.10 Enable or disable OFDMA	138

Appendix	140
A.1 Set computer to auto obtain an IPv4 address	140
A.2 Acronyms and abbreviations	147
A.3 Connect to a hidden Wi-Fi	148

1

Getting started with the router

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

1.1 Connect the router to the network

1.1.1 Wired connection

Connect your wired device, such as a computer, to the Ethernet port (**1 Gbps** or **2.5 Gbps**) of the router using an Ethernet cable.

1.1.2 Wi-Fi connection

1. Find the Wi-Fi information of the router.

When you first set up the router or reset it to factory settings, the Wi-Fi information can be found on the bottom. Otherwise, use the Wi-Fi name and password you set for Wi-Fi access.

2. Connect your Wi-Fi-enabled device, such as a smartphone, to the Wi-Fi of the router.

Tenda_FEF0_5G is used for illustration here.



When you first set up the router, if the **Unsecured Network** prompt is displayed on the page, ignore it.



---End

1.1.3 Wi-Fi connection using WPS

The WPS function enables the Wi-Fi-enabled device, such as a smartphone, to connect to the Wi-Fi of the router without entering the Wi-Fi password.



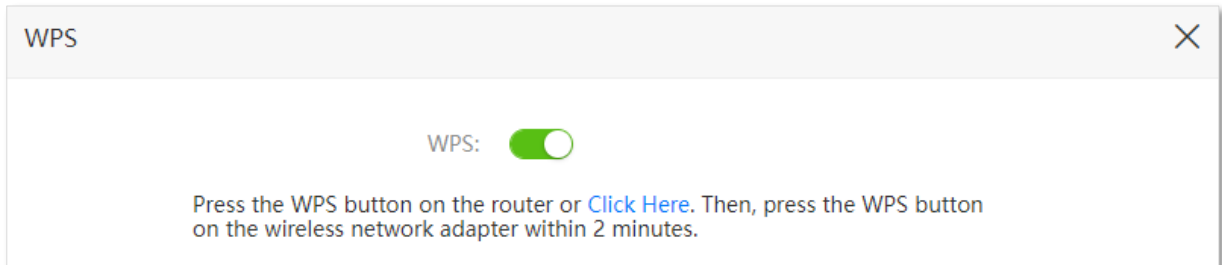
This function is only applicable to Wi-Fi-enabled devices that can use the WPS function.

1. Enable the WPS function of the router. The Wi-Fi indicator () blinks fast.
- **Method 1: Press the MESH button for 1 to 3 seconds.**



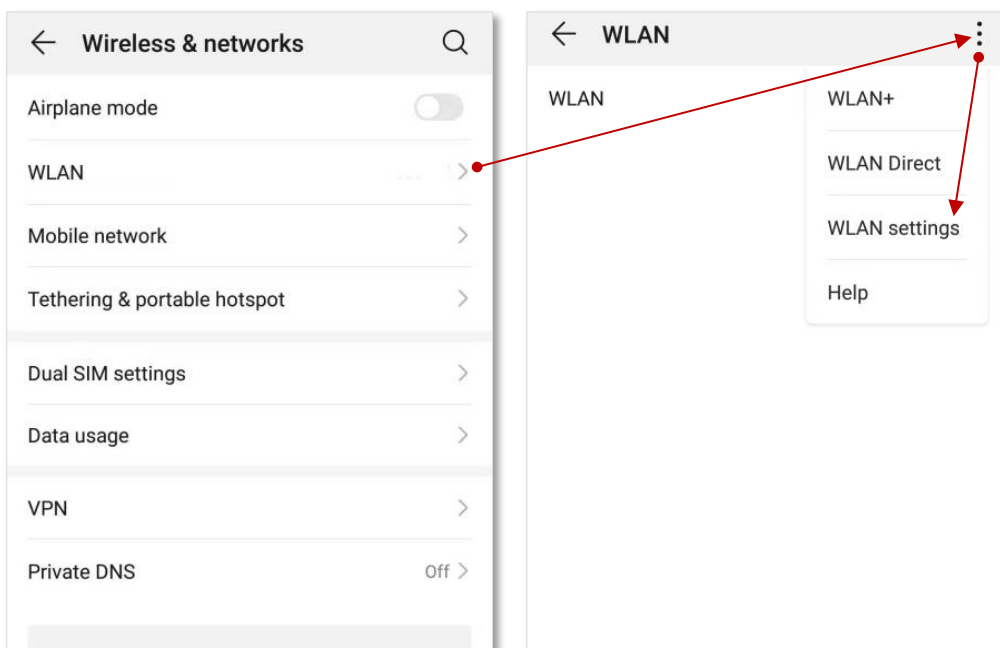
- **Method 2: Enable WPS via web UI**

- 1) [Log in to the web UI of the router](#), and navigate to **Wi-Fi Settings > WPS**.
- 2) Enable **WPS**, and click [Click Here](#).

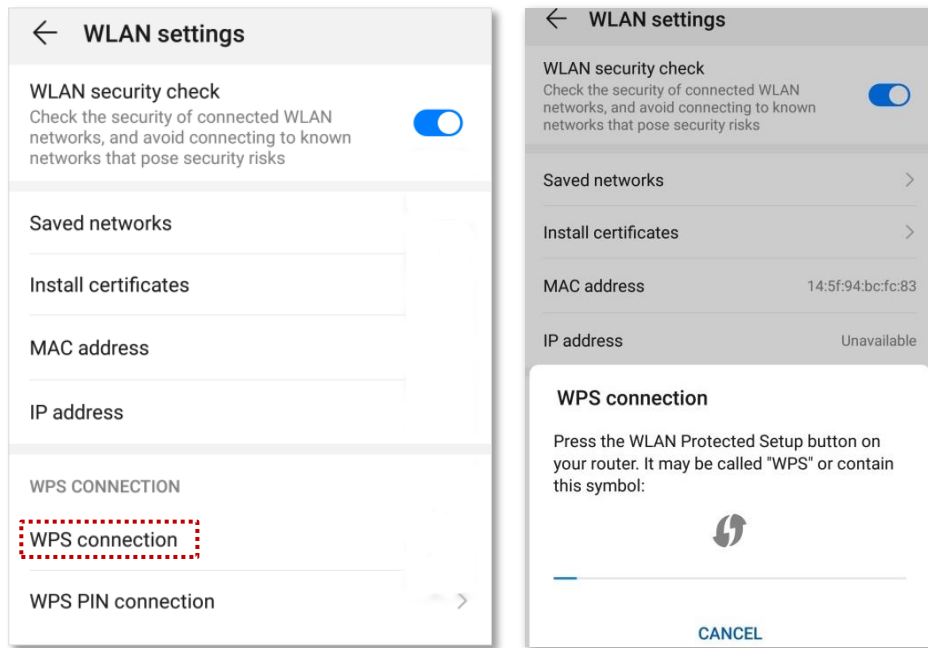


2. Configure the WPS function on your Wi-Fi-enabled devices within 2 minutes. Configurations on various devices may differ (Example: HUAWEI P10).

- 1) Find **WLAN** settings on the smartphone.
- 2) Tap **⋮**, and tap **WLAN settings**.



- 3) Tap **WPS connection**.



---End

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

1.2 Perform quick setup wizard

You can complete quick setup for internet access by following the instructions on the web UI wizard. This wizard only occurs upon your first setup or when the router is reset to factory settings.

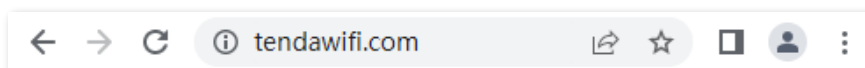
Procedure for performing quick setup wizard

1. Connect your smartphone to the Wi-Fi, or connect your computer to an Ethernet port (**1 Gbps** or **2.5 Gbps**) of the router.



The Wi-Fi information can be found on the bottom of the router.

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



3. Click **Start**.



TIP

- If the SIM card is inserted properly and the internet connection is normal, you can continue the setup in step 4.
- If **No SIM Card** is shown on the page, refer to [no SIM card inserted](#).
- If **SIM card locked** is shown on the page, refer to [unlocking the SIM card in the quick setup wizard](#).



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



TIP

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

Wi-Fi Settings

Wi-Fi Name:

Tenda_FEF0

Wi-Fi Password:

.....



☐ No Password

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

Login Password:

Login password of 5-32 characters



☐ No Password

Next

---End

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



Congratulations! You can access the internet now.

Please connect to the new Wi-Fi later.

Configuration Information

Wi-Fi Name:

Tenda_FEF0
Tenda_FEF0_5G

Wi-Fi Password:

Login Password:

Click "More" below to explore more functions of the router.

More

Now you can access the internet with:

- Wired devices: Connect to the Ethernet port of your router using an Ethernet cable.
- Wi-Fi-enabled devices: Connect to your Wi-Fi using the Wi-Fi name and password you set.

1.3 Expand existing network



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

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

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

- **MESH button networking**

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

- **Wired networking**

Connect the Ethernet port (**1 Gbps** or **2.5 Gbps**) of an existed router to a new router through an Ethernet cable for automatic networking. The wired network has good stability and small delay. If Ethernet cables have been deployed at home, you can use this mode.

- **Scanning networking**

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

1.3.1 Add more nodes

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



- If there are more than two secondary nodes, place the primary node in the key area and ensure that no more than one node is between the primary node and the secondary node.
- Before using a new router to extend the network, ensure that the existing router (primary node) has been connected to the internet and the new router (secondary node) is restored to the factory settings.
- The router can be networked with other routers that support the XMESH protocol. If the router fails to be added to an existing network, contact Tenda customer service for help. The following uses 5G06 (primary mode) and MX15 (secondary node) as an example.

MESH button networking

1. Power on the existing router (5G06) and connect it to the internet properly.
2. Place the new router (MX15) near the existing router (within 5 meters) and power on. Wait until the startup of the new router is complete. The indicator blinks green slowly.
3. Press (1 to 3 seconds) the networking button (MESH) on the new router. The indicator blinks white fast.
4. Press (1 to 3 seconds) the networking button (MESH) of the existing router within 2 minutes. The Wi-Fi indicator () blinks fast.

---End

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

Wired networking

Assume that the Ethernet cable has been deployed in advance between the living room and the bedroom in the home, the router 5G06 (primary node) placed in the living room has been connected to the internet, and now you need to deploy a router MX15 (planned as a secondary node) in the bedroom to extend the Wi-Fi.

Procedure for performing wired networking

1. Power on the existing router (5G06) and connect it to the internet properly.
2. Place the new router (MX15) where you want to deploy it, which is **bedroom** in this example. Power on the new router. Wait until the startup of the new router is complete (the indicator blinks green slowly).
3. Connect the Ethernet port (**1 Gbps** or **2.5 Gbps**) of the primary node to the Ethernet port of the new router using an Ethernet cable.

---End

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

[Log in to the web UI of the router](#), and navigate to **Mesh**. You can check and configure the added node.

Scanning networking

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

Procedure for scanning to networking

1. [Log in to the web UI of the router](#), and navigate to **Mesh**.
2. Click **Manually add** on the **Add Node** page.
3. The system discovers new nodes, ensure that the MAC address is the same as the MAC address on the label of the new router, select a node, and click **Add**.
4. Wait until the ongoing process is complete. The new node is added successfully.

---End

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

1.3.2 Position secondary nodes

After the Mesh networking is successful, follow the instructions below to select an appropriate position for the secondary nodes.

1. Relocate the secondary nodes for a better internet experience.
 - Place the secondary nodes within the wireless coverage range of the existing router.
 - Keep your nodes away from electronics with strong interference, such as microwave ovens, induction cookers, and refrigerators.
 - Place the nodes in a high position with few obstacles.
2. Power on the secondary nodes, and wait until the indicator blinks green slowly.



TIP

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

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

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

If the indicator of the new router is solid red, move it closer to other networked routers to obtain better connection quality.

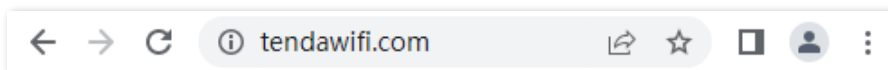
---End

2 Login and logout

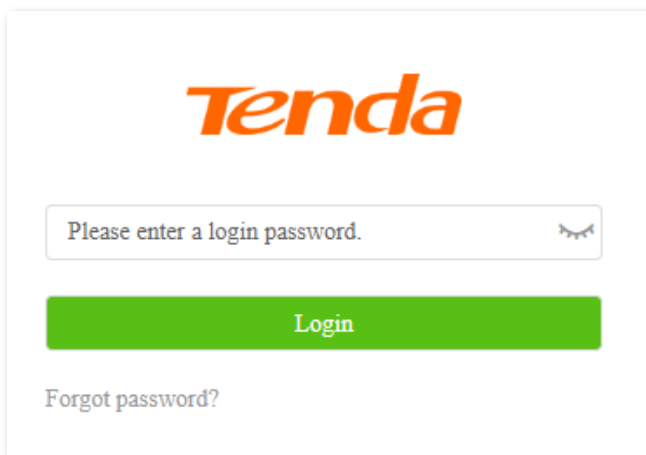
Features available in the router may vary by model and software version. Router availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual router experience.

2.1 Log in to the web UI

1. Connect your smartphone to the Wi-Fi, or connect your computer to an Ethernet port of the router.
2. Start a web browser on the device connected to the router, and visit **tendawifi.com** (computer used as an example).



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



---End



TIP

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

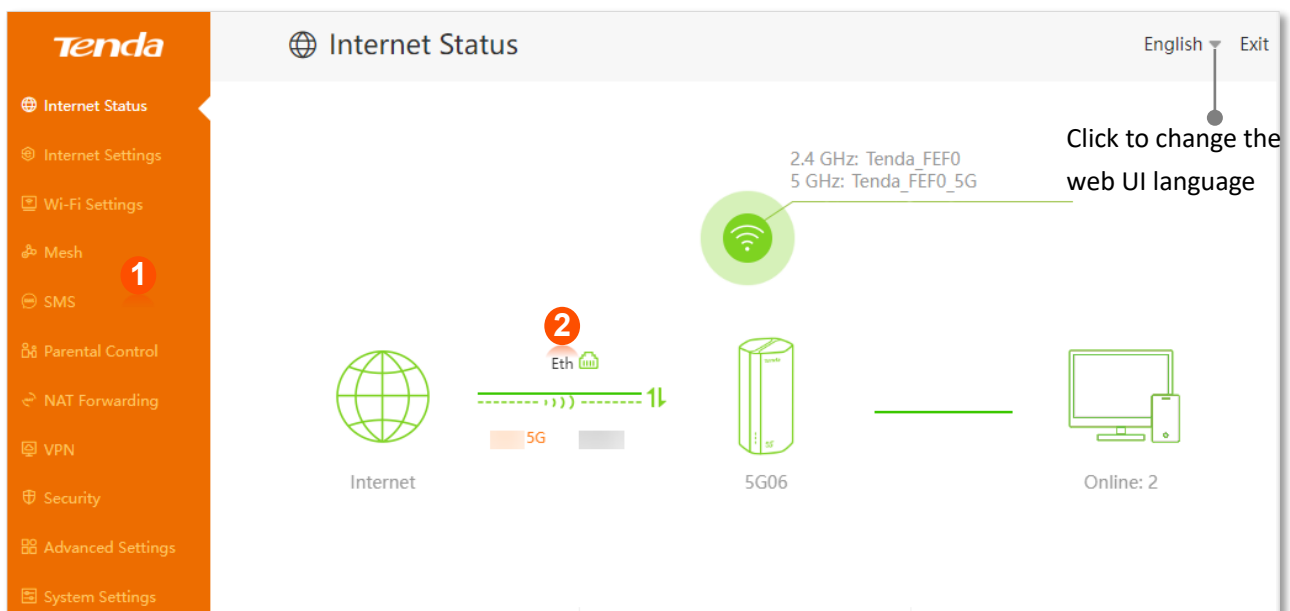
- Ensure that your Wi-Fi-enabled device is connected to the Wi-Fi of the router, or the computer has connected to the Ethernet port of the router properly.
- Disable the cellular network of your Wi-Fi-enabled device.
- Try to enter **http://tendawifi.com** or **http://192.168.0.1** in the browser address bar (not the search bar).
- Clear the cache of your web browser or try again with another web browser.
- Ensure that the computer is set to **Obtain an IP address automatically**.
- [Reset the router](#) and try again.

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 Check web UI layout

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



No.	Name	Description
1	Navigation bar	Used to display the function menu of the router. Users can select functions in the navigation bar and the configuration page appears in the configuration area.
2	Configuration area	Used to modify or check your configurations.

3 Manage internet settings

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

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

3.1 Access internet through the SIM card

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

Procedure for creating an APN profile manually

Take inserting two SIM cards as an example. Assume that:

- One of the SIM cards has an abnormal APN, and it is necessary to manually create an APN profile.
- The toggle switch at the bottom of the router is set to Auto.

1. [Log in to the web UI of the router](#), and navigate to **Internet Settings**.
2. Choose the network operator as required in the **Network Selection** field to create an APN profile.
3. Click **Create a Profile**, and enter required parameters from your ISP.
4. Confirm the APN cloud agreement, and tick the checkbox.
5. Click **Save**.

Create a Profile

Profile Name:

PDP Type:

IPv4

APN:

APN Type:

Static

User Name:

Password:

Authentication Type:

CHAP

☒ I have read and agree to the [APN Cloud Agreement](#)

Save

---End

Wait a moment. The router will use the parameters you entered to dial up for internet access.

 Internet Settings
 English ▾ Exit

Internet Settings

Network: 

Connection Status: Connected

Mobile Data: ☒

Data Roaming: ☒ Enable this function may incur roaming charges.

Mobile Data Options: auto ▾

Dial-up Settings

Network Selection: ☒  ☐ 

Profile Name: ▾ Create a Profile

PDP Type: IPv4&IPv6 ▾

APN:

User Name:

Password: 

Authentication Type: NONE ▾

MTU: 1460

Compatibility Mode: ☐

Failover Settings

Failover: ☐

Save

Parameter description

Parameter	Description
Network	Specifies the network operator corresponding to the SIM card used by the router for internet access.
Connection Status	Specifies the internet connection status of the SIM card.

Parameter	Description
Mobile Data	Used to enable or disable the mobile data traffic. When it is disabled, you cannot access the internet through the router.
Data Roaming	Used to enable or disable data roaming for the SIM card inserted in the router. Data roaming means the data usage produced when you are outside the coverage of your ISP.  TIP To use the data roaming function, you need to subscribe to the data roaming service using the SIM card.
Mobile Data Options	Specifies the mobile network type for internet access. It is recommended to select auto. – auto: Automatically select the appropriate mobile network type based on the surrounding environment. – 5G Only: Only the 5G network is used. – 4G Only: Only the 4G network is used.
Network Selection	If you need to manually create APN profiles for different SIM cards, you can select the corresponding network operator for the SIM card and then configure APN profiles.  TIP It is available only when you insert two SIM cards into the router and the toggle switch at the bottom of the router is set to Auto.
Profile Name	Generally, all these parameters are predefined in the SIM card. The router will identify these parameters automatically, which cannot be changed, and use them for dial-up.
PDP Type	
APN	
User Name	
Password	 TIP If the router cannot identify these parameters, contact your ISP for them.
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 as required.

3.2 Access internet through the WAN port

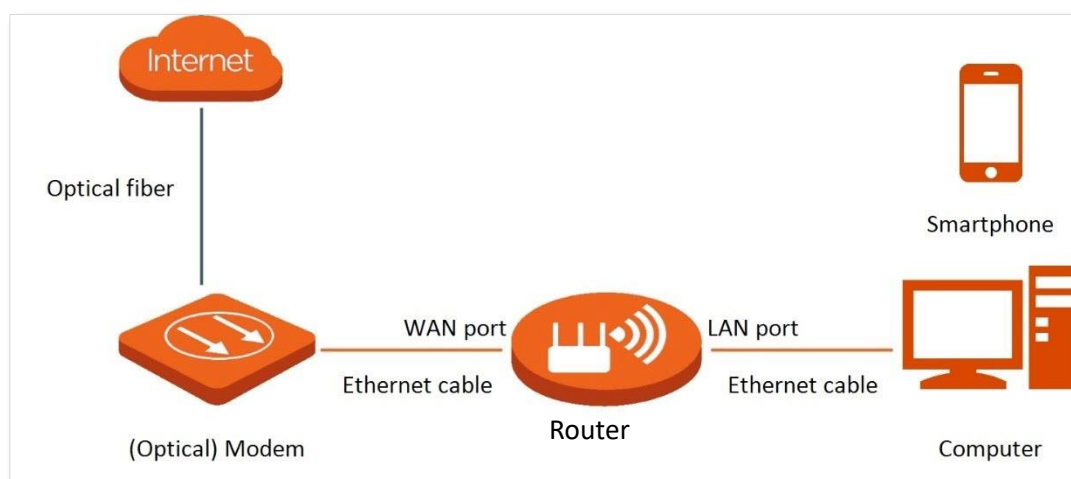
If you want to connect your broadband to the router to access the internet, you can set the router through the WAN port.



- Parameters for accessing the internet are provided by your ISP. Contact your ISP for any doubt.
- By default, the Ethernet ports (**1 Gbps, 2.5 Gbps**) act as LAN ports. When the Failover function is enabled, the 2.5 Gbps port is used as a WAN port.

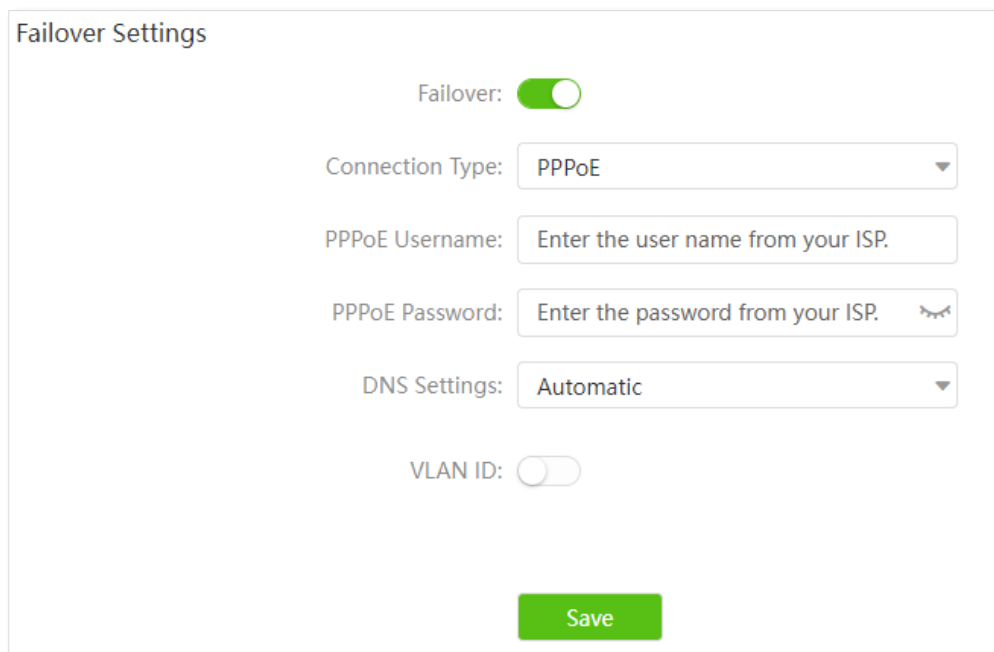
Use PPPoE account

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



Procedure for using PPPoE account

1. [Log in to the web UI of the router](#), and navigate to **Internet Settings**.
2. Enable the **Failover** function.
3. Set **Connection Type** to **PPPoE**.
4. Enter the **PPPoE Username** and **PPPoE Password**.
5. Set **DNS Settings** and **VLAN ID** as required.
It is recommended to keep the default DNS settings.
6. Click **Save**.



Failover Settings

Failover: ☒

Connection Type: PPPoE

PPPoE Username:

PPPoE Password:

DNS Settings: Automatic

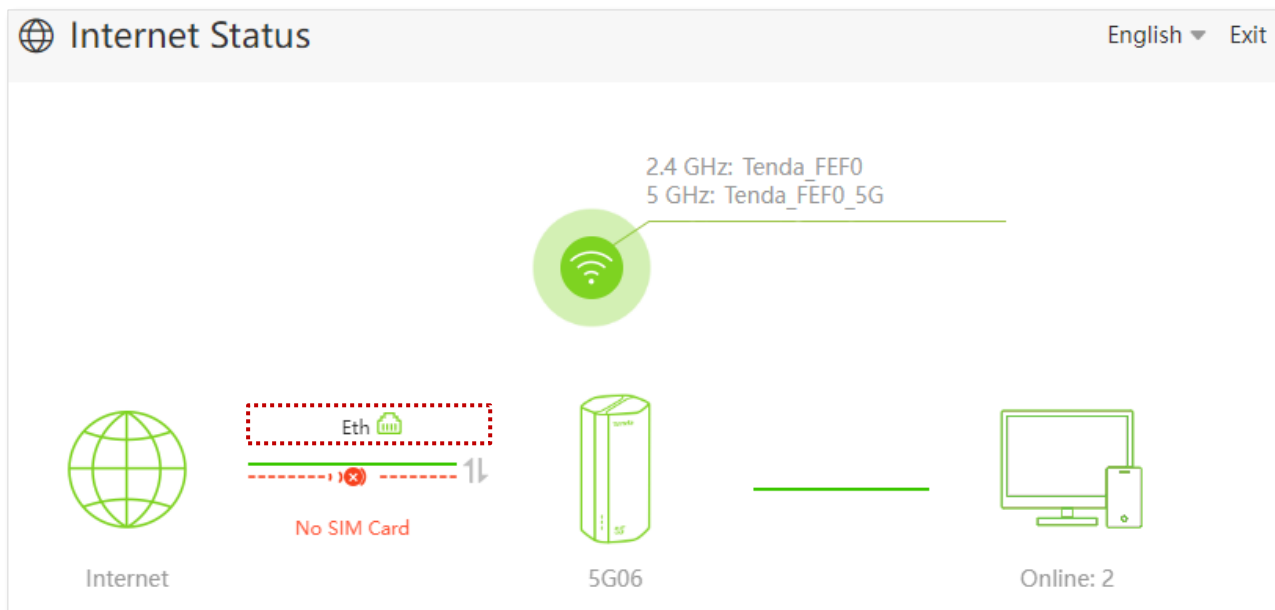
VLAN ID: ☐

Save

---End

Wait a moment until “Eth 

19



If you fail to access the internet, refer to [checking internet status](#) to find a solution.

Parameter description

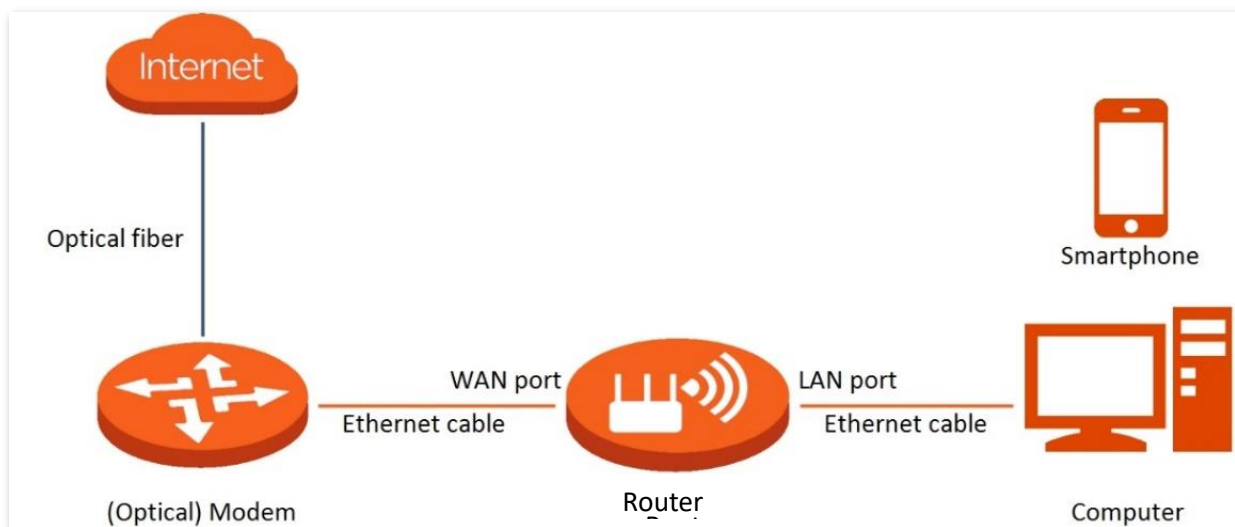
Parameter	Description
Failover	Used to enable or disable the Failover function.
Connection Type	Specifies how your router connects to the internet. Select PPPoE if you access the internet using the PPPoE user name and PPPoE password.
PPPoE Username	When PPPoE is chosen as Connection Type , you need to enter the user name and password provided by your ISP to access the internet.
PPPoE Password	
DNS Settings	Specifies the obtaining method of WAN port DNS address, which is Automatic by default. – Automatic: The router obtains a DNS server address from the DHCP server of the upstream network automatically. – Manual: The DNS server address is configured manually.
VLAN ID	Used to enable or disable the VLAN ID according to the actual network environments. When the function is enabled, the VLAN ID is required to enter. Consult your ISP for this parameter. The value range is 1 to 4094.

Use 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 5G06 as the other one.

The application scenario is shown below.



Procedure for using dynamic address

1. [Log in to the web UI of the router](#), and navigate to **Internet Settings**.
2. Enable the **Failover** function.
3. Set **Connection Type** to **Dynamic IP Address**.
4. Set **DNS Settings** and **VLAN ID** as required.
It is recommended to keep the default DNS settings.
5. Click **Save**.

Failover Settings

Failover: ☒

Connection Type:
Dynamic IP Address

DNS Settings:
Automatic

VLAN ID: ☐

Save

---End

Wait a moment until “Eth 

The screenshot shows the 'Internet Status' page. At the top, there's a header with a globe icon, the title 'Internet Status', and language options 'English' and 'Exit'. The main content area displays a network diagram. A green Wi-Fi icon is connected to a router icon. Above the router, text indicates '2.4 GHz: Tenda_FEF0' and '5 GHz: Tenda_FEF0_5G'. Below the router, a red dashed box highlights 'Eth 

If you fail to access the internet, refer to [checking internet status](#) to find a solution.

Parameter description

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

Parameter	Description
Connection Type	Specifies how your router connects to the internet, including: Select Dynamic IP Address if you can access the internet by simply plugging in an Ethernet cable.
DNS Settings	Specifies the obtaining method of WAN DNS address, which is Automatic by default. – Automatic: The router obtains a DNS server address from the DHCP server of the upstream network automatically. – Manual: The DNS server address is configured manually.
VLAN ID	Used to enable or disable the VLAN ID according to the actual network environments. When the function is enabled, the VLAN ID is required to enter. Consult your ISP for this parameter. The value range is 1 to 4094.

Use static IP address information

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

Procedure for using static IP address information

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

Failover Settings

Failover: ☒

Connection Type: Static IP Address

IP Address: . . .

Subnet Mask: . . .

Default Gateway: . . .

Primary DNS Server: . . .

Secondary DNS Server: . . .

VLAN ID: ☐

Save

---End

Wait a moment until “Eth 

The screenshot shows the 'Internet Status' window. At the top, it says 'Internet Status' with a globe icon on the left and 'English' and 'Exit' on the right. The main area displays a network diagram. At the top center is a green Wi-Fi icon with a line pointing to it from the text '2.4 GHz: Tenda_FE0' and '5 GHz: Tenda_FE0_5G'. Below this is a red dashed box containing the text 'Eth' followed by a green Ethernet icon. Below the red box is a red dashed line with a red 'X' and the text 'No SIM Card'. To the left of the Ethernet icon is a globe icon labeled 'Internet'. To the right of the Ethernet icon is a green server icon labeled '5G06'. To the right of the server icon is a green monitor and phone icon labeled 'Online: 2'.

If you fail to access the internet, refer to [checking internet status](#) to find a solution.

Parameter description

Parameter	Description
Failover	Used to enable or disable the Failover function.
Connection Type	Specifies how your router connects to the internet, including: Select Static IP Address if you want to access the internet using fixed IP information.
IP Address	When Static IP Address is chosen as Connection Type , enter the fixed IP address information provided by your ISP.
Subnet Mask	
Default Gateway	
Primary DNS Server	If your ISP only provides one DNS server, you can leave the secondary DNS server blank.
Secondary DNS Server	
VLAN ID	Used to enable or disable the VLAN ID according to the actual network environments. When the function is enabled, the VLAN ID is required to enter. Consult your ISP for this parameter. The value range is 1 to 4094.

3.3 Set Failover connection

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



- By default, the Ethernet ports (**1 Gbps, 2.5 Gbps**) act as LAN ports. When the Failover function is enabled, the 2.5 Gbps port is used as a WAN port.
- Before setting the Failover function, ensure that you insert the SIM card into the router, and connect the Ethernet port of the router to the internet at the same time.

Example of setting Failover connection

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

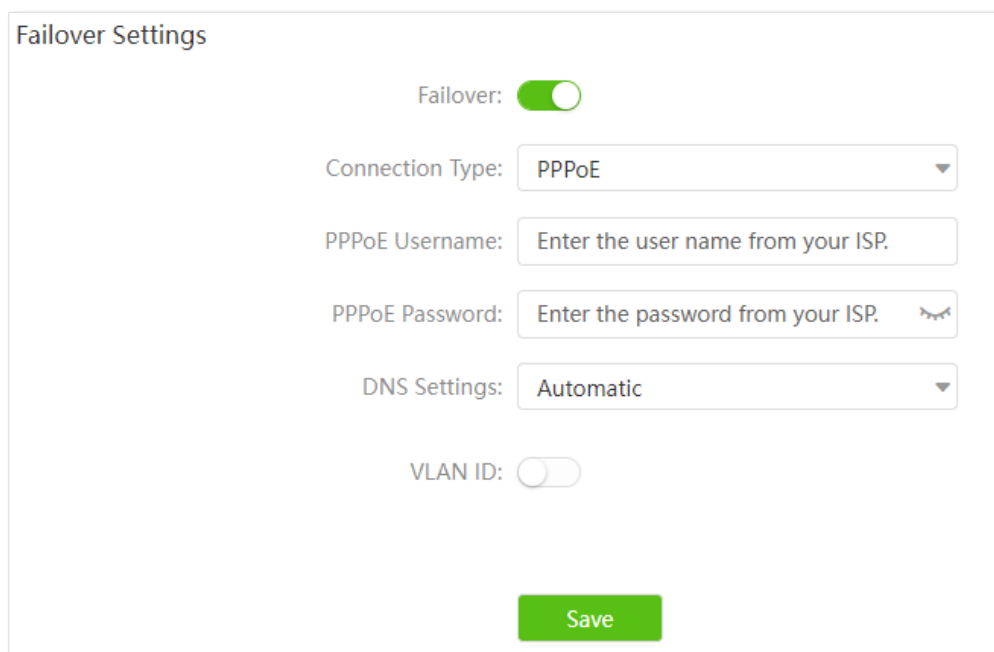
Requirements: Set the router to access the internet through the broadband, and use the SIM cards as backup in case of broadband failure.

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

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

Procedures for setting Failover connection

1. Connect the Ethernet port of the router to the LAN port of your smart home gateway.
2. [Log in to the web UI of the router](#), and navigate to **Internet Settings**.
3. Enable the **Failover** function.
4. Set **Connection Type** to **PPPoE**, and enter the **PPPoE Username** and **PPPoE Password** provided by your ISP.
5. Set **DNS Settings** and **VLAN ID** as required.
It is recommended to keep the default DNS settings.
6. Click **Save**.



Failover Settings

Failover: ☒

Connection Type:

PPPoE Username:

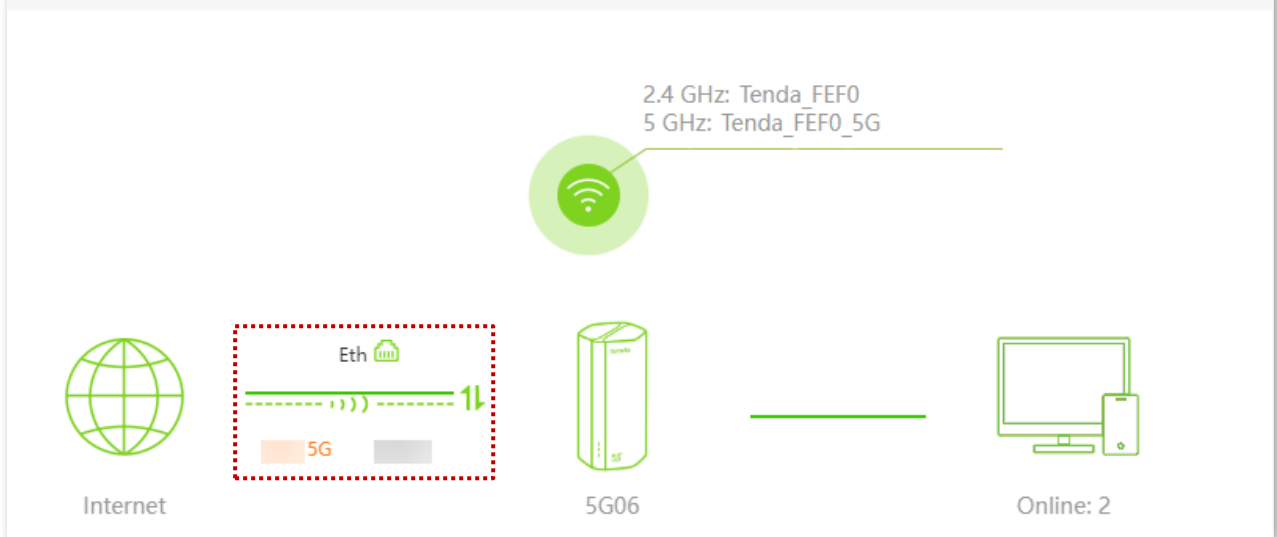
PPPoE Password:

DNS Settings:

VLAN ID: ☐

---End

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



4 Manage Wi-Fi settings

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

4.1 Change Wi-Fi name and password of main Wi-Fi

1. [Log in to the web UI of the router](#), and navigate to **Wi-Fi Settings > Wi-Fi Name & Password**.
2. Enable or disable the **Unify 2.4 GHz & 5 GHz** function as required. The following figure shows an example of disabling the Unify 2.4 GHz & 5 GHz.
 - Enable **Unify 2.4 GHz & 5 GHz**: The Wi-Fi name and password of the 2.4 GHz and 5 GHz network on the router are the same, and only one Wi-Fi name is displayed. When you connect to your router's Wi-Fi, you will automatically connect to the best quality Wi-Fi.
 - Disable **Unify 2.4 GHz & 5 GHz**: The 2.4 GHz and 5 GHz networks on the router are displayed separately. You can access the internet through either Wi-Fi. If you have Wi-Fi-enabled devices that only support 2.4GHz networks, you need to connect to the router's Wi-Fi, such as security cameras, you are recommended to disable the **Unify 2.4 GHz & 5 GHz**.
3. Change the parameters of the 2.4 GHz network.
 - 1) Change the **Wi-Fi Name** of the 2.4 GHz network, which is **John_Doe_2.4GHz** in this example.
 - 2) Set **Encryption Mode**, which is **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.
4. 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) Set **Encryption Mode**, which is **WPA2-PSK (recommended)** in this example.
 - 3) Change the **Wi-Fi Password** of the 5 GHz network, which is **Tenda+Wireless5** in this example.
5. Click **Save**.

Wi-Fi Name & Password

Unify 2.4 GHz & 5 GHz:

2.4 GHz Network:

Wi-Fi Name:

John_Doe_2.4GHz

☐ Hide

Encryption Mode:

WPA2-PSK(recommende

Wi-Fi Password:

.....

5 GHz Network:

Wi-Fi Name:

John_Doe_5GHz

☐ Hide

Encryption Mode:

WPA2-PSK(recommende

Wi-Fi Password:

.....

Save

---End

When the configuration is completed, you can connect your Wi-Fi-enabled devices to the router's Wi-Fi to access the internet.

Parameter description

Parameter	Description
Unify 2.4 GHz & 5 GHz	Used to enable or disable the Unify 2.4 GHz & 5 GHz function. When this function is enabled, the 2.4 GHz and 5 GHz Wi-Fi use the same Wi-Fi name and password. Devices connected to the Wi-Fi will use the network with better connection quality automatically.  TIP It is recommended to disable the Unify 2.4 GHz & 5 GHz function in the smart home environment.

Parameter	Description
Enable Wi-Fi Network	Used to enable or disable the Wi-Fi of the router.  TIP It is available only when the Unify 2.4 GHz & 5 GHz function is enabled.
2.4 GHz Network	You can enable or disable the 2.4 GHz network and 5 GHz network separately when the Unify 2.4 GHz & 5 GHz function is disabled. If the Wi-Fi-enabled devices, such as smartphones, are far away from the router, or blocked from the router by a wall, it is recommended that the Wi-Fi-enabled devices be connected to the 2.4 GHz Wi-Fi.
5 GHz Network	If the Wi-Fi-enabled devices are close to the router, it is recommended that the Wi-Fi-enabled devices be connected to the 5 GHz Wi-Fi.
Wi-Fi Name	Specifies the Wi-Fi name of the corresponding Wi-Fi.
Encryption Mode	Specifies the encryption modes supported by the router, including: – None: Specifies that the Wi-Fi 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. – WPA2-PSK (recommended): The network is encrypted with WPA2-PSK/AES. – WPA/WPA2-PSK: The network is encrypted with WPA-PSK and WPA2-PSK. – WPA2-PSK/WPA3-SAE: The network is encrypted with both WPA3-SAE and WPA2-PSK, improving both security and compatibility.  TIP WPA3-SAE is the upgraded version of WPA2-PSK. If your Wi-Fi-enabled device does not support WPA3-SAE, or you get poor Wi-Fi experience, it is recommended to use WPA2-PSK (recommended).
Wi-Fi Password	Specifies the password for connecting to the Wi-Fi. You are strongly recommended to set a Wi-Fi password for security.  NOTE For initial setup or after a reset, set new Wi-Fi password for privacy and security (The longer the password, the stronger the protection). The character limit and composition rules for passwords are subject to software user interface prompts.

4.2 Hide the main Wi-Fi

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

Wi-Fi Name & Password

Unify 2.4 GHz & 5 GHz: ☐

2.4 GHz Network: ☒

Wi-Fi Name: Tenda_FEF0 ☒ Hide

Encryption Mode: WPA2-PSK(recommende ▼)

Wi-Fi Password: ••••••••

5 GHz Network: ☒

Wi-Fi Name: Tenda_FEF0_5G ☒ Hide

Encryption Mode: WPA2-PSK(recommende ▼)

Wi-Fi Password: ••••••••

Save

---End

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

To connect to a hidden Wi-Fi, refer to [connecting to a hidden Wi-Fi](#).

4.3 Configure guest network

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. This function is disabled by default.

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 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 network.

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

- Wi-Fi names for 2.4 GHz and 5 GHz networks: John_Doe and John_Doe_5G.
- Wi-Fi password for guest networks: Example123
- The shared bandwidth for guests: 20 Mbps.

Procedure for configuring the guest network

1. [Log in to the web UI of the router](#), and navigate to **Wi-Fi Settings > Guest Network**.
2. Enable the **Guest Network** function.
3. Set the **2.4 GHz Wi-Fi Name**, which is **John_Doe** in this example.
4. Set the **5 GHz Wi-Fi Name**, which is **John_Doe_5G** in this example.
5. Set the **Guest Network Password**, which is **Example123** in this example.
6. Select a validity time from the **Validity** drop-down box, which is **8 hours** in this example.
7. Set the bandwidth in the **Bandwidth for Guests** drop-down box and click **Custom** to customize the bandwidth, which is **20 Mbps** in this example.
8. Click **Save**.

Guest Network

Guest Network:

2.4 GHz Wi-Fi Name:
John_Doe

5 GHz Wi-Fi Name:
John_Doe_5G

Guest Network Password:

Validity:
8 hours

Bandwidth for Guests:
20
Mbps

Save

---End

During the 8 hours after the configuration, guests can connect their Wi-Fi-enabled devices, such as smartphones, to **John_Doe** or **John_Doe_5G** to access the internet and enjoy the shared bandwidth of 20 Mbps.

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 names of the router's guest network.
5 GHz Wi-Fi Name	To distinguish the guest network from the main network, you are recommended to set different Wi-Fi names.
Guest Network Password	Specifies the password for the router's guest networks.
Validity	Specifies the validity of the guest network. The guest network function will be disabled automatically out of the validity period.
Bandwidth for Guests	Specifies the maximum upload and download speed for all devices connected to the guest network.

4.4 Configure Wi-Fi schedule

This Wi-Fi schedule function allows you to disable the Wi-Fi of the router at specified periods. This function is disabled by default.



To make the Wi-Fi schedule function work properly, ensure the system time is synchronized with the internet time. Refer to [synchronizing system time with the internet time](#) for configuration.

Procedure for configuring Wi-Fi schedule

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

---End

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

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 is disabled.

Parameter	Description
Repeat	Specifies the days on which the Wi-Fi is disabled during the specified period.
Add Period	Used to add a new Wi-Fi schedule rule.

4.5 Change network mode, channel or bandwidth

You can change the network mode, channel or bandwidth of 2.4 GHz and 5 GHz Wi-Fi.



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

Procedure for changing network mode, channel or bandwidth

1. [Log in to the web UI of the router](#), and navigate to **Wi-Fi Settings > Channel & Bandwidth**.
2. Change the **Network Mode**, **Channel** and **Bandwidth** of the corresponding Wi-Fi.
3. Click **Save**.

Channel & Bandwidth

2.4 GHz Network

Network Mode: 11b/g/n/ax mixed

Channel: Auto

Bandwidth: 20/40

5 GHz Network

Network Mode: 11a/n/ac/ax mixed

Channel: Auto

Bandwidth: 20/40/80/160

Save

---End

Parameter description

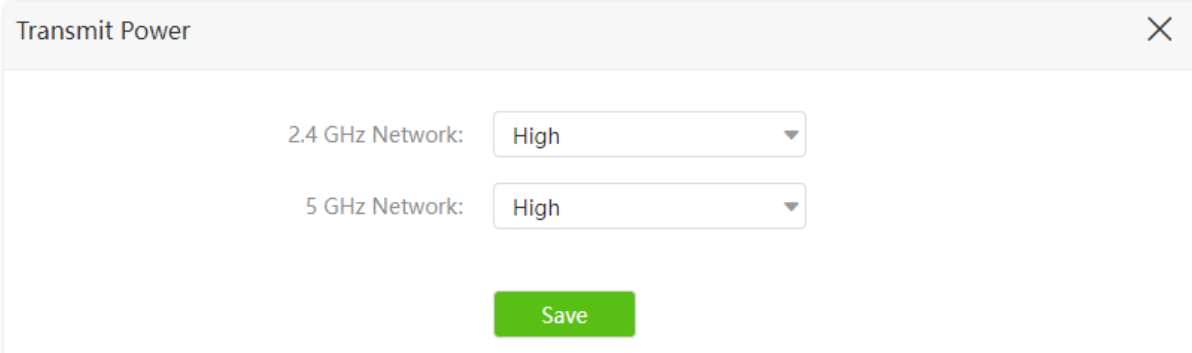
Parameter	Description
Network Mode	Specifies various protocols adopted for wireless transmission. – 11b/g mixed: It indicates that devices compliant with IEEE 802.11b or IEEE 802.11g protocol can connect to the 2.4 GHz Wi-Fi network of the router. – 11b/g/n mixed: It indicates that all devices can connect 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. – 11b/g/n/ax 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 or 802.11ax protocol. – 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. – 11a/n/ac/ax 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 or 802.11ax protocol can connect to the router.
Channel	Specifies the channel in which the Wi-Fi works. By default, the wireless channel is Auto, which indicates that the router selects a channel for the Wi-Fi 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. 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. – 160: It indicates that the channel bandwidth used by the router is 160 MHz. This option is available only at 5 GHz. – 20/40/80/160: It specifies that a router can switch its channel bandwidth among 20 MHz, 40 MHz, 80 MHz and 160 MHz based on the ambient environment. This option is available only at 5 GHz.

4.6 Configure transmit power

You can adjust the wall-penetration capability and wireless coverage of the router by setting the transmit power.

Procedure for configuring transmit power

1. [Log in to the web UI of the router](#), and navigate to **Wi-Fi Settings > Transmit Power**.
2. Select the signal strength level for **2.4 GHz Network** and **5 GHz Network** as required.
3. Click **Save**.



Transmit Power

2.4 GHz Network: High

5 GHz Network: High

Save

---End

Parameter description

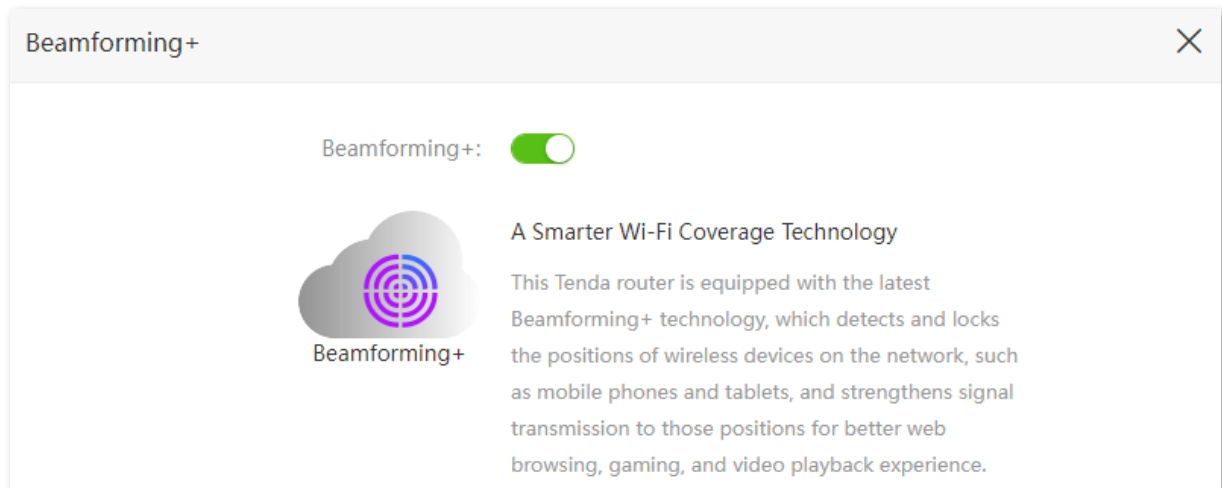
Parameter	Description
	Specify the signal strength level. The default mode is High .
2.4 GHz Network	– High: It is typically used to meet wireless coverage requirements in large or multi-barrier environments.
	– Medium: It is typically used to meet wireless coverage requirements in medium-area or less-obstacle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

4.7 Enable or disable 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.

Procedure for enabling or disabling beamforming+

1. [Log in to the web UI of the router](#), and navigate to **Wi-Fi Settings > Beamforming+**.
2. Enable or disable the **Beamforming+** function as required. The following figure is for reference only.



---End

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



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



5 Control internet access

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

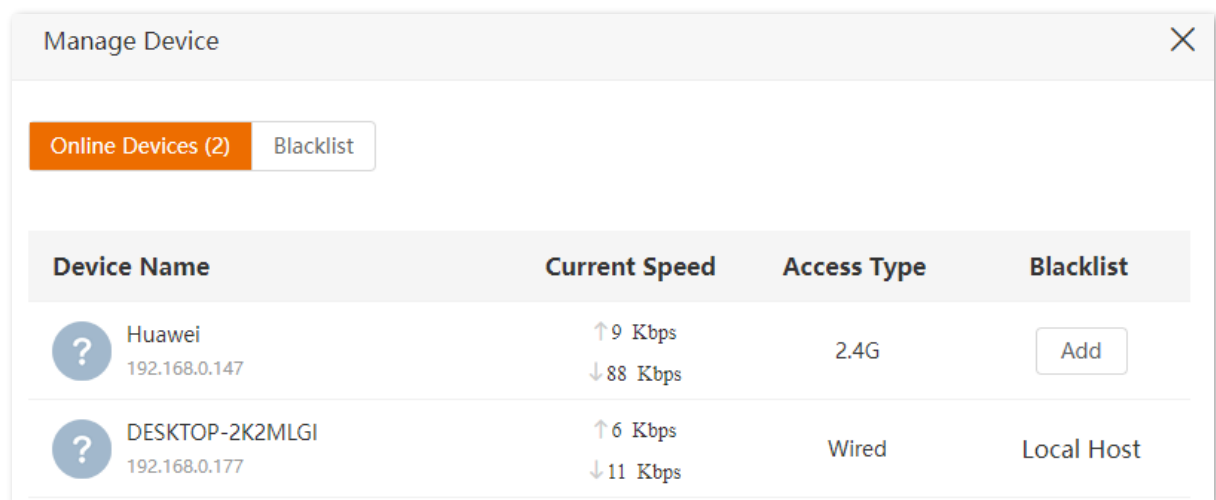
5.1 Add a device to the blacklist

You can add devices to the blacklist to block the internet access.

Procedure for adding a device to the blacklist

1. [Log in to the web UI of the router](#), and navigate to **Internet Status**.
2. Click .
3. Locate the device to be added in **Online Devices** and click **Add**.

The local host cannot be added to the blacklist.



---End

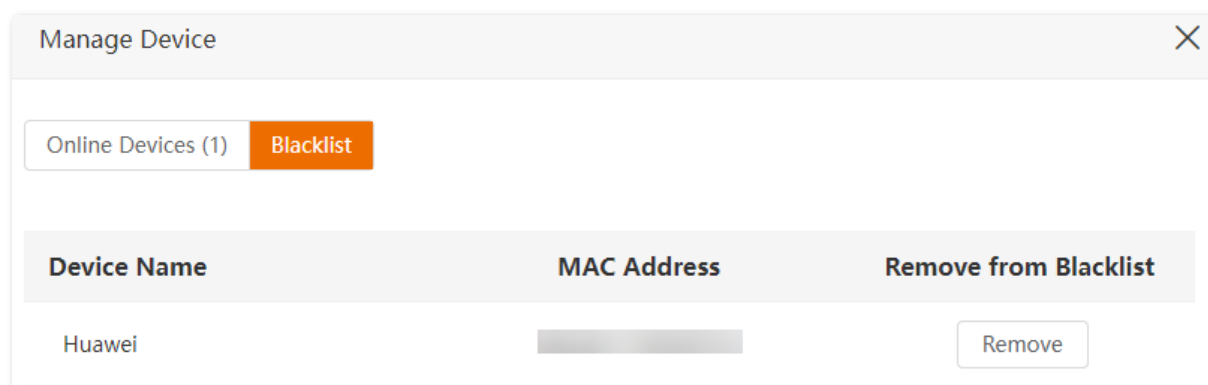
On the **Internet Status** page, click , and then click **Blacklist**, you can check the information of devices that are added to the blacklist.

5.2 Remove a device from the blacklist

You can remove devices from the blacklist as required.

Procedure for removing a device from the blacklist

1. [Log in to the web UI of the router](#), and navigate to **Internet Status**.
2. Click .
3. Choose **Blacklist**, and locate the device to be removed from the blacklist.
4. Click **Remove**.



---End

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

5.3 Add a parental control rule

With the parental control function, you can configure various parental control rules to control access to certain websites or block certain devices from accessing the internet.

Example of adding a parental control rule

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

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

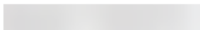
Solution: You can configure the parental control rule to reach the requirements.

Procedure for adding a parental control rule

1. [Log in to the web UI of the router](#), and navigate to **Parental Control**.

2. Configure the parental control rule.

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

Parental Control			
		English ▼ Exit	
Device Name	MAC Address	Uptime	Operation
 Kid's smartphone 192.168.0.147		1m 19s	
 DESKTOP-2K2MLGI 192.168.0.177		36m 34s	
+New			



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. In this case, the MAC address of the device is required.

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

Parental Control

Device Name: Kid's smartphone

Internet Accessible At:

08:00 ~ 22:00

☐ Every Day
☐ Mon.
☐ Tue.
☐ Wed.
☐ Thur.
☐ Fri.
☒ Sat.
☒ Sun.

Website Access Limit:

☒

Access Control Mode:

☒ Blacklist
☐ Whitelist

Blocked Websites:

Facebook, Twitter, YouTube, Instagram

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

Save

---End

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

Parameter description

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

Parameter	Description
	Used to edit, enable, disable or delete the parental control rule.
	 : Used to edit the parental control rule.
Operation	 : Used to enable the parental control rule.
	 : Used to disable the parental control rule.
	 : Used to delete the parental control rule.

5.4 Control internet access speed

You can limit the upload and download speed of devices connected to the router and allocate the bandwidth reasonably.

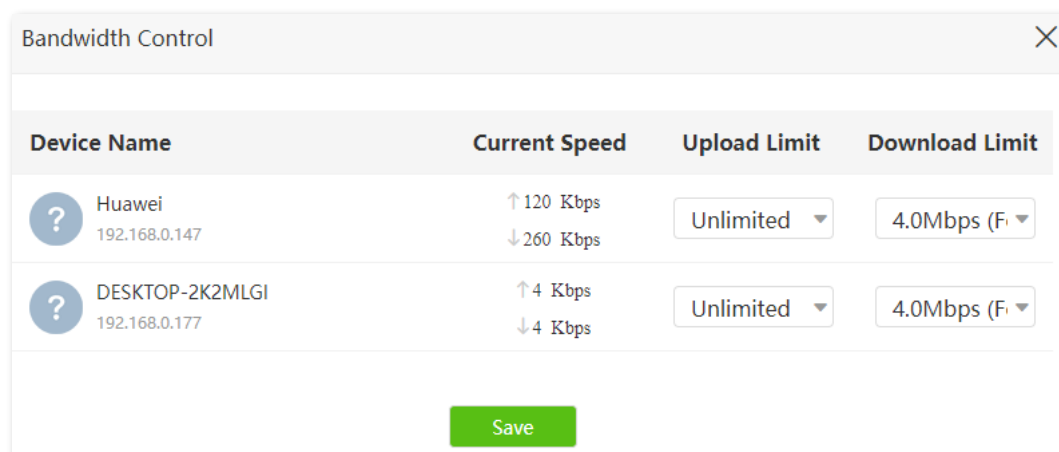
Example of setting the upload and download speed limit for users

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

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

Procedure for controlling internet access speed

1. [Log in to the web UI of the router](#), and navigate to **Advanced Settings > Bandwidth Control**.
2. Locate the devices to be controlled, and set the **Download Limit** to **4.0Mbps (For HD Video)**.
3. Click **Save**.



---End

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

Parameter description

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

5.5 Configure MAC address filter

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.

5.5.1 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 wireless devices of family members to access the internet using the Wi-Fi.

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

Assume that:

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

Procedure for configuring MAC address filter

1. [Log in to the web UI of the router](#), and navigate to **Security > Filter MAC Address**.
2. Set the **MAC Address Filter Mode** to **Whitelist**.
3. (Optional) Enter the device name in the **Whitelisted Device** field, which is **Kid 1's smartphone** in this example.

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



Click [Add all online devices to the whitelist](#), you will add all currently connected devices to the whitelist. **My phone** is used for illustration here.

Filter MAC Address

MAC Address Filter Mode:

☐

Blacklist(To disallow listed devices to access the internet)

☒

Whitelist(To allow only the listed devices to access the internet)

Whitelisted Device	MAC Address	Operation
Kid 1' s smartphone	94:C6:91:29:C2:12	+ Add
DESKTOP-2K2MLGI		Local Host

[Add all online devices to the whitelist](#)

Save

6. Repeat steps 3 - 5 to add **Kid 2's smartphone (98:9C:57:19:D0:1B)** to the whitelist.
7. Click **Save**.

Whitelisted Device	MAC Address	Operation
		+ Add
DESKTOP-2K2MLGI		Local Host
Kid 1' s smartphone	94:C6:91:29:C2:12	🗑
My phone	8C:EC:4B:B3:04:92	🗑
Kid 2' s smartphone	98:9C:57:19:D0:1B	🗑
Save		

---End

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

5.5.2 Disallow specified device to access the internet

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

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

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

Assume that:

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

Procedure for configuring MAC address filter

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

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

Filter MAC Address

MAC Address Filter Mode:

☒ Blacklist(To disallow listed devices to access the internet)

☐ Whitelist(To allow only the listed devices to access the internet)

Blacklisted Device	MAC Address	Operation
		+ Add
Kid' s smartphone	94:C6:91:29:C2:12	

Save

---End

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

6 Maintain and monitor network

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

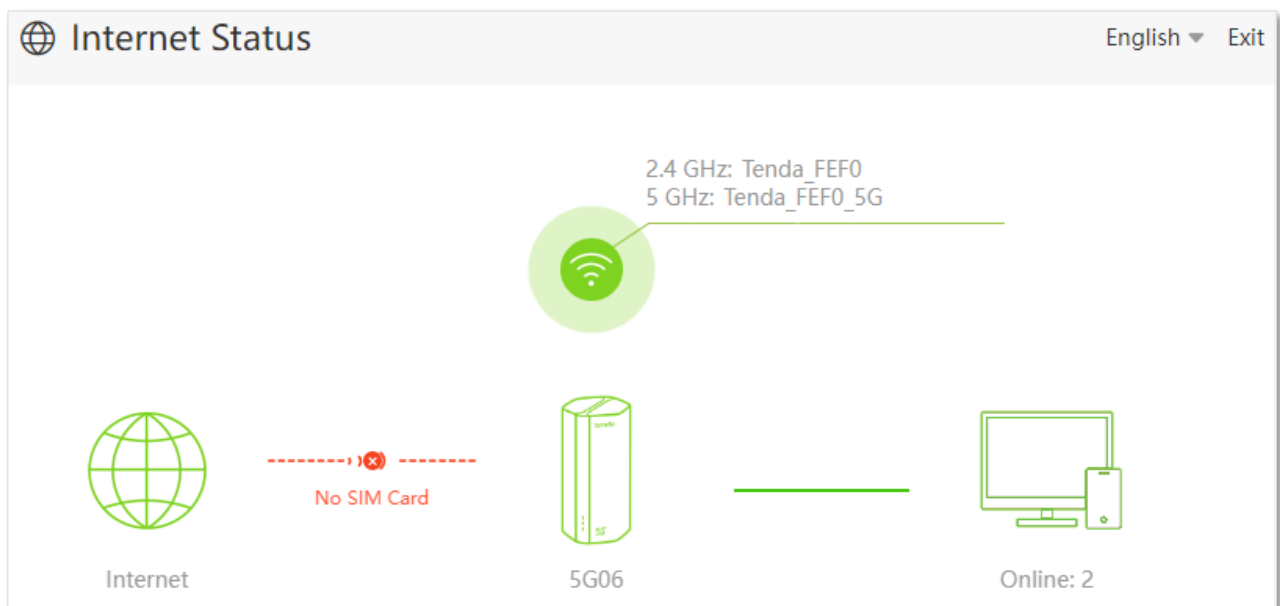
6.1 Check internet status

6.1.1 Through the SIM card

To access the page, [log in to the web UI of the router](#), and navigate to **Internet Status**. You can perform troubleshooting as prompted on the page when you access the internet through the SIM card.

No SIM card inserted

When “**No SIM Card**” is shown between the internet and the router, ensure the SIM card is inserted properly.



SIM card blocked

When “**Locked SIM**” is shown between the internet and the router, it indicates that a SIM card is blocked. Refer to [unlocking the SIM card on the web UI](#).

Automatically matching APN failed

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

Abnormal APN

When “**Abnormal APN**” is shown between the internet and the router, it indicates that you need to configure the correct APN parameters. Click **Abnormal APN** to navigate to the **Internet Settings** page and modify APN parameters.

Mobile data disabled

When “**Mobile Data Off**” is shown between the internet and the router, ensure that the **Mobile Data** function is enabled on the **Internet Settings** page.

Mobile data limit reached

When “**Mobile Data Limited**” 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.

Internet failed

When “**Internet Failed**” is shown between the internet and the router, it indicates that the connection is abnormal.

Try the following solutions:

- Navigate to **Internet Settings**, and ensure that the **Mobile Data** and **Data Roaming** functions are enabled.
- Navigate to **Internet Settings**, and ensure that the dial-up settings parameters are identified by the router automatically. If not, ensure that the SIM card is inserted properly, or refer to [creating an APN profile manually to access the internet](#) to configure the router.
- If the SIM card is identified successfully but no internet access is available, your SIM card may have run out of money. Ensure that you have an active plan.
- If the SIM card balance is enough, it is recommended that contact our technical support for help.

6.1.2 Through the WAN port

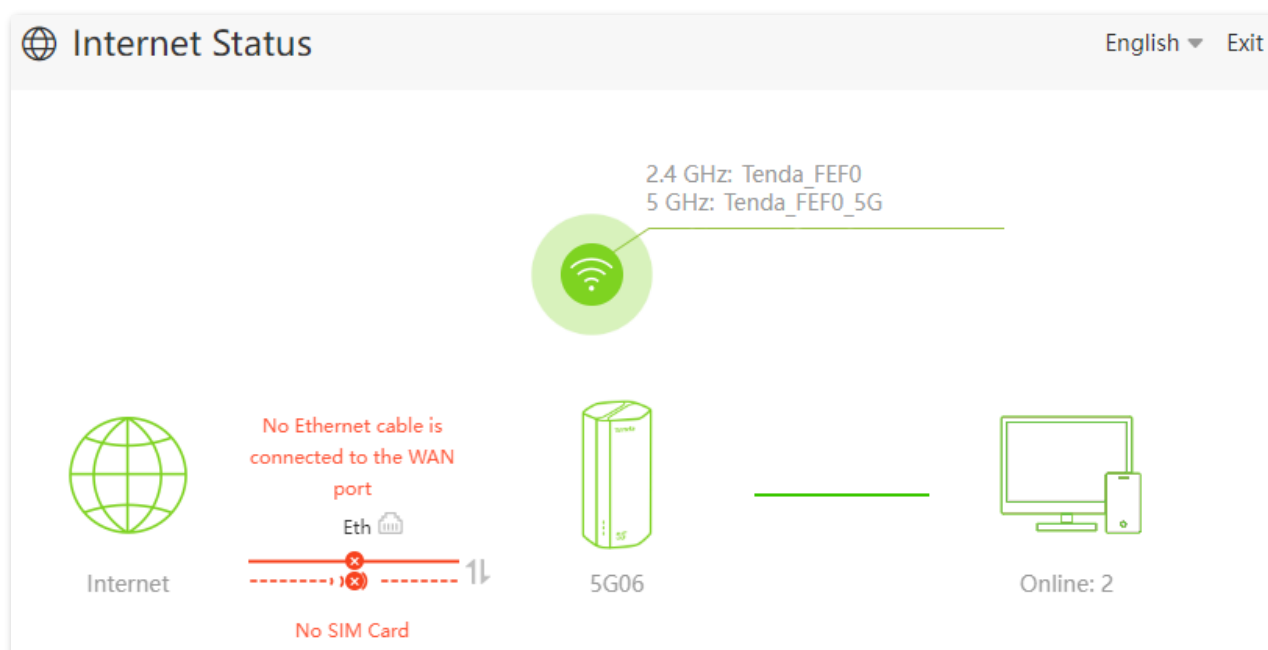
To access the page, [log in to the web UI of the router](#), and navigate to **Internet Status**. You can perform troubleshooting as prompted on the page when you access the internet through the WAN port.



- Before checking the internet status, you should connect the Ethernet port of the router to the internet using an Ethernet cable, enable the Failover function and configure internet parameters on the **Internet Settings** page.
- By default, the Ethernet ports (**1 Gbps, 2.5 Gbps**) act as LAN ports. When the Failover function is enabled, the 2.5 Gbps port is used as a WAN port.
- The connection type **PPPoE** is used for illustration here.

Ethernet cable disconnected

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



Incorrect user name and password

When “**The user name and password are incorrect.**” is shown between the internet and the router, ensure the PPPoE user name and password are entered correctly.



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

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

If the problem persists, contact your ISP for help.

No response from the remote server

When “**No response from the remote server.**” is shown between the internet and the router, it indicates that the upstream server network may be abnormal. Contact your ISP for help.

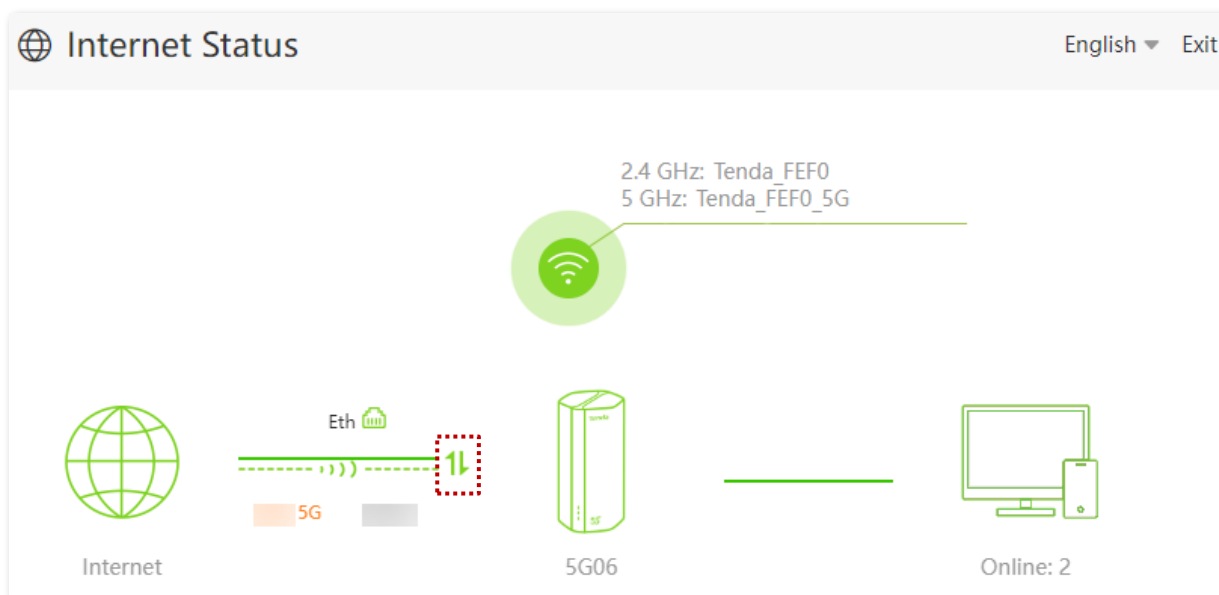
Connection disconnected

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

6.1.3 Through SIM card and WAN port

To access the page, [log in to the web UI of the router](#), and navigate to **Internet Status**.

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





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

6.2 Check WAN status

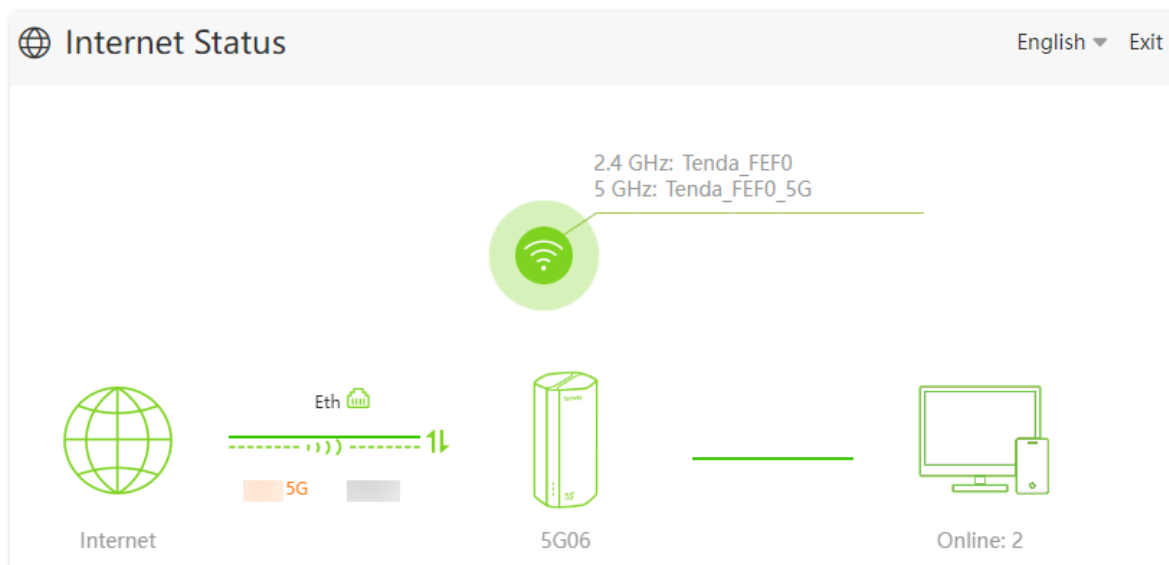
You can check the WAN status, including 5G/4G WAN status and Ethernet WAN status.



- Before checking the Ethernet WAN status, you should connect the Ethernet port of the router to the internet using an Ethernet cable, enable the Failover function and configure internet parameters on the **Internet Settings** page.
- By default, the Ethernet ports (**1 Gbps, 2.5 Gbps**) act as LAN ports. When the Failover function is enabled, the 2.5 Gbps port is used as a WAN port.

Procedure for checking WAN status

1. [Log in to the web UI of the router](#), and navigate to **Internet Status**.
2. Click .



---End

6.2.1 Check 5G/4G WAN status

You can check the information of the SIM card and 5G/4G network.

WAN Status

5G/4G WAN Status

SIM Card Status: Ready

Connection Status: Connected

Signal Strength: Normal(-85dBm)

ISP:

Mobile Network: 5G SA

Statistics: 471.169MB

Upload Speed: 10 Kbps

Download Speed: 20 Kbps

IPv4 Address:

IPv4 Subnet Mask:

IPv4 Default Gateway:

IPv4 Primary/Secondary DNS:

IPv6 Address:

IPv6 Default Gateway:

IPv6 Primary/Secondary DNS:

Access Band:

IMEI:

IMSI:

UL Frequency:

DL Frequency:

CELL ID:

CQI:

Point A ARFCN:

SSB ARFCN:

SS-RSRP:

SS-RSRQ:

SS-RSSI:

SS-SINR:

Parameter description

Parameter	Description
SIM Card Status	Specifies the SIM card status inserted in the router.
Connection Status	Specifies the internet connection status of 5G/4G mobile network.
Signal Strength	Specifies the signal strength of 5G/4G mobile network
ISP	Specifies the ISP name of the SIM card.
Mobile Network	Specifies the current network type for internet access.
Statistics	Specifies the data traffic of the SIM card that has been used.
Upload Speed	Specify the current upload and download speed of the mobile network of the router.
Download Speed	
IPv4/IPv6 Address	Specifies the IP address of the router obtained from the ISP.
IPv4 Subnet Mask	Specifies the subnet mask of the mobile network.
IPv4/IPv6 Default Gateway	Specifies the gateway IP address of the router.
IPv4/IPv6 Primary/Secondary DNS	Specifies the primary and secondary DNS server address of the router.
Access Band	Specifies the access band of the mobile network of the router.
Connecting frequency bands	Specifies the 4G/5G band that the router is working in.
IMEI	Specifies the International Mobile Equipment Identity (IMEI) of the mobile device.
IMSI	Specifies the International Mobile Subscriber Identity (IMSI) of the SIM card.
UL Frequency	These parameters are the network camping parameters of the SIM card and will change as the camped cell changes.
DL Frequency	
CELL ID	
CQI	
Point A ARFCN	
SSB ARFCN	
SS-RSRP	

Parameter	Description
SS-RSRQ	
SS-RSSI	
SS-SINR	

6.2.2 Check Ethernet WAN status

You can check the information of the Ethernet port connected to the Ethernet cable.

Ethernet WAN Status

Connection Status: Connected

Connection Type: PPPoE

Connection Duration: 2m 5s

IPv4 Address:

IPv4 Subnet Mask:

IPv4 Default Gateway:

Primary DNS:

Secondary DNS:

MAC Address:

Parameter description

Parameter	Description
Connection Status	Specifies internet connection status of WAN port connected to the Ethernet cable.
Connection Type	Specifies how your router connects to the internet, including: – PPPoE: Select this type if you access the internet using the PPPoE user name and PPPoE password. – Dynamic IP Address: Select this type if you can access the internet by simply plugging in an Ethernet cable. – Static IP Address: Select this type if you want to access the internet using fixed IP information.

Parameter	Description
Connection Duration	Specifies the connection duration of WAN port connected to the Ethernet cable.
IPv4 Address	Specifies the IP address of the router obtained from the ISP.
IPv4 Subnet Mask	Specifies the WAN subnet mask of the router.
IPv4 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 Ethernet MAC address of the router.

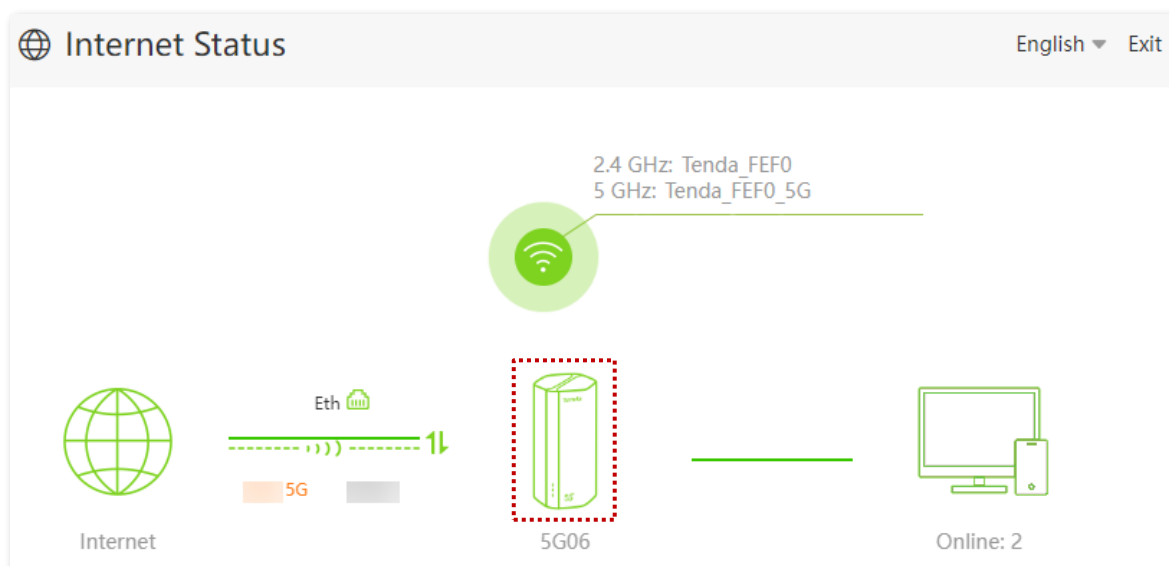
6.3 Check system information

You can check the system information, including system time, uptime, firmware version, hardware version, LAN status and Wi-Fi status.

Procedure for checking system information

1. [Log in to the web UI of the router](#), and navigate to **Internet Status**.

2. Click .



--End

6.3.1 Check basic information

You can check the basic information of the router, such as system time, uptime and firmware version and hardware version.

Information

System Time: 2025-08-09 11:24:08

Uptime: 1d 1h 48m 59s

Firmware Version: V05.06.01.06_multi

Hardware Version: V1.0

IMEI:

Parameter description

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

6.3.2 Check LAN status

You can check the LAN information, such as LAN IPv4/IPv6 address and MAC address.

LAN Status

IPv4 Address: 192.168.0.1/24

IPv6 Address:

MAC Address:

Parameter description

Parameter	Description
IPv4 Address	Specifies the LAN IPv4 address of the router, which is the IP address for logging in to the web UI of the router.
IPv6 Address	Specifies the LAN IPv6 address of the router.
MAC Address	Specifies the LAN MAC address of the router.

6.3.3 Check Wi-Fi status

You can check the information of 2.4 GHz and 5 GHz networks, including the visibility, Wi-Fi name, bandwidth, channel and MAC address.

Wi-Fi Status

2.4 GHz Network:

Wi-Fi Network: Visible

Wi-Fi Name: Tenda_FEF0

Bandwidth: 20MHz

Channel: Auto

MAC Address:

5 GHz Network:

Wi-Fi Network: Visible

Wi-Fi Name: Tenda_FEF0_5G

Bandwidth: 160MHz

Channel: Auto

MAC Address:

Parameter description

Parameter	Description
Wi-Fi Network	Specifies whether the Wi-Fi network is hidden.
Wi-Fi Name	Specifies the Wi-Fi name of the router.
Bandwidth	Specifies the bandwidth of the respective Wi-Fi.

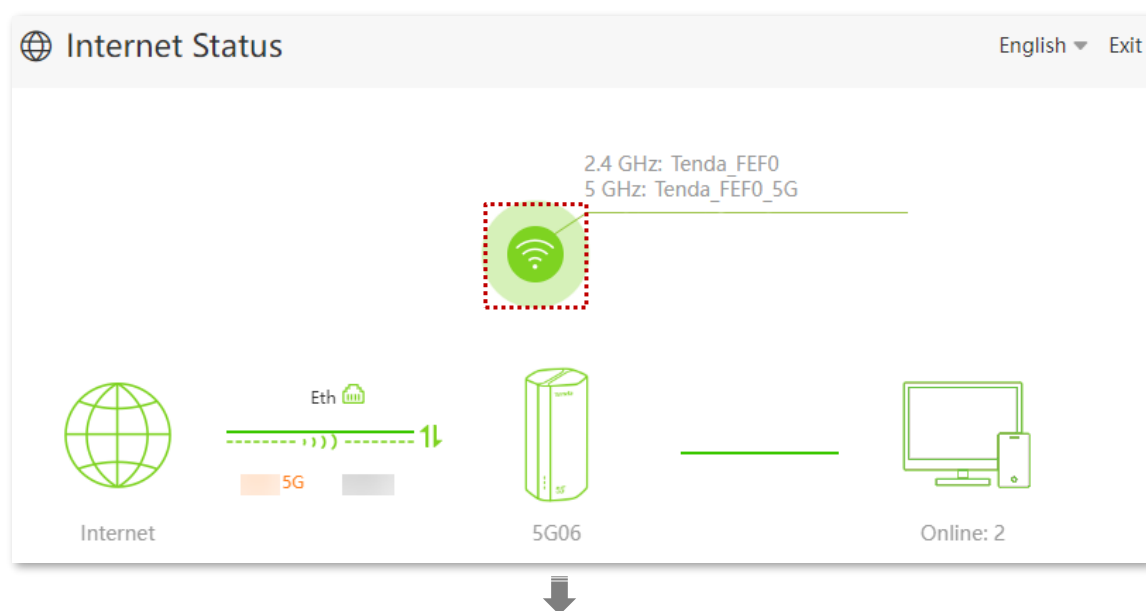
Parameter	Description
Channel	Specifies the channel that the respective Wi-Fi works in.
MAC Address	Specifies the MAC address of the respective Wi-Fi.

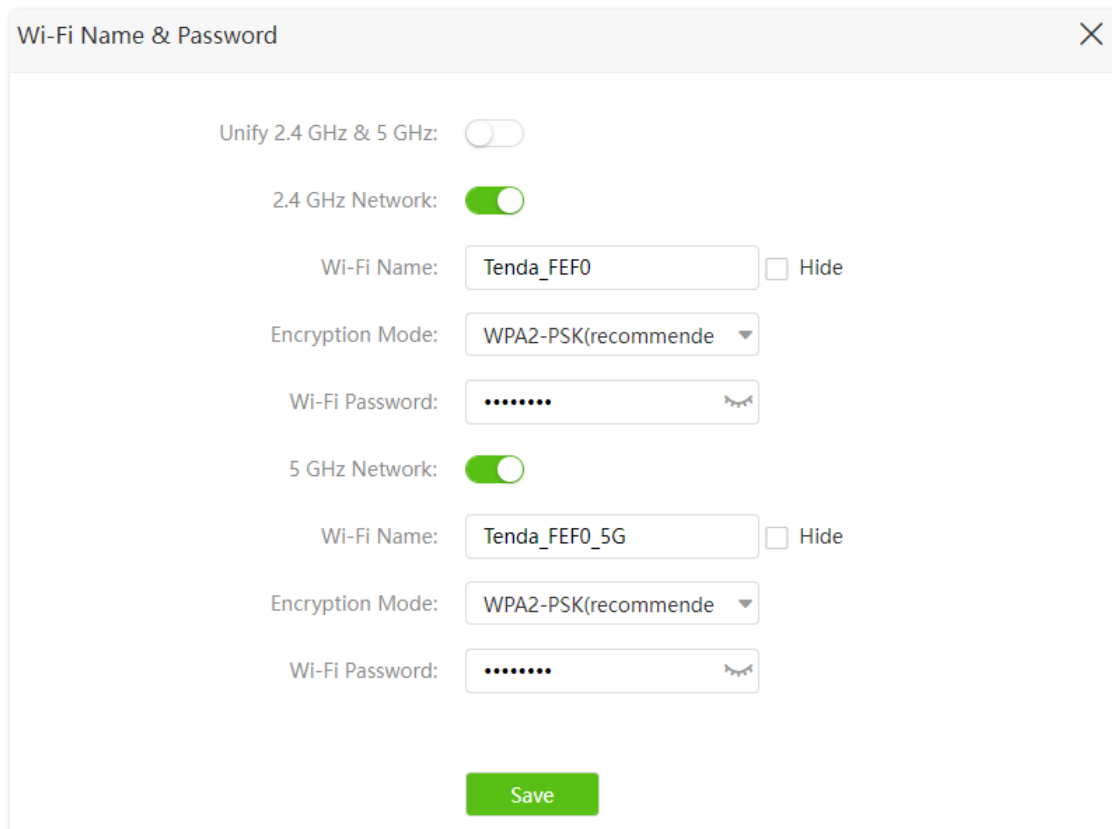
6.4 Check or configure Wi-Fi information

You can check or configure the Wi-Fi information of the router.

Procedure for checking or configuring Wi-Fi information

1. [Log in to the web UI of the router](#), and navigate to **Internet Status**.
2. Click .





The image shows a web-based configuration window titled "Wi-Fi Name & Password". It contains settings for two Wi-Fi networks: 2.4 GHz and 5 GHz. At the top, there is a toggle for "Unify 2.4 GHz & 5 GHz" which is currently turned off. For the 2.4 GHz Network, the "Wi-Fi Name" is "Tenda_FEF0" with a "Hide" checkbox, the "Encryption Mode" is "WPA2-PSK(recommende)", and the "Wi-Fi Password" is masked with dots. The 5 GHz Network has a "Wi-Fi Name" of "Tenda_FEF0_5G" with a "Hide" checkbox, the "Encryption Mode" is "WPA2-PSK(recommende)", and the "Wi-Fi Password" is also masked. A green "Save" button is located at the bottom center of the window.

---End

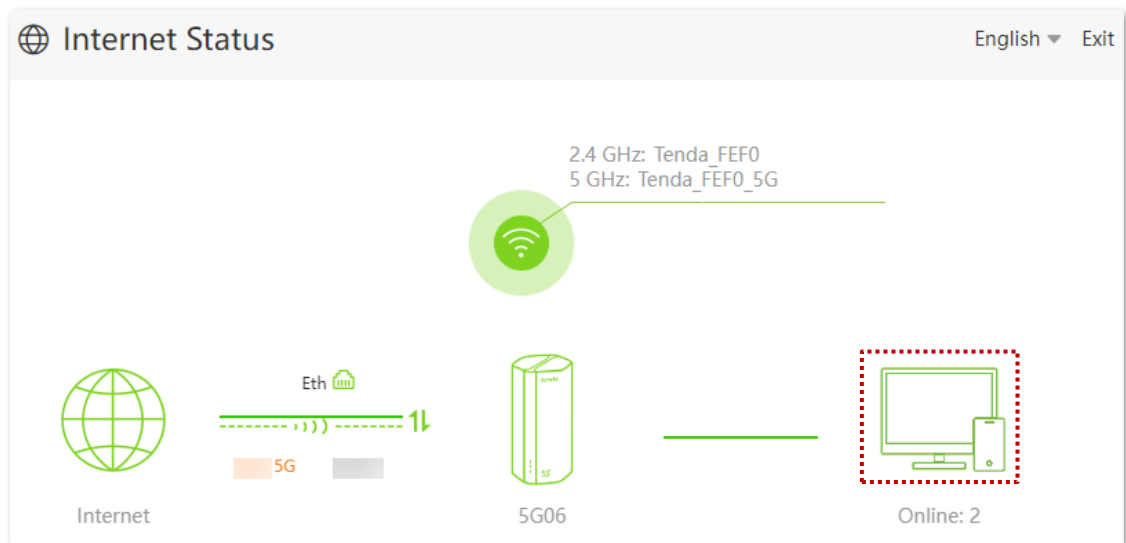
You can change Wi-Fi parameters as required. For details, see [Wi-Fi settings](#).

6.5 Check online or blacklisted devices

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

Procedure for checking online or blacklisted devices

1. [Log in to the web UI of the router](#), and navigate to **Internet Status**.
2. Click .
3. Check online devices on the **Online Device** tab, or check blacklisted devices on the **Blacklist** tab.



Manage Device

Online Devices (2) Blacklist

Device Name	Current Speed	Access Type	Blacklist
? Huawei 192.168.0.147	↑ 9 Kbps ↓ 88 Kbps	2.4G	Add
? DESKTOP-2K2MLGI 192.168.0.177	↑ 6 Kbps ↓ 11 Kbps	Wired	Local Host

---End

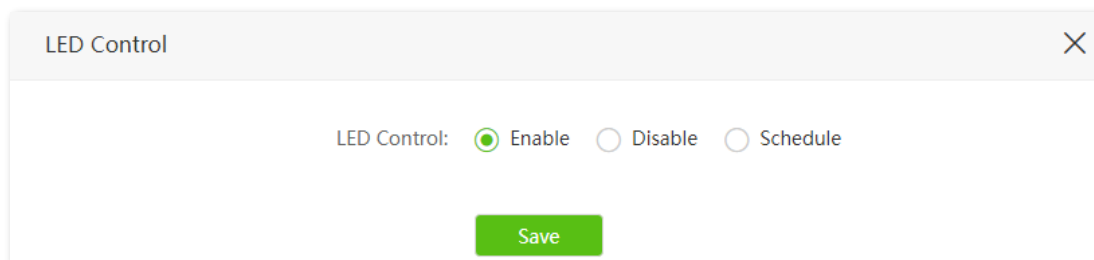
Parameter description

Parameter	Description
Online Devices	Device Name
	Current Speed
	Access Type
	Blacklist
Blacklist	Device Name
	MAC Address
	Remove from Blacklist

6.6 Control indicators

6.6.1 Enable or disable indicators

1. [Log in to the web UI of the router](#), and navigate to **Advanced Settings** > **LED Control**.
2. Set **LED Control** to **Enable** or **Disable** as required.
3. Click **Save**.



LED Control

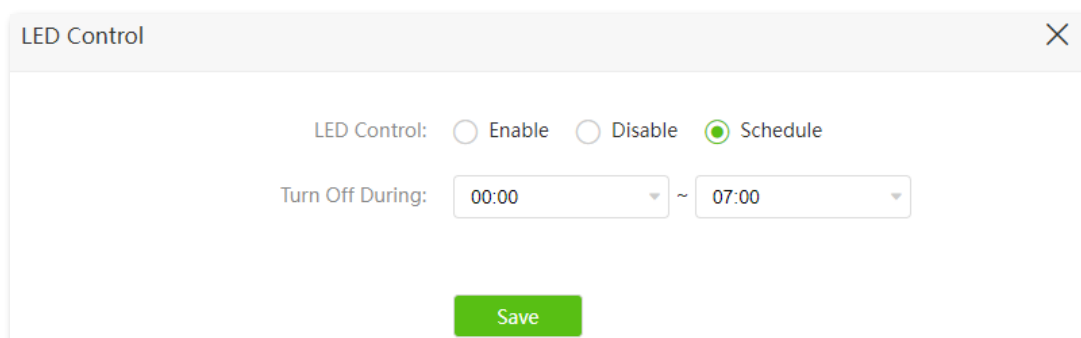
LED Control: ☒ Enable ☐ Disable ☐ Schedule

Save

---End

6.6.2 Schedule indicators to turn off

1. [Log in to the web UI of the router](#), and navigate to **Advanced Settings** > **LED Control**.
2. Set **LED Control** to **Schedule**.
3. Specify the period when the indicators are turned off, which is **00:00 ~ 07:00** in this example.
4. Click **Save**.



LED Control

LED Control: ☐ Enable ☐ Disable ☒ Schedule

Turn Off During: 00:00 ~ 07:00

Save

---End

Parameter description

Parameter	Description
Schedule	Indicators are only turned off during the specified period.

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

6.7 TR069

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

To access the page, [log in to the web UI of the router](#), and navigate to **Advanced Settings > TR069 Settings**.

TR069 Settings

TR069:

ACS

URL:

ACS User Name:

hgw

ACS Password:

hgw

Enable Scheduled Notification:

Scheduled Notification Interval:

43200

Unit: Second

Connection Request

Connection Request User Name:

itms

Connection Request Password:

itms

Port:

7547

STUN Connection

Enable STUN:

STUN Server Address:

STUN Server Port:

Save

Parameter description

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

6.8 Configure system time

The time-based functions require an accurate system time. The system time of the router can be synchronized with the internet or set manually. By default, it is synchronized with the internet.

6.8.1 Sync system time with the internet time

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

Procedure for synchronizing system time with internet time

1. [Log in to the web UI of the router](#), and navigate to **System Settings > Time Settings**.

2. Select **Sync with internet time** for **System Time**.
3. Select your time zone from the **Select Time Zone** menu.
4. If you live in a region that observes daylight saving time, turn on **DST** (Daylight Saving Time), then select the start time and end time of DST.
5. Click **Save**.

Time Settings

System Time: ☒ Sync with internet time ☐ Manual

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

Current Time: 2025-08-09 14:14:13 (synchronized with internet time)

DST: ☒

Start 2025: Mar. Last Sun. 01:00

End 2025: Oct. Last Sun. 01:00

Status: DST not use

Save

---End

After the configuration is completed, you can check whether **System Time** is correct.

Parameter description

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

Parameter	Description
Start 2025	Specifies the start time of DST. It is available only when DST is enabled.
End 2025	Specifies the end time of DST. It is available only when DST is enabled.
Status	Specifies whether the DST is used. It is available only when DST is enabled.

6.8.2 Set the time manually

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

Procedure for setting the time manually

1. [Log in to the web UI of the router](#), and navigate to **System Settings > Time Settings**.
2. Select **Manual** for **System Time**.
3. Set **Date** and **Time** as required.

---End

After the configuration is completed, you can check whether **System Time** is correct.

6.9 Change login password

For initial setup or after a reset, set the new login password to ensure privacy and security. The longer the password, the higher the security.



The character limit and composition rules for passwords are subject to software user interface prompts.

Procedure for changing login password

1. [Log in to the web UI of the router](#), and navigate to **System Settings > Login Password**.
2. In the **Old Password**, enter the current password for logging in to the router's web UI.
3. Set a new login password in the **New Password**.
4. Enter the new login password again in the **Confirm Password**.
5. Click **Save**.

Login Password

Old Password:

New Password:

Confirm Password:

Save

---End

6.10 Reboot and reset

6.10.1 Reboot the router

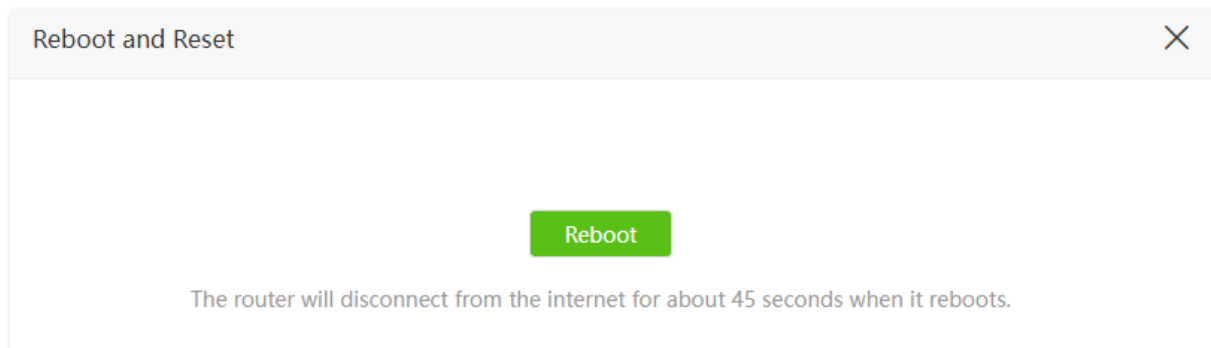
If any parameter fails to take effect or the router does not work properly, you can try rebooting the router.



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

Procedure for rebooting the router

1. [Log in to the web UI of the router](#), and navigate to **System Settings > Reboot and Reset**.
2. Click **Reboot**.



---End

Wait for a moment until the ongoing process finishes.

6.10.2 Reset the router

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

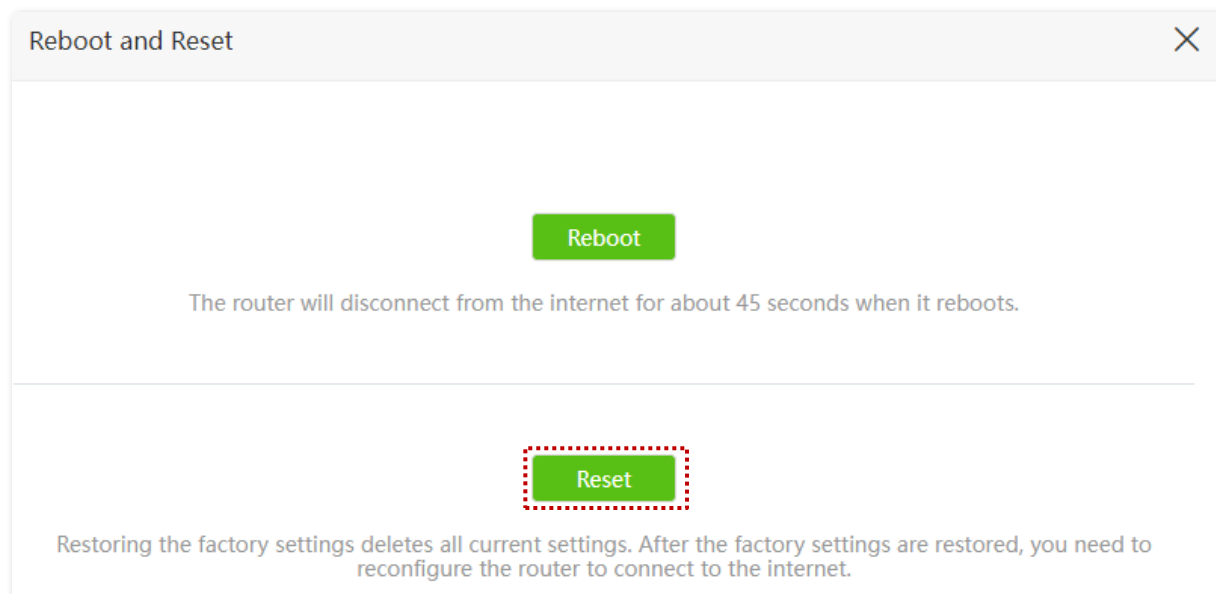


NOTE

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

Method 1: Reset the router on the web UI

1. [Log in to the web UI of the router](#), and navigate to **System Settings > Reboot and Reset**.
2. Click **Reset**.



---End

Wait for a moment until the ongoing process finishes.

Method 2: Reset the router using the reset button

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

6.11 Upgrade firmware

You can upgrade the firmware of the router to obtain the latest functions and more stable performance. The router supports online firmware upgrade and local firmware upgrade.

6.11.1 Online upgrade

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

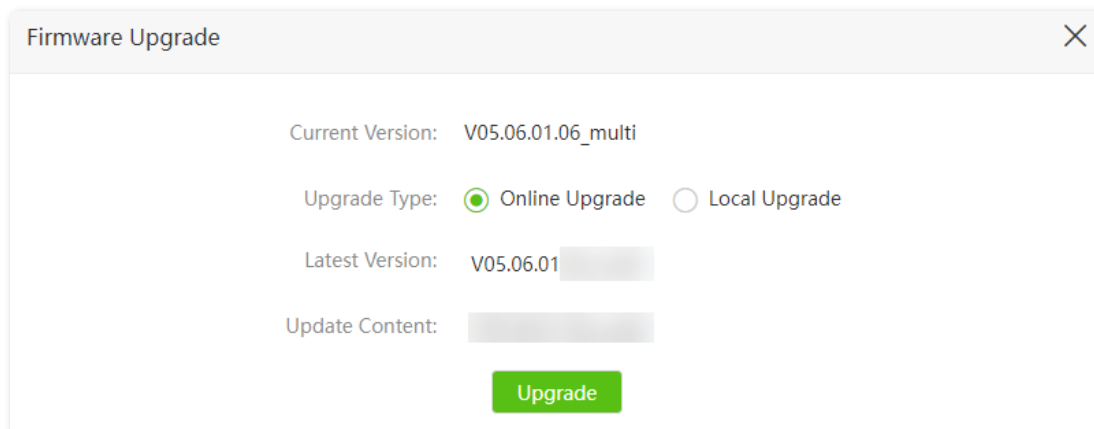


Do not disconnect the router from power or internet during this process. Otherwise, the upgrade may fail or the router may be damaged.

Procedure for performing online upgrade

1. [Log in to the web UI of the router](#), and navigate to **System Settings > Firmware Upgrade**.

2. Select **Online Upgrade** for **Upgrade Type**.
3. Wait until a new firmware version is detected. The following figure is for reference only.



Firmware Upgrade

Current Version: V05.06.01.06_multi

Upgrade Type: ☒ Online Upgrade ☐ Local Upgrade

Latest Version: V05.06.01

Update Content:

Upgrade

4. Click **Upgrade**.

---End

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

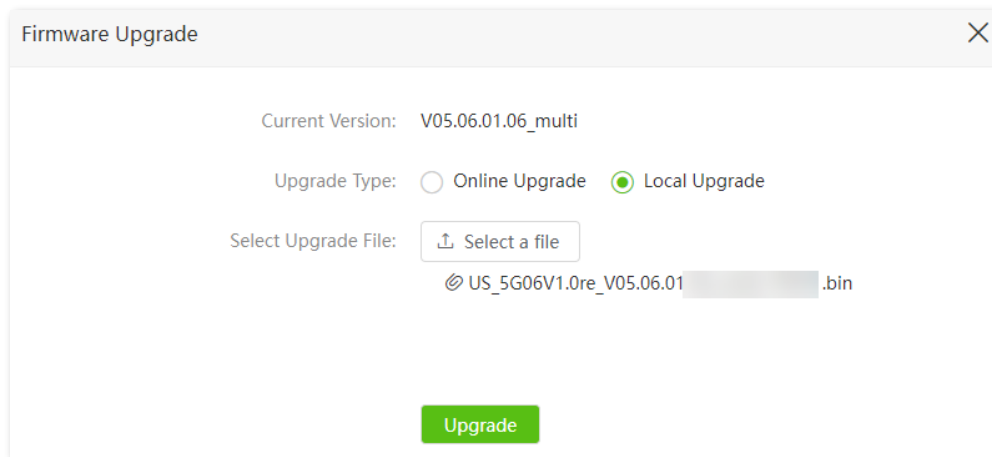
6.11.2 Local upgrade



To prevent the router from being damaged:

- Ensure that the firmware is applicable to the router. Generally, the firmware upgrade file suffixed with **.bin**.
- It is recommended to upgrade the firmware by connecting an Ethernet port to a computer and performing the upgrade on the web UI.
- When you are upgrading the firmware, do not power off the router.

1. Go to www.tendacn.com. Download an applicable firmware of the router to your local computer and unzip it.
2. [Log in to the web UI of the router](#), and navigate to **System Settings > Firmware Upgrade**.
3. Select **Local Upgrade** for **Upgrade Type**.
4. Select and upload the firmware that has been downloaded to your computer in step 1, and click **Upgrade**.



---End

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

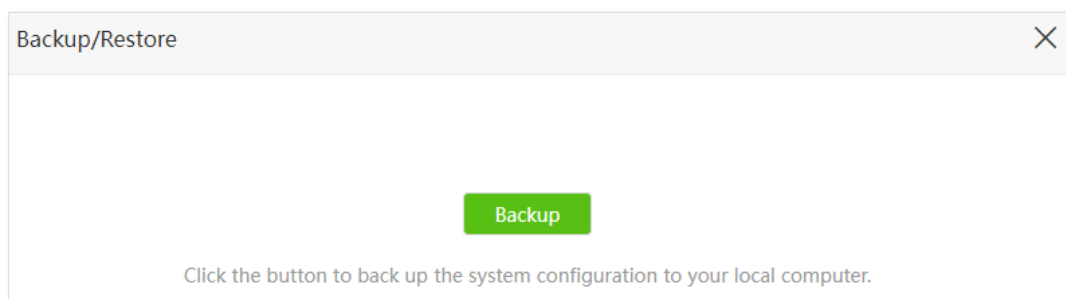
6.12 Backup and Restore

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

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

6.12.1 Backup the configurations of the router

1. [Log in to the web UI of the router](#), and navigate to **System Settings** > **Backup/Restore**.
2. Click **Backup**.



---End

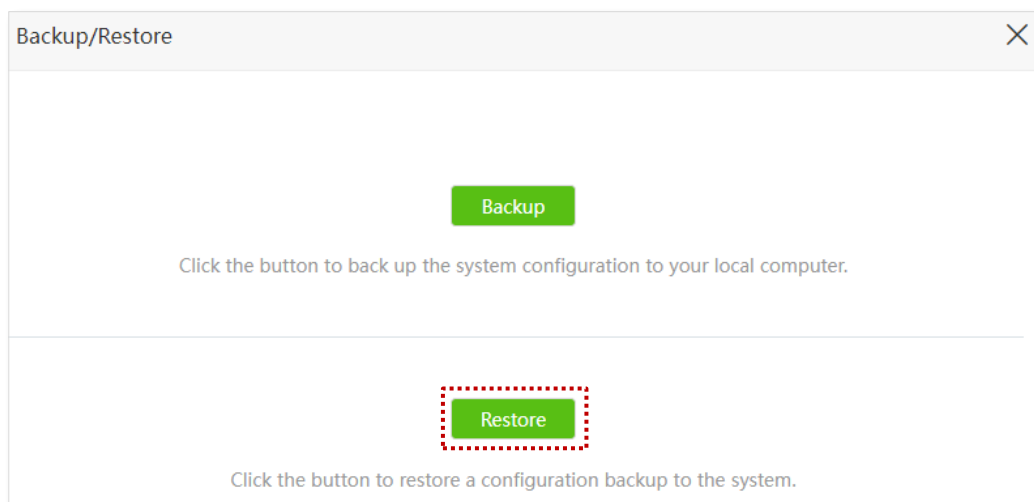
A file named **RouterCfm.cfg** will be downloaded to your local host.



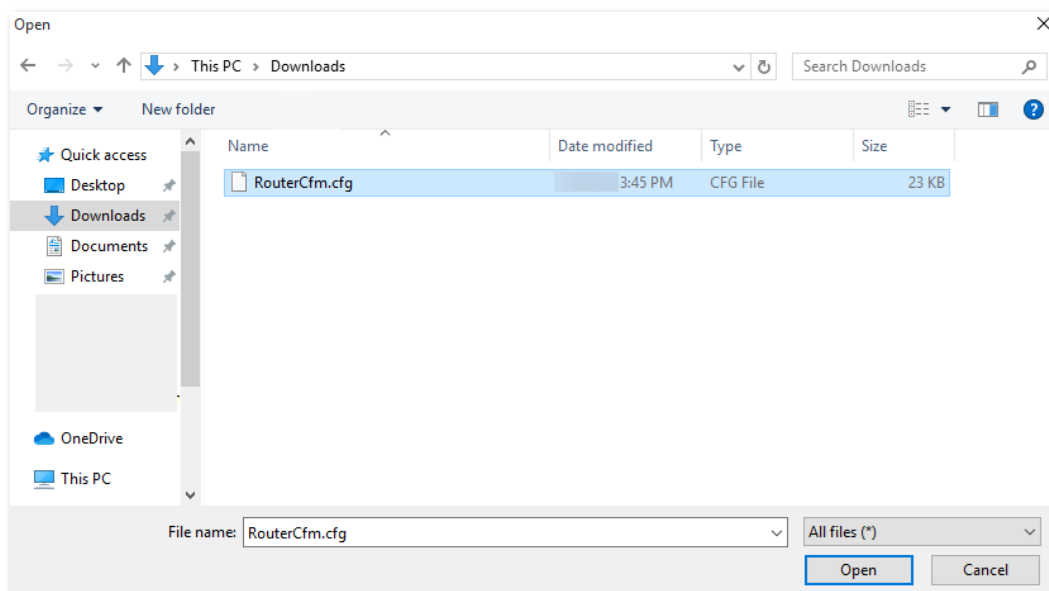
If the browser prompts you “This type of file can harm your computer. Do you want to keep RouterCfm.cfg anyway?”, select **Keep**.

6.12.2 Restore previous configurations of the router

1. [Log in to the web UI of the router](#), and navigate to **System Settings > Backup/Restore**.
2. Click **Restore**.



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



---End

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

6.13 Configure remote management

Generally, the web UI of the router can only be accessed on devices that are connected to the router by an Ethernet 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. This function is disabled by default.

Example of configuring remote management

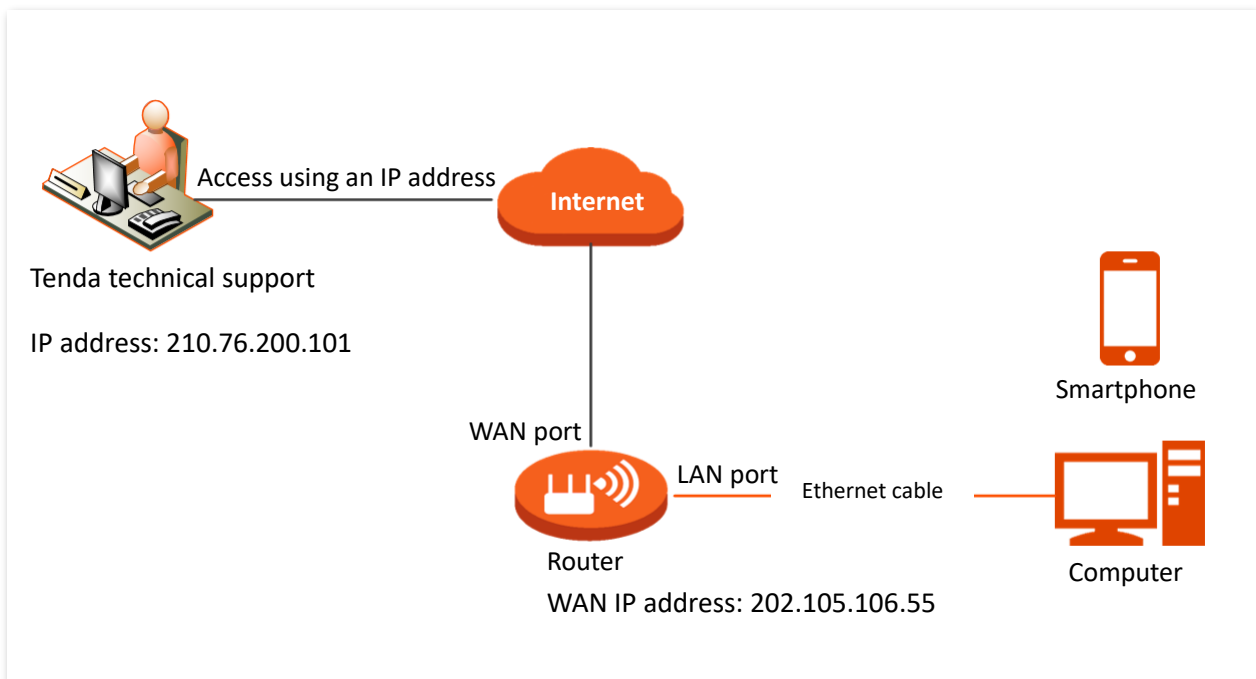
Scenario: You encounter a problem in configuring the router, and the router can access internet.

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:

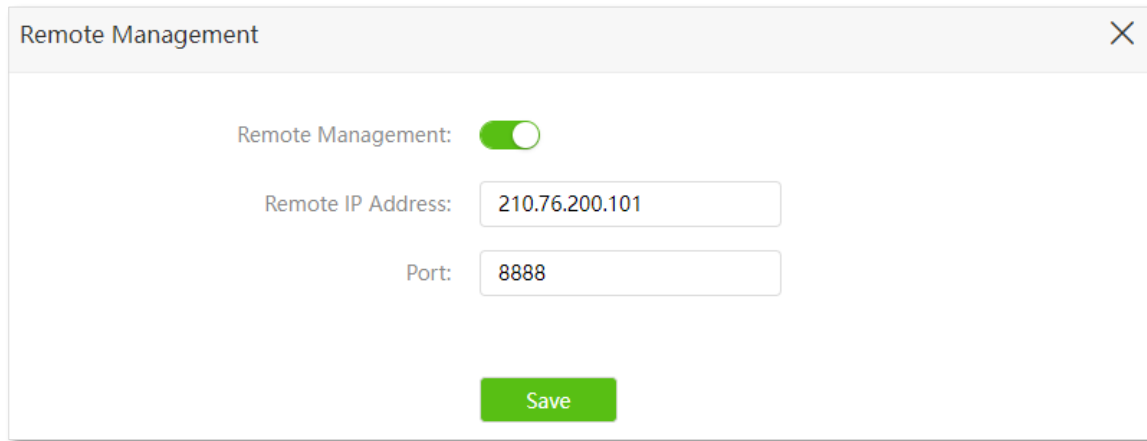
- IP address of Tenda technical support: 210.76.200.101
- WAN port IP address of the router: 202.105.106.55



Procedure for configuring remote management

1. [Log in to the web UI of the router](#), and navigate to **System Settings > Remote Management**.
2. Enable the **Remote Management** function.

3. Enter the IP address that can access the web UI remotely, which is **210.76.200.101** in this example.
4. (Optional) Specify the port number of the router which is opened for remote management.
5. Click **Save**.



---End

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

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 function is enabled, the web UI can also be accessed through “http://the domain name of the router:port number”.

6.14 Check or export system logs

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.

The log recording time depends on the system time of the router. To ensure that the log recording time is accurate, set the system time of the router first. Navigate to [Time Settings](#) page to calibrate the router's system time.



NOTE

Rebooting the router or clicking **Clear** will clear all previous system logs.

Procedure for checking or exporting system logs

1. [Log in to the web UI of the router](#), and navigate to **System Settings > System Log**.
2. (Optional) Click **Export** to export the system logs to your local host.

System Log			
Note: If the router is not connected to the internet, the default login time is 2023-X-X XX:XX:XX.			
Number	Time	Type	Log Content
1	2025-08-09 15:45:14	system	web 192.168.0.177 login
2	2025-08-09 15:45:12	system	web 192.168.0.177 login time expired
3	2025-08-09 15:44:48	system	User 192.168.0.177 login expired.
4	2025-08-09 15:16:35	system	web 192.168.0.177 login
5	2025-08-09 15:14:42	system	Admin logout
6	2025-08-09 15:12:41	system	Sync time success!
7	2025-08-09 15:12:01	system	web 192.168.0.177 login
8	2025-08-09 15:11:53	system	Lte wan internet connected!
9	2025-08-09 15:11:53	system	Lte wan internet connected!
10	2025-08-09 15:11:49	system	Cpe registration state 2
Page 1, Total 2 pages Total 17 items < 1 2 >			
Export Clear			

---End

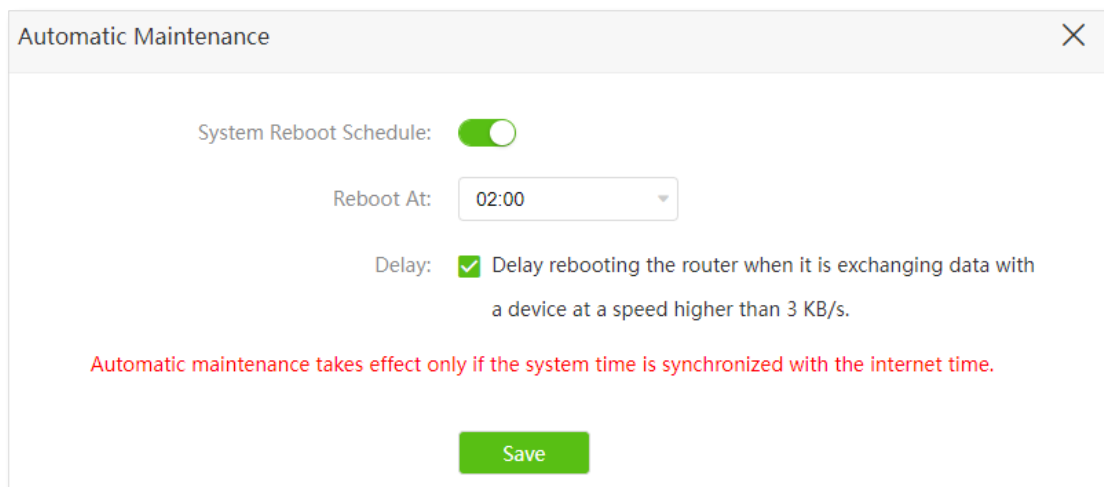
6.15 Configure automatic maintenance

Automatic maintenance enables you to make the router restart regularly, improving the stability and service life of the router. This function is disabled by default.

Procedure for configuring automatic maintenance

1. [Log in to the web UI of the router](#), and navigate to **System Settings > Automatic Maintenance**.
2. Enable the **System Reboot Schedule** function.

3. Specify the time when the router reboots automatically every day.
4. Tick **Delay** as required.
 - 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, the router will delay rebooting.
 - Unticked: The function is disabled. The router reboots immediately when the specified time for rebooting approaches.
5. Click **Save**.



The screenshot shows a window titled "Automatic Maintenance" with a close button (X) in the top right corner. Inside the window, there are three main settings:

- System Reboot Schedule:** A green toggle switch is turned on.
- Reboot At:** A dropdown menu showing "02:00".
- Delay:** A green checkmark is next to the text "Delay rebooting the router when it is exchanging data with a device at a speed higher than 3 KB/s."

Below these settings, a red text message reads: "Automatic maintenance takes effect only if the system time is synchronized with the internet time."

At the bottom center, there is a green button labeled "Save".

---End

The router will automatically reboot at the specified time.

7 Manage mobile settings

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

7.1 Configure 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 configuration 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.



Take inserting two SIM cards as an example, and set the toggle switch at the bottom of the router to Auto.

7.1.1 Unlock the SIM card

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

Unlock the SIM card in the quick setup wizard

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

Procedure for unlocking the SIM card in the quick setup wizard

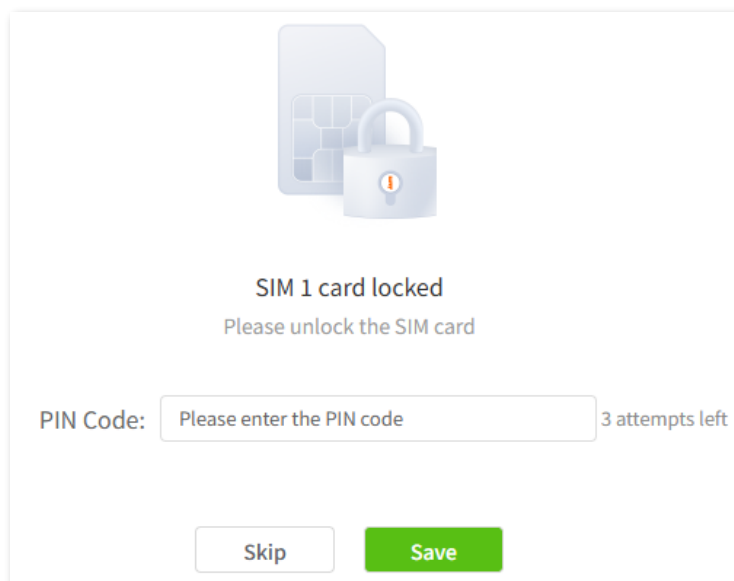
1. [Log in to the web UI of the router.](#)
2. Click **Start**.



3. Enter the **PIN Code**, and click **Save**. The following figure is for reference only.



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



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

---End

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

Unlock the SIM card on the web UI

When “**Locked SIM**” is shown between the internet and the router, it indicates that you need to enter the PIN code. Click **Locked SIM** to navigate to the **SIM PIN** page and configure the related parameters.

Procedure for unlocking the SIM card on the web UI

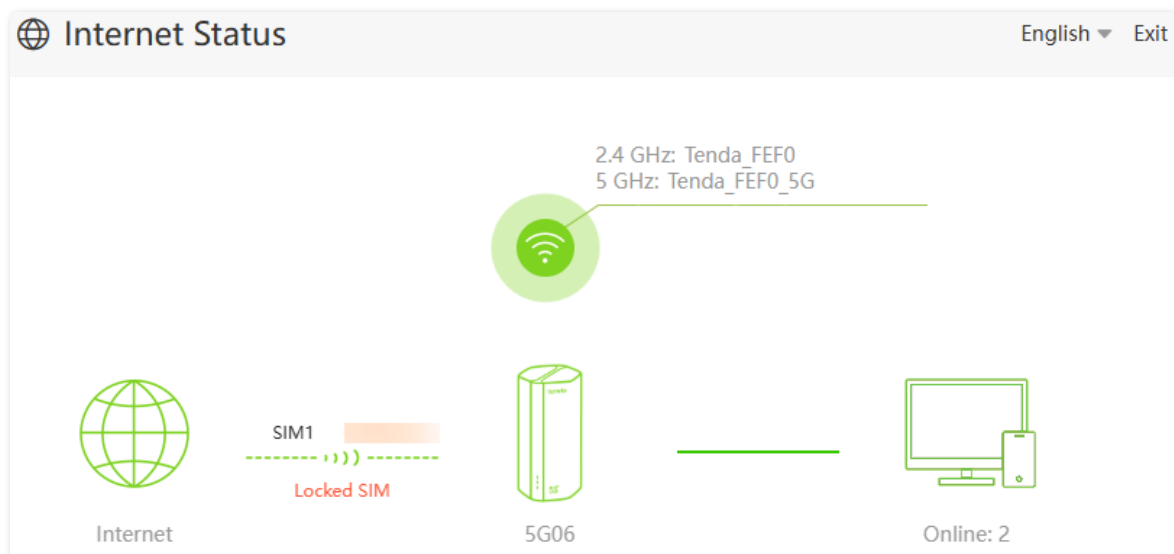
1. [Log in to the web UI of the router.](#)
2. Unlock the SIM card.



Take inserting two SIM cards as an example, and set the toggle switch at the bottom of the router to Auto.

- **Method 1:**

- 1) Click **Locked SIM**.



- 2) Enter the **PIN Code**, and click **Save**.

SIM PIN

SIM Card Status: PIN Required

PIN Lock: ☒

PIN Code: 3 attempts left

Save

• **Method 2:**

- 1) Navigate to **Advanced Settings > SIM PIN**.
- 2) In the **Network Selection** field, choose the SIM card as required to unlock.
- 3) Enter the **PIN Code**, and click **Save**.

SIM PIN

Network Selection: ☒ SIM1 ☐

SIM Card Status: PIN Required

PIN Lock: ☒

PIN Code: 3 attempts left

Save

---End

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

NOTE

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

7.1.2 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.

Procedure for disabling PIN lock for the SIM card



Take inserting two SIM cards as an example, and set the toggle switch at the bottom of the router to Auto.

1. [Log in to the web UI of the router](#), and navigate to **Advanced Settings > SIM PIN**.
2. In the **Network Selection** field, choose the SIM card as required to disable the PIN.
3. Disable **PIN Lock**.
4. Enter the original **PIN Code**, and click **Save**.



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

SIM PIN

Network Selection: ☒ ☐

SIM Card Status: PIN unlocked

PIN Lock: ☐

PIN Code: 3 attempts left

Save

---End

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

7.1.3 Enable PIN lock for the SIM card

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



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

Procedure for enabling PIN lock for the SIM card



Take inserting two SIM cards as an example, and set the toggle switch at the bottom of the router to Auto.

1. [Log in to the web UI of the router](#), and navigate to **Advanced Settings > SIM PIN**.
2. In the **Network Selection** field, choose the SIM card as required to enable the PIN.
3. Enable **PIN Lock**.
4. Specify a **PIN Code**, and click **Save**.

SIM PIN

Network Selection: ☒ ☐

SIM Card Status: Ready

PIN Lock: ☒

PIN Code: 3 attempts left

Save

---End

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

7.1.4 Use PUK code to set PIN code

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

Procedure for using PUK code to set PIN code



Take inserting two SIM cards as an example, and set the toggle switch at the bottom of the router to Auto.

1. [Log in to the web UI of the router](#), and navigate to **Advanced Settings > SIM PIN**.
2. In the **Network Selection** field, choose the SIM card as required to unlock the PUK.
3. Enter the **PUK Code**.
4. Enter a new PIN code in the **New PIN Code**.
5. Enter a new PIN code again in the **Confirm New PIN Code**.
6. Click **Save**.

The screenshot shows a web interface titled "SIM PIN" with a close button (X) in the top right corner. The interface contains the following elements:

- Network Selection:** A toggle switch with two positions. The first position is selected, indicated by a green dot.
- SIM Card Status:** Displays "PUK Required".
- PUK Code:** A text input field with the placeholder "Please enter the PUK code". To the right of the field, it says "10 attempts left".
- New PIN Code:** A text input field with the placeholder "Please enter a new PIN code".
- Confirm New PIN Code:** A text input field with the placeholder "Enter the new PIN code again".
- Save:** A green button at the bottom center.

---End

7.2 Configure mobile data

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

Example of configuring mobile data

Scenario: You inserted two SIM cards 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:

- The toggle switch at the bottom of the router is set to Auto.
- Available data traffic of each SIM card: 10 GB
- Start date of data usage record: 1st each month
- Smartphone number: 188****5555
- Alert percentage: 80%

Procedure for configuring mobile data

1. [Log in to the web UI of the router](#), and navigate to **Advanced Settings > Mobile Data**.
2. Configure mobile data settings of the SIM1 card.
 - 1) Choose the network operator in the **Network Selection** field to configure mobile data settings.
 - 2) (Optional) Click **Update** to update the current usage data in **Total Used**.
 - 3) Enable **Data Limit**.
 - 4) Set **Monthly Allowance** to **10**, and choose **GB** in the drop-down box.
 - 5) Set **Usage Alert** to **80%**, and set **SMS Alert of Usage** to **188****5555**.
 - 6) Enable **Monthly Data Statistics**.
 - 7) Set **Start Date** to **1**, and click **Save**.
3. Refer to step 2 to configure mobile data settings of the SIM2 card.

Mobile Data

Network Selection:

☒
☐

Total Used: 382.704 MB

Update

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

Data Limit:

☒

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

Monthly Allowance:

10

GB

Usage Alert:

80%

SMS Alert of Usage:

188****5555

Send Test Message

Note: This function may cause SMS charges.

Monthly Data Statistics:

☒

Start Date:

1

Save

---End

After the configuration is completed, you will receive an SMS message when the data traffic usage reaches 8 GB and will not be able to use the corresponding SIM card to access the internet through the router when the data traffic usage reaches 10 GB.



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**.

Parameter description

Parameter	Description
Network Selection	If you need to configure mobile data settings for different SIM cards, you can select the corresponding network operator for the SIM card and then configure mobile data settings.  TIP It is available only when you insert two SIM cards into the router and the toggle switch at the bottom of the router is set to Auto.
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 data of Total Used at the date specified in Start Date.
Start Date	Specifies the date at which the router clears the data statistics of the last month and start to record in the following month.

7.3 Configure PCI&Band lock

This function is primarily used to lock onto higher-quality bands or cells, ensuring network stability.

- The core function of band locking is to enhance connection stability and transmission speed by locking onto specific 4G/5G frequency bands. Since 4G/5G frequency bands vary among different ISPs, configuration should be based on the ISP's frequency bands.
- Cell locking requires locking onto specific base station cells through radio frequency parameters (such as EARFCN_DL, Pci), and is suitable for scenarios requiring a fixed connection to a strong-signal cell (such as high-quality cells with the smallest RSRP value).



Without guidance from technical personnel, it is recommended to keep the default settings. Otherwise, network disconnection may occur.

Procedure for configuring PCI&Band lock

1. [Log in to the web UI of the router](#), and navigate to **Advanced Settings > PCI&Band lock**.
2. Enable **Search Band** and **Lock Cell**.
3. Select the 4G/5G frequency bands or **Cell_Band** to be locked as required.
4. Click **Lock**. The following figure is for reference only.

PCI&Band lock

Search Band: ☒

Result:
5G: ☒ N28
4G: ☐ B1 ☐ B3 ☐ B5 ☐ B8 ☐ B40 ☐ B41

Lock Cell: ☒

Lock

Re-search

Mode	PLMN_Name	Cell_Band	Bandwidth	EARFCN DL	Pci	Cid
NR	CHINA BROA...	☐ 28	30MHz	152650	567	c1e788047
		☐ 28	30MHz	152650	91	c1ecd503e
		☐ 28	30MHz	152650	640	c1e2bd03e
	CHN-CT	☒ 78	100MHz	627264	336	81b208001
	China Mobile	☐ 28	30MHz	152650	567	c1e788047
		☐ 28	30MHz	152650	91	c1ecd503e
		☐ 28	30MHz	152650	640	c1e2bd03e

Lock

Re-search

---End

7.4 Perform ISP update

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.



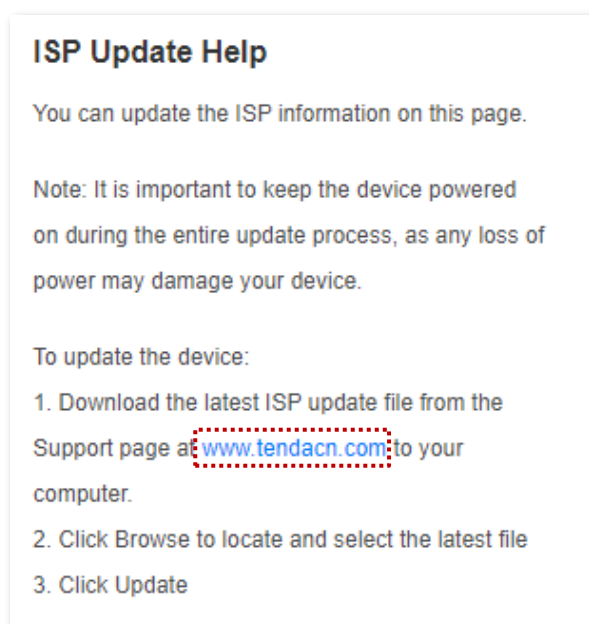
To prevent the router from being damaged:

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

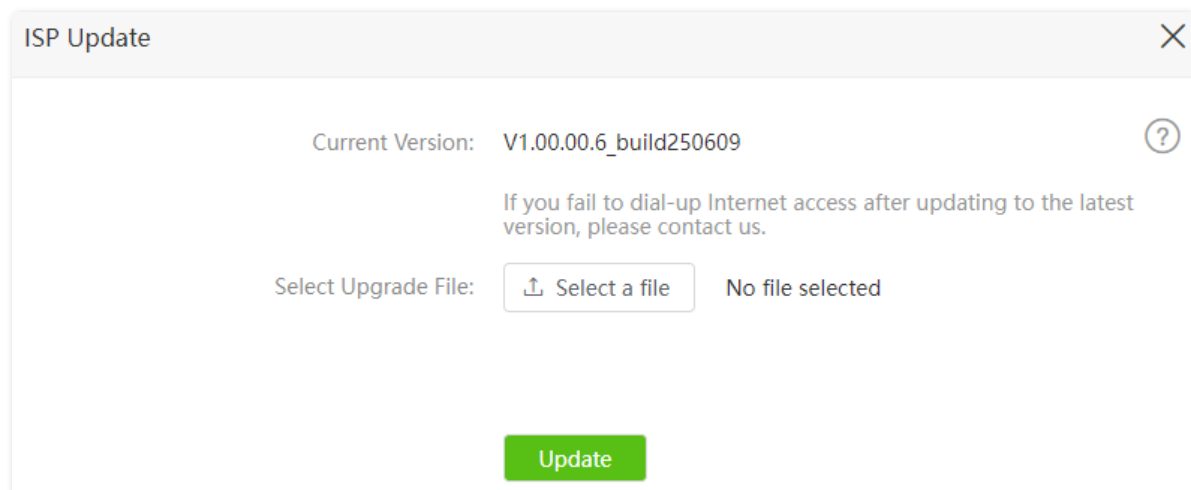
Procedure for performing ISP update

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

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



3. Click **Select a file**. Select and upload the ISP update file downloaded in step 2.
4. Click **Update**.



---End

Wait for a moment until the configuration is completed. 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.

7.5 Manage SMS messages

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

7.5.1 Send SMS messages

Send SMS messages to a new smartphone number

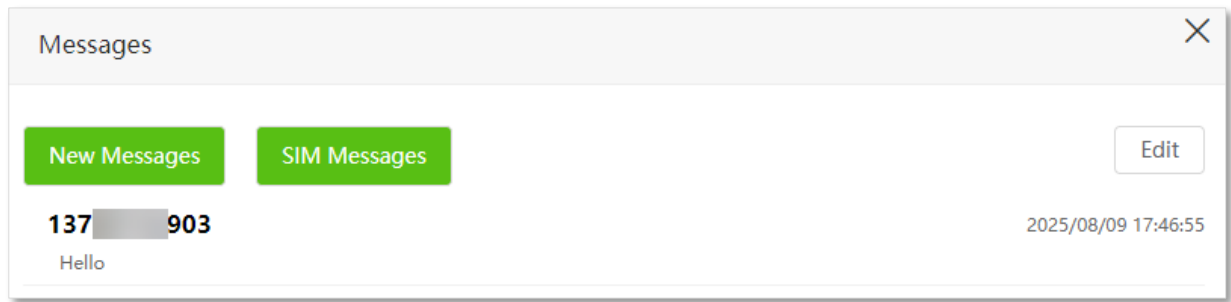
1. [Log in to the web UI of the router](#), and navigate to **SMS > Messages**.
2. Click **New Messages**.
3. Enter the smartphone number in the **Send To** column.
4. Enter the message content in the **Messages** column at the bottom.
5. Click **Send** at the bottom right corner.

The screenshot shows a web browser window titled 'Messages' with a close button (X) in the top right corner. Inside the window, there is a header bar with a back arrow and the text 'New Messages'. Below this is a large text input area with the placeholder text 'Send To'. At the bottom of the window, there is a footer bar with the text 'Messages' on the left and a 'Send' button on the right.

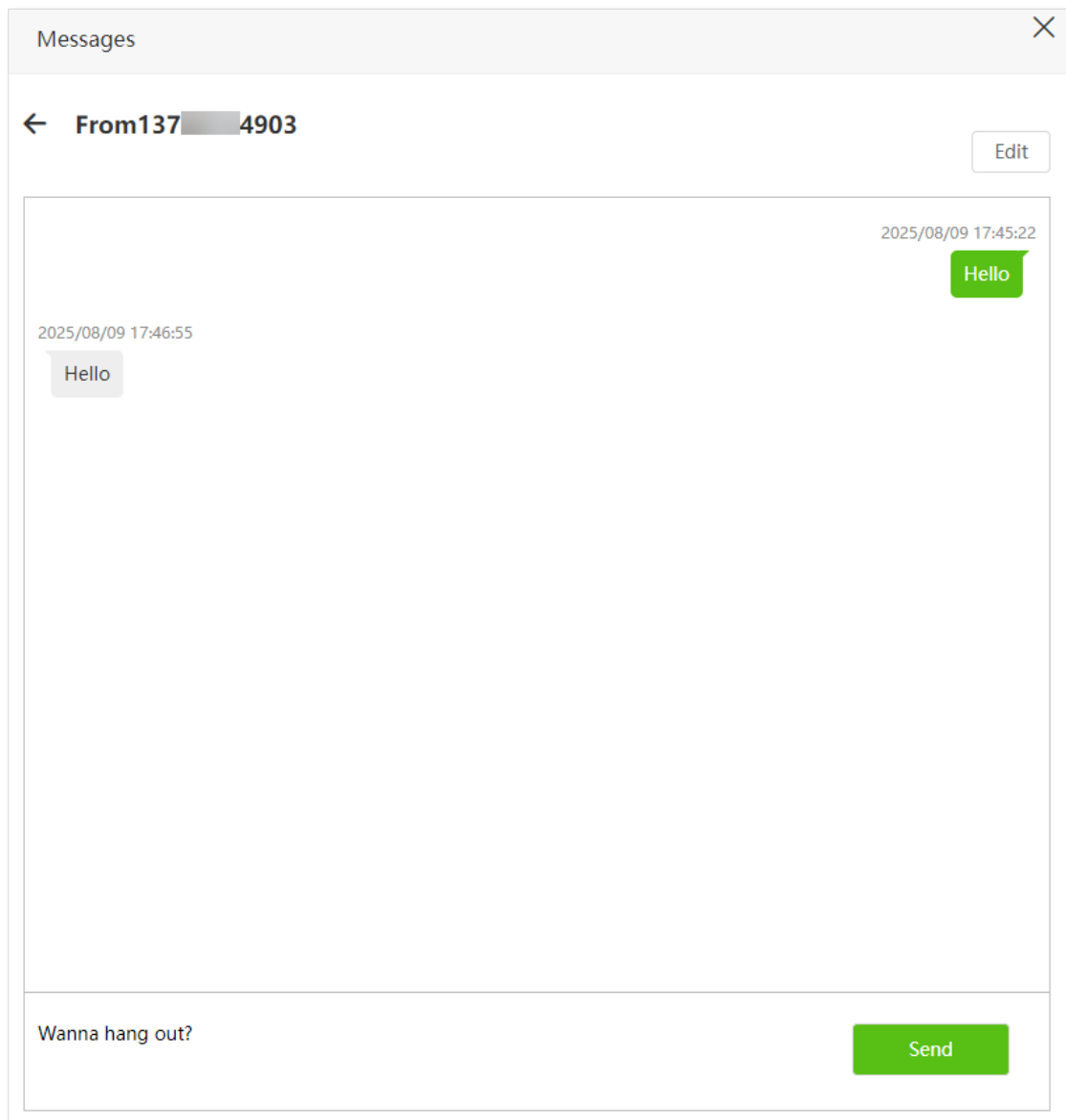
---End

Send SMS messages to an existing smartphone number

1. [Log in to the web UI of the router](#), and navigate to **SMS > Messages**.
2. Click the targeted smartphone number.



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



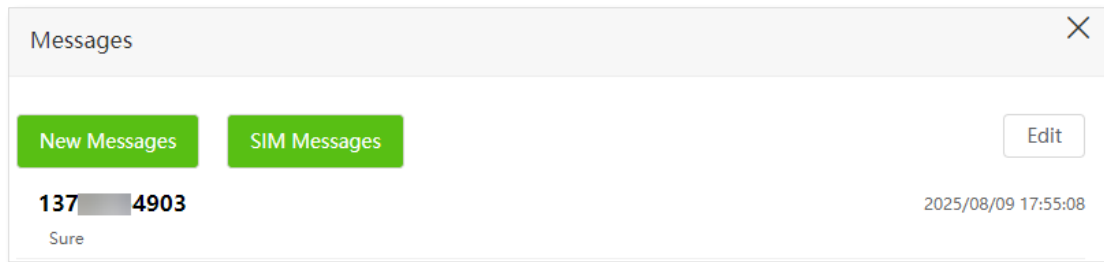
---End

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

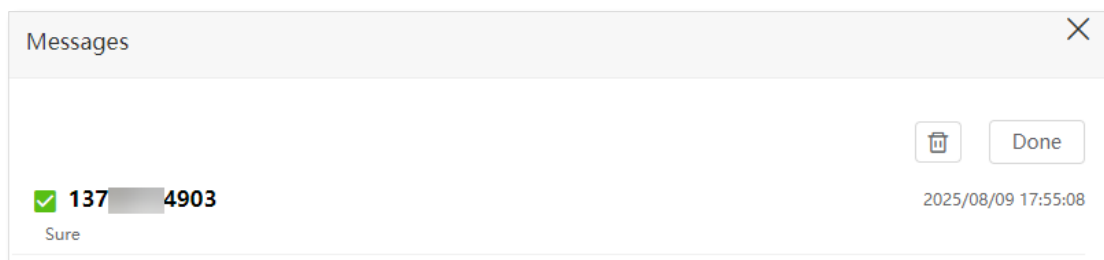
7.5.2 Delete SMS messages

Delete all SMS messages of the same smartphone numbers

1. [Log in to the web UI of the router](#), and navigate to **SMS > Messages**.
2. Click **Edit** in the upper right corner.



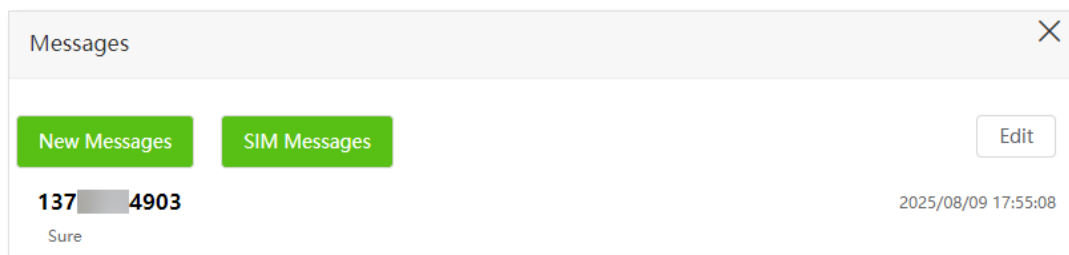
3. Select the smartphone number to be deleted messages.
4. Click  to delete messages. (You can click **Done** to exit the editing mode).



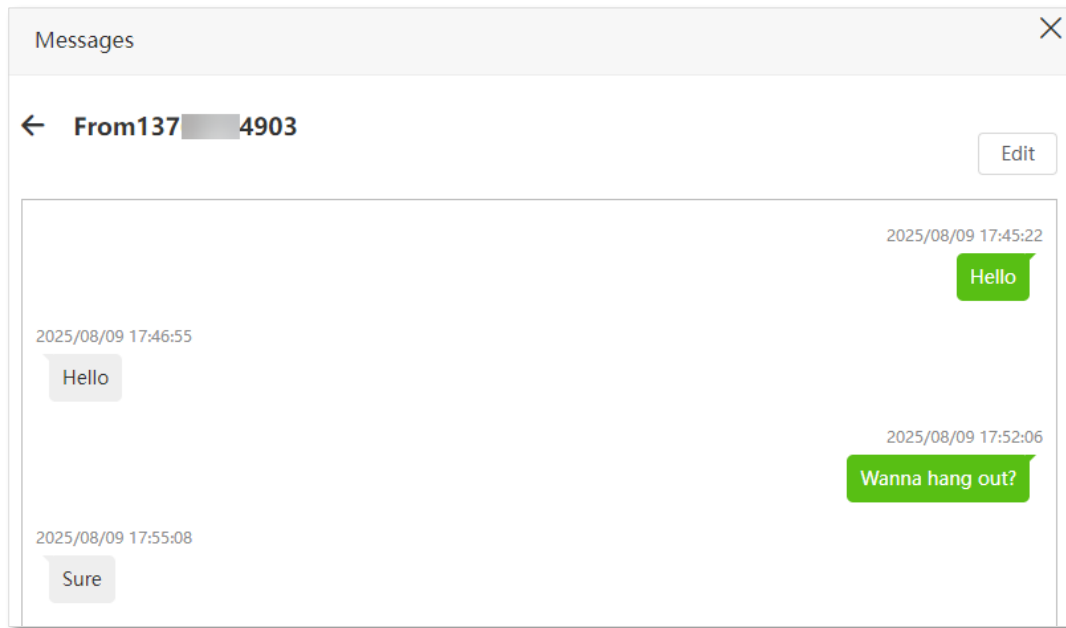
---End

Delete certain SMS messages of the same smartphone number

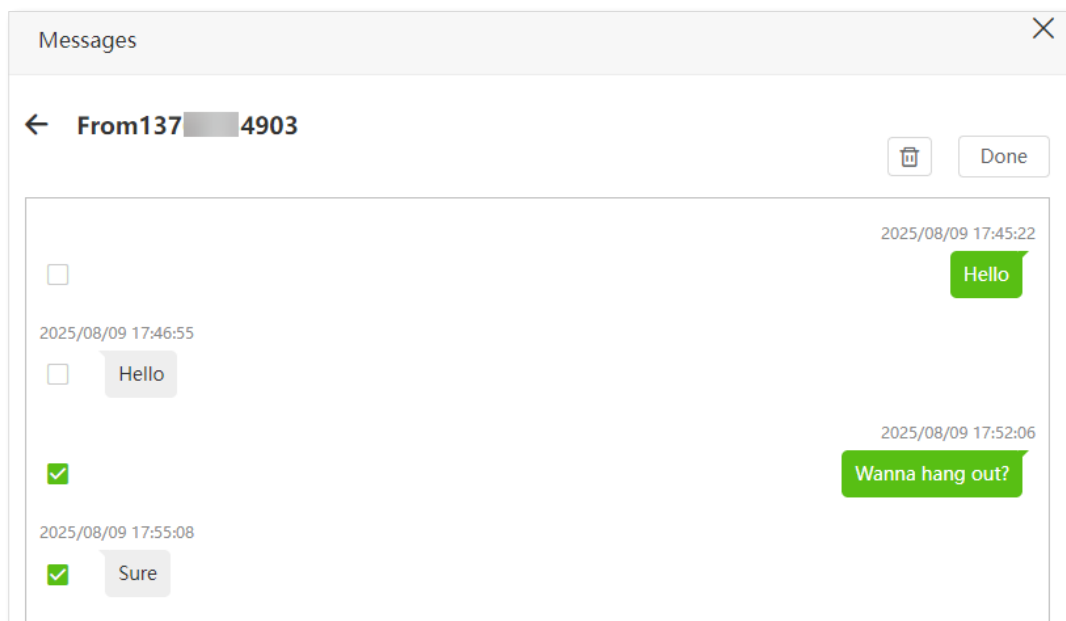
1. [Log in to the web UI of the router](#), and navigate to **SMS > Messages**.
2. Click the targeted smartphone number.



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



4. Select the messages to be deleted.
5. Click  to delete messages. (You can click **Done** to exit the editing mode).



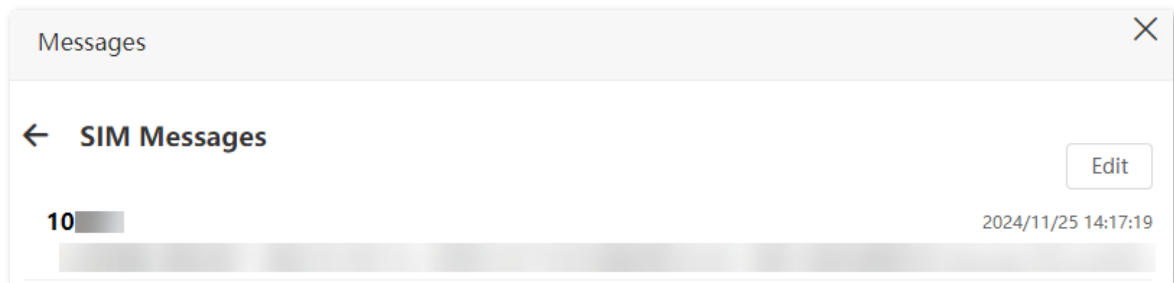
---End

Delete certain messages of the SIM card

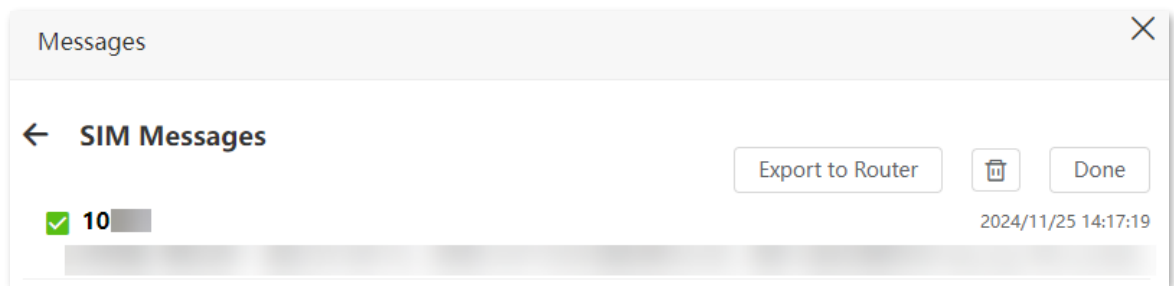


This function is available only when messages are stored in the SIM card.

1. [Log in to the web UI of the router](#), and navigate to **SMS > Messages**.
2. Click **SIM Messages**.
3. Click **Edit** in the upper right corner.



4. Select the smartphone number to be deleted messages.
5. Click  to delete messages. (You can click **Done** to exit the editing mode).



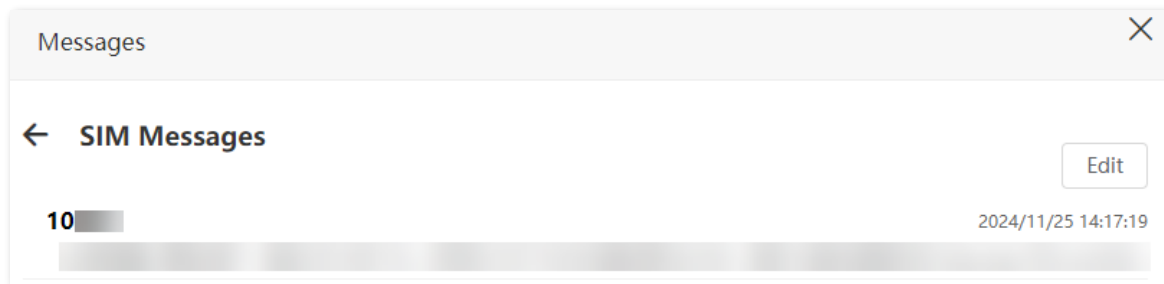
---End

7.5.3 Export SMS messages

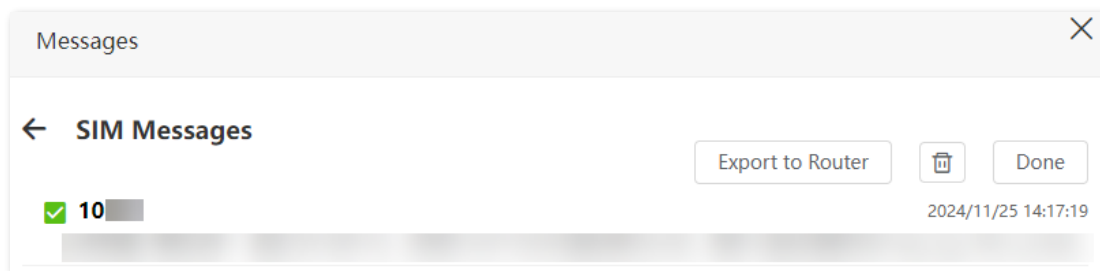
For Wi-Fi-enabled devices (such as smartphones), SMS messages can be stored on the SIM card. When the SIM card is inserted into the router, you can export messages in the SIM card to the router to check them on the web UI of the router.

Procedure for exporting SMS messages

1. [Log in to the web UI of the router](#), and navigate to **SMS > Messages**.
2. Click **SIM Messages**.
3. Click **Edit** in the upper right corner.



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



---End

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

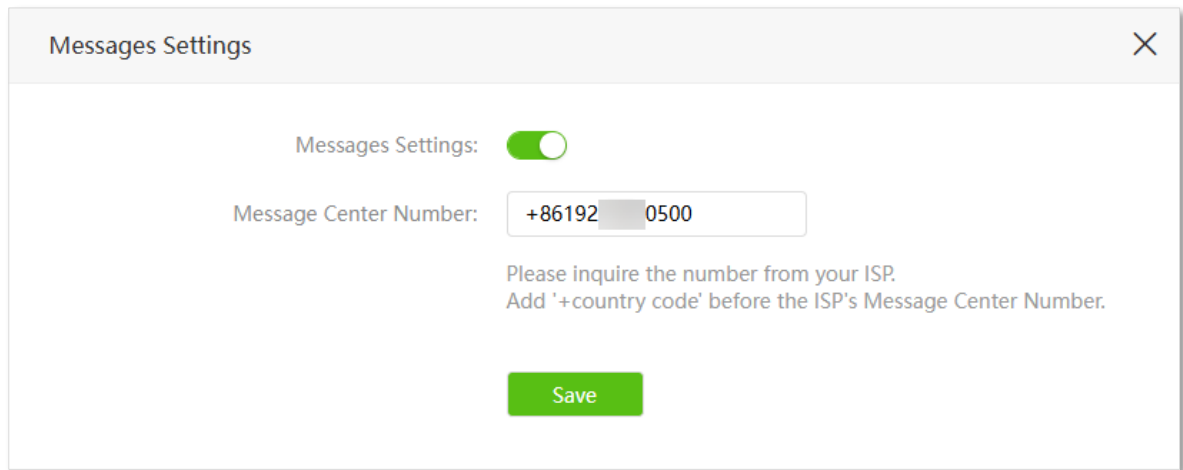
7.6 Set the message center number

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

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

Procedure for setting the message center number

1. [Log in to the web UI of the router](#), and navigate to **SMS > Messages Settings**.
2. Enable **Messages Settings**.
3. Enter the correct **Message Center Number** provided by your ISP.
4. Click **Save**. The following figure is for reference only.

A screenshot of a 'Messages Settings' dialog box. At the top, the title 'Messages Settings' is on the left and a close button 'X' is on the right. Below the title bar, there is a 'Messages Settings:' label followed by a green toggle switch that is turned on. Underneath, the 'Message Center Number:' is followed by a text input field containing '+86192' and '0500'. Below the input field, there is a note: 'Please inquire the number from your ISP. Add '+country code' before the ISP's Message Center Number.' At the bottom center, there is a green 'Save' button.

---End

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

7.7 Inquire information by sending USSD commands

You can inquire specific information or perform specific operations by sending a special code or command to your ISP.



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

Procedure for inquiring information by sending USSD commands

1. [Log in to the web UI of the router](#), and navigate to **SMS > USSD**.
2. Enter a **USSD CMD**, which is ***108#** in this example.
3. Click **Send**.

USSD

USSD CMD: *108#

Send

USSD Read:

---End

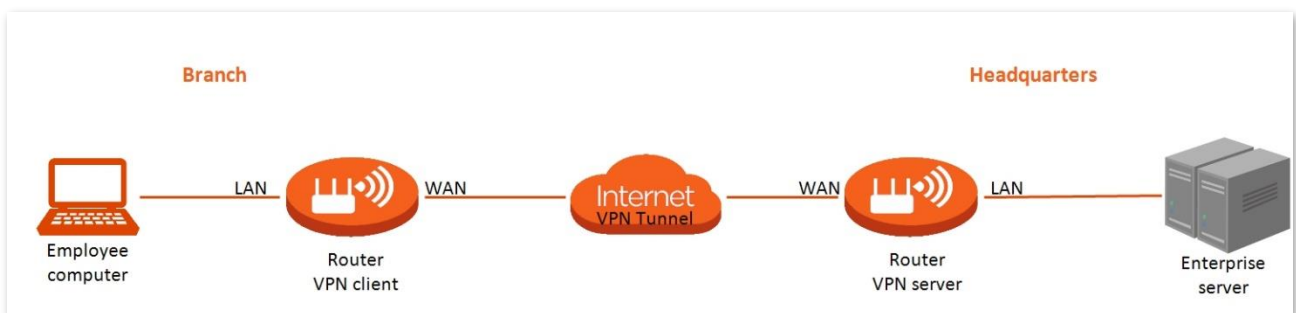
Wait a moment, you will get the desired information you want in the **USSD Read** box.

8 Use VPN to access network

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

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

The typology of a VPN network is shown below.



8.1 Configure OpenVPN server

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

Example of configuring OpenVPN server

Scenario: When traveling on business, enterprise employees need to remotely access the internal network resources of the enterprise, such as internal websites, file shares or databases.

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

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

Assume that:

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

Procedure for configuring OpenVPN server

I. Configure the router

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

OpenVPN Server

OpenVPN Server: ☒

Service Type: ☒ UDP ☐ TCP

Service Port:

VPN Subnet/Netmask:

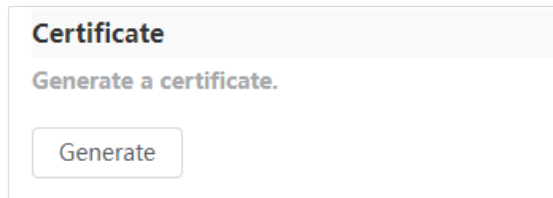
Client Access:

Save

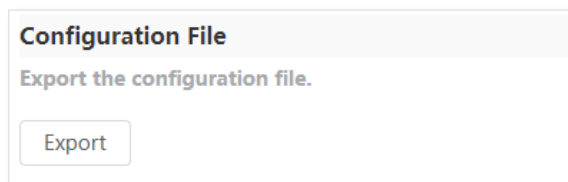
3. Click **Generate** in the **Certificate** module to generate a certificate.



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



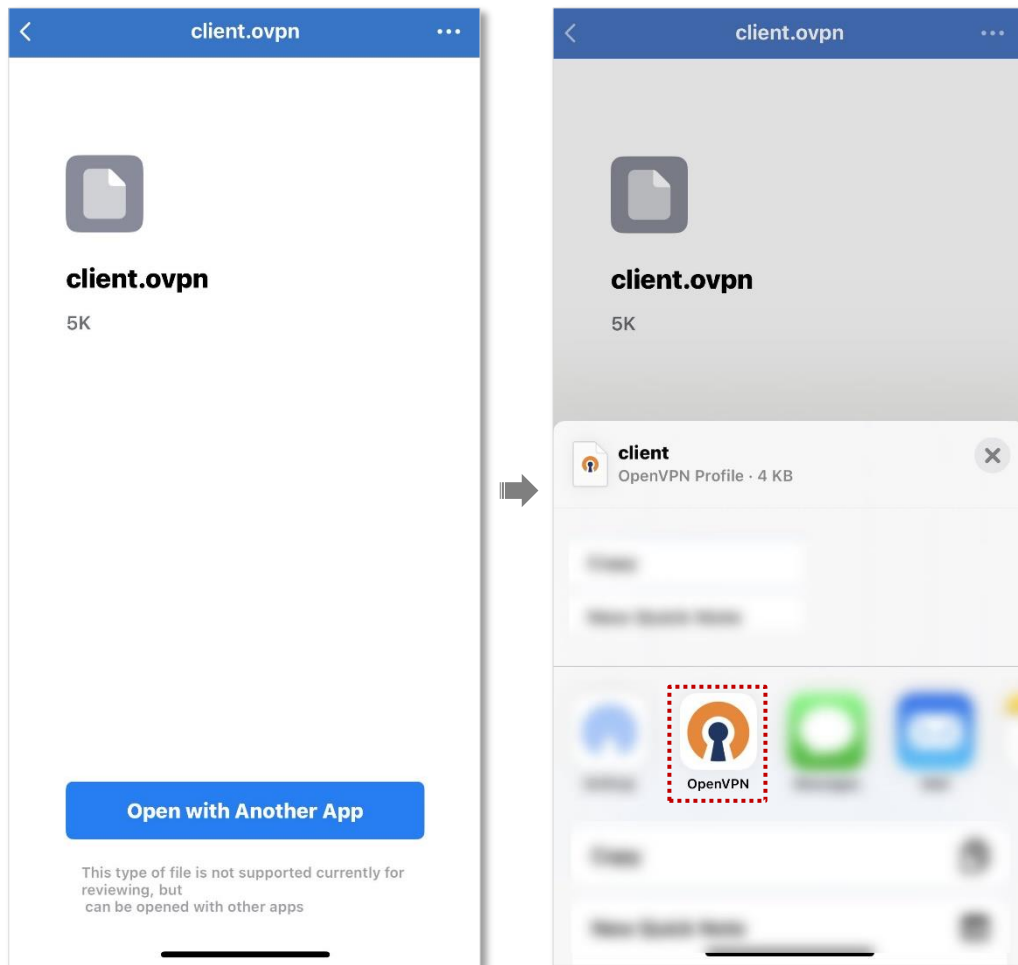
4. Click **Export** in the **Configuration File** module to download the configuration file to your local host. And send the configuration file suffixed with **.ovpn** to employees on business trips.



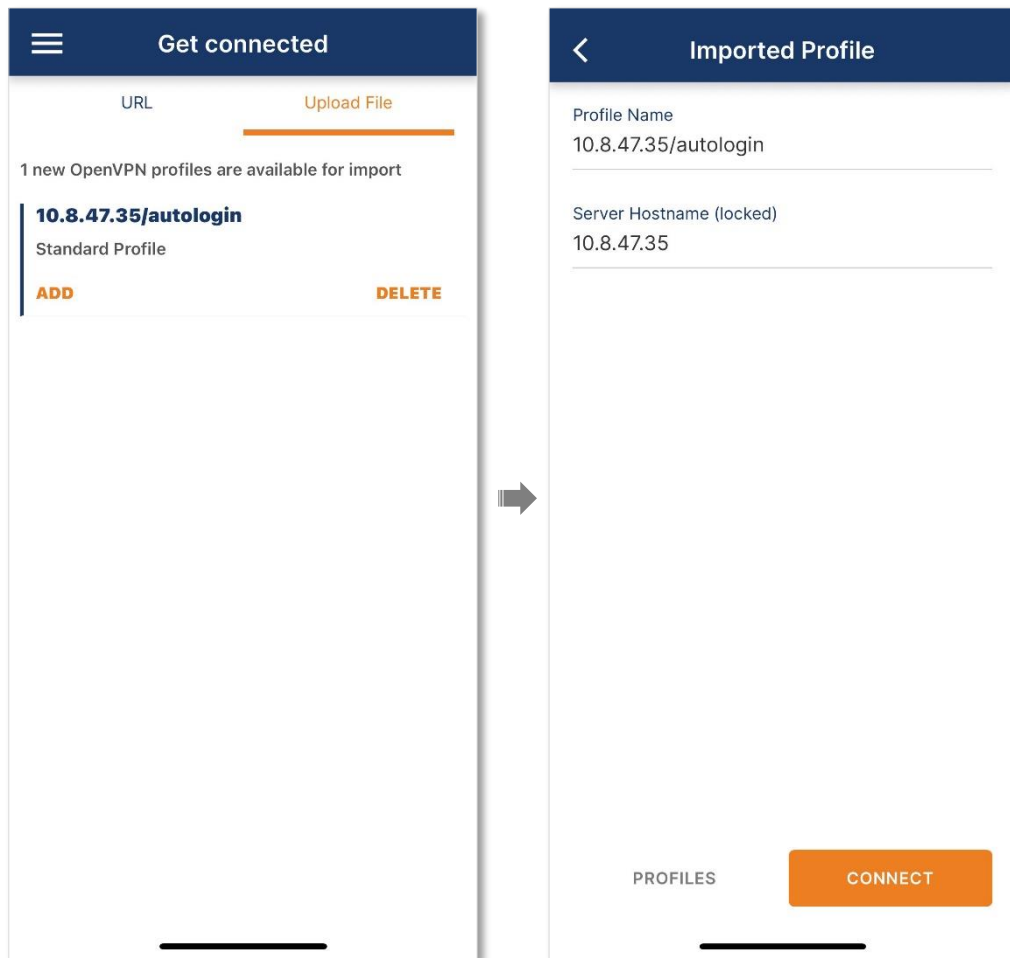
II. Connect the OpenVPN server (Example: iPhone)

1. Employees on business trips download the OpenVPN client to the smartphone.
 - 1) Start the browser, and visit the OpenVPN official website (<https://openvpn.net/>) in the address bar.
 - 2) Navigate to **Home > Resources > Download OpenVPN** to download the OpenVPN client.
2. Receive and tap the configuration file suffixed with **.ovpn**, then tap **Open with Another App**.

The following figure is for reference only.
3. Tap **OpenVPN**.

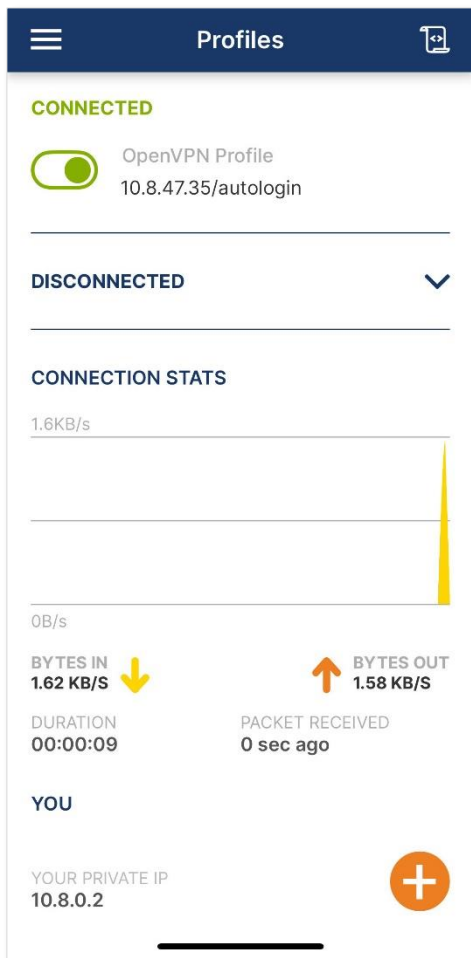


4. Tap **ADD** to import the OpenVPN profile.
5. Tap **CONNECT**.



---End

Wait until the connection is successful. Employees on business trips can access headquarters resources through the VPN.



To verify, you can check the VPN connections in the **OpenVPN connection** module on the web UI of the router.

Parameter description

Parameter	Description
OpenVPN Server	Used to enable or disable the OpenVPN server.
Service Type	Specifies the service type, including UDP and TCP .
Service Port	Specifies the service port to be customized. The value range is 1025 – 65535.
VPN Subnet/Netmask	Specifies the VPN subnet IP address and subnet mask. The netmask cannot be changed.

Parameter	Description
Client Access	Specifies the type of the client access, including Internet and Home Network and Home Network Only. – Internet and Home Network: The client can access the home network, internet sites or services with a geographic limitation when you are abroad. The client's default route will be changed. – Home Network Only: The client can only access the home network, and the client's default route will not be changed.

8.2 Configure L2TP client

This router can function as a L2TP client and connect to L2TP servers. This function is disabled by default.

Example of accessing VPN resources with the router

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

Requirements: Access the VPN resources of your ISP.

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

Assume that:

- The IP address of the L2TP server is **113.88.112.220**.
- The user name and password assigned by the L2TP server are both **admin1**.

Procedure for accessing VPN resources with the router

1. [Log in to the web UI of the router](#), and navigate to **VPN > L2TP Client**.
2. Enable **L2TP Client**.
3. Set **Server IP Address/Domain Name**, which is **113.88.112.220** in this example.
4. Set **User Name** and **Password**, which are both **admin1** in this example.
5. Click **Save**.

L2TP Client

L2TP Client: ☒

Server IP Address/Domain Name:

113.88.112.220

User Name:

admin1

Password:

Status:

Disconnected

Save

---End

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

L2TP Client

L2TP Client: ☒

Server IP Address/Domain Name:

113.88.112.220

User Name:

admin1

Password:

Status:

Connected

Obtained L2TP Client IP Address:

192.168.101.253

Save

Parameter description

Parameter	Description
L2TP Client	Used to enable or disable the L2TP client function.

107

Document version: V1.0

Parameter	Description
Server IP Address/Domain Name	Specifies the IP address or domain name of the L2TP server that the router connects to. Generally, when a router serves as the L2TP server at the peer side, the domain name or IP address should be that of the WAN port whose L2TP server function is enabled.
User Name	Specify the user name and password that the L2TP server assigns to the L2TP clients.
Password	
Status	Specifies the connection status of the VPN connection.
Obtained L2TP Client IP Address	Specifies the IP address assigned by the L2TP server to the router.

8.3 Configure IPsec

IPsec, abbreviated for Internet Protocol Security, is a protocol suite for transmitting data over the internet in a secure and encrypted manner.

Procedure for adding a new IPsec VPN

1. [Log in to the web UI of the router](#), and navigate to **VPN > IPsec**.
2. Click **+New** to configure the IPsec function.



3. Configure IPsec parameters as required.
When **Key Exchange Method** is set to **Auto (IKE)**, you can click **Show Advanced Settings** to display the advanced parameters of auto negotiation.
4. Click **Save**.

← Add IPSec VPN

×

IPSec Status: ☒

Mobile Data Options:

Tunnel mode

Connection Name:

Negotiation Mode:

Initiator

Protocol:

ESP

Remote Gateway: URL

Local LAN IP/Prefix Length:

Remote LAN IP/Prefix Length:

Key Exchange Method:

Auto (IKE)

Authentication Method: Pre-shared Key

Pre-shared Key:

DPD: ☐

Show Advanced Settings ▾

Save



Phase 1

Exchange Mode:

Main

Encryption Algorithm:

DES

Integrity Algorithm:

SHA1

Diffie-Hellman Group:

768 bit

Local ID Type:

IP Address

Remote ID Type:

IP Address

Key Lifetime:

3600

s (Range: 600 to 604800)

Phase 2

Perfect Forward Secrecy:

☐

Encryption Algorithm:

DES

Integrity Algorithm:

SHA1

Diffie-Hellman Group:

768 bit

Key Lifetime:

3600

s (Range: 600 to 604800)

Save

---End

Parameter description

Parameter	Description
IPSec Status	Used to enable or disable the IPSec function.
Mobile Data Options	Specifies the IPSec mobile data options. Tunnel mode is generally used between two security gateways.
Connection Name	Specifies the name of the IPSec connection.

Parameter	Description
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. – 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: 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. – 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.
Authentication Method	Specifies the shared key mode, which indicates a shared key string negotiated by IPsec parties with some way in advance.

Parameter	Description
Pre-shared Key	Specifies the pre-shared key used during negotiation. This parameter must be the same with that of the peer gateway.
DPD	Specifies whether to enable the DPD Detection. This function can detect whether the remote tunnel site is valid.
DPD Interval	Specifies the interval at which the router sends DPD frames. The default value is 10. If the router does not receive the confirmation of DPD frames within the valid period, it will initialize the IPSec SA from the local to the remote device.
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 the 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.  TIP When Key Exchange Method is set to Manual, the ESP Integrity Algorithm can be set to None.
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.

Parameter	Description
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.
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.
ESP Integrity Key	Used to set the ESP integrity key. Both IPSec communication parties should have the same key.
ESP Outgoing SPI	SPI (Security Parameter Index) is used to identify an IPSec SA with the IP address and security protocol of the remote gateway. – ESP Outgoing SPI: Keep this value same as the ESP incoming SPI value of the remote gateway.
ESP Incoming SPI	– ESP Incoming SPI: Keep this value same as the ESP outgoing SPI value of the remote gateway.

8.4 Configure Wireguard client

The Wireguard client establishes secure VPN connections to enable encrypted communication between cross-platform devices. Its features are as follows:

- Secure access and privacy protection: Support establishing encrypted tunnels with networks in other regions over public or insecure networks (such as public Wi-Fi).
- Cross-platform compatibility: Compatible with systems such as Windows, iOS, Android, and macOS.
- High performance and secure encryption: It is based on UDP transmission and runs in kernel space for fast transfer speeds, while utilizing modern encryption technologies (such as pre-shared keys) to defend against quantum computing attacks and being easy to debug and maintain.

Procedure for configuring Wireguard

I. Configure the Wireguard server

II. Configure the router

1. [Log in to the web UI of the router](#), and navigate to **VPN > Wireguard client**.
2. Enable the **WireGuard** function.
3. Enter the **Description** (the rule name), which is **Test** in this example.
4. (Optional) Click **Select a file**. Select and upload the config file downloaded from the Wireguard server. Then you will see the detailed parameters, and you can directly perform step 9. Otherwise, continue to configure the next step.
5. Click **RENEW KEY** to update the **Public Key** as required, and the **Private Key** of the **Interface** will also be updated.
6. Set the IP address of the local site (IP of the Wireguard communication interface), which is **12.0.0.2/24** in this example.
7. (Optional) Set **DNS Server** and **MTU Size** as required.
8. Enter the **Public Key**, **Pre-Shared Key** (optional), **Allowed IPs**, **Endpoint Address** (the IP address of the public network), **Endpoint Port**, **Persistent Keepalive** (the public network NAT connection interval) of the peer site. The parameter configurations in the figure below are for example only.
9. Click **Save**.

Wireguard client

WireGuard: ☒

Status: Disconnected

Description:

Public Key: 9VYb7muu7qEYArI8m8iOBKMXvs79ctnCPp6iNjVoVCc= 

Import from Config File:

Interface:

Private Key:

Address:

DNS Server 1: Optional

DNS Server 2: Optional

MTU Size: Optional

Peer:

Public Key:

Pre-Shared Key: Optional

Allowed IPs1: +

Endpoint Address:

Endpoint Port:

Persistent Keepalive: Optional

---End

When **Connected** is shown behind **Status**, you can access web servers or FTP servers within the LAN.

Wireguard client

WireGuard: ☒

Status: **Connected**

9 Configure more settings

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

9.1 Manage LAN settings

You can:

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

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

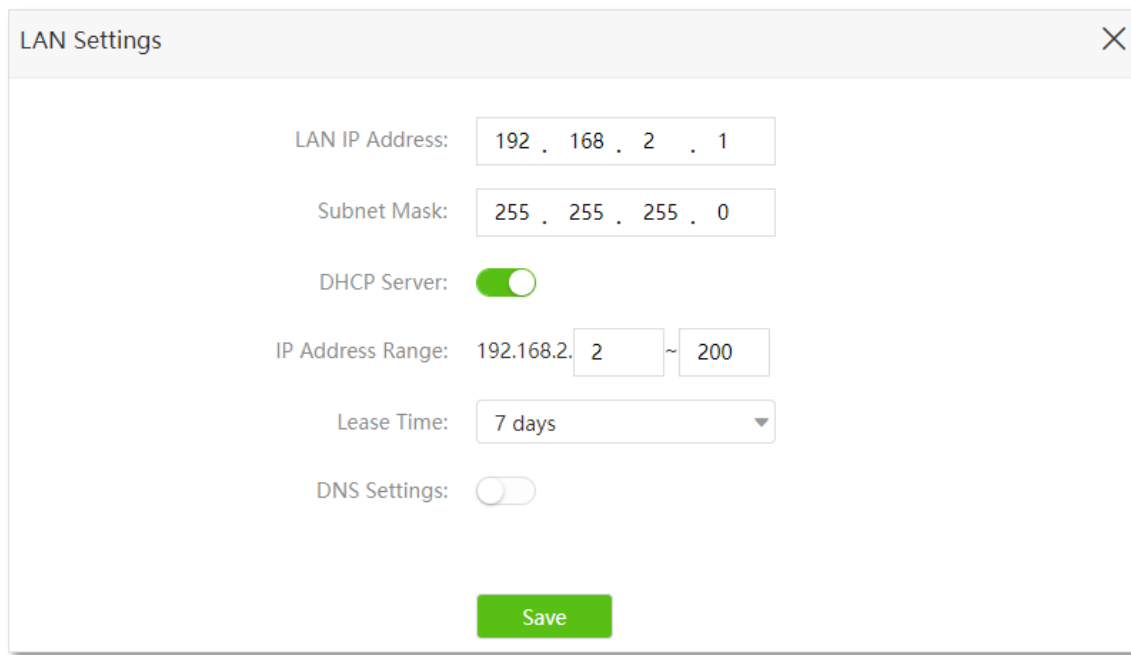
- **Configure the DNS information assigned to clients.**

9.1.1 Change LAN IP address

Assume that you want to change the router login address to 192.168.2.1 and retain the default subnet mask.

Procedure for changing LAN IP address

1. [Log in to the web UI of the router](#), and navigate to **System Settings > LAN Settings**.
2. Change the **LAN IP Address**, which is **192.168.2.1** in this example.
3. Click **Save**.



4. Confirm the prompt information, and click **OK**.

---End

After the LAN IP address is successfully changed, the login page is automatically displayed. If not, ensure that the IP address of the Ethernet (or local connection) of the computer is set to **Obtain an IP address automatically** and **Obtain DNS server address automatically**, and then try again to access the new LAN IP address.



If the new LAN IP address is not on the same network segment as the IP address of the original LAN port, the system automatically changes the DHCP address pool to make it on the same network segment as the new LAN IP address.

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.

9.1.2 Use the router as a DHCP server

DHCP is short for Dynamic Host Configuration Protocol. The DHCP server can automatically assign IP addresses, subnet masks, gateways, and DNS information to clients on the LAN.

If this function is disabled, you need to manually configure an IP address on the client to access the internet. Unless other specified, keep the DHCP server enabled.

Procedure for using the router as a DHCP server

1. [Log in to the web UI of the router](#), and navigate to **System Settings > LAN Settings**.
2. Enable **DHCP Server**.
3. Specify the range of IP addresses that the router assigns in **IP Address Range** field.
4. (Optional) Select a value from **Lease Time** menu. It is recommended to keep the default value.
5. Enable or disable **DNS Settings** as required.
 - When it is disabled, the LAN IP address of the router is used as the DNS address of the client.
 - When it is enabled, **Primary DNS Server** must be set and **Secondary DNS Server** is optional.
6. Click **Save**.

LAN Settings

LAN IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255 . 255 . 255 . 0

DHCP Server: ☒

IP Address Range: 192.168.0. 2 ~ 200

Lease Time: 7 days

DNS Settings: ☒

Primary DNS Server: . . .

Secondary DNS Server: . . .

Save

---End

Parameter description

Parameter	Description
DHCP Server	Used to enable or disable the DHCP server. Once enabled, the DHCP server automatically assigns internet parameters such as IP address, subnet mask and gateway address to the client. This function is recommended to be enabled.
IP Address Range	Specifies the range of IP addresses that can be assigned to devices connected to the router. The default range is 192.168.0.100 to 192.168.0.200.  TIP It is available only when DHCP Server is enabled.
Lease Time	Specifies the valid duration of the IP address that is assigned to a client. When the lease time reaches half, the client will send a DHCP Request to the DHCP server for renewal. If the renewal succeeds, the lease is renewed based on the time of the renewal application. If the renewal fails, the renewal process is repeated again at 7/8 of the lease period. If it succeeds, the lease is renewed based on the time of the renewal application. If it still fails, the client needs to reapply for IP address information after the lease expires.  TIP It is available only when DHCP Server is enabled.
DNS Settings	Specifies whether to allocate another DNS address to the client.  TIP – It is available only when DHCP Server is enabled. – This router has the DNS proxy function.
Primary DNS Server	Specifies the primary DNS address of the router, which is assigned to the clients. You can change it if necessary. Make sure that the primary DNS server is the IP address of the correct DNS server or DNS proxy. Otherwise, you may fail to access the internet.  TIP It is available only when DNS Settings is enabled.
Secondary DNS Server	Specifies the secondary DNS address of the router used to assign to the clients. It is an optional field and is left blank by default.  TIP It is available only when DNS Settings is enabled.

9.2 Configure DHCP reservation

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

Assign static IP addresses to LAN clients

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

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

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

Assume that the information of the FTP server includes:

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

Procedure for assigning static IP addresses to LAN clients

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



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

---End

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

DHCP Reservation

Device Name	MAC Address	IP Address	Status	Operation
Optional			---	+ Add
DESKTOP-2K2MLGI		192.168.0.148		
FTP server	D4:61:DA:1B:CD:89	192.168.0.136		

9.3 Configure static route

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.

Example of adding a static route rule

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

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.

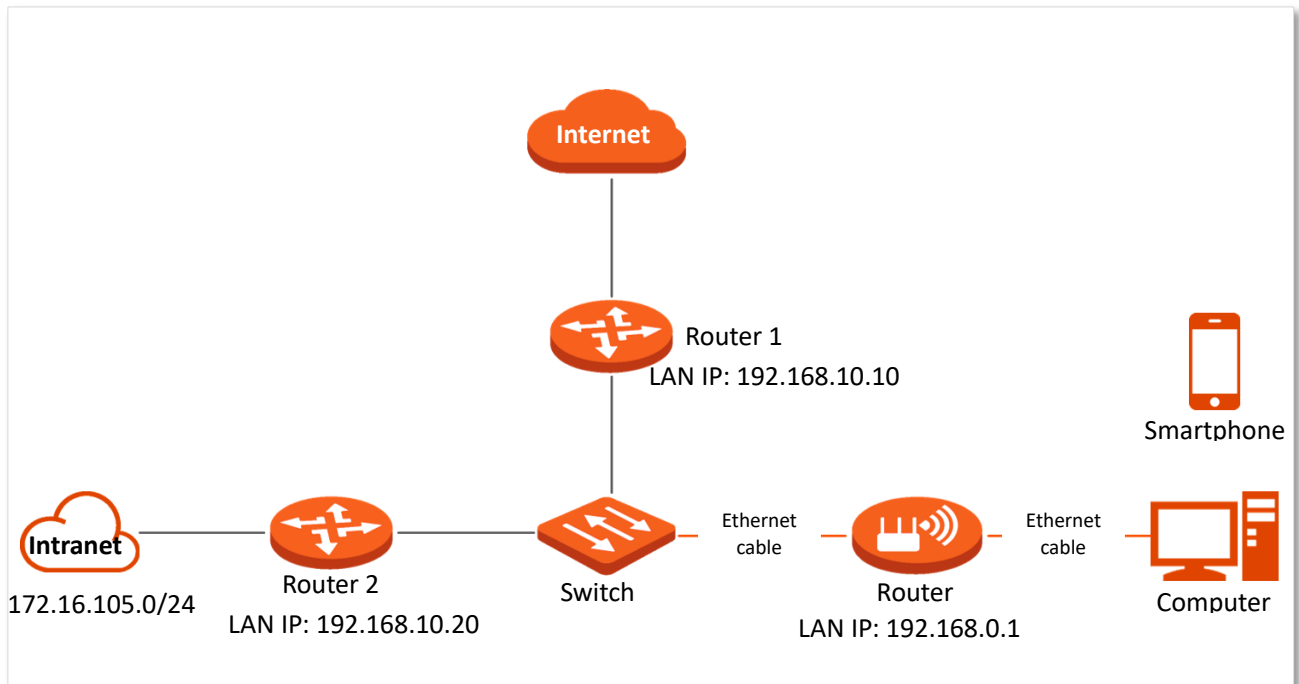
Assume the LAN IP addresses of these devices are:

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

The information about the intranet:

- IP address: 172.16.105.0

- Subnet mask: 255.255.255.0



Procedure for adding a static route rule

1. [Log in to the web UI of the router.](#)
2. Configure the router to access the internet in **Internet Settings**. For details, refer to [using dynamic IP address](#).
3. Add a static route rule.
 - 1) Navigate to **Advanced Settings > Static Route**.
 - 2) Enter the IP address of the destination network, which is **172.16.105.0** in this example.
 - 3) Enter the subnet mask of the destination network, which is **255.255.255.0** in this example.
 - 4) Enter the ingress IP address of the next hop route, which is **192.168.10.20** in this example.
 - 5) Click **+Add**.

Static Route ✕

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

---End

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

Parameter description

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

9.4 Configure virtual server

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.

Example of enabling internet users to access LAN resources with the virtual server function

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.

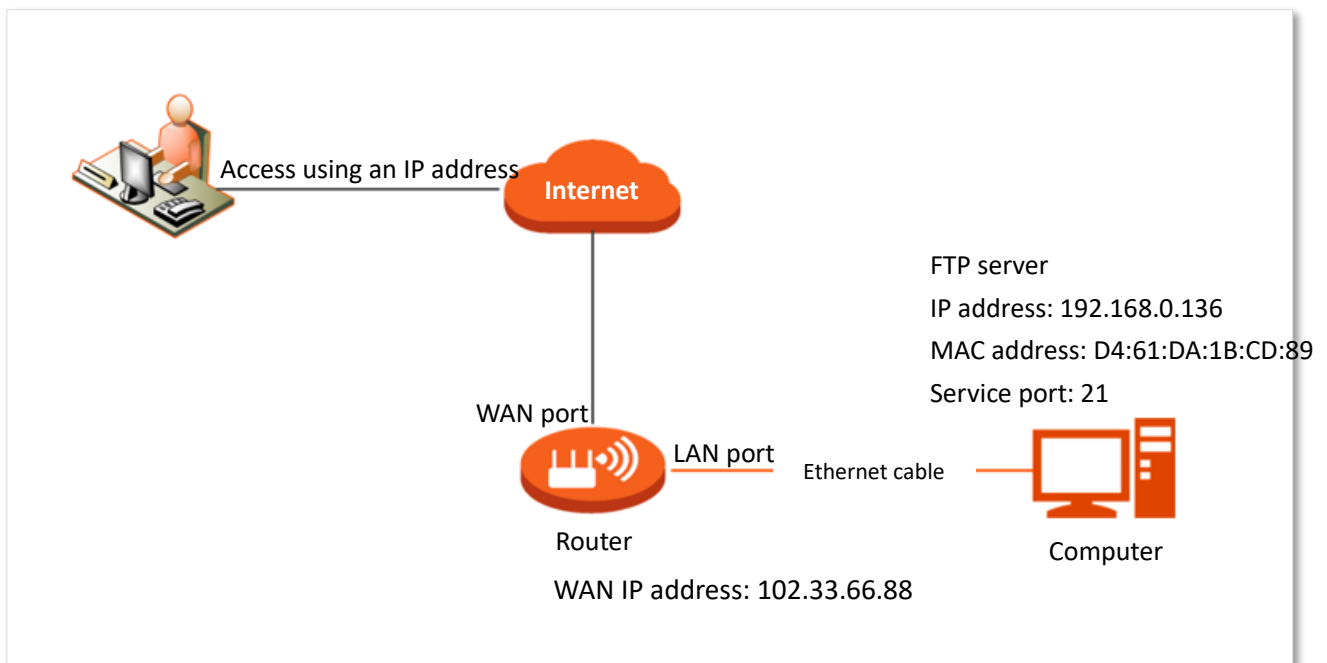
Solution: You can configure the virtual server function to reach the requirements.

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.



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



Procedure for enabling internet users to access LAN resources

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

Virtual Server

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

3. Assign a fixed IP address to the host where the server locates.
 - 1) Navigate to **Security > DHCP Reservation**.
 - 2) Specify a **Device Name** for the host of the server, which is **FTP server** in this example.
 - 3) Enter the **MAC Address** of the host of the server, which is **D4:61:DA:1B:CD:89** in this example.
 - 4) Set the **IP Address** reserved for the host, which is **192.168.0.136** in this example.
 - 5) Click **+ Add**.

DHCP Reservation

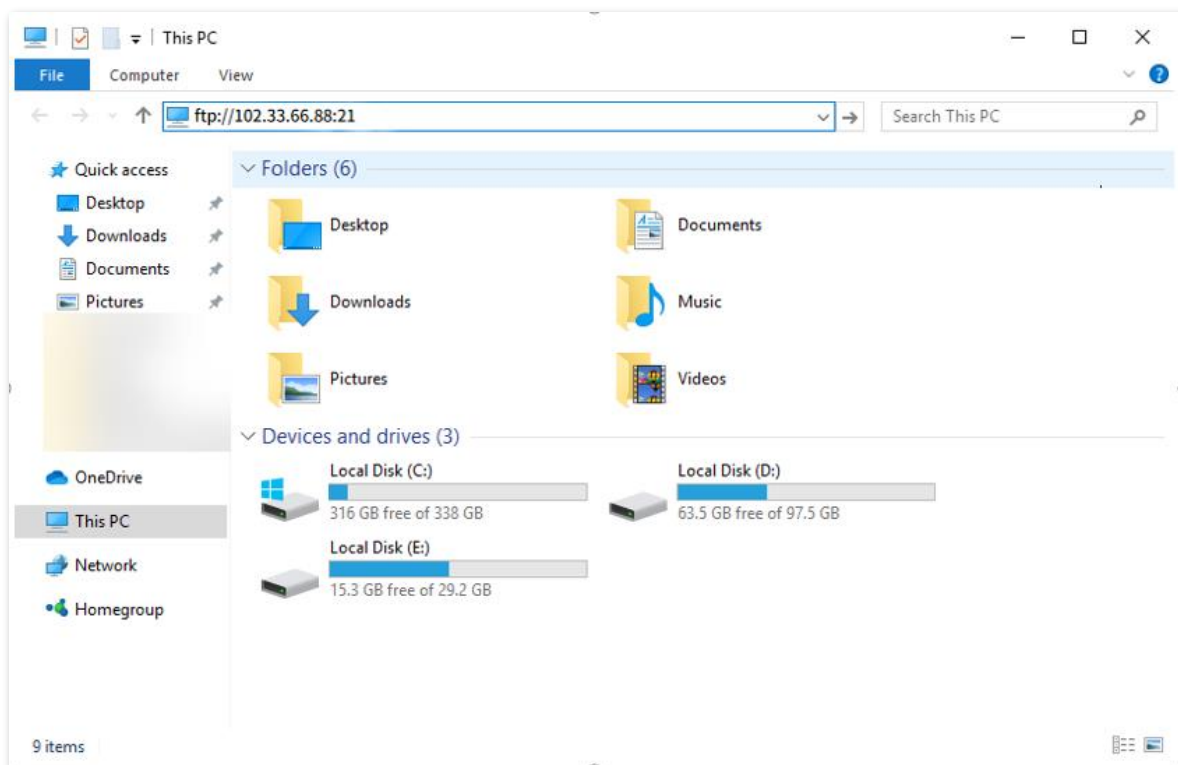
Device Name	MAC Address	IP Address	Status	Operation
FTP server	D4:61:DA:1B:CD:89	192.168.0.136	<input button"="" type="text" value="+ Add"/>	

---End

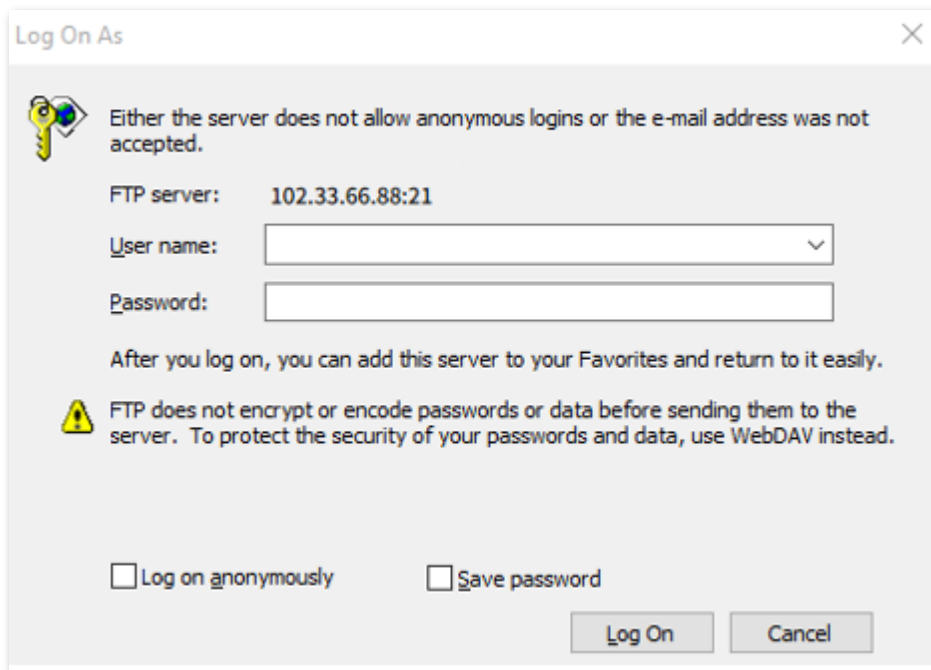
Parameter description

Parameter	Description
Internal IP Address	Specifies the IP address of the server within the LAN of the router.
LAN Port	Specifies the service port number of the server under the LAN of the router.
WAN Port	Specifies the port of the router which is opened and accessible to internet users.
Protocol	Specifies the transport layer protocol of the service. If you are not sure about this parameter, TCP&UDP is recommended.

After the configuration is completed, Internet users can successfully access the FTP server by using the “*Intranet service application layer protocol name://WAN IP address of the router:WAN port number*”. In this example, the address is **ftp://102.33.66.88:21**. You can find the WAN IP address of the router [checking WAN status](#).



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](#).



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.

9.5 Configure DMZ host

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. This function is disabled by default.



- 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.

Example of enabling internet users to access LAN resources with the DMZ host function

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.

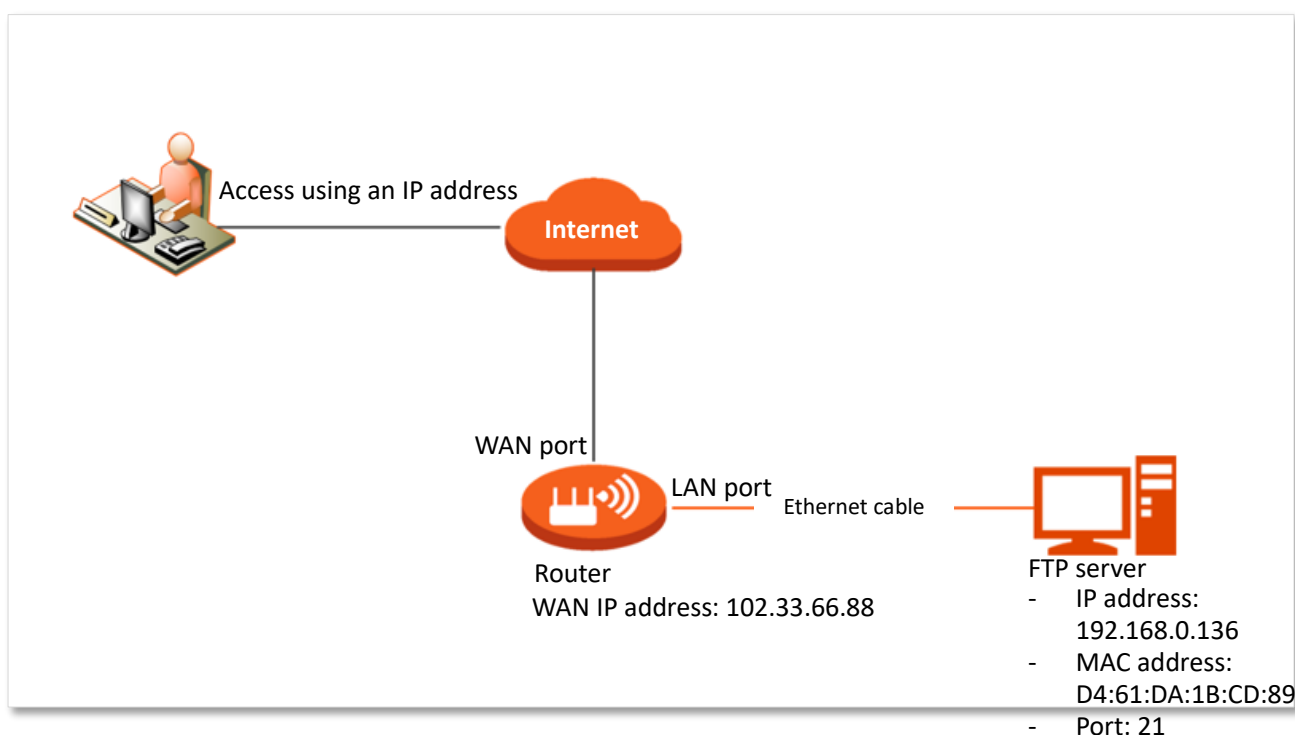
Solution: You can configure the DMZ host function to reach the requirements.

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
- WAN IP address of the router: 102.33.66.88.



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 to 172.31.255.255. Private IP addresses of class C range from 192.168.0.0 to 192.168.255.255.

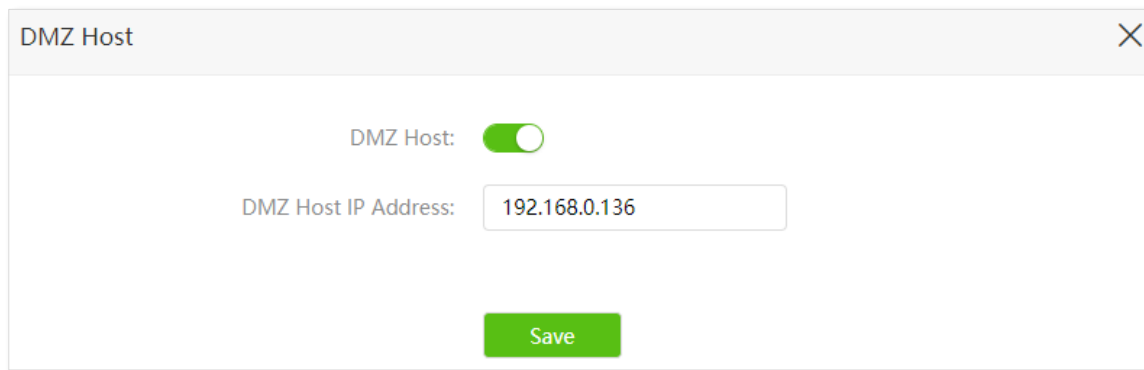


Procedure for enabling internet users to access LAN resources

1. [Log in to the web UI of the router.](#)

2. Set the server host as the DMZ host.

- 1) Navigate to **NAT Forwarding > DMZ Host**.
- 2) Enable the **DMZ Host** function.
- 3) Enter the IP address of the host, which is **192.168.0.136** in this example.
- 4) Click **Save**.



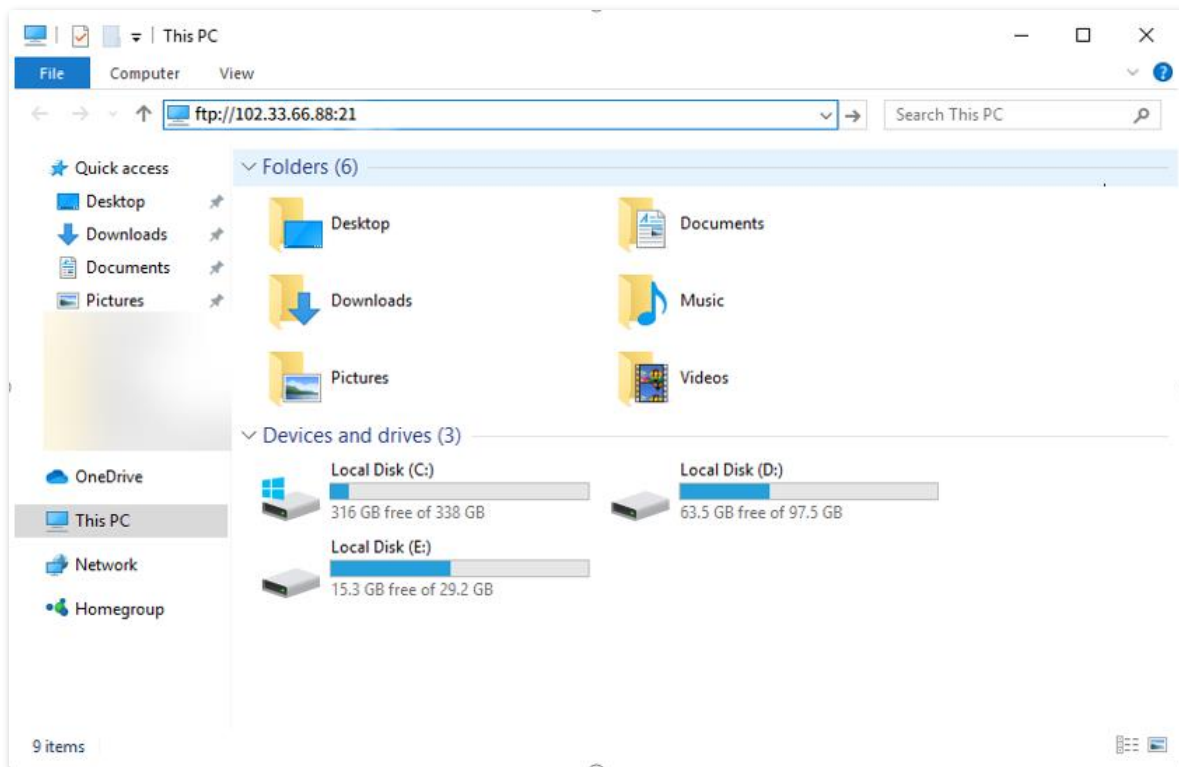
3. [Assign a fixed IP address to the host where the server locates.](#)

----End

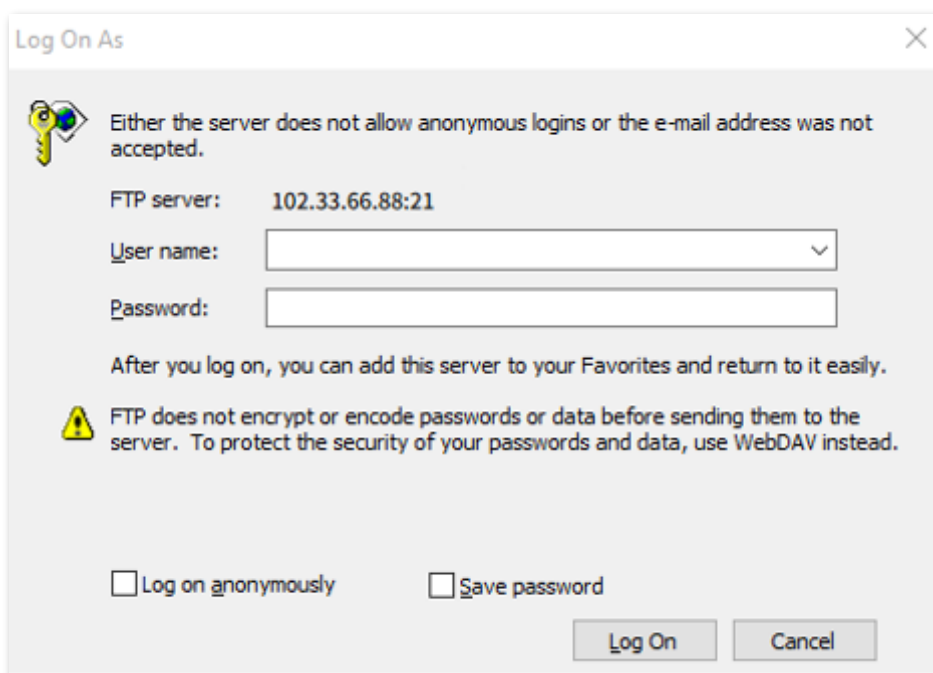
After the configuration is completed, Internet users can successfully access the DMZ host by using the “*Intranet service application layer protocol name://WAN IP address of the router:intranet service port number*”. In this example, the address is **ftp://102.33.66.88:21**. You can find the WAN IP address of the router in [checking WAN status](#).



If the default intranet service port number is 80, 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](#).



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

9.6 ALG

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

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

ALG

L2TP Pass-through: ☒

IPSec Pass-through: ☒

FTP ALG: ☒

TFTP ALG: ☒

H323 ALG: ☒

SIP ALG: ☒

RTSP ALG: ☒

Save

Parameter description

Name	Description
L2TP Pass-through	If you select L2TP protocol when you create a VPN connection on your computer in the LAN of the router, it takes effect only when this checkbox is selected.
IPSec Pass-through	If you select IPsec protocol when you create a VPN connection on your computer in the LAN of the router, it takes effect only when this checkbox is selected.
FTP ALG	The users on LAN can share resources on the FTP server on WAN only when it is selected.

Name	Description
TFTP ALG	It is a simple protocol used for files transfer. The TFTP ALG processes TFTP packets that initiate the request and creates pinholes to allow return packets from the reverse direction.
H323 ALG	The IP phone and network conference function can be used on the computers connected to the router only when it is selected.
SIP ALG	The IP phone function can be used on the computers connected to the router only when it is selected.
RTSP ALG	The users on LAN can check video on demand when it is selected.

9.7 Firewall

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

To access the page, [log in to the web UI of the router](#), and navigate to **Security > Firewall**.

Firewall

ICMP Flood Attack Defense: ☒

TCP Flood Attack Defense: ☒

UDP Flood Attack Defense: ☒

Ignore Ping Packet From WAN Port: ☒

Save

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.
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.

9.8 Improve network connections with UPnP

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

When any program that supports the UPnP function is launched, you can find the port conversion information on this page when the program sends any requests.

Procedure for enabling or disabling the UPnP function

1. [Log in to the web UI of the router](#), and navigate to **NAT Forwarding > UPnP**.
2. Enable or disable the **UPnP** function as required.
3. Click **Save**.

The image shows a web-based configuration window titled "UPnP". At the top, there is a toggle switch labeled "UPnP:" which is currently turned on (green). Below this is a table with five columns: "Remote Host", "Internet Port", "Local Host", "Internal Port", and "Protocol". The table is currently empty. At the bottom of the window, there is a green "Save" button.

-----End

Parameter description

Parameter	Description
UPnP	Used to enable or disable the UPnP function.
Remote Host	Specifies the address of remote host to receive and send responses.
Internet Port	Specifies the port set on the router to map to the outer.
Local Host	Specifies the address of inner host to receive and send responses.
Internal Port	Specifies the host port which needs to be mapped.
Protocol	Specifies the mapping protocol.

9.9 Configure DDNS

DDNS normally interworks with the port mapping, DMZ host and remote web management, so that 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. This function is disabled by default.

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

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

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

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

Assume that the information of the FTP server includes:

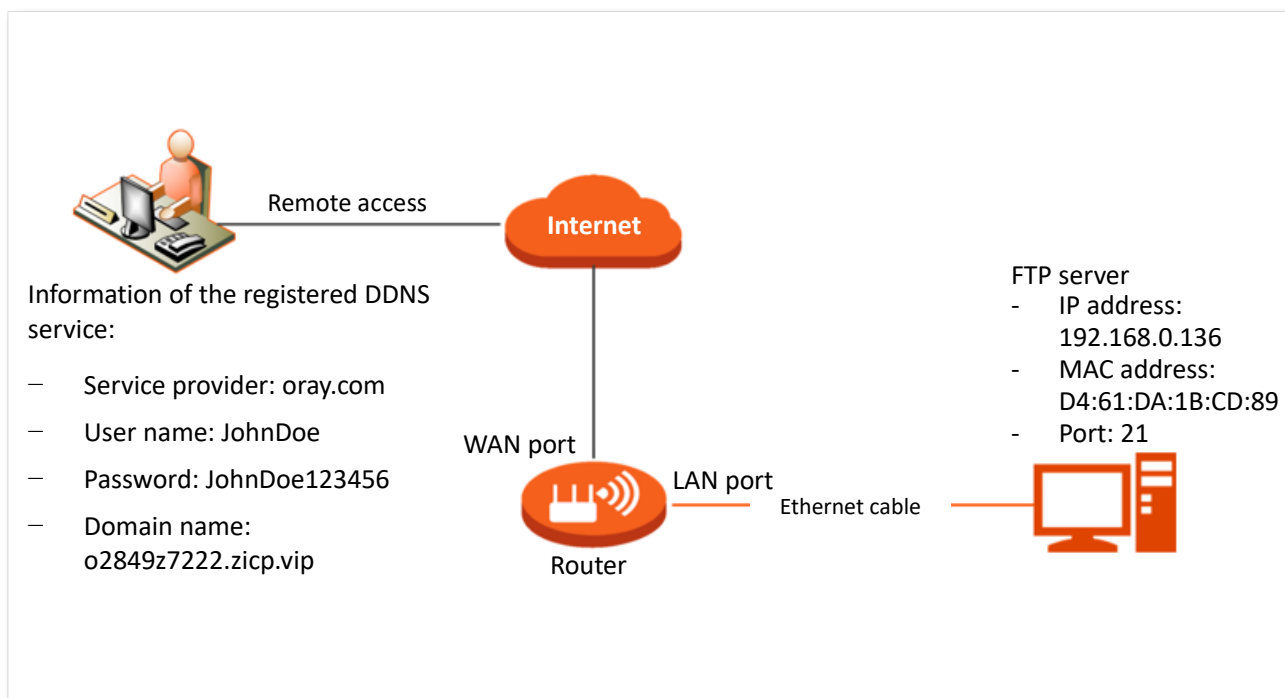
- IP address: 192.168.0.136
- MAC address of the host: D4:61:DA:1B:CD:89
- Service port: 21

The information of the registered DDNS service:

- Service provider: oray.com
- User name: JohnDoe
- Password: JohnDoe123456
- Domain name: o2849z7222.zicp.vip



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 to 172.31.255.255. Private IP addresses of class C range from 192.168.0.0 to 192.168.255.255.



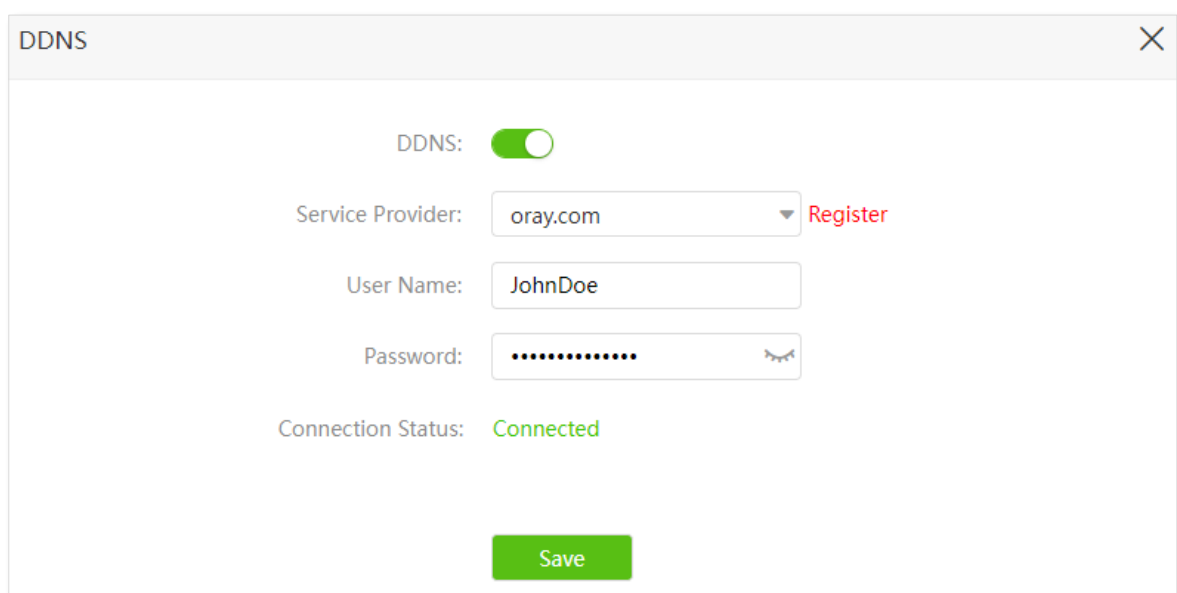
Procedure for enabling internet users to access LAN resources

1. [Log in to the web UI of the router.](#)

2. Configure the DDNS function.

- 1) Navigate to **NAT Forwarding > DDNS**.
- 2) Enable the **DDNS** function.
- 3) Choose a **Service Provider**, which is **oray.com** in this example.
- 4) Enter the **User Name** and **Password**, which are **JohnDoe** and **JohnDoe123456** in this example.
- 5) Click **Save**.

Wait until **Connected** is displayed behind **Connection Status**, which indicates that the configuration is successful.



DDNS

DDNS: ☒

Service Provider: oray.com [Register](#)

User Name: JohnDoe

Password:

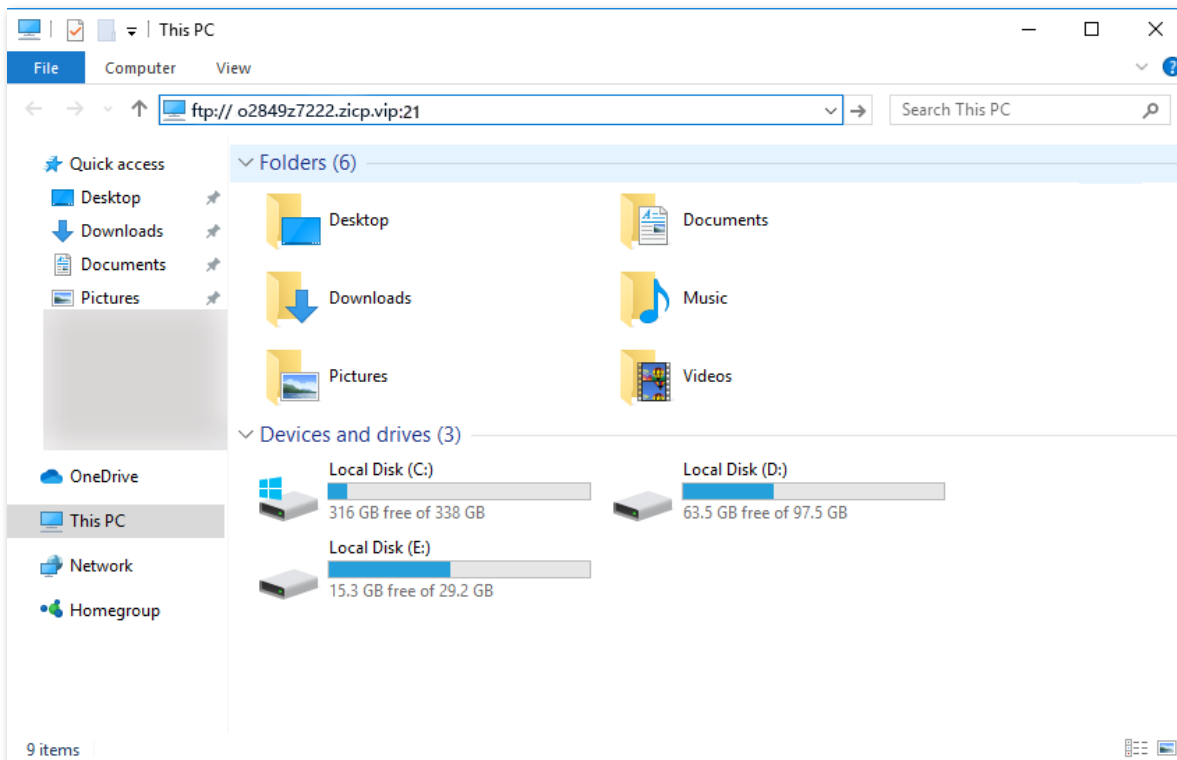
Connection Status: Connected

Save

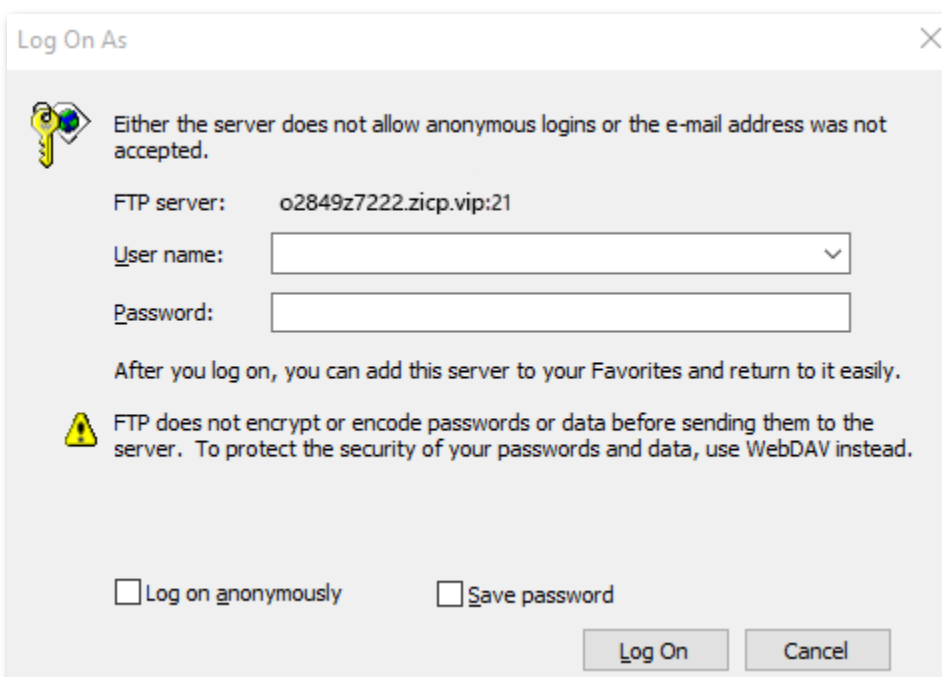
3. Configure the virtual server function (refer to [Virtual server](#)).

---End

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



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





After the configuration is completed, if internet users still cannot access the FTP server, try the following methods:

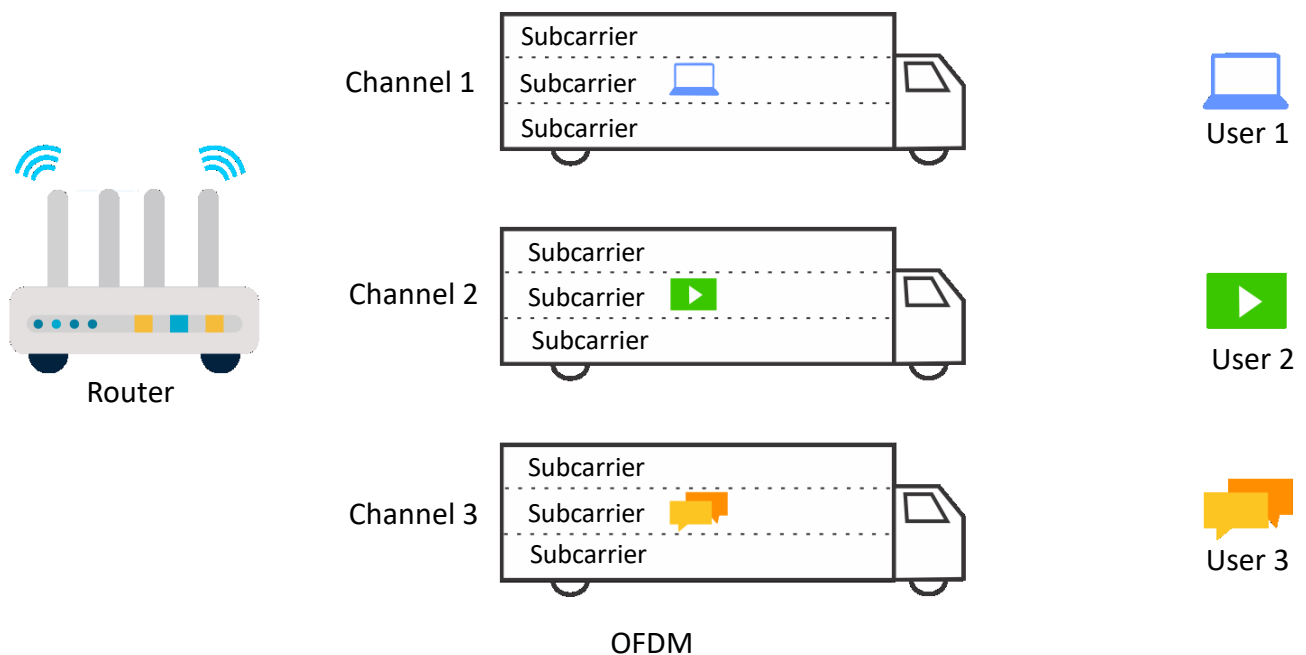
- Ensure that the LAN port number configured in the virtual server function is the same as the service port number set on the server.
- Close the firewall, antivirus software and security guards on the host of the FTP server and try again.

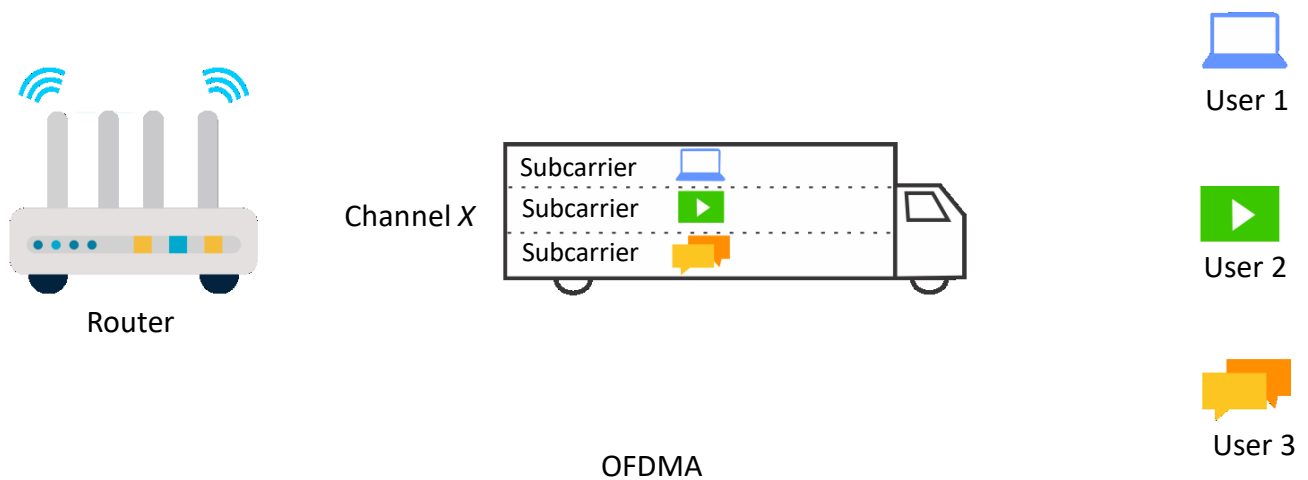
9.10 Enable or disable OFDMA

In telecommunications, Orthogonal Frequency-division Multiplexing (OFDM) is a type of digital transmission and a method of encoding digital data on multiple carrier frequencies. OFDM divides a channel into subcarriers, but only a single user can transmit on all sub-carriers at any given time.

Orthogonal Frequency-division Multiple Access (OFDMA) is a multi-user version of the popular OFDM digital modulation scheme. It also divides a channel into subcarriers which is further divided into subsets, called Resource Units (RUs). These RUs can be assigned to multiple users, therefore allowing simultaneous low-data-rate transmission from several users.

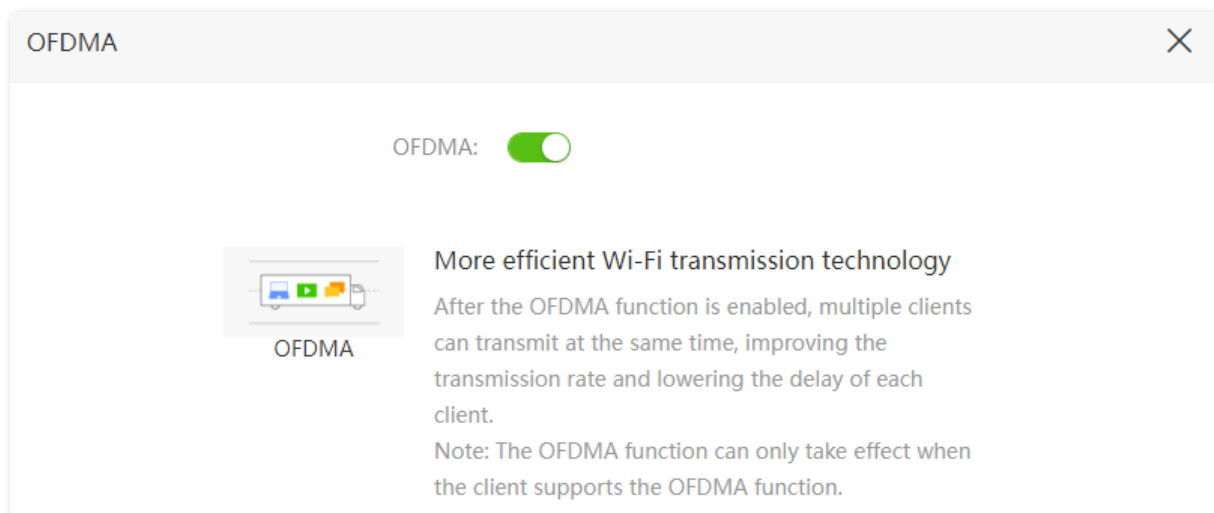
The mechanisms of OFDM and OFDMA are illustrated as below respectively.





Procedure for enabling or disabling OFDMA

1. [Log in to the web UI of the router](#), and navigate to **Wi-Fi Settings > OFDMA**.
2. Enable or disable the **OFDMA** function as required. The following figure is for reference only.



---End

Appendix

A.1 Set computer to auto obtain an IPv4 address

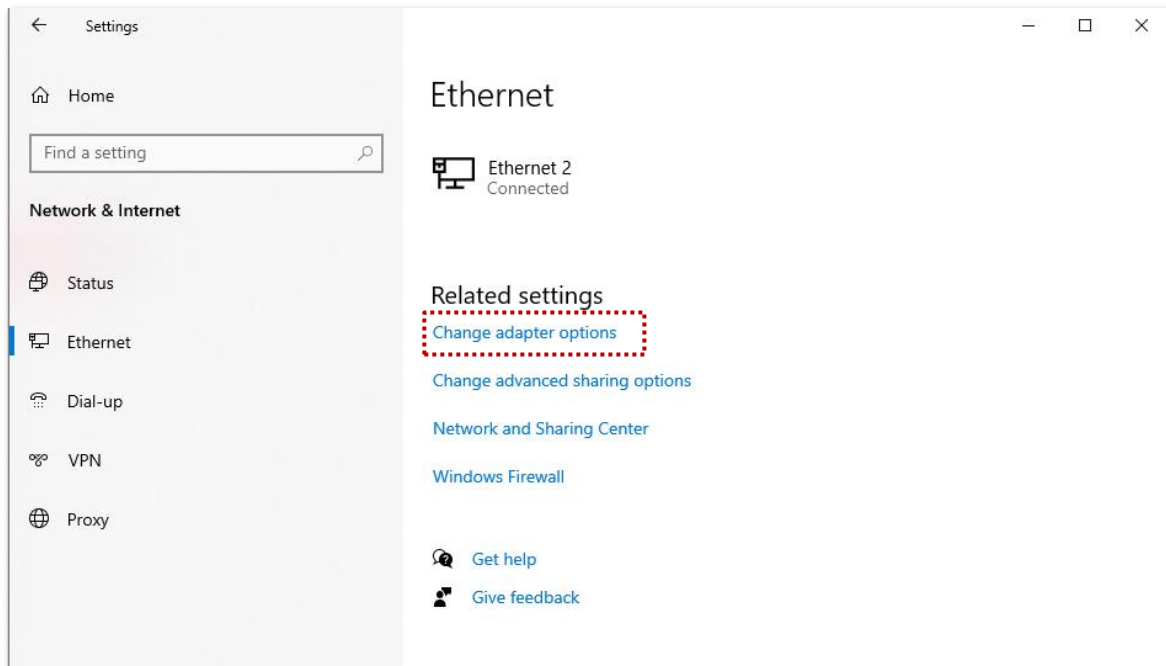
Perform the configuration procedures corresponding to [Windows 10](#), [Windows 8](#) and [Windows 7](#) and as required. A computer installed with a wired network adapter is used as an example to describe the procedures. The procedures for configuring computers installed with a Wi-Fi adapter are similar.

A.1.1 Windows 10

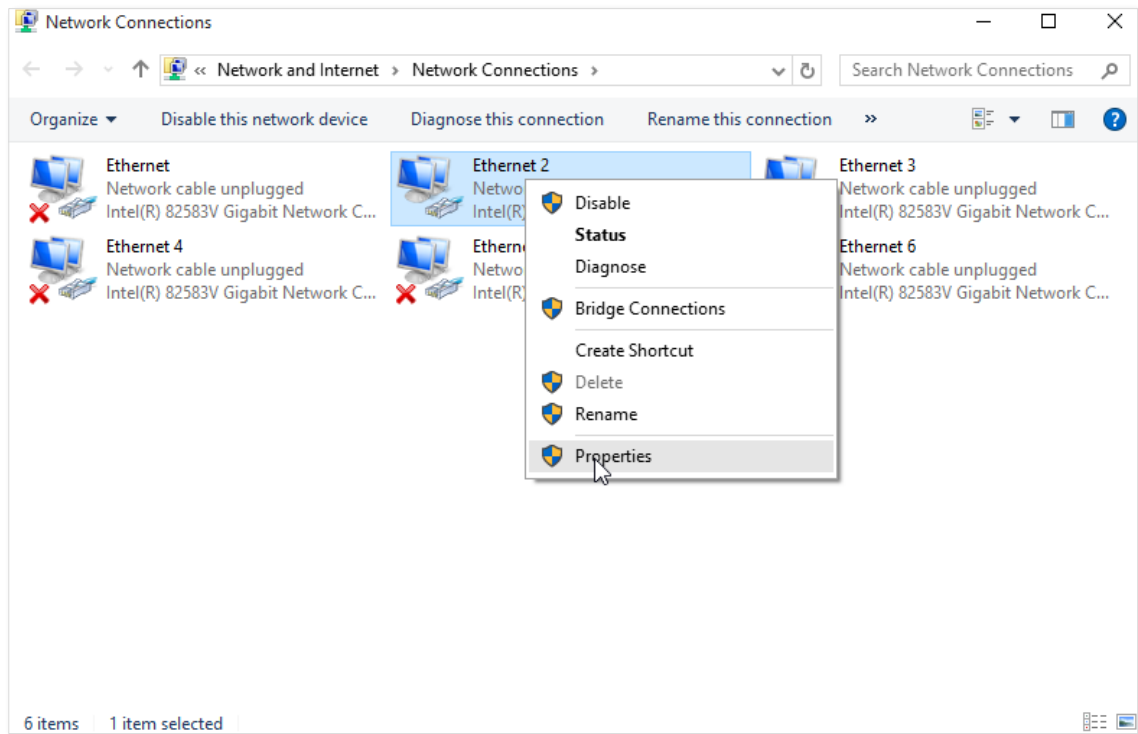
1. Click  in the bottom right corner of the desktop and choose **Network & Internet settings**.

Network & Internet settings

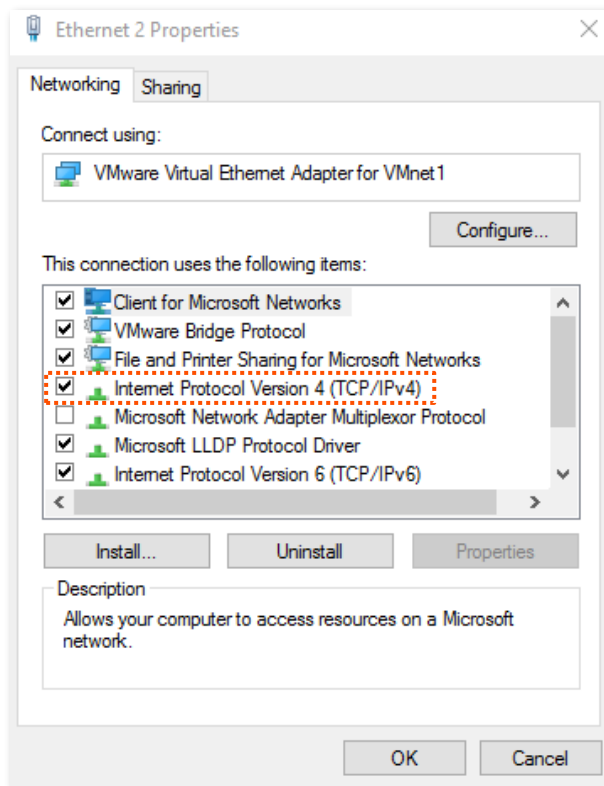
2. Click **Change adapter options**.



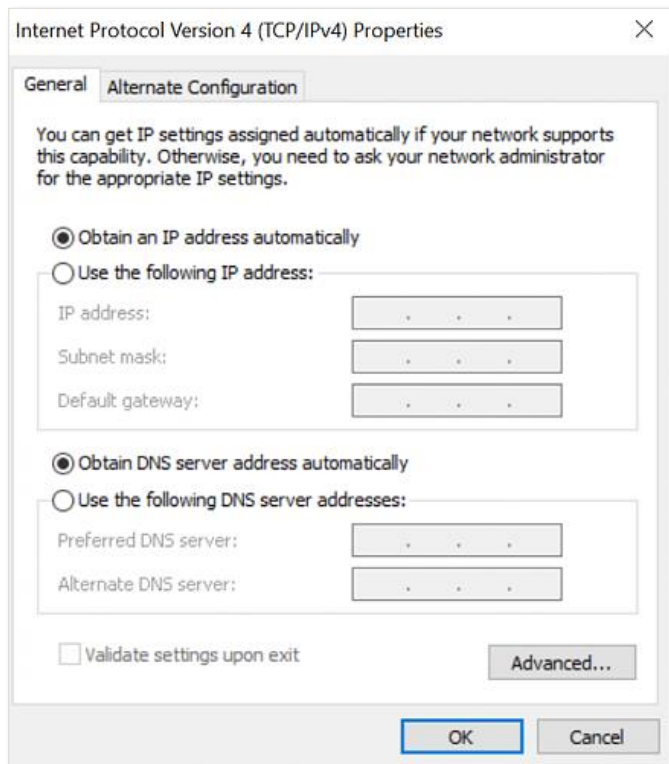
3. Right-click on the connection which is being connected, and then click **Properties**.



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



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

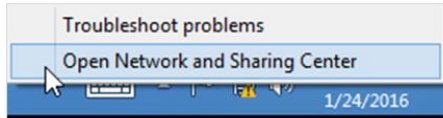


6. Click **OK** in the **Ethernet Properties** window.

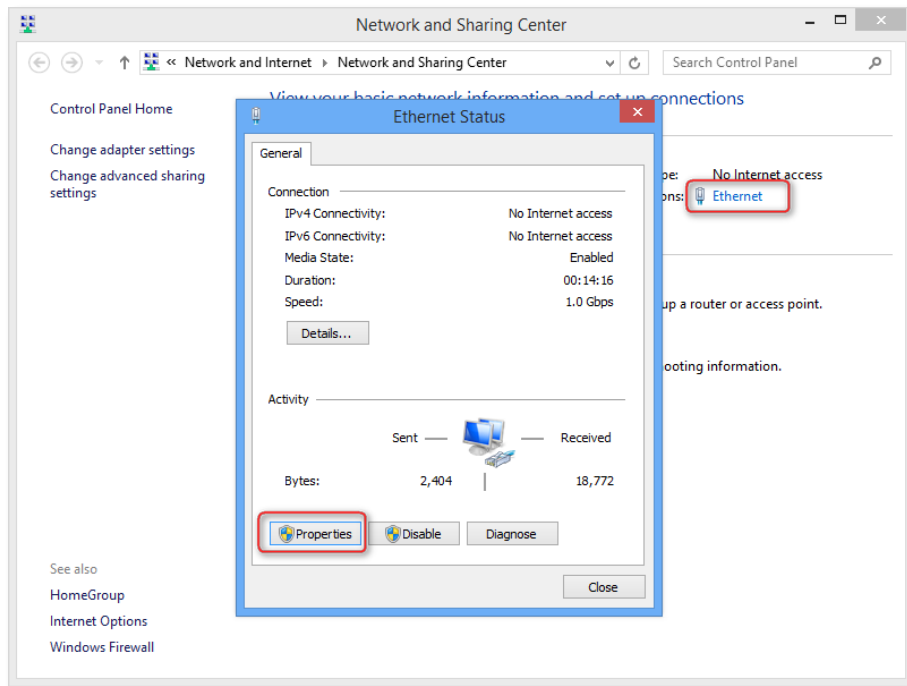
---End

A.1.2 Windows 8

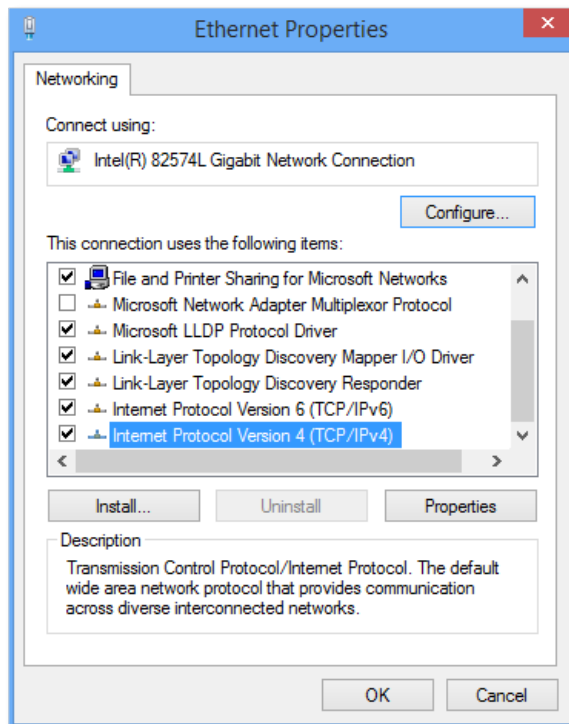
1. Right-click  in the bottom right corner of the desktop and choose **Open Network and Sharing Center**.



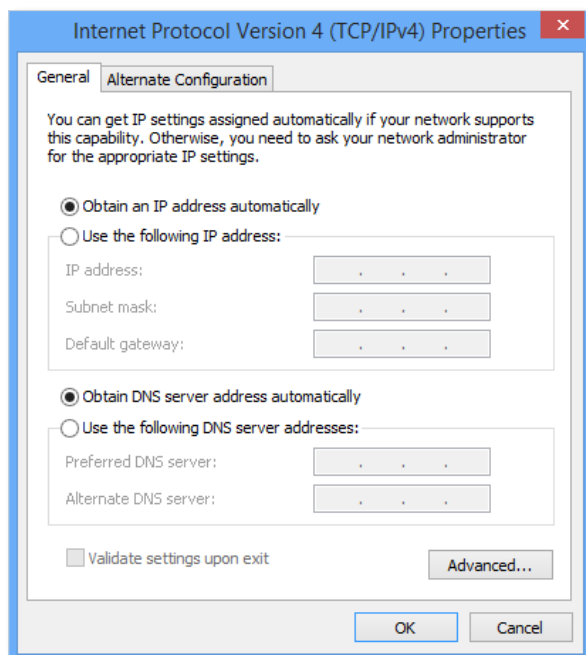
2. Click **Ethernet** and then **Properties**.



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



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

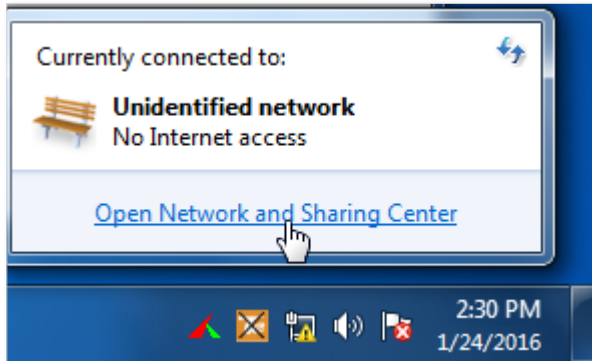


5. Click **OK** in the **Ethernet Properties** window.

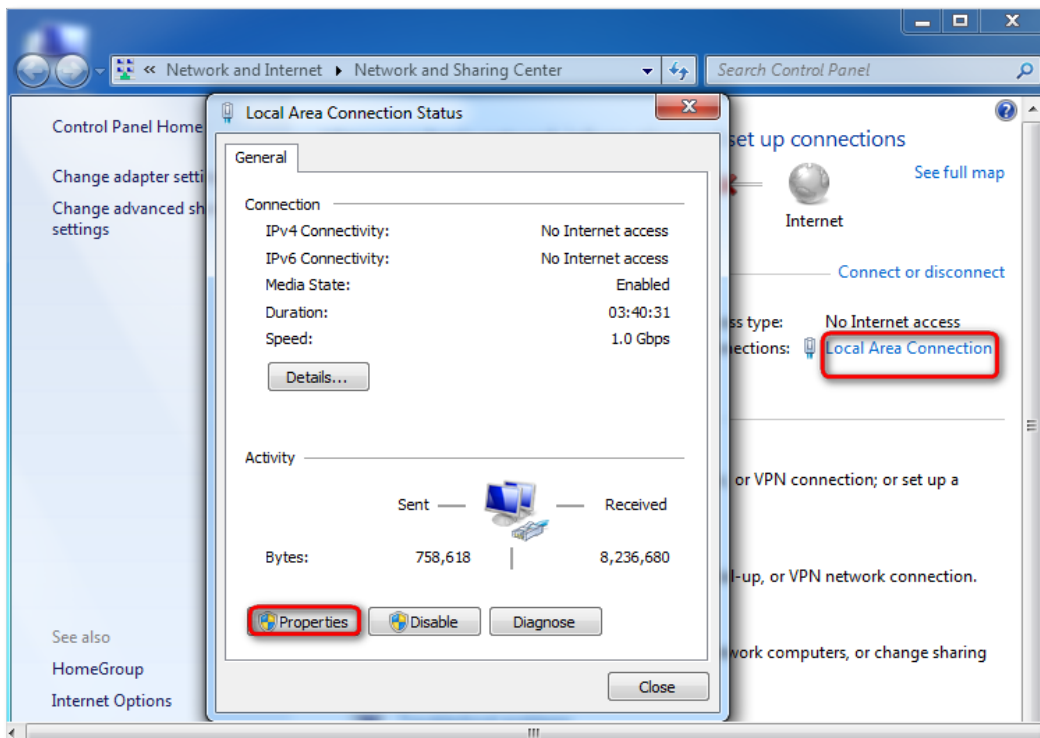
---End

A.1.3 Windows 7

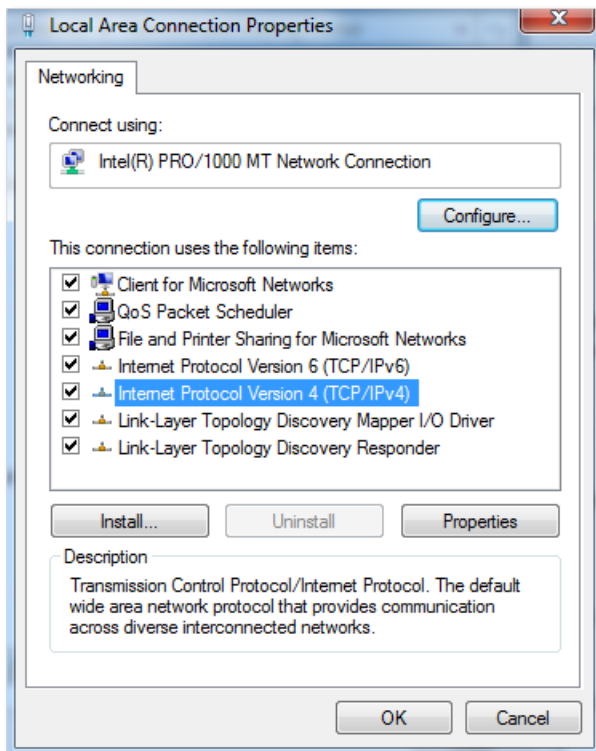
1. Click  in the bottom right corner of the desktop and choose **Open Network and Sharing Center**.



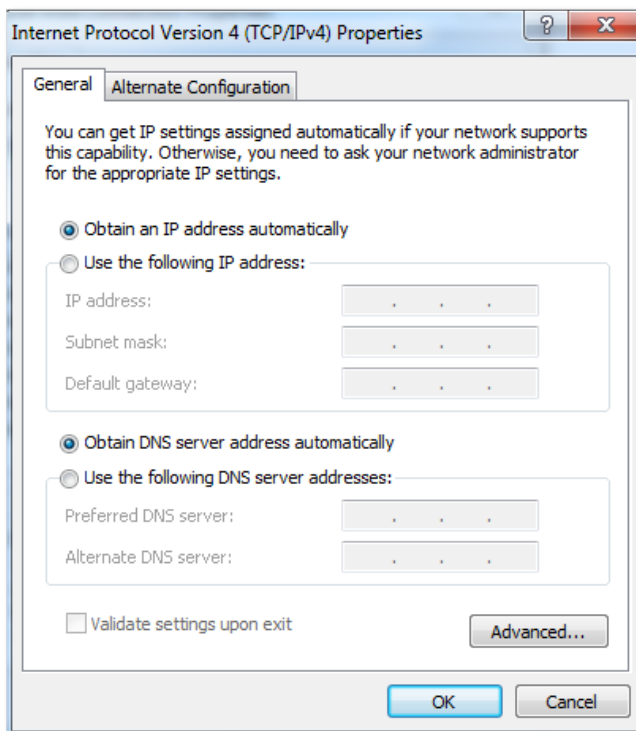
2. Click **Local Area Connection** and then **Properties**.



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



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



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
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
MAC	Medium Access Control
MTU	Maximum Transmission Unit
OFDMA	Orthogonal Frequency-division Multiple Access
PIN	Personal Identification Number
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point to Point Tunneling Protocol
PUK	Personal Identification Number Unlock Key

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

A.3 Connect to a hidden Wi-Fi

When a Wi-Fi 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: WPA2-PSK (recommended)
- Wi-Fi password: Tenda+Wireless245

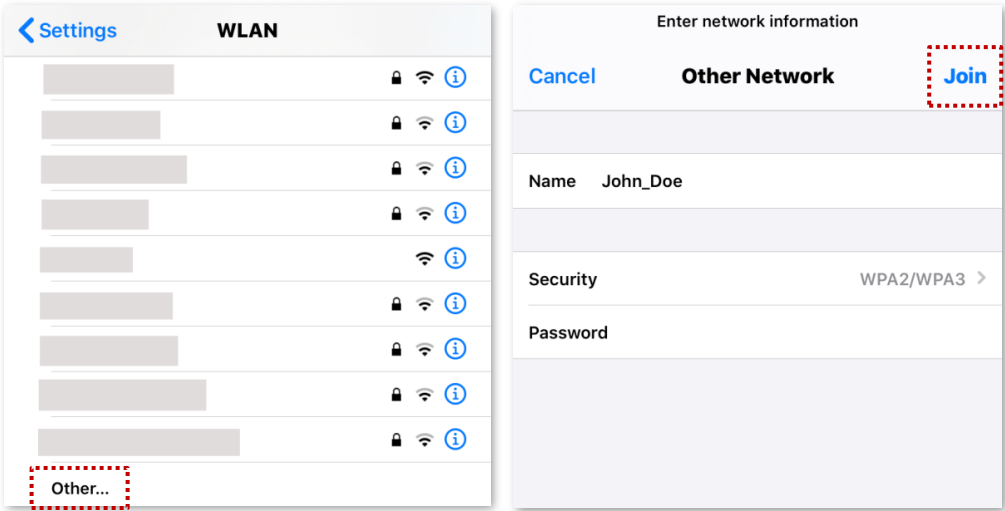


If you do not remember the wireless parameters of the Wi-Fi, [log in to the web UI of the router](#) and navigate to **Wi-Fi Settings > Wi-Fi Name & Password** to find them.

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

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

6. Tap **Join**.



---End

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