

Tenda

User Guide

AX1500 Wi-Fi 6 5G NR Router

5G01



Copyright statement

© 2024 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

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

Applicable product

This user guide is applicable to 5G01. All screenshots herein, unless other specified, are taken from 5G01.

Conventions

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


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

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

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

Item	Presentation	Example
Cascading menus	>	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 configuration, loss of data or damage to device.

Symbol**Meaning****TIP**

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

For more documents

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

Technical support

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

Email address: support@tenda.cn

Website: www.tendacn.com

Revision history

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

Version	Date	Description
V1.0	2024-07-20	Original publication.

Contents

1 Mesh networking	1
1.1 Overview	1
1.2 Set up as an add-on node	2
1.2.1 MESH button networking	2
1.2.2 Wired networking	4
1.2.3 Scanning networking	5
2 Connect the router to the internet	8
2.1 Wireless connection	8
2.2 Wired connection	9
2.3 WPS connection	10
2.3.1 Method 1: Use the WPS button	10
2.3.2 Method 2: Use the web UI	12
3 Login and logout	14
3.1 Login with smartphone or tablet	14
3.2 Login with computer	16
3.3 Log out of the web UI	18
4 Web UI layout	19
5 Internet settings	20
5.1 Access internet through a SIM card	20
5.1.1 Change mobile network preference	22
5.1.2 Create an APN profile manually	24
5.2 Access internet through the WAN port	25
5.2.1 Use a PPPoE account	25
5.2.2 Use a dynamic IP address	27
5.2.3 Use static IP address information	29
5.3 Set Failover connection	31

5.3.1 Overview	31
5.3.2 Example of setting up Failover connection	31
6 WiFi settings	33
6.1 Change the WiFi name and WiFi password	33
6.2 Configure guest WiFi	36
6.2.1 Overview	36
6.2.2 Example of setting the guest WiFi	37
7 Network status	39
7.1 View network status	39
7.1.1 Access internet through a SIM card	39
7.1.2 Access internet through the WAN port	40
7.1.3 Access internet through SIM card and WAN port	41
7.2 View WAN status	43
7.2.1 View 4G/5G WAN status	43
7.2.2 View Ethernet WAN status	45
7.2.3 View IPv6 status	46
7.3 View system information	48
7.3.1 View basic information	48
7.3.2 View LAN status	49
7.3.3 View WiFi status	49
7.4 View wireless information	51
7.5 View the number of Mesh nodes and clients	52
7.6 View network status, node and client details	53
8 Client management	56
8.1 Add a client to the blacklist	56
8.1.1 Method 1	56
8.1.2 Method 2	57
8.2 Remove a client from the blacklist	59
8.3 Internet access speed control	60

8.4 Example of setting MAC address filter	61
8.5 Configure parental control	63
8.5.1 Overview	63
8.5.2 Example of adding a parental control rule	64
9 Mobile settings	67
9.1 Data limit	67
9.1.1 Overview	67
9.1.2 Example of data limit configurations	68
9.2 SIM PIN	70
9.2.1 Unlock the SIM card	70
9.2.2 Enable PIN lock for the SIM card	73
9.2.3 Disable PIN lock for the SIM card	74
9.2.4 Use PUK code to set PIN code	75
9.3 ISP update	76
9.4 Manage SMS messages	78
9.4.1 Send SMS messages	78
9.4.2 Delete SMS messages	81
9.5 Inquire information by sending USSD commands	83
9.6 Set the message center number	84
10 Optimize network performance	85
10.1 One-click optimization	86
10.2 Configure channel & bandwidth	87
10.3 UPnP	89
11 Remote access	90
11.1 VPN	90
11.1.1 PPTP server	90
11.1.2 PPTP/L2TP client	97
11.1.3 OpenVPN server	99
11.2 DMZ host	103

11.2.1 Overview	103
11.2.2 Example of setting DMZ host	104
11.3 Remote web management	107
11.3.1 Overview	107
11.3.2 Example of setting remote web management	108
11.4 DDNS	110
11.4.1 Overview	110
11.4.2 Example of setting DDNS	111
11.5 Port mapping	114
11.5.1 Overview	114
11.5.2 Example of setting port mapping	115
12 Network security	118
12.1 Change login password	118
12.2 Firewall	120
13 Advanced settings	122
13.1 Turn on or turn off indicators	122
13.1.1 Turn on or turn off indicators of all nodes	122
13.1.2 Turn on or turn off indicators of single node	122
13.2 Configure LAN settings	124
13.2.1 Overview	124
13.2.2 Change LAN IP address	127
13.2.3 Change DHCP server	128
13.2.4 Assign static IP address to LAN client	129
13.3 Static routing	131
13.3.1 Overview	131
13.3.2 Example of adding a static route rule	132
14 System maintenance	135
14.1 Reboot device	136
14.1.1 Reboot all nodes	136

14.1.2 Reboot single node	137
14.2 Configure system time	138
14.2.1 Sync system time with the internet time	138
14.2.2 Synchronize with local time	140
14.3 Upgrade firmware	141
14.3.1 Online upgrade	141
14.3.2 Local upgrade	142
14.4 Backup & Restore	144
14.4.1 Backup the configurations of the router	144
14.4.2 Restore previous configurations of the router	144
14.4.3 Reset	145
14.5 Automatic system maintenance	148
14.6 System log	149
Appendix	150
A.1 Set computer to auto obtain an IPv4 address	150
A.1.1 Windows 10	150
A.1.2 Windows 8	153
A.1.3 Windows 7	155
A.2 Acronyms and abbreviations	157

1 Mesh networking

1.1 Overview



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

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

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

- **MESH button networking**

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

- **Wired networking**

Connect the LAN port (such as LAN1 or WAN/LAN2) of an existed node to a new node 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**

Add other routers to the network of this router through the configuration of the web UI of the router.

1.2 Set up as an add-on node

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

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

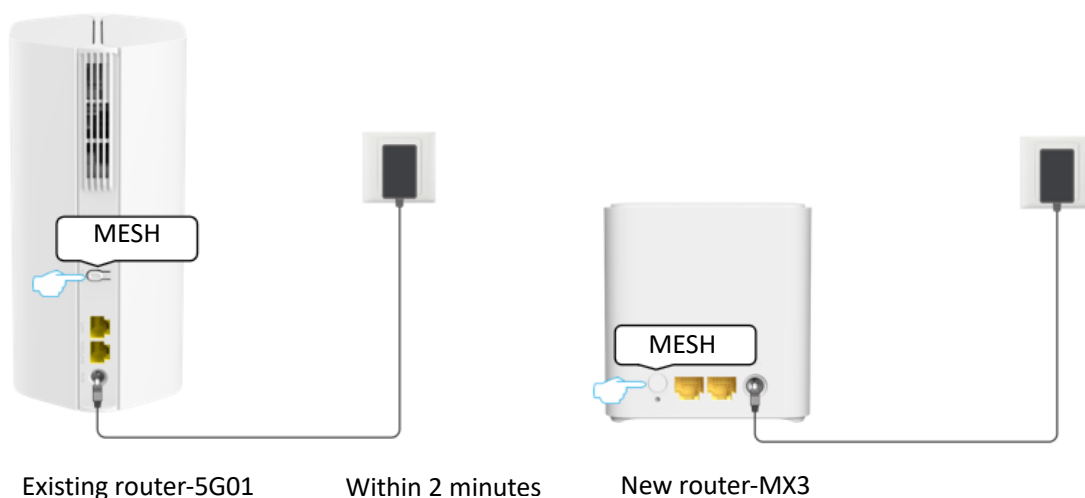



- If there are more than two secondary nodes, place the primary node in the key area and ensure that no more than one node is between the primary node and the secondary node.
- Before using a new router to extend the network, ensure that the existing router (primary node) has been connected to the internet 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 5G01 (primary mode) and MX3 (secondary node) as an example.

1.2.1 MESH button networking

Step 1 Add to the existed network.

1. Power on the existing router (5G01) and connect it to the internet properly.
2. Place the new router (MX3) near the existing router (within 3 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 existing router. The WiFi indicator (📶) blinks fast.
4. Press (1 to 3 seconds) the networking button (MESH) of the new router within 2 minutes. The indicator blinks green fast.



When the WiFi indicator () of the existing router blinks slowly for 10 seconds and then lights solid on, the networking is successful and the new router becomes a secondary node in the network.

Step 2 Select an appropriate position for the new router.




1. For a better internet experience, you can relocate the wireless router by referring to the following relocation tips:
 - Place the new router within the wireless coverage range of the existing router.
 - Keep your nodes away from electronics with strong interference, such as microwave ovens, induction cookers, and refrigerators.
 - Place the nodes in a high position with few obstacles.
2. Power on the new router, and wait until the indicator blinks green slowly.



TIP

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

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

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

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

---End

To access the internet with:

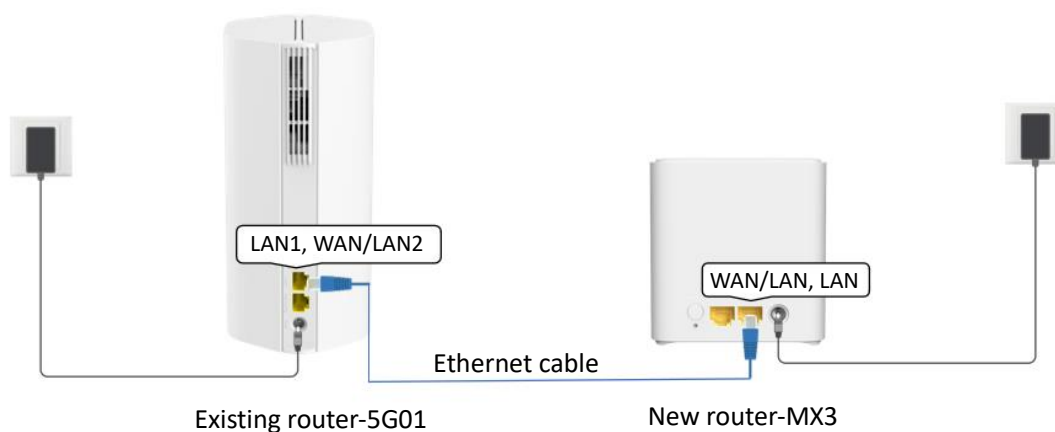
- **Wired devices:** Connect to a LAN port of the router using an Ethernet cable.
- **WiFi-enabled devices:** Connect to the WiFi network using the WiFi name and password you set.

Repeat [this section](#) to add other routers.

1.2.2 Wired networking

Assume that the Ethernet cable has been deployed in advance between the living room and the bedroom in the home, the router 5G01 (primary node) placed in the living room has been connected to the internet, and now you need to deploy a router MX3 (planned as a secondary node) in the bedroom to extend the WiFi network.

- Step 1** Power on the existing router (5G01) and connect it to the internet properly.
- Step 2** Place the new router (MX3) where you want to deploy it, which is **bedroom** in this example. Power on the new router (MX3). Wait until the startup of the new router (MX3) is complete (the indicator blinks green slowly).
- Step 3** Connect the LAN port (LAN1, WAN/LAN2) of the primary node to the LAN port (LAN, WAN/LAN) of the new router (MX3) using an Ethernet cable.



---End

The wireless router will automatically network. Please wait about 1 minute. When the indicator of the new router (MX3) turns solid green, the networking is successful. The MX3 becomes a secondary node in the network.

To access the internet with:


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

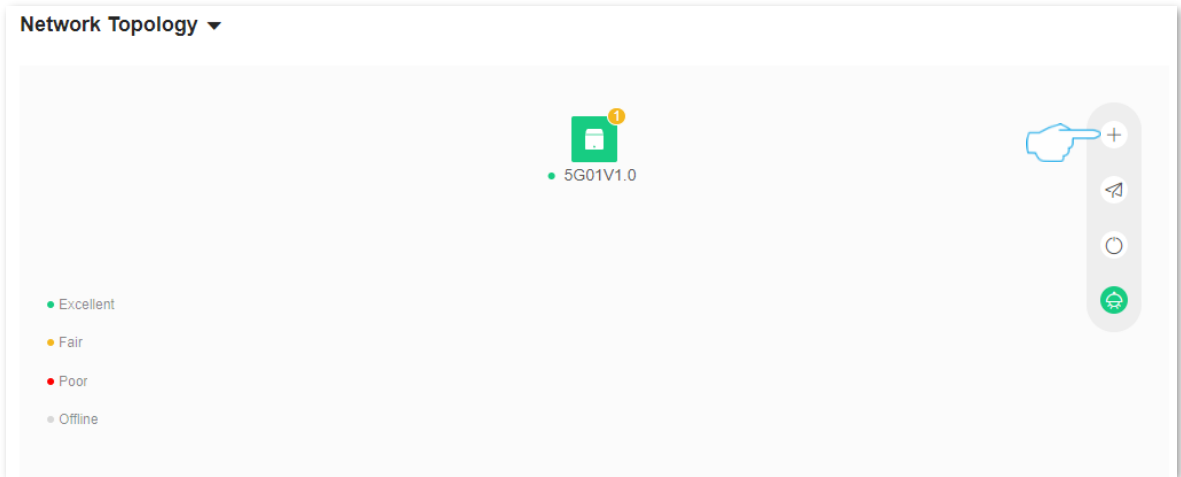


- After the wired networking is successful, if the Ethernet cable connecting the two routers are removed, the system automatically switches to the wireless networking. To obtain better internet access experience after switching to a WiFi network, go to [select an appropriate position for the new router](#).
 - If there is still a router to network, repeat [this section](#).
 - To obtain a better wireless internet experience, keep your nodes away from electronics with strong interference, such as microwave ovens, induction cookers, and refrigerators.
-

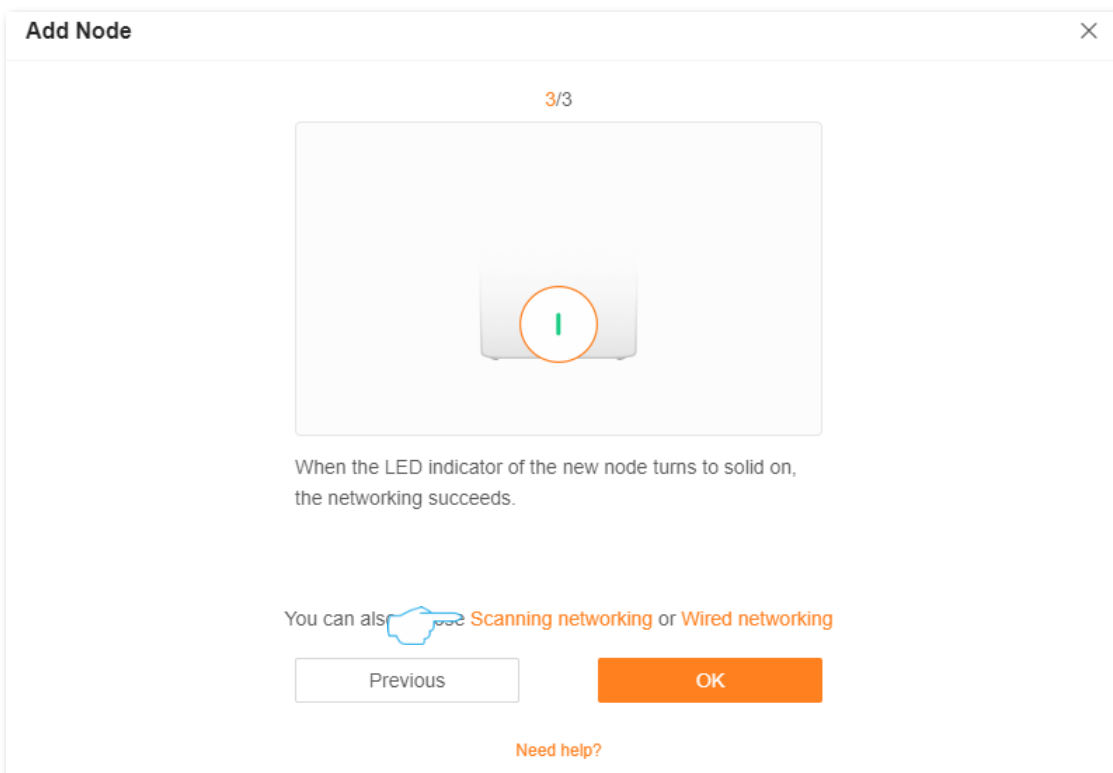
1.2.3 Scanning networking

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

Step 2 Navigate to **Network Status**, and click  in the **Network Topology** module.



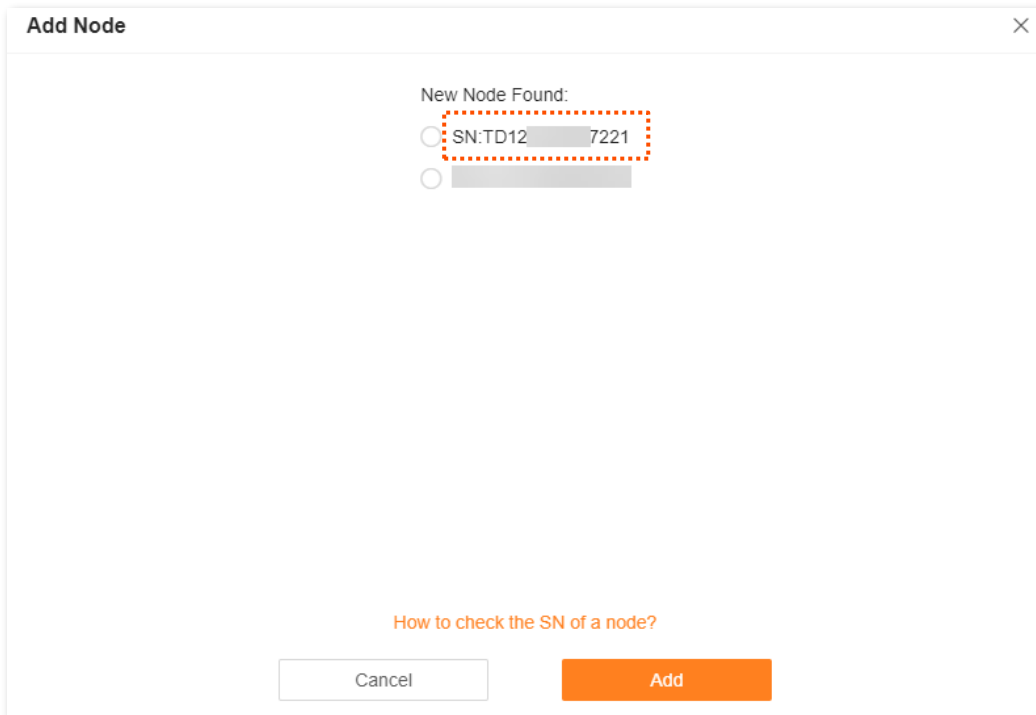
Step 3 Click **Next > Next**, and click **Scanning networking**.



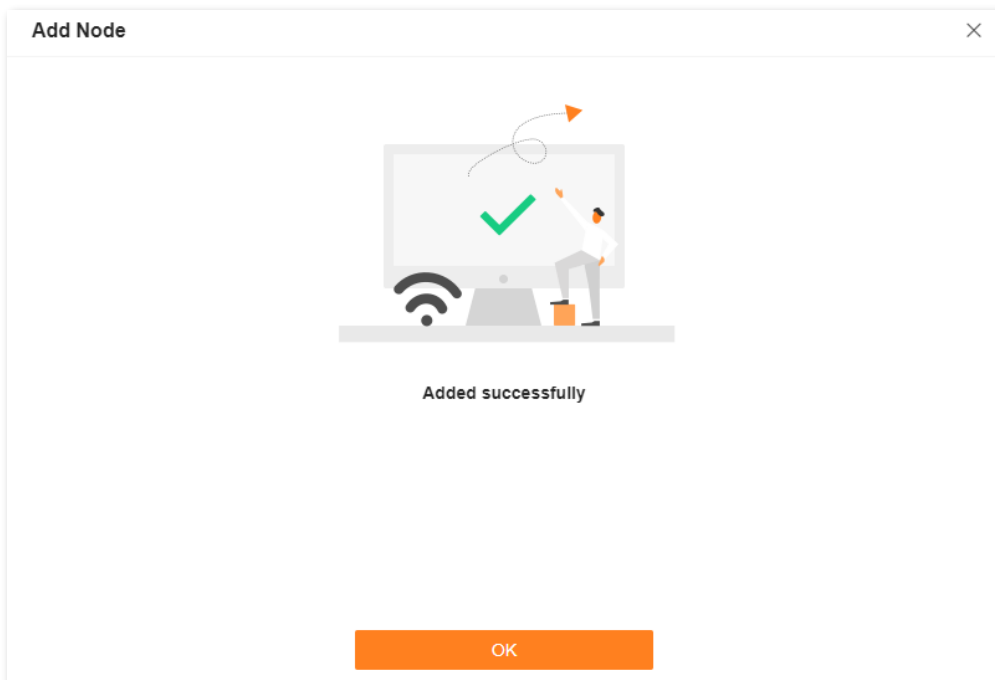
Step 4 The system discovers new nodes, ensure that the SN is the same as the SN on the label of the new router, select a node, and click **Add**. The following figure is for reference only.



You can add only one node at a time by scanning.



Step 5 Wait until the ongoing process is complete, and click **OK**.



---End

If the indicator of new node lights solid on and the new node is displayed in **Network Topology**, the node is added successfully.

To access the internet with:

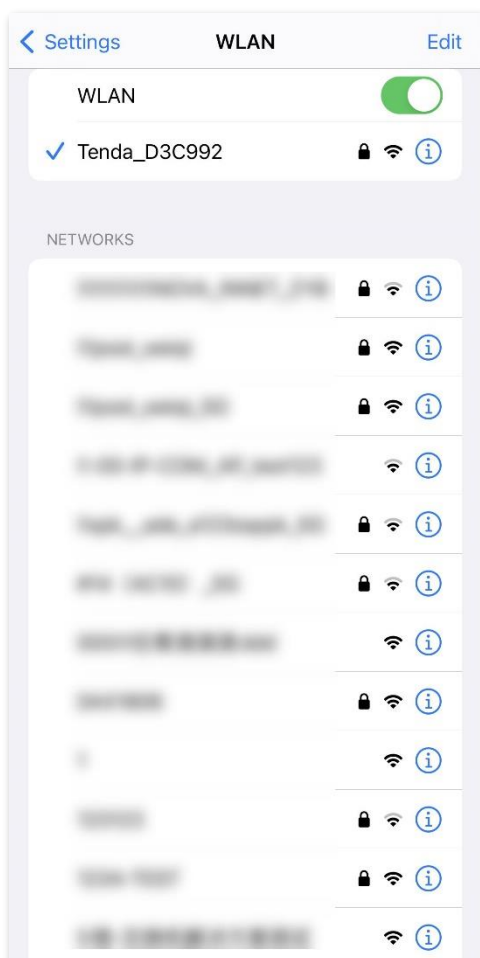
- **Wired devices:** Connect to a LAN port of the router using an Ethernet cable.
- **WiFi-enabled devices:** Connect to the WiFi network using the WiFi name and password you set.

2

Connect the router to the internet

2.1 Wireless connection

Connect your WiFi-enabled device, such as a smartphone, to the WiFi network of the router. Tenda_D3C992 is used for illustration here.



- For first time login, connect your WiFi-enabled device to the WiFi network of the router using the WiFi name labeled on the bottom panel of the router.
- When you log in to the router again, you can connect to the WiFi network using the new WiFi name and password.

2.2 Wired connection

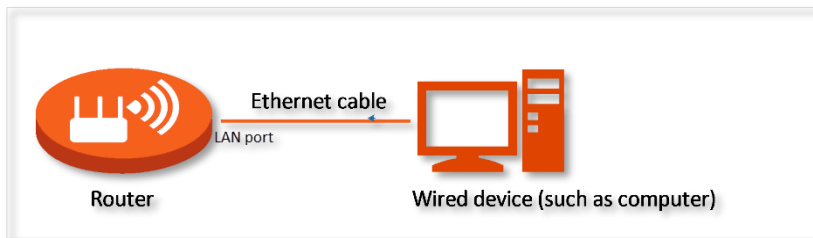
Connect your wired device, such as a computer, to the LAN port of the router using an Ethernet cable.



TIP

The WAN/LAN2 port is the WAN/LAN multiplexing port.

- It is LAN port by default. Used to connect to such devices as computers, switches or game machines.
- When the Failover function is enabled, the WAN/LAN port only serves as a WAN port. Used to connect to Modem or Ethernet jack.



2.3 WPS connection

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




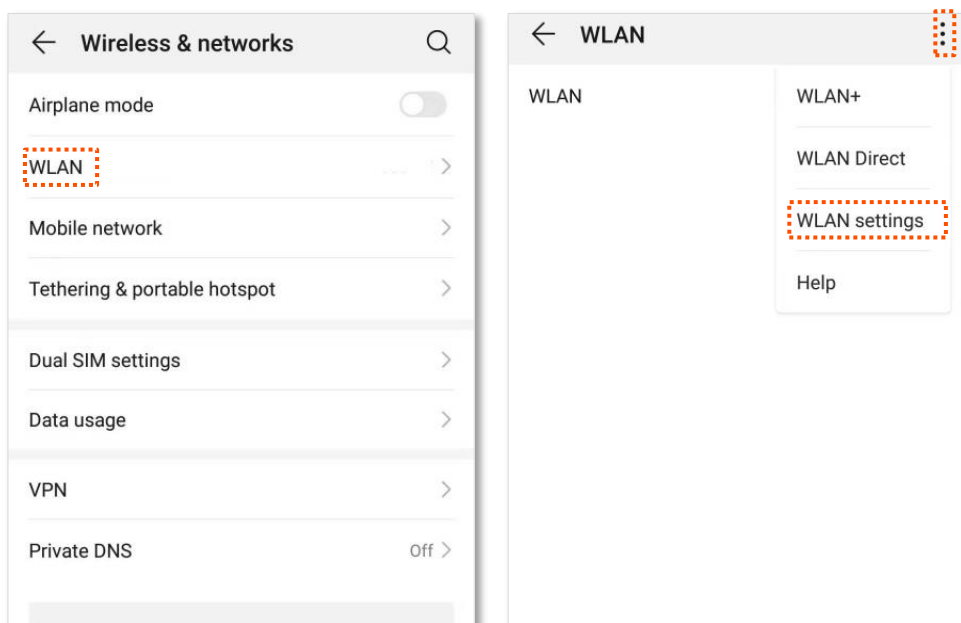
This function is only applicable to WiFi-enabled devices that can use WPS function.

2.3.1 Method 1: Use the WPS button

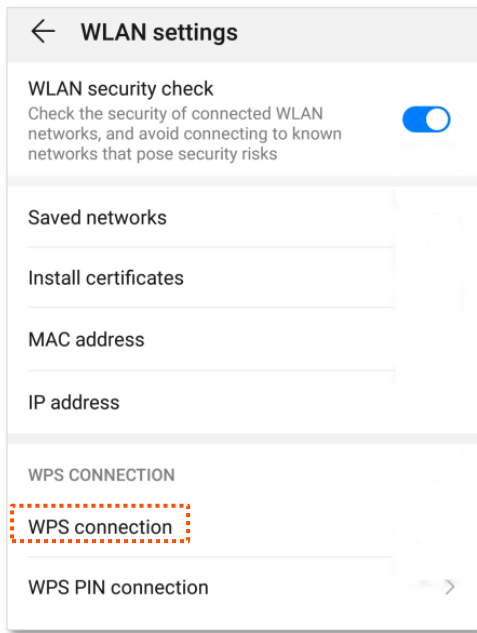
Step 1 Hold down the MESH button for 1 to 3 seconds. The WiFi indicator (📶) blinks fast.

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

1. Find **WLAN** settings on the smartphone.
2. Tap , and choose **WLAN settings**.

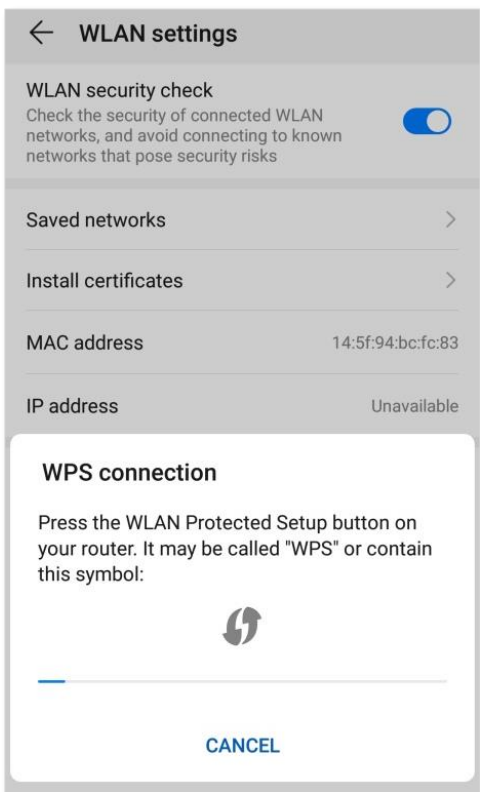


3. Choose WPS connection.



---End

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

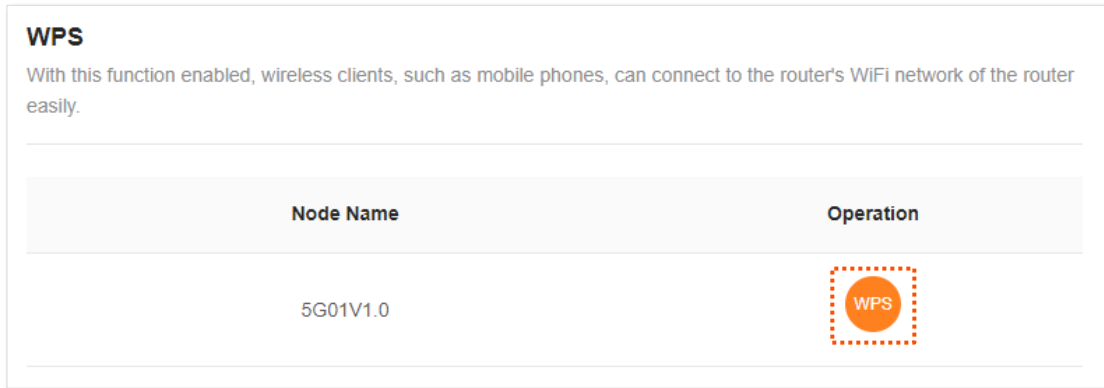


2.3.2 Method 2: Use the web UI


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

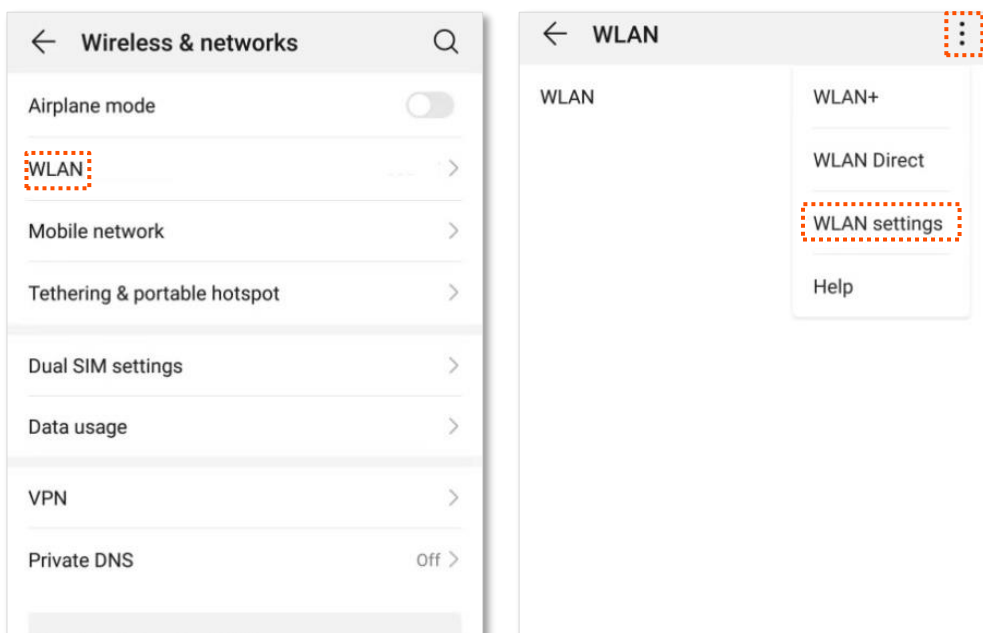
Step 2 Navigate to **More > WiFi Settings > WPS.**

Step 3 Click  .

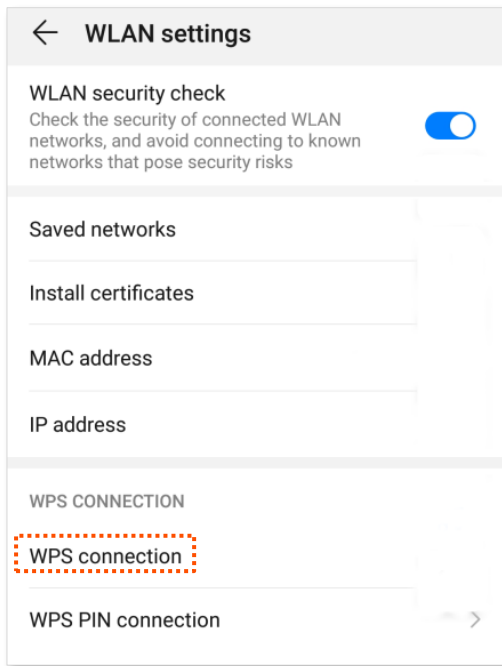


Step 4 Configure the WPS function on your WiFi-enabled devices **within 2 minutes**. Configurations on various devices may differ (Example: HUAWEI P10).

1. Find **WLAN** settings on the smartphone.
2. Tap , and choose **WLAN settings**.

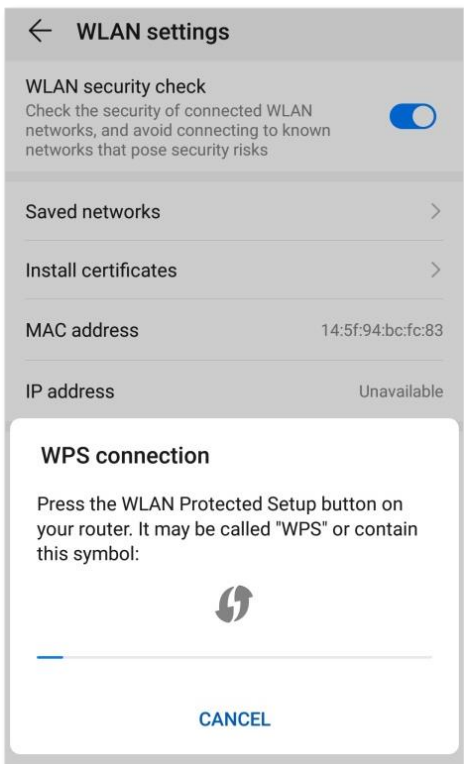


3. Choose WPS connection.



---End

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



3 Login and logout

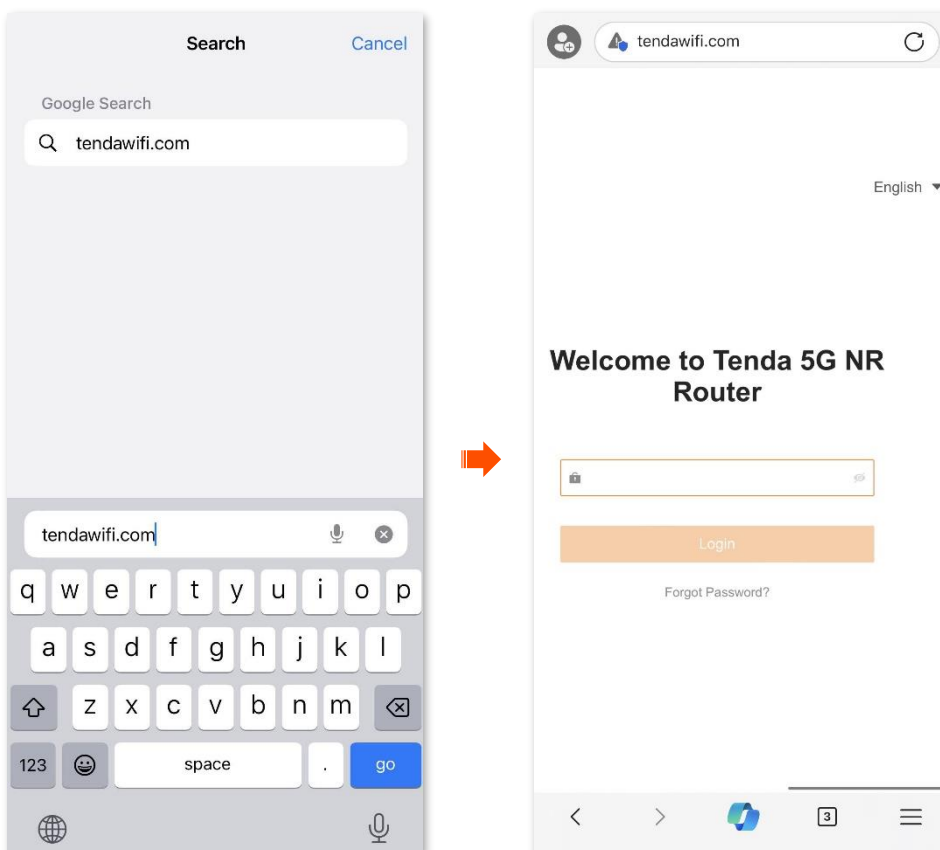
3.1 Login with smartphone or tablet

iPhone is used for illustration here. Other mobile clients are similar.

- Step 1** [Connect the smartphone to the WiFi network of the router.](#)
- Step 2** Start a browser on your smartphone, visit the router's management address **tendawifi.com**, and log in to the web UI of the router.
- Step 3** Enter your login password, and click **Login**. The following figure is for reference only.

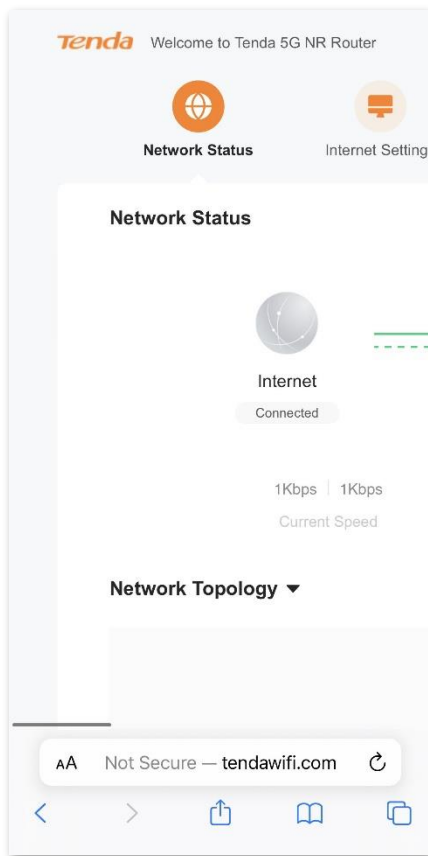


TIP
If you forgot your login password, try to log in using your WiFi password. If the problem persists, [reset the router](#) and try again.



----End

Successfully logged in to the web UI of the router. You can zoom in and out of the page to view or configure settings as required. The following figure is for reference only.

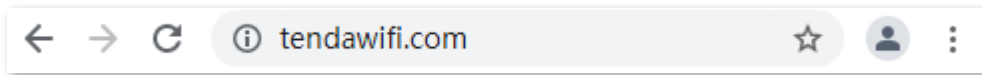


If the above page does not appear, try the following solutions:

- Ensure that your WiFi-enabled device is connected to the WiFi network of the router.
- Disable the cellular network of your WiFi-enabled device.
- Clear the cache of your web browser or try again with another web browser.
- Try to log in to the web UI of the router with the default IP address **192.168.0.1**.
- [Reset the router](#) and try again.

3.2 Login with computer

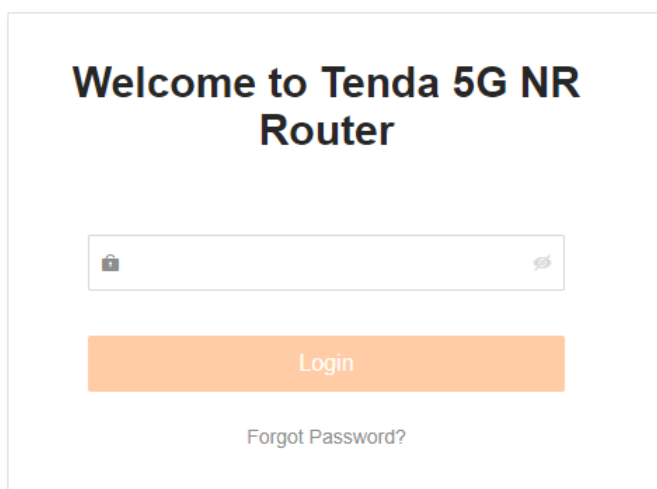
Step 1 Start a browser [on the computer connected to the router](#) and enter **tendawifi.com** in the address bar to log in to the web UI.



Step 2 Enter your login password, and click **Login**. The following figure is for reference only.

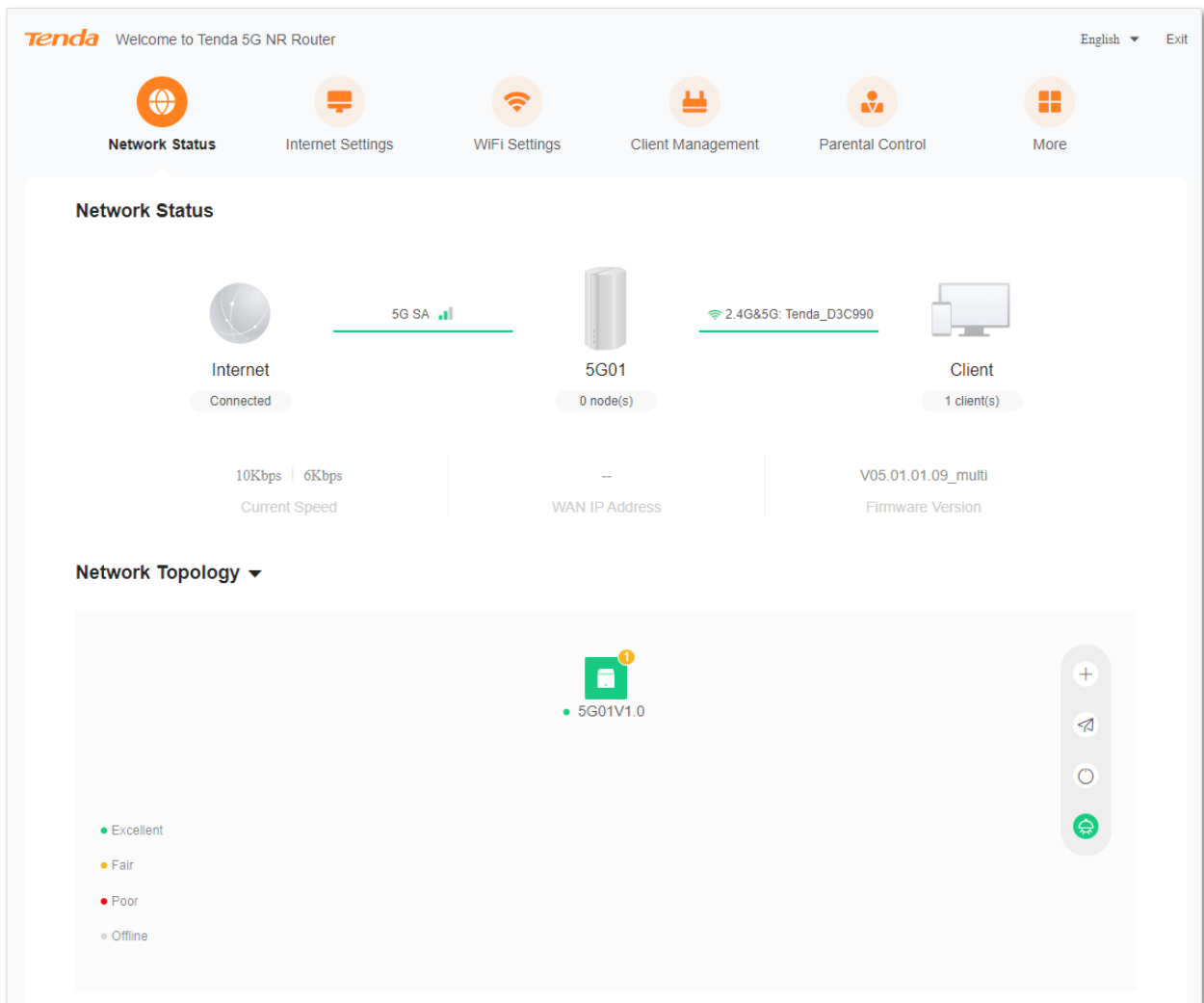


If you forgot your login password, try to log in using your WiFi password. If the problem persists, [reset the router](#) and try again.



---End

Successfully logged in to the web UI of the router. You can configure the router as required. The following figure is for reference only.



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

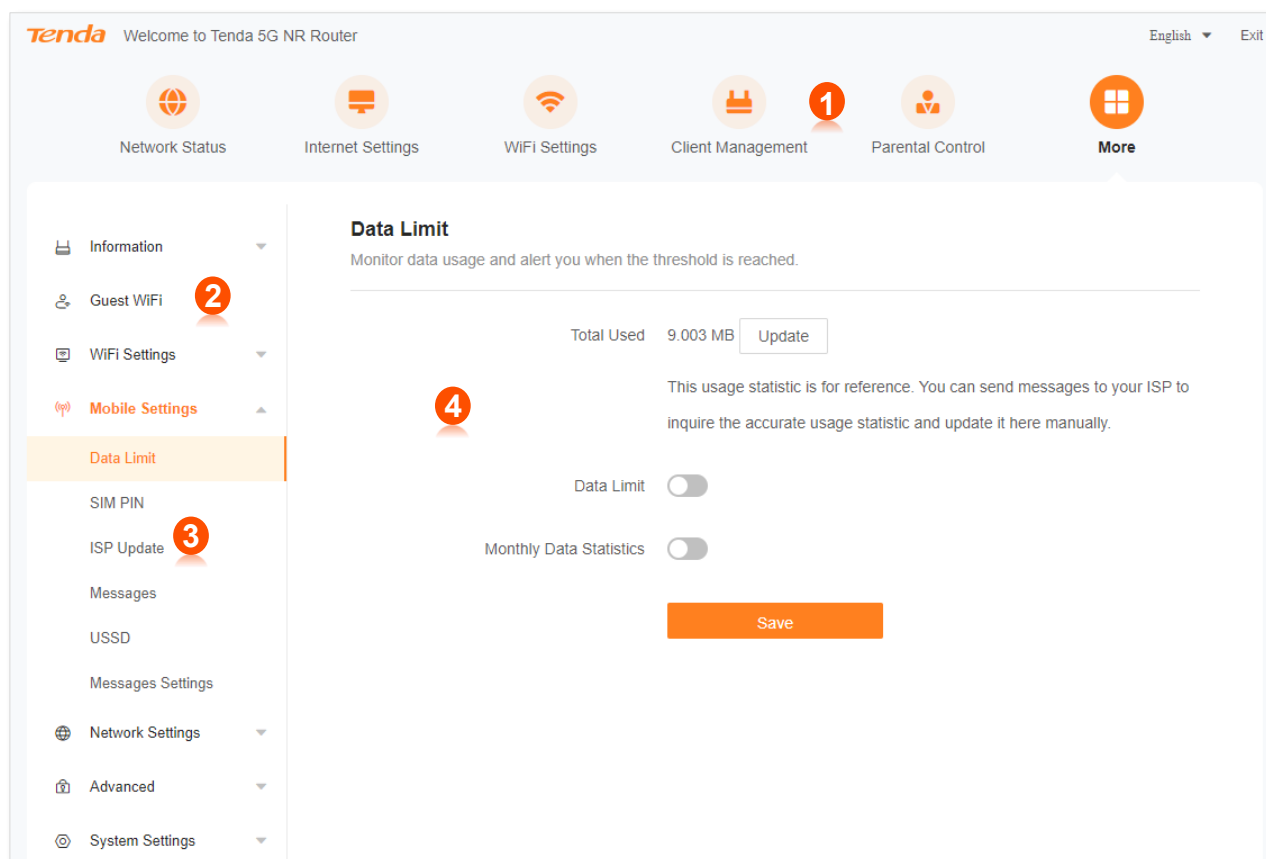
- Ensure that the router is powered on properly.
- Ensure that the computer has connected to the LAN port of the router properly.
- Clear the cache of your web browser or try again with another web browser.
- Try to log in to the web UI of the router with the default IP address **192.168.0.1**.
- Ensure that the computer is set to **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
- [Reset the router](#) and try again.

3.3 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.

4 Web UI layout

The web UI of the router consists of four sections, including the level-1 navigation bar, level-2 navigation bar, level-3 navigation bar and the configuration area. See the following figure.



No.	Name	Description
1	Level-1 navigation tree	
2	Level-2 navigation tree	Used to display the function menu of the router. Users can select functions in the navigation bar and the configuration page will appear in the configuration area.
3	Level-3 navigation tree	
4	Configuration area	Used to view or modify your configurations.

5 Internet settings

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

5.1 Access internet through a SIM card

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

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

Internet Settings

Connection Status Connected

Mobile Data

Data Roaming
This function may cause Roaming charge

Mobile Data Options 5G NSA Preferred

Profile Name ctlte(Default:1) [Create a Profile](#)

PDP Type IPv4v6

APN ctlte

User Name

Password

Authentication Type NONE

MTU 1500



Compatibility Mode


Failover Settings

Failover ⓘ

[Disconnect](#)

Parameter description

Parameter	Description	
Internet Settings	Connection Status	Specifies the internet connection status of the SIM card.
	Mobile Data	Used to enable or disable the mobile data traffic. When it is disabled, you cannot access the internet through the router.
	Data Roaming	Used to enable or disable data roaming for the SIM card inserted in the router.
		Data roaming means the data usage produced when you are outside the coverage of your ISP. You can disable data roaming to avoid roaming data usage and charges.
		 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. <ul style="list-style-type: none"> - 5G SA Preferred: 5G SA, 5G NSA, 4G and 3G can be used in sequence based on the signal strength. - 5G NSA Preferred: 5G NSA, 5G SA and 4G can be used in sequence based on the signal strength. - 4G Only: Only the 4G network is used. - 3G Only: Only the 3G network is used. 	
Dial-up Settings	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	If the router fails to identify these parameters of your SIM card, you have to enter them manually by clicking Create a Profile and dial up for internet access.
	User Name	 TIP If the router cannot identify these parameters, contact your ISP for them.
	Password	
	Authentication Type	
	Create a Profile	Used to create an APN dial-up profile when the router fails to identify these parameters automatically.
MTU	Maximum Transmission Unit (MTU) is the largest data packet transmitted by a network device. The default MTU value is 1500. Do not change the value unless necessary.	

Parameter	Description
Compatibility Mode	<p>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.</p> <p> TIP</p> <p>It is applicable to some ISPs limited plans. The TTL and HL values can be modified for packet capture analysis as required.</p>
Failover Settings	<p>Failover</p> <p>Used to enable or disable the Failover function. When the Failover function is enabled, 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. For details, see Set Failover connection.</p>

5.1.1 Change mobile network preference

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

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

Configuration procedure:

- Step 1** [Log in to the web UI of the router](#).
- Step 2** Navigate to **Internet Settings**.
- Step 3** Enable **Mobile Data** and **Data Roaming**.
- Step 4** Set **Mobile Data Option** to **4G Only**.
- Step 5** Click **Connect**.

Internet Settings

Connection Status **Connected**

Mobile Data

Data Roaming
This function may cause Roaming charge

Mobile Data Options

Profile Name [Create a Profile](#)

PDP Type

APN

User Name

Password

Authentication Type

MTU

Compatibility Mode

Failover Settings

Failover ⓘ

---End

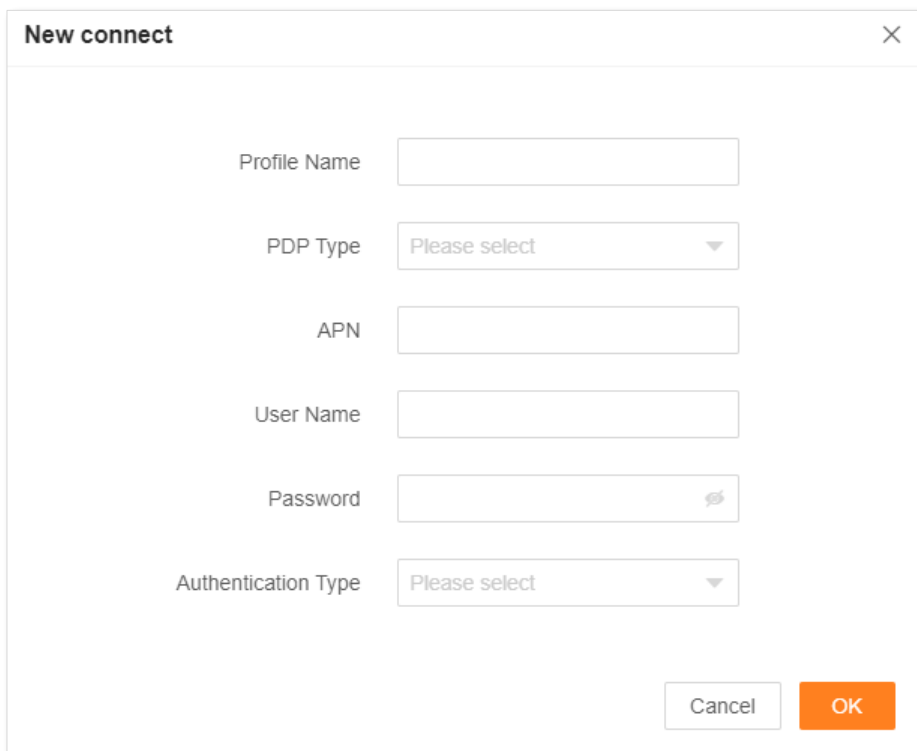
After the configuration is completed, refresh the configuration page. When **Connected** is shown after **Connection Status**, you can use the 4G network only to access the internet outside the coverage of your ISP.

5.1.2 Create an APN profile manually

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.

Configuration procedure:

- Step 1** [Log in to the web UI of the router.](#)
- Step 2** Navigate to **Internet Settings**.
- Step 3** Click **Create a Profile**.
- Step 4** Enter required parameters inquired from your ISP.
- Step 5** Click **OK**.



The screenshot shows a 'New connect' dialog box with the following fields:

- Profile Name:
- PDP Type:
- APN:
- User Name:
- Password:
- Authentication Type:

Buttons: Cancel, OK

---End

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

5.2 Access internet through the WAN port

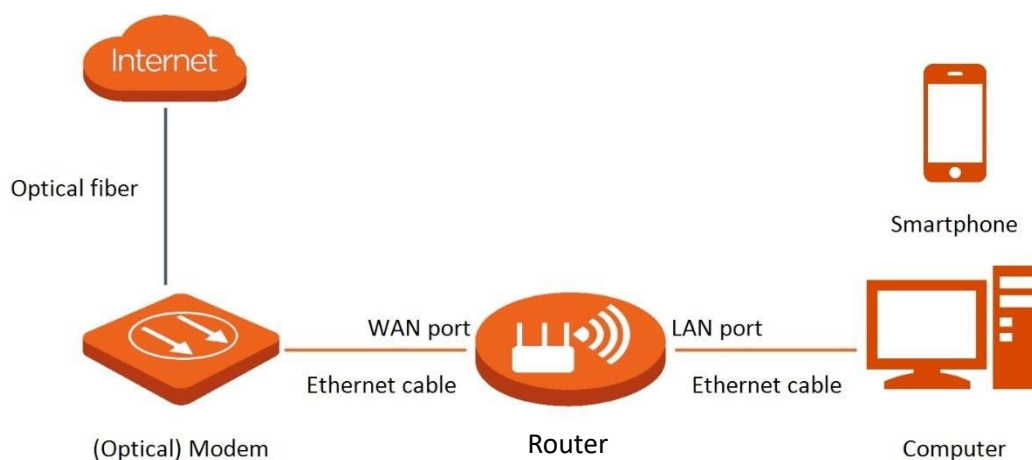
If you want to connect your broadband to the router to access the internet, you can set the router through the WAN port.



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

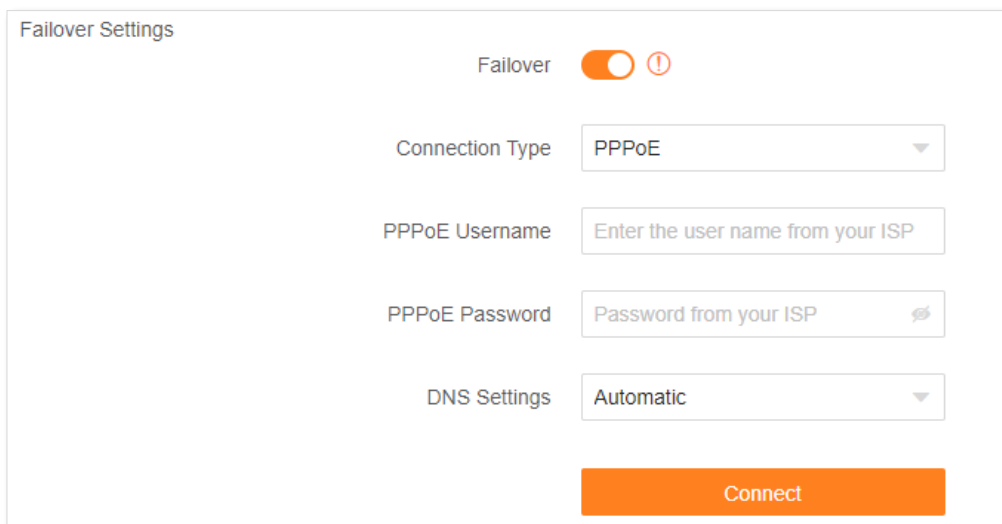
5.2.1 Use a PPPoE account

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



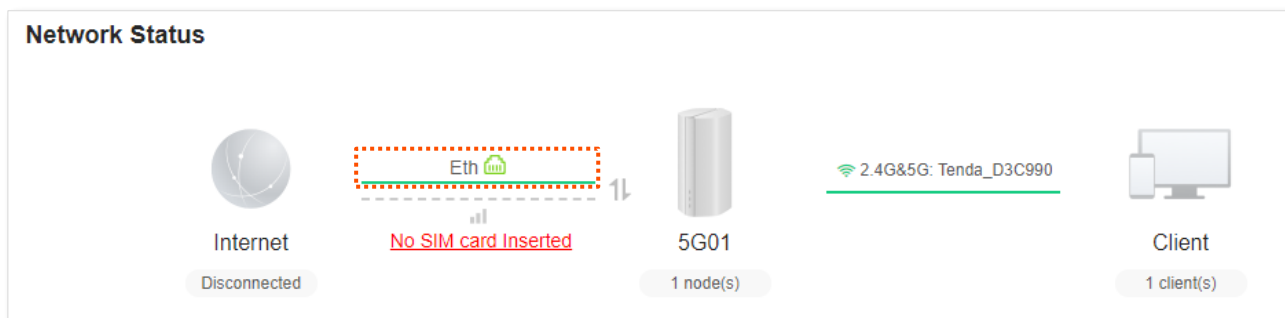
Configuration procedure:

- Step 1** [Log in to the web UI of the router.](#)
- Step 2** Navigate to **Internet Settings**.
- Step 3** Enable the **Failover** function.
- Step 4** Set **Connection Type** to **PPPoE**.
- Step 5** Enter the **PPPoE Username** and **PPPoE Password**.
- Step 6** Click **Connect**.



---End

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



If you fail to access the internet, refer to [View network 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: <ul style="list-style-type: none"> - PPPoE: Select this type if you access the internet using the PPPoE user name and PPPoE password. - Dynamic IP: Select this type if you can access the internet by simply plugging in an Ethernet cable. - Static IP: Select this type if you want to access the internet using fixed IP information.
PPPoE Username	When PPPoE is chosen as Connection Type , you need to enter the user name and password provided by your ISP to access the internet.
PPPoE Password	

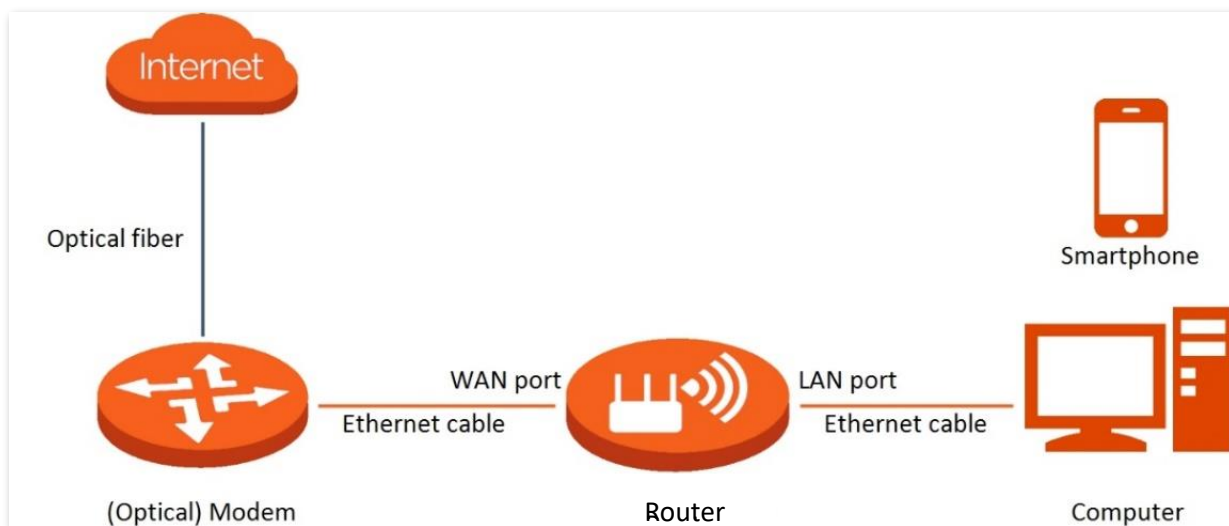
Parameter	Description
DNS Settings	<p>Specifies the obtaining method of WAN port DNS address, which is Automatic by default.</p> <ul style="list-style-type: none"> - Automatic: The router obtains a DNS server address from the DHCP server of the upstream network automatically. - Manual: The DNS server address is configured manually.

5.2.2 Use a dynamic IP address

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

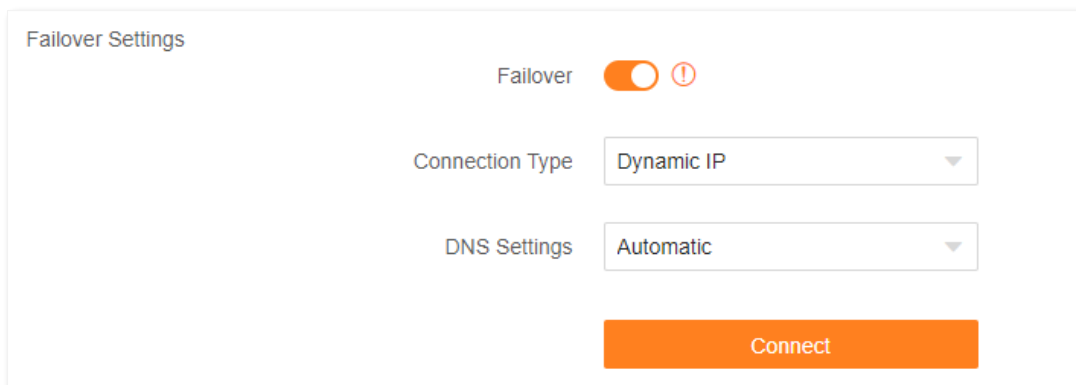
- Your ISP does not provide PPPoE user name and password, or any information including IP address, subnet mask, default gateway and DNS server.
- You have a router with internet access and want to add a 5G01 as the other one.

The application scenario is shown below.



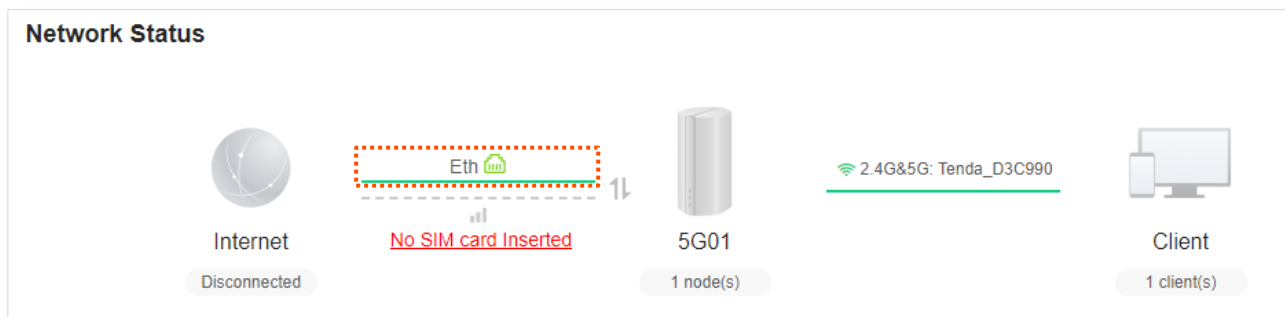
Configuration procedure:

- Step 1** [Log in to the web UI of the router.](#)
- Step 2** Navigate to **Internet Settings**.
- Step 3** Enable the **Failover** function.
- Step 4** Set **Connection Type** to **Dynamic IP**.
- Step 5** Click **Connect**.



---End

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



If you fail to access the internet, refer to [View network 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: <ul style="list-style-type: none"> - PPPoE: Select this type if you access the internet using the PPPoE user name and PPPoE password. - Dynamic IP: Select this type if you can access the internet by simply plugging in an Ethernet cable. - Static IP: Select this type if you want to access the internet using fixed IP information.
DNS Settings	Specifies the obtaining method of WAN DNS address, which is Automatic by default. <ul style="list-style-type: none"> - 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.

5.2.3 Use static IP address information

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

Configuration procedure:

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

Failover Settings

Failover ⓘ

Connection Type: Static IP

IP Address: . . .

Subnet Mask: . . .


Default gateway: . . .

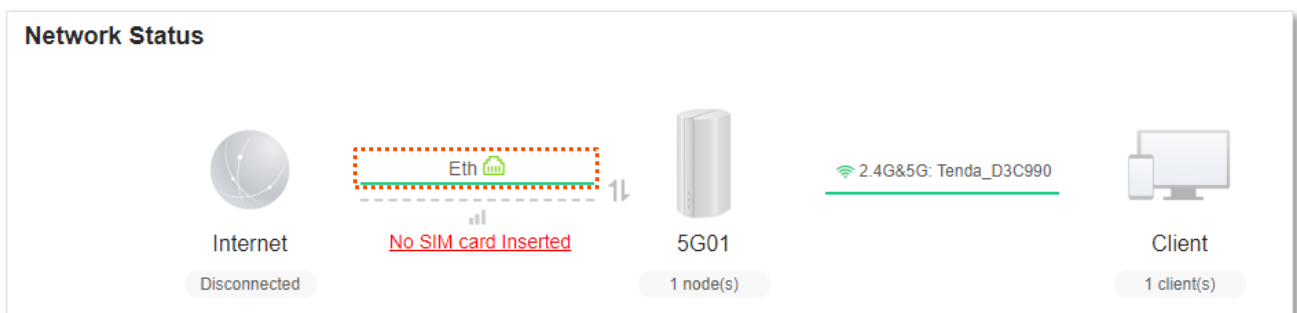
Primary DNS: . . .

Secondary DNS: . . .

Connect


---End

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



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

Parameter description

Parameter	Description
Failover	Used to enable or disable the Failover function.
Connection Type	<p>Specifies how your router connects to the internet, including:</p> <ul style="list-style-type: none"> - PPPoE: Select this type if you access the internet using the PPPoE user name and PPPoE password. - Dynamic IP: Select this type if you can access the internet by simply plugging in an Ethernet cable. - Static IP: Select this type if you want to access the internet using fixed IP information.
IP Address	When Static IP is chosen as Connection Type , enter the fixed IP address information provided by your ISP.
Subnet Mask	
Default Gateway	 TIP
Primary DNS	If your ISP only provides one DNS server, you can leave the secondary DNS server blank.
Secondary DNS	

5.3 Set Failover connection

5.3.1 Overview

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



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

To access the configuration page, [log in to the web UI of the router](#), and navigate to **Internet Settings**, and locate the **Failover Settings** part. This function is disabled by default. When this function is enabled, the page is shown as below.

Failover Settings

Failover ⚠

Connection Type

DNS Settings

5.3.2 Example of setting up Failover connection

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

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

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

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

Configuring procedures:

- Step 1** Connect the WAN/LAN port of the router to the LAN port of your smart home gateway.
- Step 2** [Log in to the web UI of the router](#).
- Step 3** Navigate to **Internet Settings**.

- Step 4** Enable the **Failover** function.
- Step 5** Set **Connection Type** to **PPPoE**, and enter the **PPPoE Username** and **PPPoE Password** provided by your ISP.
- Step 6** Click **Connect**.

Failover Settings

Failover ⓘ

Connection Type

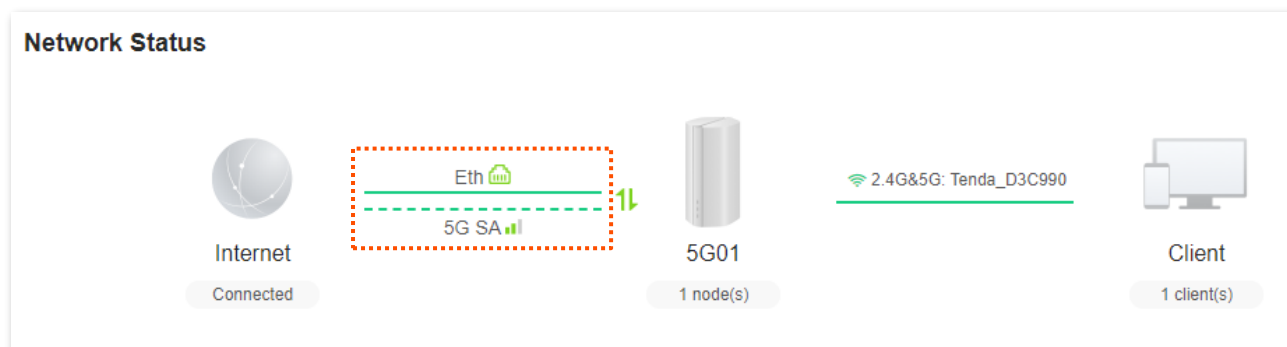
PPPoE Username

PPPoE Password

DNS Settings

---End

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



6 WiFi settings

6.1 Change the WiFi name and WiFi password

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

Step 2 Navigate to **WiFi Settings**.

Step 3 Enable or disable the **Unify 2.4 GHz & 5 GHz** function as required. The following figure shows an example of disabling the Unify 2.4 GHz & 5 GHz.

- Enable **Unify 2.4 GHz & 5 GHz**: The WiFi name and password of the 2.4 GHz and 5 GHz network on the router are the same, and only one WiFi name is displayed. When you connect to your router's WiFi network, you will automatically connect to the best quality WiFi.
- 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 WiFi network. If you have WiFi-enabled devices that only support 2.4GHz networks, you need to connect to the router's WiFi network, such as security cameras, you are recommended to disable the **Unify 2.4 GHz & 5 GHz**.

Step 4 Change the parameters of the 2.4 GHz WiFi network.

1. Change the **WiFi Name** of the 2.4 GHz WiFi network, which is **John_Doe_2.4GHz** in this example.
2. Set **Security**, which is **WPA2-PSK (Recommended)** in this example.
3. Change the **WiFi Password** of the 2.4 GHz WiFi network, which is **Tenda+Wireless24** in this example.

Step 5 Change the parameters of the 5 GHz WiFi network.

1. Change the **WiFi Name** of the 5 GHz WiFi network, which is **John_Doe_5GHz** in this example.
2. Set **Security**, which is **WPA2-PSK (Recommended)** in this example.
3. Change the **WiFi Password** of the 5 GHz WiFi network, which is **Tenda+Wireless5** in this example.

Step 6 Click **Save**.

WiFi Settings

Unify 2.4 GHz & 5 GHz

The 2.4 GHz WiFi network and 5 GHz WiFi network share the same WiFi name and WiFi password, so clients can automatically connect to the best WiFi network.

2.4 GHz WiFi

WiFi Name:

Security:

WiFi Password ⓘ:

5 GHz WiFi

WiFi Name:

Security:



WiFi Password ⓘ:

---End

When the configuration is completed, you can connect your WiFi-enabled devices to any WiFi networks of the router 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 WiFi networks share the same WiFi name and password. Devices connected to the WiFi network will use the network with better connection quality automatically.
2.4 GHz WiFi	You can enable or disable the 2.4 GHz WiFi network and 5 GHz WiFi network separately when the Unify 2.4 GHz & 5 GHz function is disabled. If the WiFi-enabled devices, such as smartphones, are far away from the router, or blocked from the router by a wall, it is recommended that the WiFi-enabled devices be connected to the 2.4 GHz WiFi network.
5 GHz WiFi	If the WiFi-enabled devices are close to the router, it is recommended that the WiFi-enabled devices be connected to the 5 GHz WiFi network.
WiFi Name	Specifies the WiFi network name (SSID) of the corresponding WiFi network.

Parameter	Description
Security	<p>Specifies the encryption modes supported by the router, including:</p> <ul style="list-style-type: none"> - Not encrypted: Specifies that the WiFi network is not encrypted and any clients can access the network without a password. This option is not recommended as it leads to low network security. - WPA2-PSK (Recommended): The network is encrypted with WPA2-PSK/AES. - WPA3-SAE/WPA2-PSK: The network is encrypted with both WPA3-SAE and WPA2-PSK, improving both security and compatibility. <p> TIP</p> <p>WPA3-SAE is the upgraded version of WPA2-PSK. If your WiFi-enabled device does not support WPA3-SAE, or you get poor WiFi experience, it is recommended to use WPA2-PSK (Recommended).</p>
WiFi Password	<p>Specifies the password for connecting to the WiFi network. You are strongly recommended to set a WiFi password for security.</p> <p> TIP</p> <p>It is recommended to use the combination of numbers, uppercase letters, lowercase letters and special symbols in the password to enhance the security of the WiFi network.</p>

6.2 Configure guest WiFi

6.2.1 Overview

On this page, you can enable or disable the guest WiFi function and change the WiFi name and password of the guest WiFi.

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

To access the configuration page, [log in to the web UI of the router](#) and navigate to **More > Guest WiFi**. This function is disabled by default. When this function is enabled, the page is shown as below.

Guest WiFi

Clients connecting to the guest network can only access the internet and communicate with other clients under the guest network.

Guest WiFi

2.4 GHz WiFi Name

5 GHz WiFi Name

WiFi Password 🔒

Validity ▼

Shared Bandwidth ▼

Parameter description

Parameter	Description
Guest WiFi	Used to enable or disable the guest WiFi function.
2.4 GHz WiFi Name	Specify the WiFi names of the router's guest WiFi networks.
5 GHz WiFi Name	To distinguish the guest WiFi from the main network, you are recommended to set different WiFi network names.
WiFi Password	Specifies the password for the router's two guest WiFi networks.

Parameter	Description
Validity	Specifies the validity of the guest WiFi. The guest WiFi function will be disabled automatically out of the validity period.
Shared Bandwidth	Specifies the maximum upload and download speed for all devices connected to the guest WiFi.

6.2.2 Example of setting the guest WiFi

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

Requirements: Prevent the use of WiFi network by guests from affecting the network speed of your computer for work purposes.

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

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

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

Configuration procedure:

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

Step 2 Navigate to **More > Guest WiFi**.

Step 3 Enable **Guest WiFi**.

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

Step 5 Set the **5 GHz WiFi Name**, which is **John_Doe_5G** in this example.

Step 6 Set the **WiFi Password**, which is **Example123** in this example.

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

Step 8 Set the bandwidth in the **Shared Bandwidth** drop-down box, which is **20 Mbps** in this example.

Step 9 Click **Save**.


Guest WiFi

Clients connecting to the guest network can only access the internet and communicate with other clients under the guest network.

Guest WiFi

2.4 GHz WiFi Name

5 GHz WiFi Name

WiFi Password 

Validity ▼

Shared Bandwidth ▼

---End

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

7 Network status

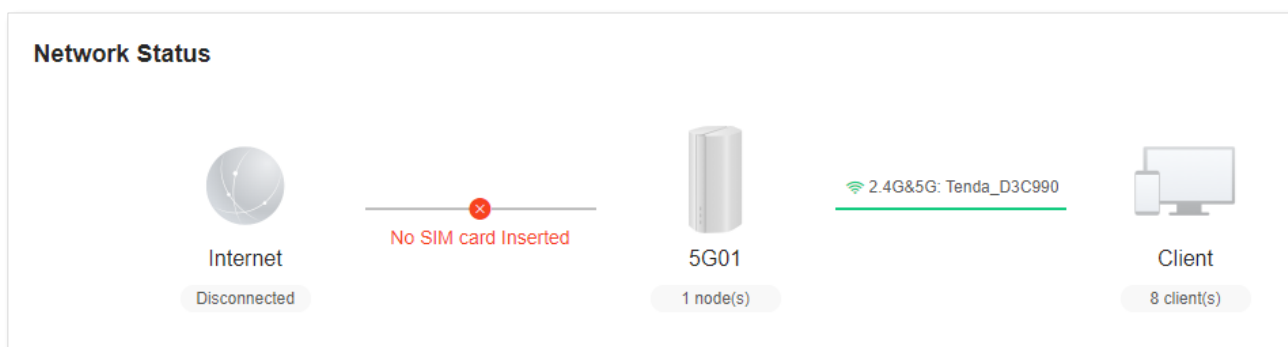
7.1 View network status

7.1.1 Access internet through a SIM card

To access the configuration page, [log in to the web UI of the router](#), and navigate to **Network 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 Inserted**” is shown between the internet and the router, ensure the SIM card is inserted properly.



SIM card blocked

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

APN not correctly identified

When “**APN not correctly identified**” is shown between the internet and the router, it indicates that you need to configure the correct APN parameters. Click [APN not correctly identified](#) to navigate to the **Internet Settings** page and modify APN parameters.

Data traffic disabled

When “**The data traffic has been manually disabled. Please enable it.**” is shown between the internet and the router, ensure that the **Mobile Data** function is enabled on the **Internet Settings** page.

Network connection disabled

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

Monthly data limit reached

When “**The monthly data limit is reached.**” is shown between the internet and the router, it indicates that the router will disconnect from the internet automatically when the limit is reached. Refer to [Data Limit](#) to modify the related parameters.

Connection failed

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

Try the following solutions:

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

7.1.2 Access internet through the WAN port

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

The connection type **PPPoE** is used for illustration here.



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

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

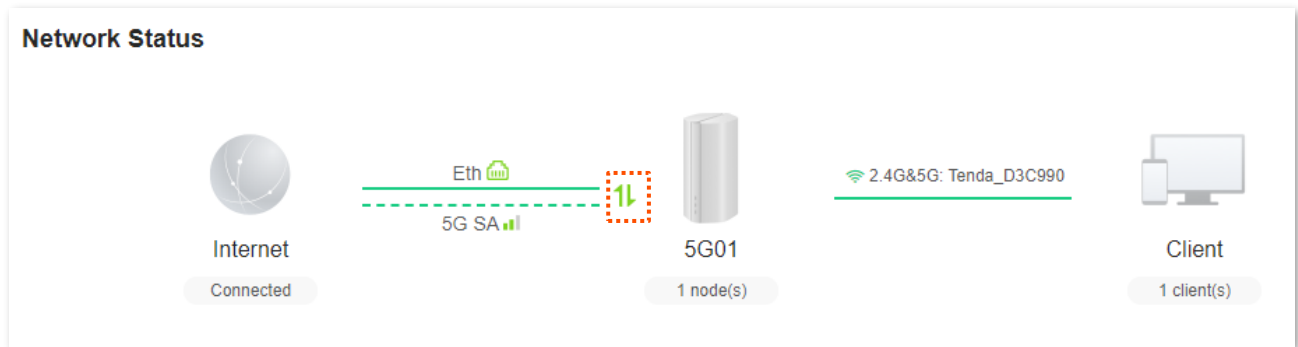
When “**No response from the remote server.**” is shown between the internet and the router, it indicates that the upstream server network may be abnormal. Contact your ISP for help.

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.

7.1.3 Access internet through SIM card and WAN port

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



TIP

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

7.2 View WAN status

On this page, you can view the WAN status, including 4G/5G WAN status, Ethernet WAN status and IPv6 status.

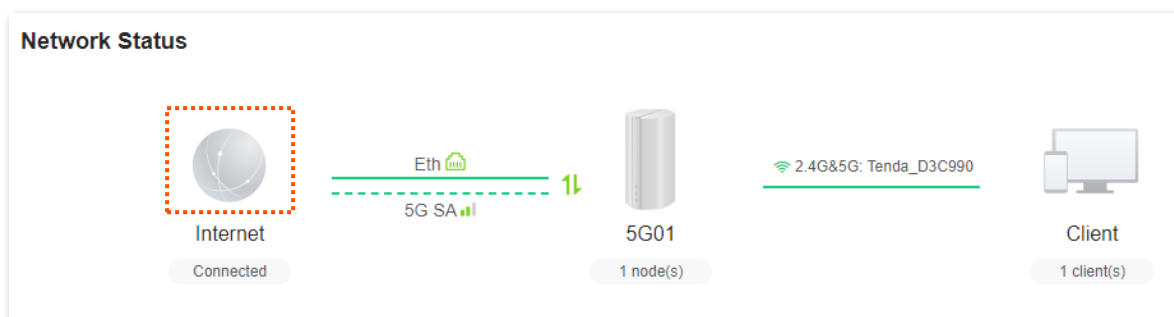


Before checking the Ethernet WAN status, you should connect the WAN/LAN port of the router to the internet using an Ethernet cable, enable the Failover function and configure internet parameters on the **Internet Settings** page.

To access the page:

- Method 1

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



- Method 2

[Log in to the web UI of the router](#), and navigate to **More > Information > WAN Status**.

7.2.1 View 4G/5G WAN status

In this part, you can view the information of the SIM card and 4G/5G network.

4G/5G WAN informations	
SIM card status	Ready
SIM card number	[REDACTED]
Signal Strength	Good
ISP name	[REDACTED]
Cellular access type	5G SA
Connecting frequency bands	[REDACTED]
Registration time	Wed Jul 3 14:38:38 2024
NR PCI	[REDACTED]
Cell ID	[REDACTED]
Data	1.48GB(Total usage)
Download Speed	0.00KB/s
Upload Speed	0.04KB/s
IP address	[REDACTED]
Subnet mask	255.255.255.0
Default gateway	[REDACTED]
Primary DNS	[REDACTED]
Secondary DNS	[REDACTED]
MAC address	[REDACTED]

Parameter description

Parameter	Description
SIM card status	Specifies the SIM card status inserted in the router.
SIM card number	Specifies the SIM card number inserted in the router.
Signal Strength	Specifies the signal strength of 4G/5G mobile network, including Excellent , Good and Fair .
ISP name	Specifies the ISP name of the SIM card.
Cellular access type	Specifies the current network type for internet access.
Connecting frequency bands	Specifies the 4G/5G band that the router is working in.

Parameter	Description
Registration time	Specifies the time of the network registration.
NR PCI	Specify the Cell information for the current registered network.
Cell ID	
Data	Specifies the data traffic of the SIM card that has been used.
Download Speed	Specify the current upload and download speed of the mobile network of the router.
Upload Speed	
IP address	Specifies the IP address of the router obtained from the ISP.
Subnet mask	Specifies the subnet mask of the mobile network.
Default gateway	Specifies the gateway IP address of the router.
Primary DNS	Specify the IP address of primary and secondary DNS servers of the router.
Secondary DNS	
MAC address	Specifies the 4G/5G MAC address of the router.

7.2.2 View Ethernet WAN status

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

Ethernet WAN Status	
Internet Connection Status	Connected
Internet Connection Type	PPPoE
Connected time	48minute(s)
IP Address	
Subnet Mask	255.255.255.255
Default gateway	
Primary DNS	
Secondary DNS	
MAC Address	

Parameter description

Parameter	Description
Internet Connection Status	Specifies internet connection status of WAN port connected to the Ethernet cable.
Internet Connection Type	Specifies how your router connects to the internet, including: <ul style="list-style-type: none"> - PPPoE: Select this type if you access the internet using the PPPoE user name and PPPoE password. - Dynamic IP Address: Select this type if you can access the internet by simply plugging in an Ethernet cable. - Static IP Address: Select this type if you want to access the internet using fixed IP information.
Connection time	Specifies the connection duration of WAN port connected to the Ethernet cable.
IP Address	Specifies the IP address of the router obtained from the ISP.
Subnet Mask	Specifies the WAN subnet mask of the router.
Default gateway	Specifies the gateway IP address of the router.
Primary DNS	Specify the IP address of primary and secondary DNS servers of the router.
Secondary DNS	
MAC Address	Specifies the Ethernet MAC address of the router.

7.2.3 View IPv6 status

In this part, you can view the IPv6 status information of the router.

IPv6 Status	
Connection Type	DHCP
IPv6 WAN Address	
Default IPv6 Gateway	
Primary IPv6 DNS	
Secondary IPv6 DNS	
IPv6 LAN Address	

Parameter description

Parameter	Description
Connection Type	Specifies the IPv6 connection type of the router.
IPv6 WAN Address	Specifies the WAN IPv6 address of the router.
Default IPv6 Gateway	Specifies the primary DNS server address of IPv6 network.
Primary IPv6 DNS	Specify the primary and secondary DNS server addresses of IPv6 network.
Secondary IPv6 DNS	
IPv6 LAN Address	Specifies the LAN IPv6 address of the router.

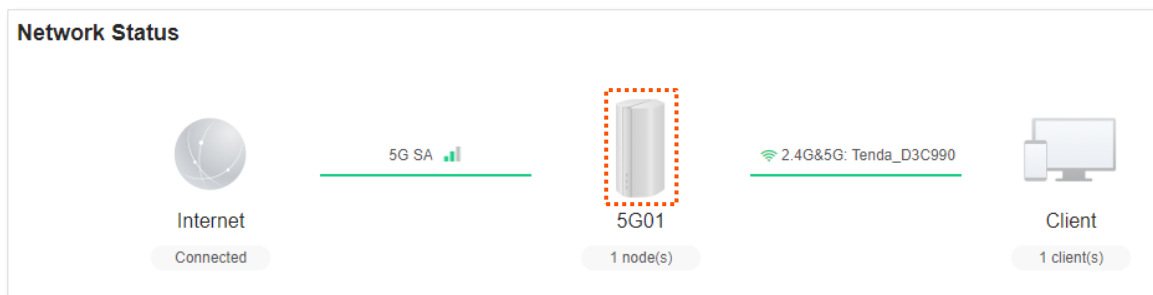
7.3 View system information

On this page, you can view the system information, including system time, runtime, firmware version, hardware version, LAN status and WiFi status.

To access the page:

Method 1

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

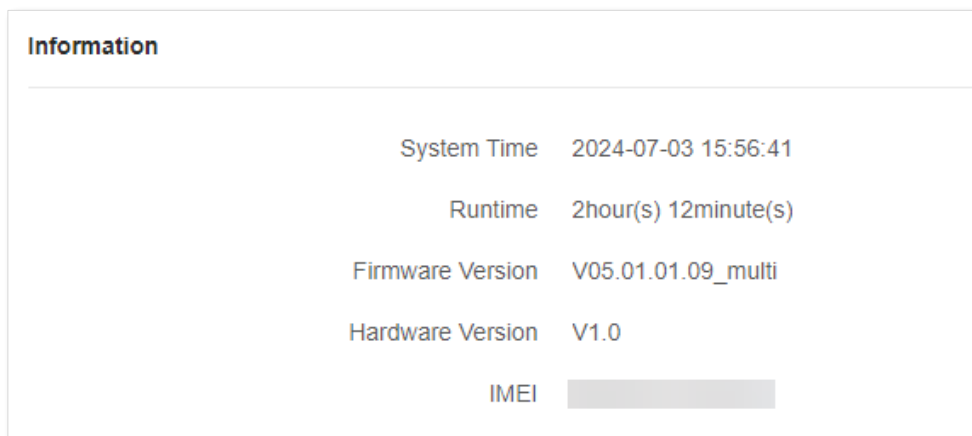


Method 2

[Log in to the web UI of the router](#), and navigate to **More > Information > System Status**.

7.3.1 View basic information

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



Parameter description

Parameter	Description
System Time	Specifies the system time of the router.
Runtime	Specifies operating time of the router since it is powered on.

Parameter	Description
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.

7.3.2 View LAN status

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

LAN Status	
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
MAC Address	

Parameter description

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

7.3.3 View WiFi status

In this part, you can view the information of 2.4 GHz and 5 GHz WiFi network, including the visibility, WiFi name and security.

Wi-Fi Status

2.4 GHz WiFi Status

Status Visible

Wi-Fi Name Tenda_D3C990

Security WPA2-PSK (Recommended)

Channel

Bandwidth 20

MAC Address

5 GHz WiFi Status

Status Visible

Wi-Fi Name Tenda_D3C990

Security WPA2-PSK (Recommended)

Channel

Bandwidth 80

MAC Address

Parameter description

Parameter	Description
Status	Specifies whether the corresponding WiFi networks are enabled or disabled and whether they are visible.
WiFi Name	Specifies the 2.4 GHz WiFi or 5 GHz WiFi names of the router.
Security	Specifies the encryption mode of the respective WiFi network.
Channel	Specifies the channel that the respective WiFi network works in.
Bandwidth	Specifies the bandwidth of the respective WiFi network.
MAC Address	Specifies the MAC address of the respective WiFi network.

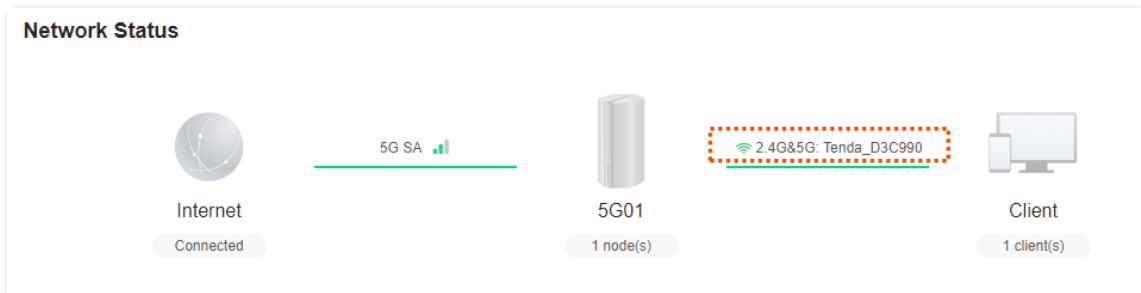
7.4 View wireless information

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

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

Step 2 Navigate to **Network Status**.

Step 3 Click the WiFi name of the router.



---End

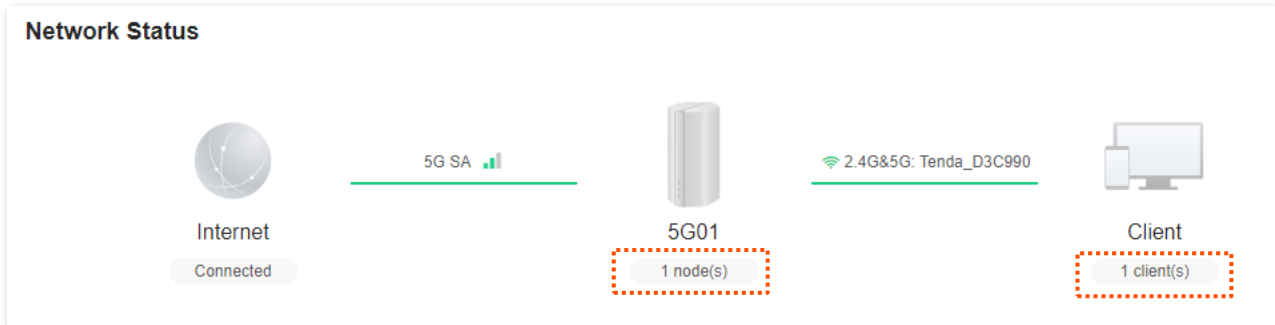
You can change wireless parameters as required. For details, see [WiFi settings](#).

The screenshot shows the 'WiFi Settings' page. It includes a toggle for 'Unify 2.4 GHz & 5 GHz' which is turned on. Below this, there is a text box for 'WiFi Name' containing 'Tenda_D3C990', a dropdown for 'Security' set to 'WPA2-PSK (Recommended)', and a text box for 'WiFi Password' with masked characters. A 'Save' button is located at the bottom.

7.5 View the number of Mesh nodes and clients

In this page, you can view the total number of Mesh nodes and clients on the **Network Status** page.

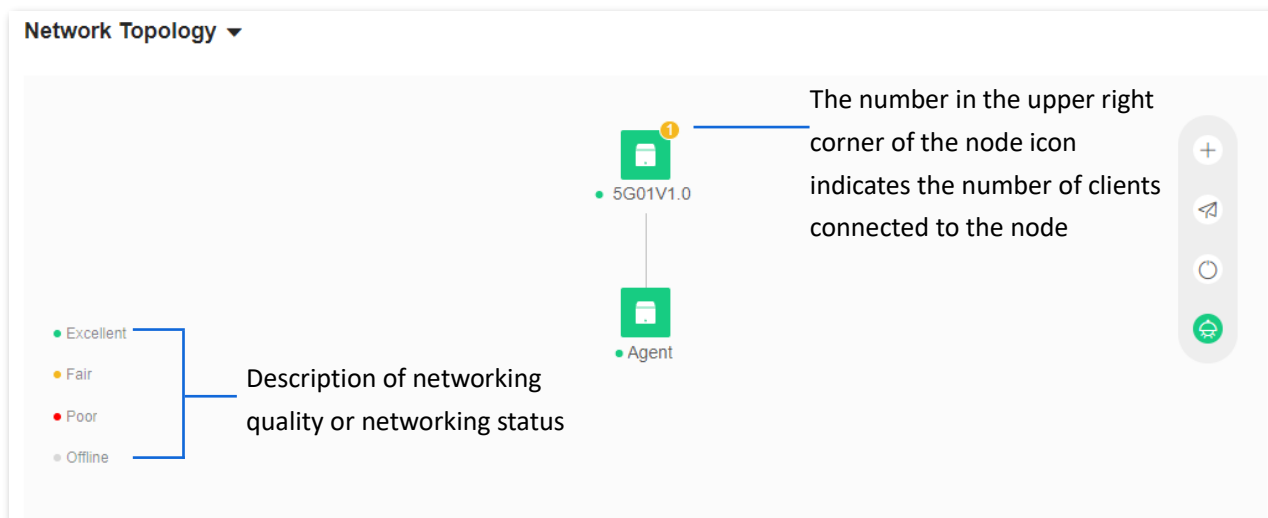
If you want to view or set up more device information, refer to [Client management](#).




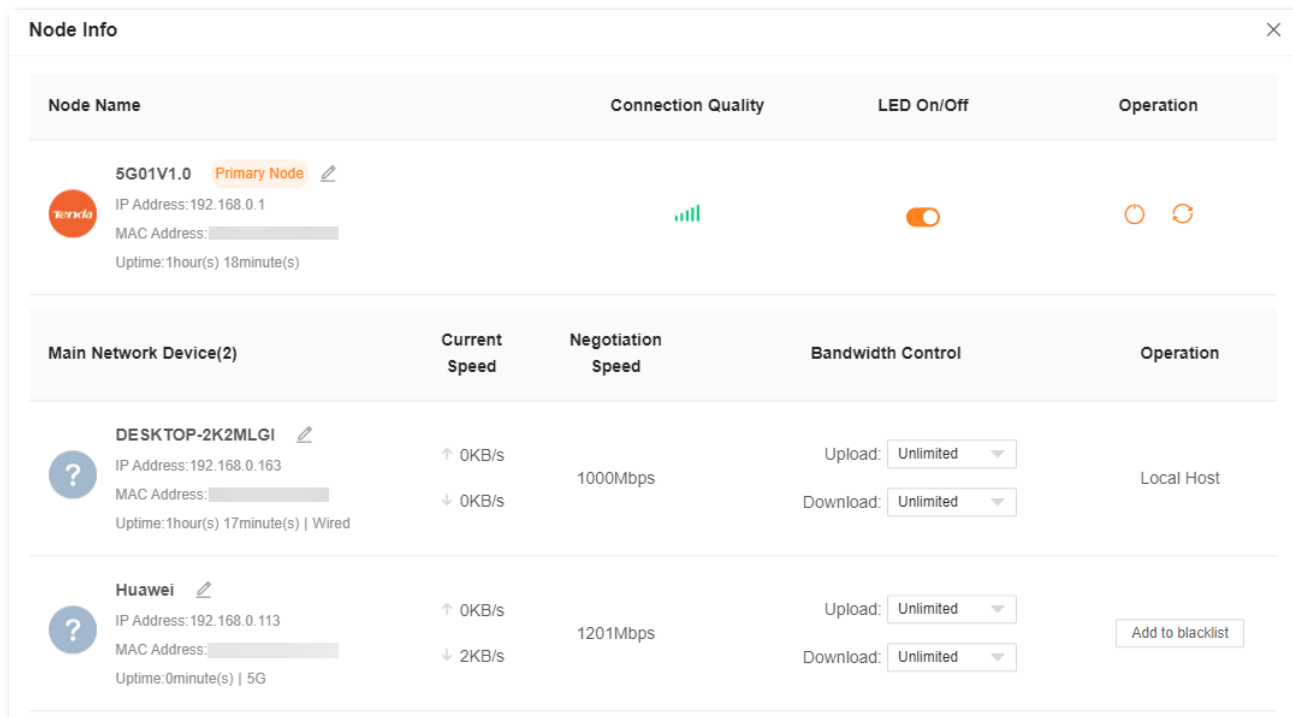
7.6 View network status, node and client details

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







In the **Network Topology** module, you can view the networking conditions, the number of Mesh nodes, the quality of networking connections, and the number of clients connected to a node.






Click  to view detailed information about the node, including IP address, MAC address, uptime, and client's information connected to the node.



Parameter description

Parameter	Description
	Used to add a new node for Mesh networking.
	Used to optimize WiFi networks with one click.  TIP When your clients are stuck for internet access or cannot receive WiFi signals, you can optimize the WiFi network with one click.
	Used to reboot all nodes.  TIP Rebooting the node will disconnect all connections. Perform this operation when the network is relatively idle.
	Used to turn on or turn off indicators on all nodes.
Node Name	Specifies the Mesh node name, IP address, MAC address and uptime.
Connection Quality	Specifies the network quality of the nodes.
LED On/Off	Used to turn on or turn off the indicator display of the node.
Main Network Device	Specifies the name, IP address, MAC address, uptime, and access mode of the clients currently connected to the node. You can customize the clients name as required.
Offline Device	Specifies the name and MAC address of the clients connected to the Mesh network. You can customize the clients name as required.
Current Speed	Specifies the real-time upload and download speed of the clients.
Negotiation Speed	Specifies the maximum speed negotiation between the clients and the node.
Bandwidth Control	Used to limit the maximum upload and download speed of the clients.

Parameter	Description
Operation	<p>Perform operations on nodes or clients.</p> <ul style="list-style-type: none"> <li data-bbox="430 302 1404 414">–  : Used to reboot the node. During the reboot, all connections will be disconnected. Therefore, perform this operation when the network is relatively idle. <li data-bbox="430 436 1404 571">–  : Used to restore the primary node to factory settings. After the primary node is restored to factory settings, the entire network cannot access the internet, and you need to reconfigure the internet settings. You are recommended to Back up configuration of the primary node before restoring the factory settings. <li data-bbox="430 593 1404 705">–  : Used to remove a secondary node. Removing a node narrow the WiFi coverage, and the removed node will no longer join the current network automatically. <li data-bbox="430 728 1404 817">– Add to blacklist: Used to add the clients to the blacklist. The clients displayed as Local Host belongs to the current management network and cannot be added to the blacklist. <li data-bbox="430 840 1021 873">– Delete: Used to delete selected offline devices.

8 Client management

8.1 Add a client to the blacklist

8.1.1 Method 1

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

Step 2 Navigate to **Client Management**.

Step 3 Locate the device that not allowed to access the internet and click **Add to blacklist**. The following figure is for reference only.

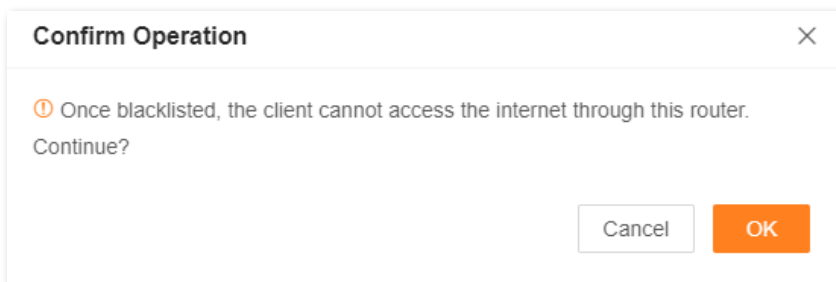
The screenshot shows the 'Client Management' interface with a table of devices. The table has columns for device name, current speed, negotiation speed, bandwidth control, and operation. Two devices are listed: 'DESKTOP-2K2MLGI' and 'Huawei'. The 'Huawei' device has a blue hand icon pointing to the 'Add to blacklist' button.

Main Network Device(2)	Current Speed	Negotiation Speed	Bandwidth Control	Operation
DESKTOP-2K2MLGI IP Address: 192.168.0.163 MAC Address: [REDACTED] Uptime: 1hour(s) 2minute(s) Wired	↑ 0KB/s ↓ 0KB/s	1000Mbps	Upload: Unlimited Download: Unlimited	Local Host
Huawei IP Address: 192.168.0.113 MAC Address: [REDACTED] Uptime: 0minute(s) 5G	↑ 4KB/s ↓ 2KB/s	1201Mbps	Upload: Unlimited Download: Unlimited	Add to blacklist

Parameter description

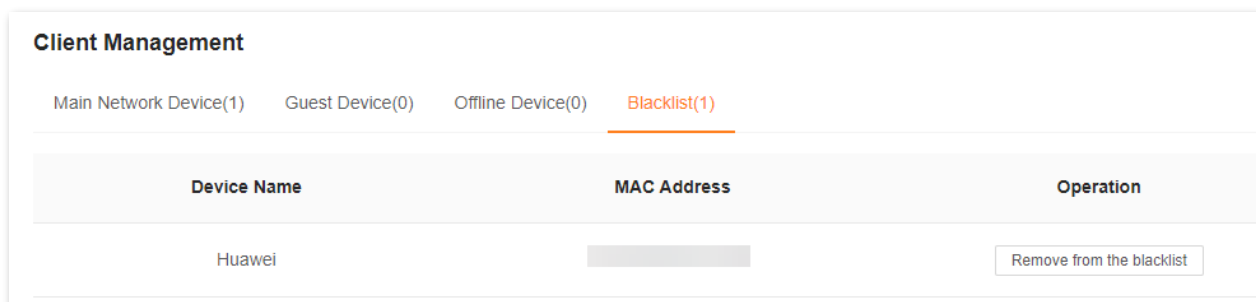
Parameter	Description
All Nodes	Used to filter the clients connected to each node. When a router is networked with other routers through Mesh networking, you can click the primary node name or other node name to display only the devices under the corresponding node.
Main Network Device	Specifies the clients connected to the main network.
Guest Device	Specifies the clients connected to guest WiFi.
Offline Device	Specifies the clients that has been connected to the router network.
Blacklist	Specifies the clients cannot access the internet through the router.

Step 4 Click **OK**.



---End

The client is removed from the device list and displayed on the blacklist now.

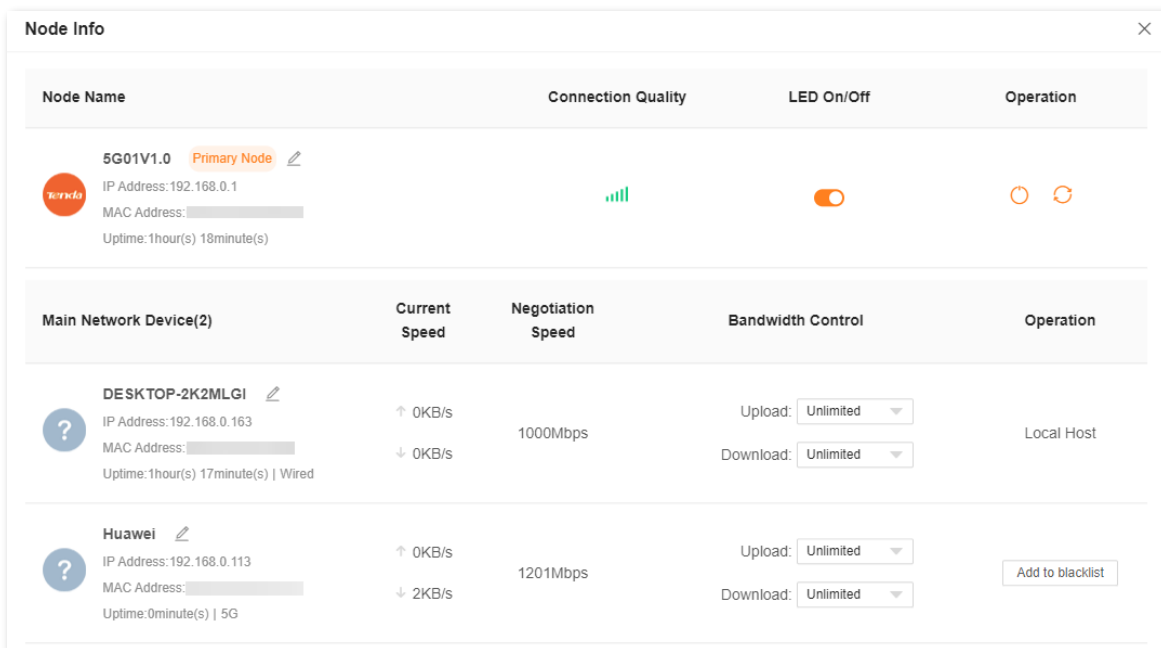


8.1.2 Method 2

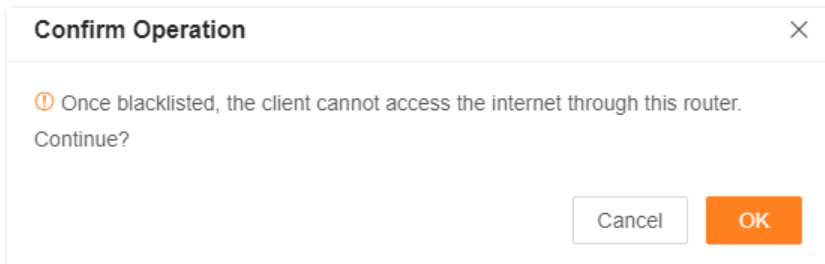
Step 1 [Log in to the web UI of the router.](#)

Step 2 Click  in the **Network Topology** module of the **Network Status**.

Step 3 Locate the device that disallowed to access the internet on **Node Info**, and click **Add to blacklist**. The following figure is for reference only.



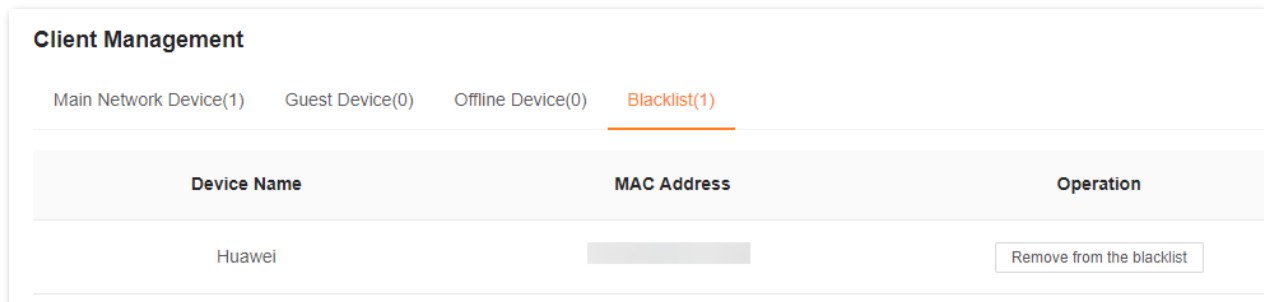
Step 4 Click **OK**.



---End

Navigate to **Client Management**, and click **Blacklist**. You can view the blacklisted devices.

A blacklisted device cannot access the internet through a router.



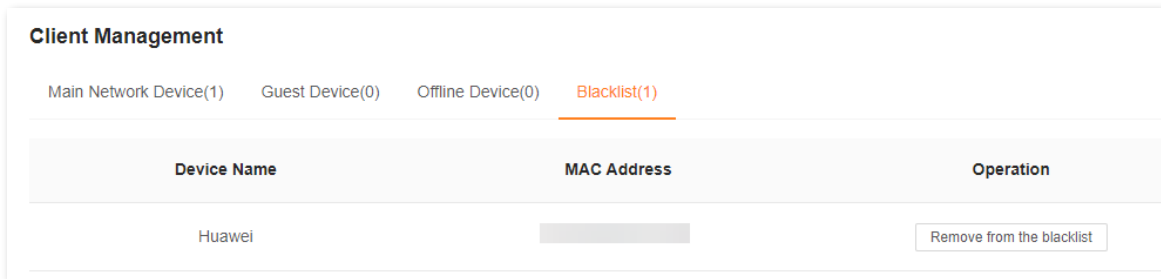
8.2 Remove a client from the blacklist

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

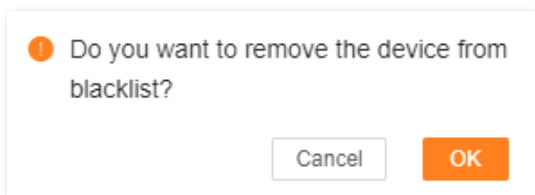
Step 2 Navigate to **Client Management**.

Step 3 Select **Blacklist** on the right.

Step 4 Click **Remove from the blacklist** under **Operation** in the line of the client to be removed from the blacklist.



Step 5 Click **OK**.



---End

The client is removed from the blacklist. It can access the network upon the next connection.

8.3 Internet access speed control

You can control the bandwidth of the devices connected to the router, so that the limited bandwidth is properly allocated.

Configuration procedure:

- Step 1** [Log in to the web UI of the router.](#)
- Step 2** Navigate to **Client Management**.
- Step 3** Locate the device according to the device name, and set the maximum speed for **Upload** and **Download**.

In this example, set **Download** to **512KB/s**. Click the drop-down list of **Download**, select **Custom (KB/s)**, enter **512**, and click anywhere on the page. The system automatically saves the settings.

The screenshot shows the 'Client Management' interface. At the top, there are tabs for 'Main Network Device(1)', 'Guest Device(0)', 'Offline Device(1)', and 'Blacklist(0)'. A dropdown menu is set to 'All Nodes'. Below this is a table with columns: 'Main Network Device(1)', 'Current Speed', 'Negotiation Speed', 'Bandwidth Control', and 'Operation'. The device 'DESKTOP-2K2MLGI' is listed with IP Address: 192.168.0.163, MAC Address: [redacted], and Uptime: 2minute(s) | Wired. Its Current Speed is 0KB/s (upload) and 0KB/s (download). Negotiation Speed is 1000Mbps. Under Bandwidth Control, Upload is set to 'Unlimited' and Download is set to '512 KB/s'. The Operation column shows 'Local Host'.

---End

After the configuration is completed, the maximum download speed of the device for which **Bandwidth Control** is set to **512KB/s**.

Parameter description

Parameter	Description
Current Speed	Specifies the real-time upload and download speed of the client.
Negotiation Speed	Specifies the connection speed negotiated between the client and the router.
Bandwidth Control	Used to limit the maximum upload and download speed used by the router.

8.4 Example of setting MAC address filter

With the MAC address filter function, you can add the client to the blacklist. It indicates that the specified client is prohibited from accessing the internet through the router.

Scenario: You want to prohibit your kid's phone and computer from accessing the internet.

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

Assume that:

Client	MAC address	Status
Your kid's phone	42:C6:4D:2B:D8:16	Connected
Your kid's computer	98:9C:57:19:D0:1B	Disconnected


Configuration procedure:

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

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

Step 3 Enable **MAC Address Filter.**

Step 4 Add the kid's computer to the blacklist.

1. Click .
2. Select **Manual** in **Select Device.**
3. Set **Device Name**, which is **Kid's computer** in this example.
4. Enter **MAC Address** of the client, which is **98:9C:57:19:D0:1B** in this example.
5. Click **OK.**

Step 5 Add the kid's phone to the blacklist.

1. Click .
2. Select the kid's phone name in the **Select Device**, which is **Huawei** in this example.
3. Click **OK.**

Step 6 Click **Save.**



MAC Address Filter

Allow or disallow internet access through this router for specified clients.

MAC Address Filter

Filter mode Blacklist(Only block internet access from client with listed MAC address)

Blacklist Device +

Device Name	MAC Address	Operation
Kid's computer	98:9C:57:19:D0:1B	
Huawei	42:C6:4D:2B:D8:16	

2 items in total < 1 >

---End

After the configuration is completed, devices with MAC addresses of 98:9C:57:19:D0:1B and 42:C6:4D:2B:D8:16 cannot access the internet through the router.

8.5 Configure parental control

8.5.1 Overview

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

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

You can click **Add Parental Control Rule** to configure the parental control function.

Add Parental Control Rule ✕

Client

Group Name

Selected clients +

Control Period

Internet Access → ⌵ Mon. ✕ +6 ⌵

[Add control period](#)



URL Filter

Filter mode Only block access to listed URLs
 Only allow access to listed URLs

URL

[Add URL](#)

Parameter description

Parameter	Description
Client	Group Name Specifies the name of the client group that the parental control rule applies to.
	Selected clients Specifies the clients that the parental control rule applies to.
Control Period	Used to enable or disable the internet access control period function.
Internet Access	Used to set the internet access control period of the specified clients.  TIP If you want to set more than one periods, click Add control period .
URL Filter	Used to enable or disable the URL filter function.
Filter mode	Specifies the website filter mode.
URL	Specifies the websites that the Selected clients are blocked from accessing or allowed to access.  TIP – If you want to set more than one URL, click Add URL . – URL filter supports keywords but does not support Chinese characters. If you want a precise limit, write the complete URL, for example: www.google.com.

8.5.2 Example of adding a parental control rule

Scenario: You want to configure your kid's internet access through the router. Your kid cannot access such websites as Facebook, Twitter, YouTube and Instagram from 8:00 to 22:00 on Sunday.

Requirements: Devices cannot access to websites, including kid's phones and computers.

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

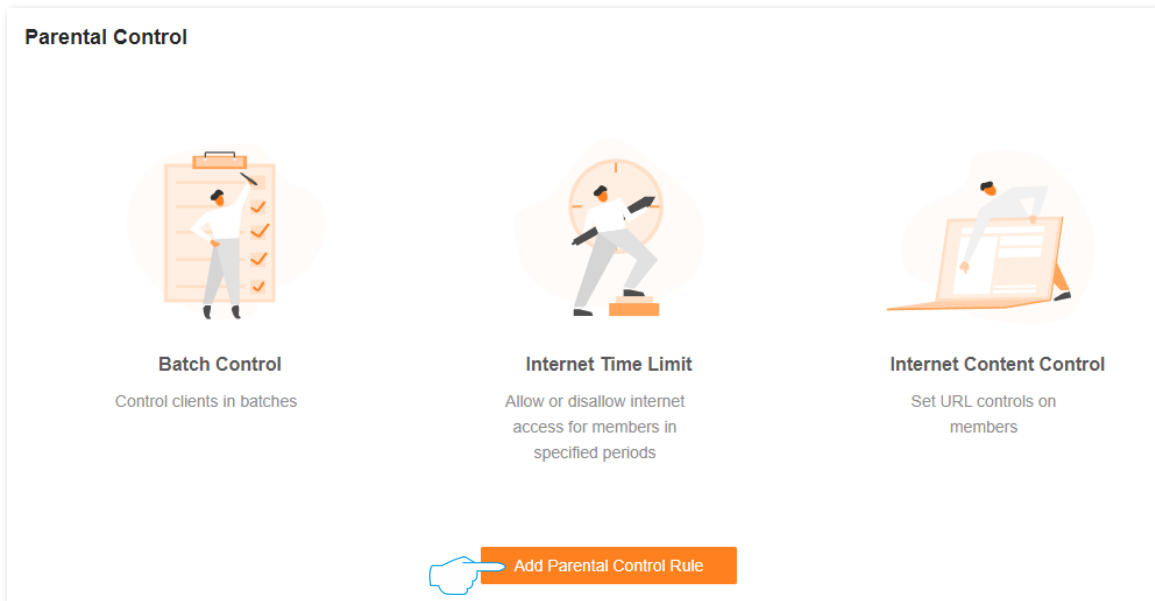
To add such a rule:

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

Step 2 Navigate to **Parental Control**.

Step 3 Set parental control rule.

1. Click **Add Parental Control Rule**.



2. Set **Group Name**, which is **Kid's phone and computer** in this example.
3. Click **+** beside **Selected clients**.
4. Enable **Control Period**, and set control period of the client, which are **08:00-22:00** and **Sun.** in this example.



TIP
By default, the internet access period is set to Monday to Sunday. If the requirements are different, manually change it.

5. Enable **URL Filter**.
6. Set **Filter mode** to **Only block access to listed URLs**.
7. Enter **Facebook, Twitter, YouTube, and Instagram** for URL.
8. Click **Save**.

Add Parental Control Rule ✕

Client

Group Name

Selected clients

Control Period

Internet Access →

Add control period

URL Filter

Filter mode Only block access to listed URLs
 Only allow access to listed URLs

URL

Add URL

---End

After the configuration is completed, your kid cannot access Facebook, Twitter, YouTube and Instagram from 8:00 to 22:00 on Sunday.

9 Mobile settings

9.1 Data limit

9.1.1 Overview

On this page, you can view and update data usage statistics, and configure data usage settings, such as data usage limit and usage alert.

To access the configuration page, [log in to the web UI of the router](#), and navigate to **More > Mobile Settings > Data Limit**.

Data Limit

Monitor data usage and alert you when the threshold is reached.

Total Used 1.778 GB

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 GB

Usage Alert 80%

SMS Alert of Usage

Note: This function may cause SMS charges.

Monthly Data Statistics

Start Date

Parameter description

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

9.1.2 Example of data limit configurations

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

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

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

Assume that:

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

Configuration procedure:

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

Step 2 Navigate to **More > Mobile Settings > Data Limit**.

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

- Step 4** Enable **Data Limit**.
- Step 5** Set **Monthly Allowance** to **10**, and choose **GB** in the drop-down box.
- Step 6** Set **Usage Alert** to **80%**, and set **SMS Alert of Usage** to **188****5555**.
- Step 7** Enable **Monthly Data Statistics**.
- Step 8** Set **Start Date** to **1**, and click **Save**.

Data Limit

Monitor data usage and alert you when the threshold is reached.

Total Used 1.778 GB

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

Usage Alert 80%

SMS Alert of Usage

Note: This function may cause SMS charges.

Monthly Data Statistics

Start Date

---End

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



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

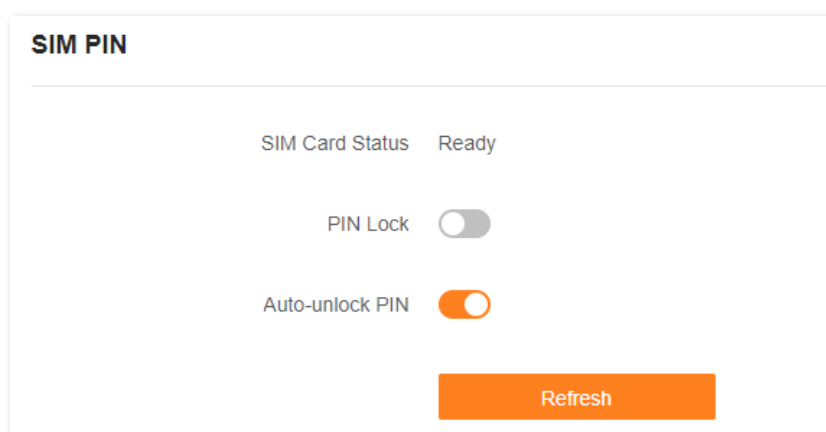
- Change the **Total Usage** by clicking **Update**.
- Disable **Data Limit**.
- Navigate to **Internet Settings**, and click **Connect** at the bottom of the page.

9.2 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 **More > Mobile Settings > SIM PIN**.

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



9.2.1 Unlock the SIM card

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

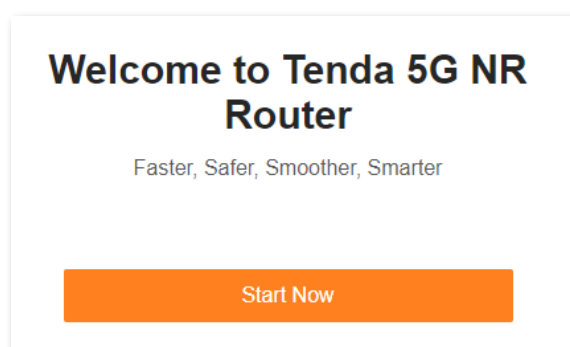
Unlock the SIM card in the quick setup wizard

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

Configuration procedure:

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

Step 2 Click **Start Now**.



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

Please unlock the SIM card

Auto-unlock PIN

Enable is recommended. The device will automatically unlock the PIN and start next time without manual unlocking.

PIN Code 3 attempts left

Save

 **NOTE**

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

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

---End

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

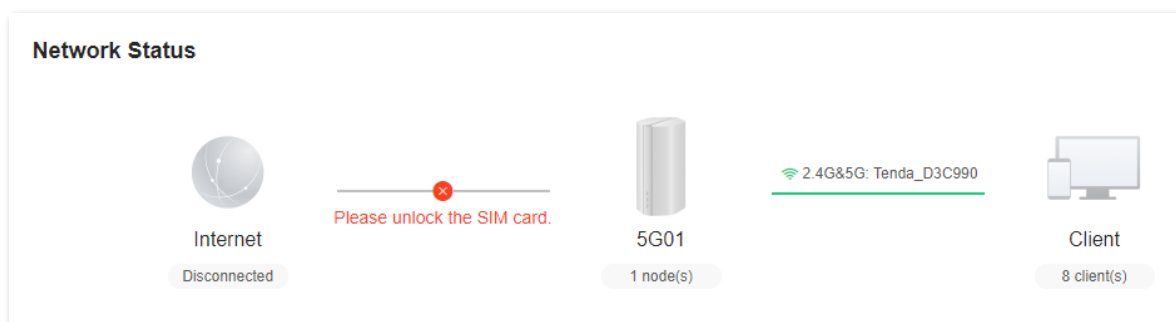
Unlock the SIM card on the web UI

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

Procedure:

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

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



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

SIM PIN

SIM Card Status PIN required

PIN Lock

Auto-unlock PIN

PIN Code 3 attempts left

Save

 **NOTE**

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

---End

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

9.2.2 Enable PIN lock for the SIM card

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



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

Configuration procedure:

- Step 1** [Log in to the web UI of the router.](#)
- Step 2** Navigate to **More > Mobile Settings > SIM PIN.**
- Step 3** Enable **PIN Lock.**
- Step 4** Specify a **PIN Code**, and click **Save.**

A screenshot of a web interface titled "SIM PIN". The page shows the following configuration options: "SIM Card Status" is "Ready"; "PIN Lock" is a toggle switch that is turned on; "Auto-unlock PIN" is a toggle switch that is turned on; "PIN Code" is a text input field containing the placeholder text "Please enter the PIN code" and "3 attempts left" to its right; and a large orange "Save" button at the bottom.

---End

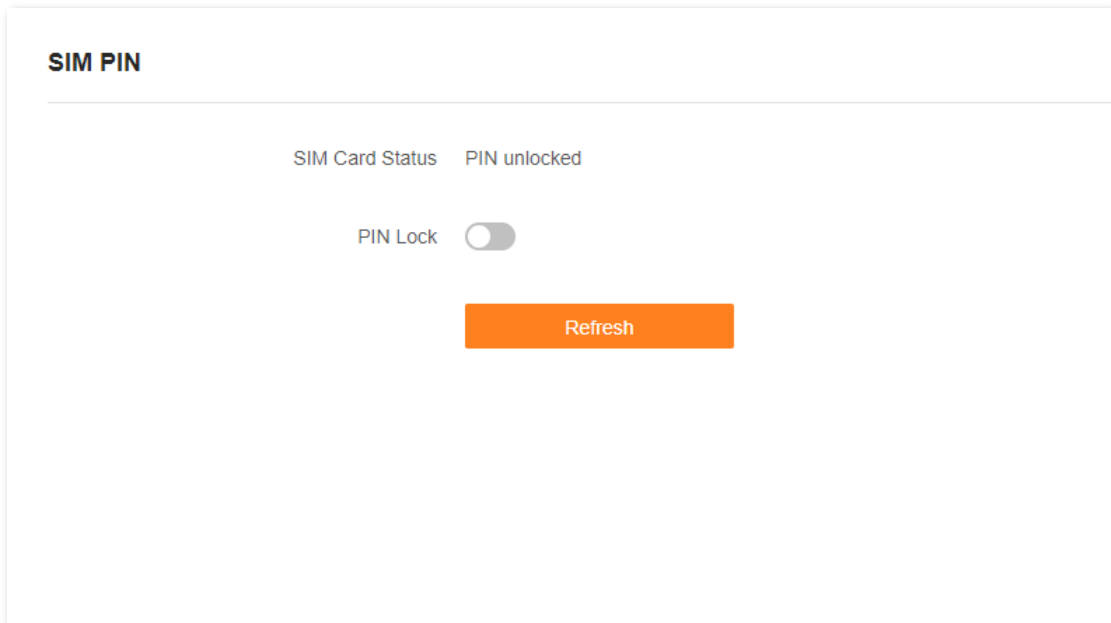
After the configuration is completed, the SIM card is protected by PIN lock.

9.2.3 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.

Configuration procedure:

- Step 1** [Log in to the web UI of the router.](#)
- Step 2** Navigate to **More > Mobile Settings > SIM PIN.**
- Step 3** Disable **PIN Lock.**



---End

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

9.2.4 Use PUK code to set PIN code

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

To access the configuration page, [log in to the web UI of the router](#), and navigate to **More > Mobile Settings > SIM PIN**.

SIM PIN

SIM Card Status	PUK required
PUK Code	<input type="text"/> 10 attempts left
New PIN Code	<input type="text"/>
Confirm New PIN Code	<input type="text"/>

9.3 ISP update

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



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.

Configuration procedure:

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

Step 2 Navigate to **More > Mobile Settings > ISP Update.**

Step 3 Click ⓘ , and click **www.tendacn.com** on the **ISP Update Help** page. The following figure is for reference only.

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



Step 4 Click **Select File** on the **ISP Update** page.

Step 5 Select and upload the ISP update file that has been downloaded in **Step 3**, and click **Update.**

ISP Update

Current Version V1.00.00.1_build240613 ⓘ

If you fail to dial-up Internet access after updating to the latest version, please contact us.

Select Upgrade File

No file chosen

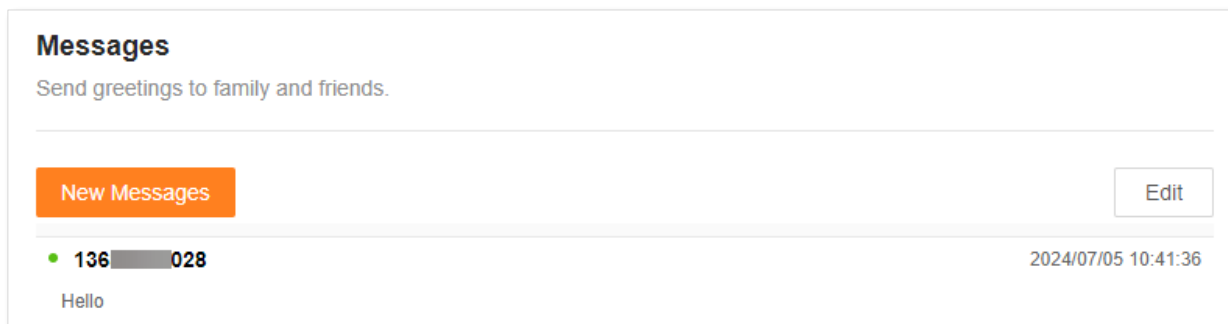
---End

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.

9.4 Manage SMS messages

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

To access the configuration page, [log in to the web UI of the router](#), and navigate to **More > Mobile Settings > Messages**.



9.4.1 Send SMS messages

Send SMS messages to a new phone number

- Step 1** [Log in to the web UI of the router](#).
- Step 2** Navigate to **More > Mobile Settings > Messages**.
- Step 3** Click **New Messages**.
- Step 4** Enter the phone number in the **Send To** column.
- Step 5** Enter the message content in the message column at the bottom.
- Step 6** Click **Send** at the bottom right corner.

Messages
Send greetings to family and friends.

← **New Messages**

Send To

← Enter the message content

Send

---End

Send SMS messages to an existing phone number

- Step 1** [Log in to the web UI of the router.](#)
- Step 2** Navigate to **More > Mobile Settings > Messages.**
- Step 3** Click the targeted phone number.

Messages
Send greetings to family and friends.

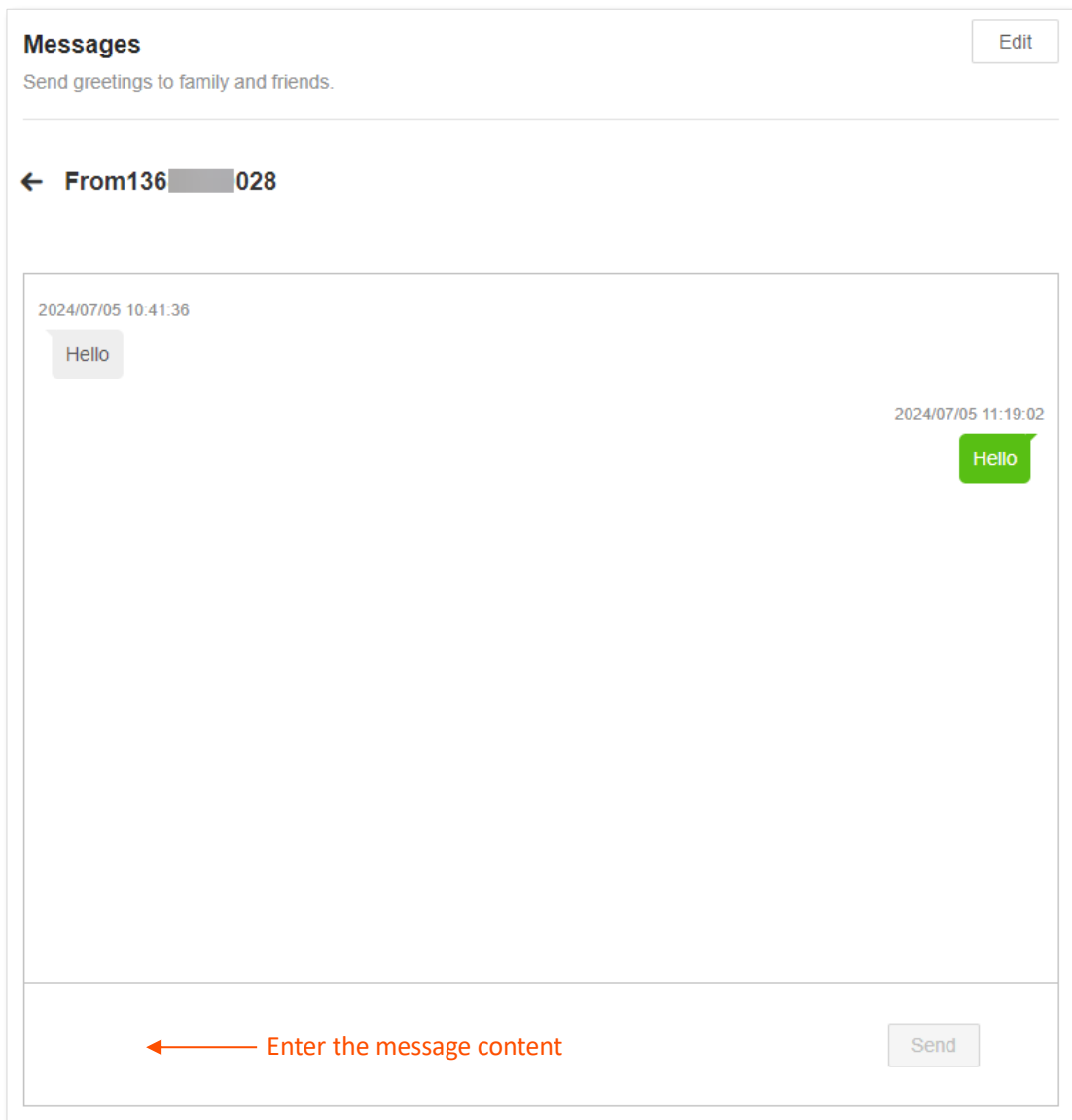
New Messages Edit

136 028 2024/07/05 10:41:36

Hello

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

Step 5 Click **Send**.

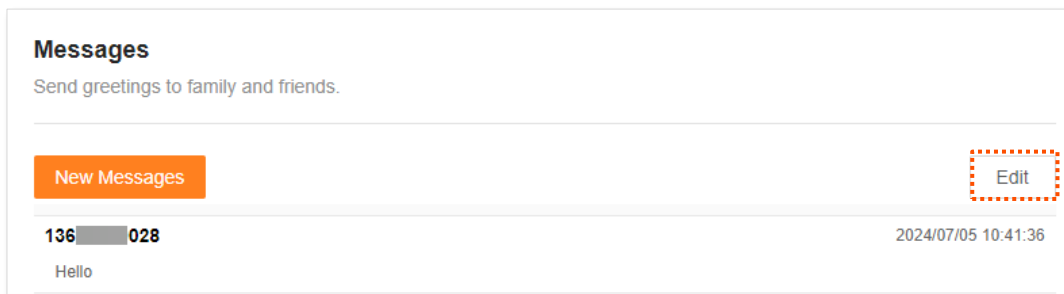


---End

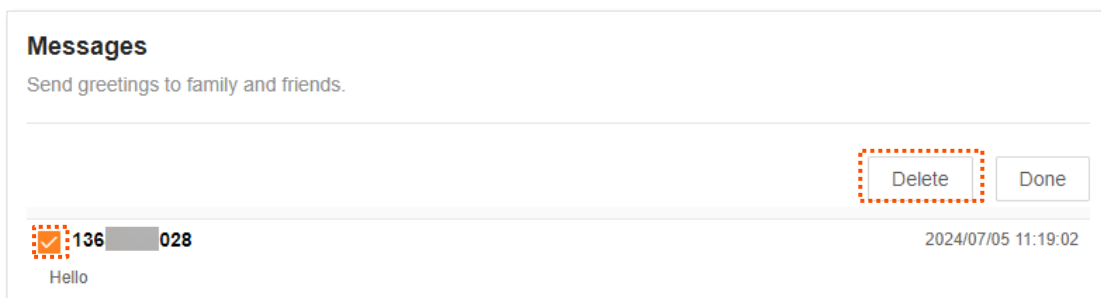
9.4.2 Delete SMS messages

Delete all messages of the same phone numbers

- Step 1** [Log in to the web UI of the router.](#)
- Step 2** Navigate to **More > Mobile Settings > Messages.**
- Step 3** Click **Edit.**



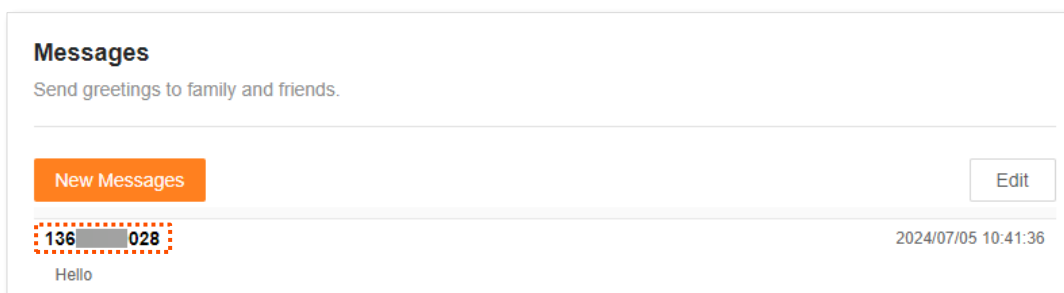
- Step 4** Select the phone number to be deleted.
- Step 5** Click **Delete** to delete messages of the phone numbers. (You can click **Done** to exit the editing mode).



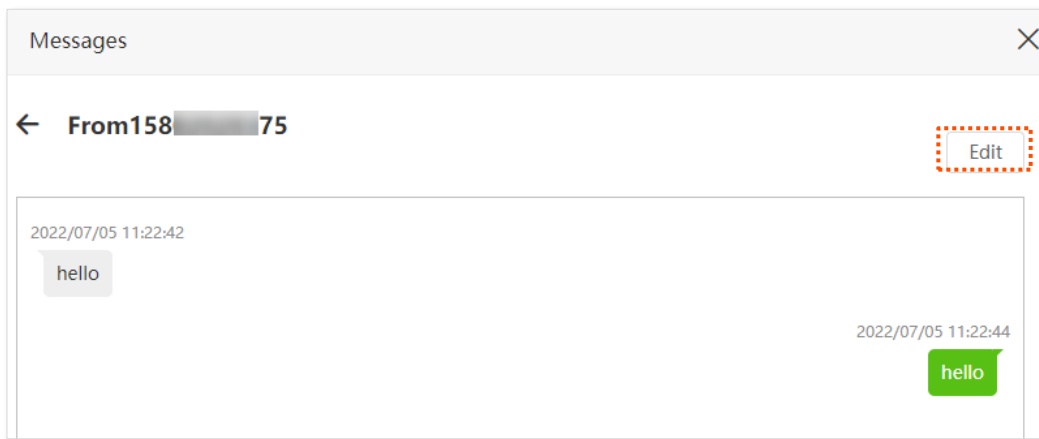
---End

Delete certain messages of the same phone number

- Step 1** [Log in to the web UI of the router.](#)
- Step 2** Navigate to **More > Mobile Settings > Messages.**
- Step 3** Click the targeted phone number.

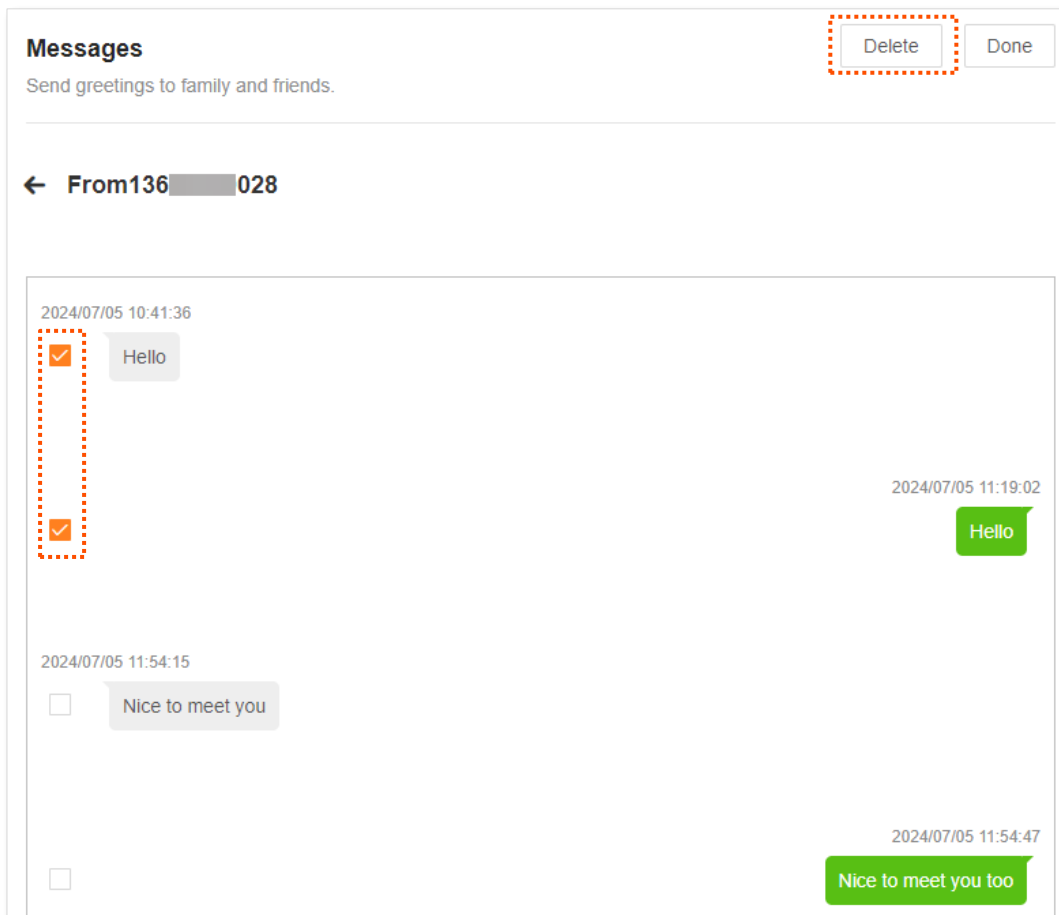


Step 4 Click **Edit**.



Step 5 Select the messages to be deleted.

Step 6 Click **Delete** (click **Done** to exit the editing mode).



---End

9.5 Inquire information by sending USSD commands

With the USSD function, 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.

Configuration procedure:

- Step 1** [Log in to the web UI of the router.](#)
- Step 2** Navigate to **More > Mobile Settings > USSD**.
- Step 3** Enter a **USSD CMD**, such as ***108#**.
- Step 4** Click **Send**.

A screenshot of a web interface titled "USSD". It features a text input field labeled "USSD CMD" containing the text "*108#". To the right of the input field is a button labeled "Send". Below the input field and button is a large, empty rectangular box, likely intended for displaying the response from the USSD command.

---End

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

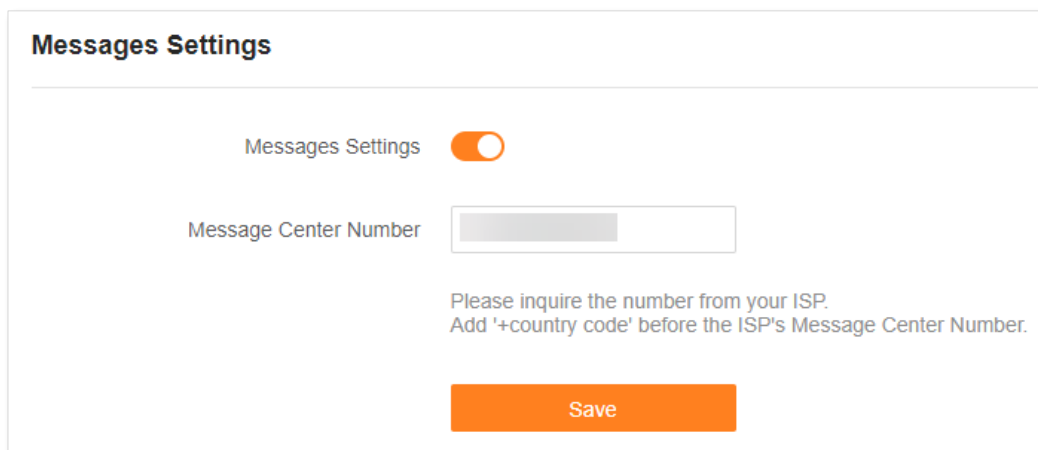
9.6 Set the message center number

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.

Configuration procedure:

- Step 1** [Log in to the web UI of the router.](#)
- Step 2** Navigate to **More > Mobile Settings > Messages Settings.**
- Step 3** Enable **Messages Settings.**
- Step 4** Enter the correct **Message Center Number** provided by your ISP.
- Step 5** Click **Save.**



Messages Settings

Messages Settings

Message Center Number

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

Save

---End

10


Optimize network performance

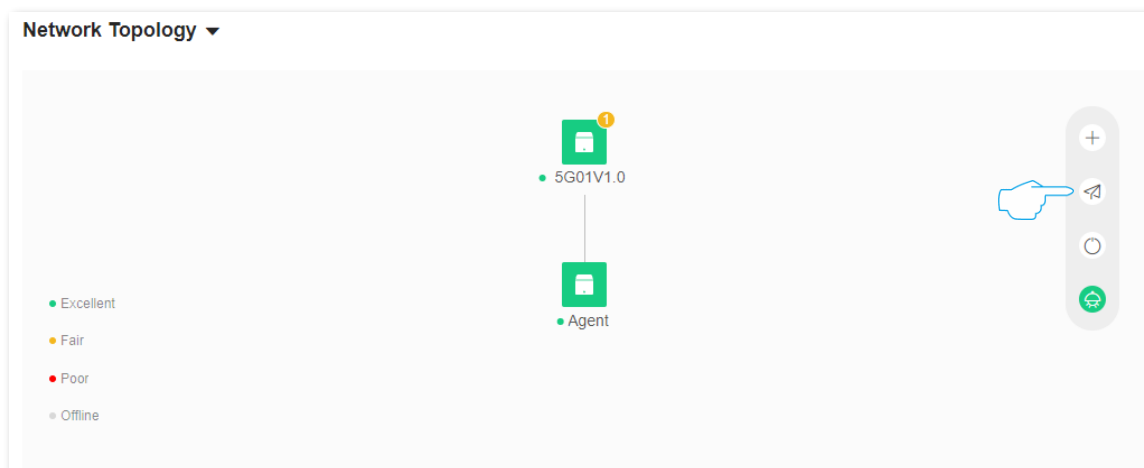
10.1 One-click optimization

If you get stuck when you access the internet, you can try to optimize the WiFi network with one click to solve the problem.

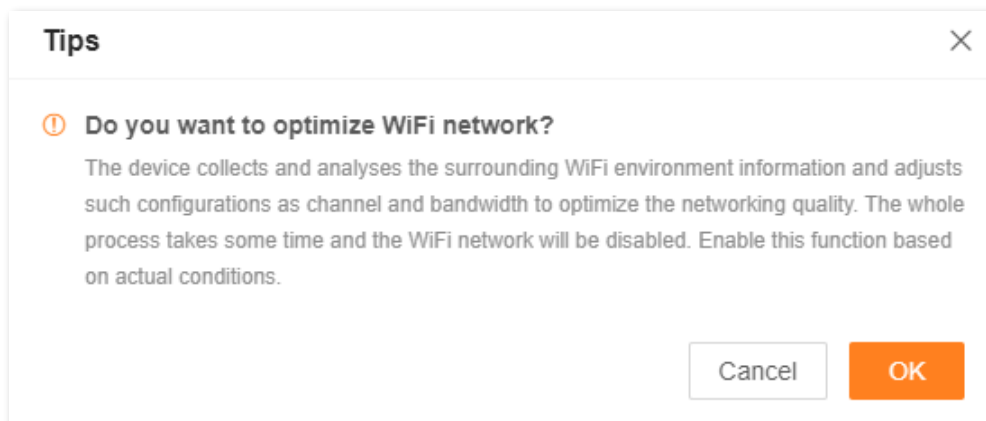
Configuration procedure:

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

Step 2 Navigate to **Network Status**, and click  in the **Network Topology** module.



Step 3 Click **OK**.



---End

10.2 Configure channel & bandwidth

On this page, you can change network mode, channel and bandwidth of 2.4 GHz and 5 GHz WiFi networks.

To access the configuration page, [log in to the web UI of the router](#), and navigate to **More > WiFi Settings > Channel & Bandwidth**.

**TIP**

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

Channel & Bandwidth

You can modify the advanced parameters of the WiFi network here, such as Network Mode, Channel, and Bandwidth. If no professional guidance is available, you are recommended to keep the default settings to prevent the performance from being weakened.

2.4 GHz WiFi

Network Mode	802.11b/g/n
Channel	Auto <small>Current Channel:1</small>
Bandwidth	20/40MHz <small>Current Bandwidth:20</small>

5 GHz WiFi

Network Mode	802.11a/n/ac/ax
Channel	Auto <small>Current Channel:36</small>
Bandwidth	20/40/80MHz <small>Current Bandwidth:80</small>

Save

Parameter description

Parameter	Description
Network Mode	<p>Specifies various protocols used for wireless transmission.</p> <p>2.4 GHz WiFi network supports the 802.11b/g/n Mixed mode.</p> <p>802.11b/g/n: Indicates that devices compliant with the IEEE 802.11b or IEEE 802.11g protocol, and devices working at 2.4 GHz and compliant with the IEEE 802.11n can connect to the 2.4 GHz WiFi network of the router.</p> <p>5 GHz WiFi network supports the 802.11a/n Mixed, 802.11a/n/ac Mixed and 802.11a/n/ac/ax Mixed modes.</p> <ul style="list-style-type: none"> - 802.11a/n: Indicates that devices compliant with the IEEE 802.11a protocol, and devices working at 5 GHz and compliant with the IEEE 802.11n can connect to the router. - 802.11a/n/ac: Indicates that devices compliant with the IEEE 802.11a or IEEE 802.11ac protocol, and devices working at 5 GHz and compliant with the IEEE 802.11n can connect to the router. - 802.11a/n/ac/ax: Indicates that devices compliant with the IEEE 802.11a or IEEE 802.11ac protocol, and devices working at 5 GHz and compliant with the IEEE 802.11n or IEEE 802.11ax protocol can connect to the router.
Channel	<p>Specifies the channel in which the WiFi network works.</p> <p>By default, the wireless channel is Auto, which indicates that the router selects a channel for the WiFi network automatically. You are recommended to choose a channel with less interference for better wireless transmission efficiency. You can use a third-party tool to scan the WiFi signals nearby to understand the channel usage situations.</p>
Bandwidth	<p>Specifies the bandwidth of the wireless channel of a WiFi network. Please change the default settings only when necessary.</p> <ul style="list-style-type: none"> - 20MHz: It indicates that the channel bandwidth used by the router is 20 MHz. - 40MHz: It indicates that the channel bandwidth used by the router is 40 MHz. - 20/40MHz: 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. - 80MHz: It indicates that the channel bandwidth used by the router is 80 MHz. This option is available only at 5 GHz. - 20/40/80MHz: It specifies that a router can switch its channel bandwidth among 20 MHz, 40 MHz, and 80 MHz based on the ambient environment. This option is available only at 5 GHz.

10.3 UPnP

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

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

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.

UPnP

Once enabled, the router automatically opens port for application programs in the LAN that support UPnP, such as Xunlei, BitComet and Anychat, providing smoother user experience.

UPnP

UPnP List

Remote Host	External Port	Internal Host	Internal Port	Protocol
No Data				

Parameter description

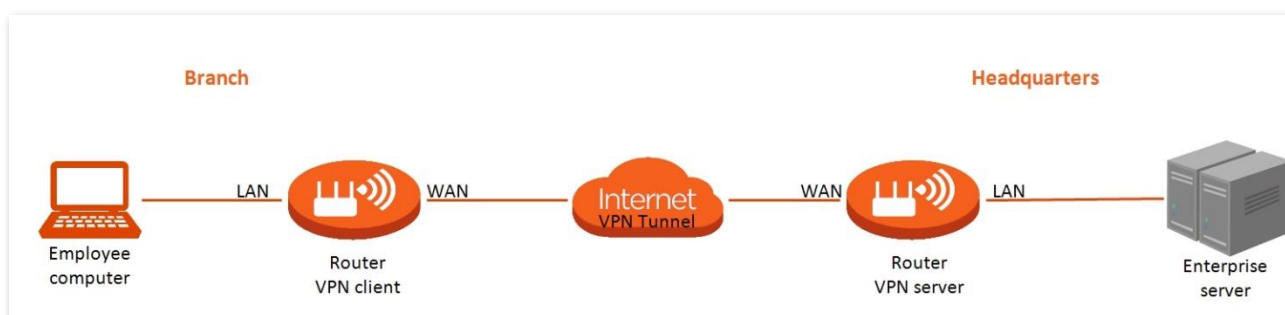
Parameter	Description
UPnP	Used to enable or disable the UPnP function.
Remote Host	Specifies the address of remote host to receive and send responses.
External Port	Specifies the port set on the router to map to the outer.
Internal Host	Specifies the address of inner host to receive and send responses.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

11 Remote access

11.1 VPN

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

The typology of a VPN network is shown below.



11.1.1 PPTP server

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

Enable PPTP server

To access the configuration page, [log in to the web UI of the router](#), and navigate to **More > Advanced > VPN > PPTP Server**. Enable the **PPTP Server**, and click **Save**.

VPN

VPN is a virtual private network built on the internet. It uses the tunneling technology to create a virtual private tunnel between two points, ensuring communication data security.

PPTP Server
PPTP/L2TP Client
OpenVPN Server

PPTP Server

Address Pool Range . . . -

MPPE Encryption

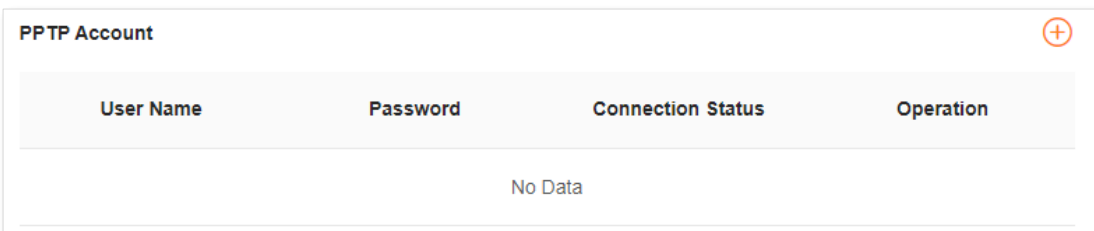
Parameter description


Parameter	Description
PPTP Server	Used to enable or disabled the PPTP server. When it is enabled, the router functions as a PPTP server, which can accept the connections from PPTP clients.
Address Pool Range	Specifies the range of IP address within which the PPTP server can assign to PPTP clients. It is recommended to keep the default settings.
MPPE Encryption	Used to enable or disable 128-bit data encryption. The encryption settings should be the same between the PPTP server and PPTP clients. Otherwise, the communication will fail.

Add PPTP user account





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

Advanced > VPN > PPTP Server. Click  , set the user name and password, and click **OK**.



PPTP Account 			
User Name	Password	Connection Status	Operation
No Data			

Parameter description

Parameter	Description
User Name	Specify the VPN user name and password that the VPN user needs to enter when making PPTP dial-ups (VPN connections).
Password	
Connection Status	Specifies the connection status of the VPN connection.
Operation	<p>The available operations include:</p> <ul style="list-style-type: none">  : Indicates that the PPTP user account is available. You can click it to disable the account.  : Indicates that the PPTP user account is unavailable. You can click it to enable the account.  : Used to edit a PPTP user account.  : Used to delete a PPTP user account.

View online PPTP users

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

To access the configuration page, [log in to the web UI of the router](#), and navigate to **More > Advanced > VPN > PPTP Server**.

Online PPTP User			
User Name	Dial-In IP Address	Assigned IP Address	Uptime
No online client			

Parameter description

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

Example of setting PPTP server

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

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

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

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


Configuration procedure:

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

Step 2 Enable the PPTP server function.

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

Step 3 Add PPTP user name and password for the PPTP server.

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

VPN

VPN is a virtual private network built on the internet. It uses the tunneling technology to create a virtual private tunnel between two points, ensuring communication data security.

PPTP Server
PPTP/L2TP Client
OpenVPN Server

PPTP Server

Address Pool Range . . . - 10.0.0.

MPPE Encryption

Save


PPTP Account +

User Name	Password	Connection Status	Operation
admin1	admin1	● Offline	✓ ✎ 🗑️

---End

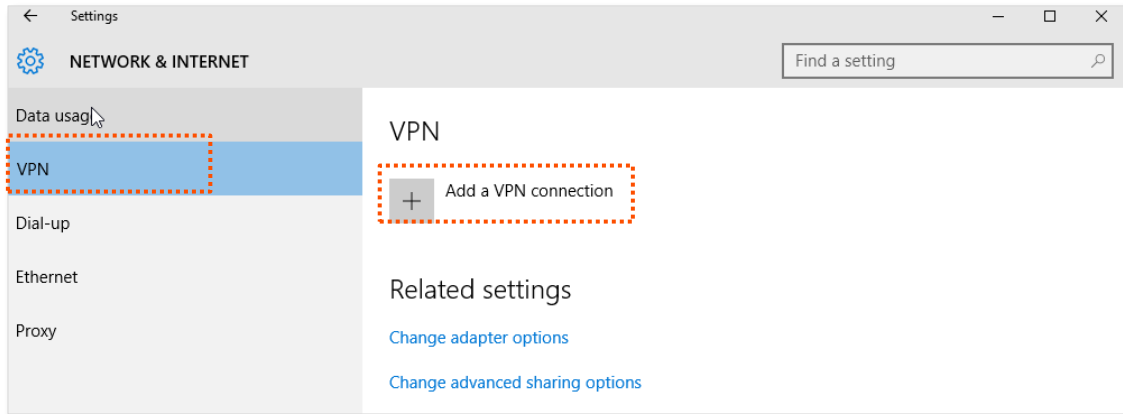
When the configuration is completed, internet users can access the FTP server by following these steps:

Step 1 Perform VPN dial-up.

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



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



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

Add a VPN connection

Connection name
VPN connection

Server name or address
113.88.112.220

VPN type
Point to Point Tunneling Protocol (PPTP)

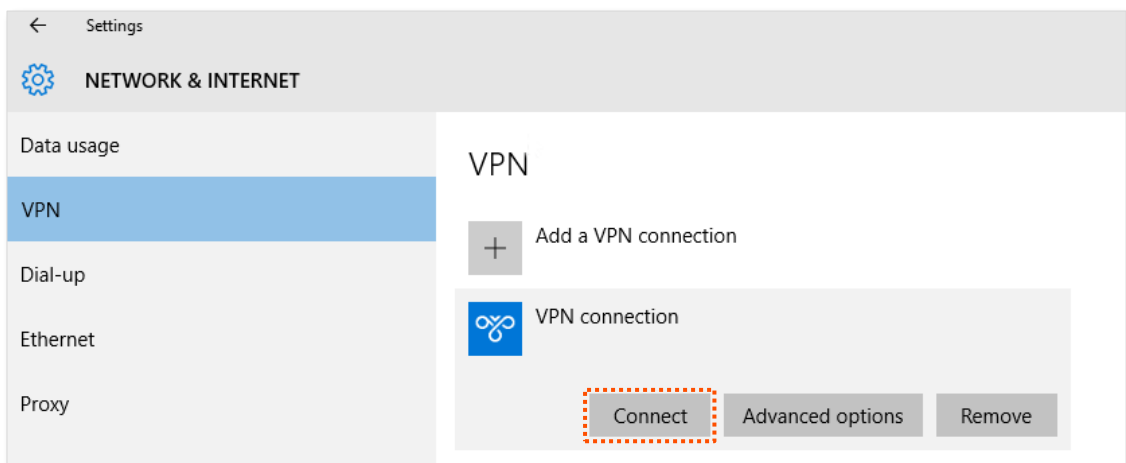
Type of sign-in info
User name and password

User name (optional)
admin1

Password (optional)
•••••


Save Cancel

4. Find the VPN connection added, and click **Connect**.



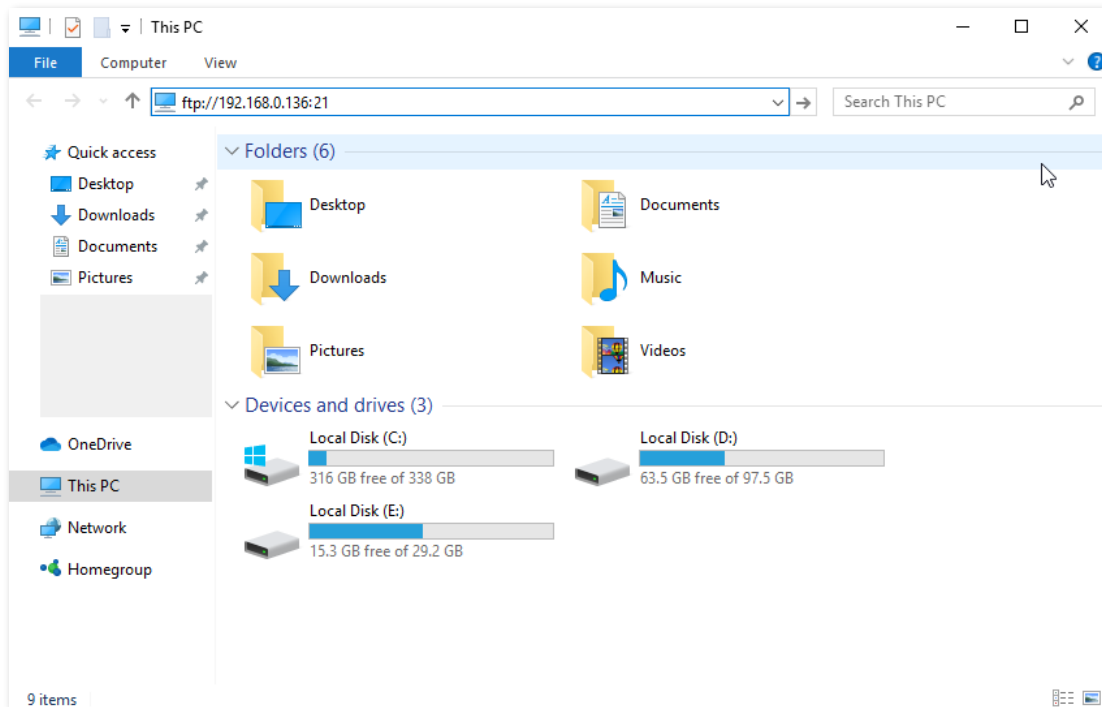
Wait a moment, the VPN connection is successful.

Step 2 Access the FTP server.

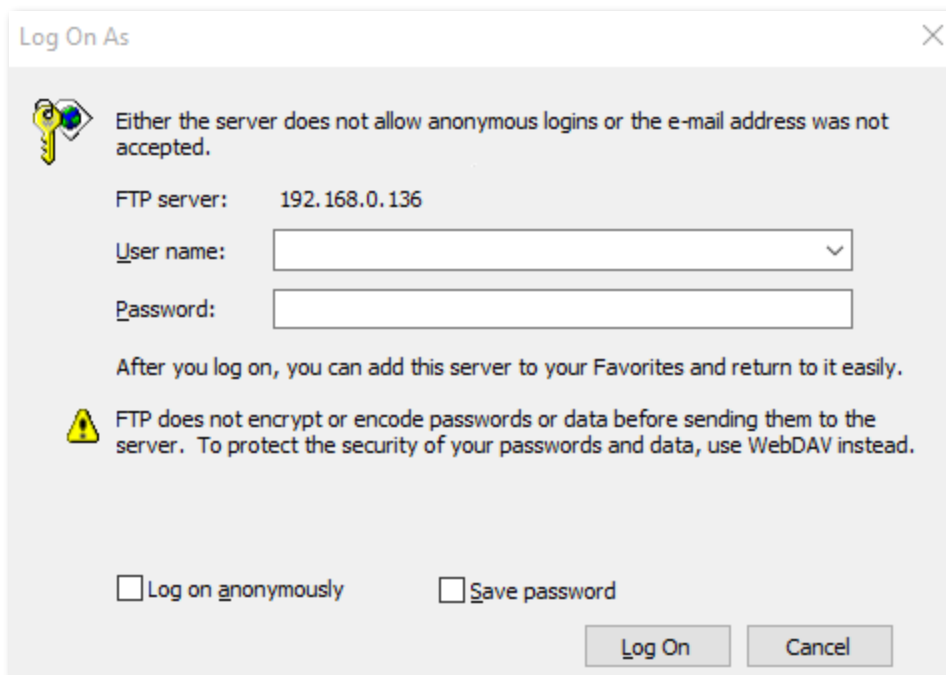
1. Click the  icon on the desktop, and enter the address in the address bar to access the FTP server, which is **ftp://192.168.0.136:21** in this example.



If the LAN service port is not the default port number, the access format is "LAN service application layer protocol name://Server IP address: LAN service port".



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



---End

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

11.1.2 PPTP/L2TP client

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

Enable PPTP/L2TP client

To access the configuration page, [log in to the web UI of the router](#), and navigate to **More > Advanced > VPN > PPTP/L2TP Client**. Enable the **PPTP/L2TP Client**, and click **Save**.

Parameter description

Parameter	Description
PPTP/L2TP Client	Used to enable or disable the PPTP/L2TP client function.
Client Type	Specifies the client type that the router serves as. <ul style="list-style-type: none"> - PPTP: When the router is connecting to a PPTP server, choose this option. - L2TP: When the router is connecting to a L2TP server, choose this option.
Server IP/Domain Name	Specifies the IP address or domain name of the PPTP/L2TP server that the router connects to. Generally, when a router serves as the PPTP/L2TP server at the peer side, the domain name or IP address should be that of the WAN port whose PPTP/L2TP server function is enabled.
User Name	Specify the user name and password that the PPTP/L2TP server assigns to the PPTP/L2TP clients.
Password	
Status	Specifies the connection status of the VPN connection.

Access VPN resources with the router

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

Requirements: Access the VPN resources of your ISP.

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

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

Configuration procedure:

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

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

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

Step 4 Select **PPTP** as **Client Type**.

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

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

Step 7 Click **Save**.

VPN

VPN is a virtual private network built on the internet. It uses the tunneling technology to create a virtual private tunnel between two points, ensuring communication data security.

PPTP Server **PPTP/L2TP Client** OpenVPN Server

PPTP/L2TP Client

Client Type

Server IP/Domain Name

User Name

Password

Status

---End

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

11.1.3 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.

Example of setting OpenVPN server

Scenario: 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: 10.8.0.0
- Client Access: Internet and Home Network

Configuration procedure:

I. Configure the router

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

Step 2 Enable the OpenVPN server function, and set the relative parameters as required.

1. Navigate to **More > Advanced > VPN > OpenVPN Server**.
2. Enable **OpenVPN Server**.
3. Set **Service Type** and **Service Port**, which are **UDP** and **1194** respectively in this example.
4. Set **VPN Subnet**, which is **10.8.0.0** in this example.
5. Set **Client Access**, which is **Internet and Home Network** in this example.
6. Click **Save** above the **OpenVPN connection** module.

VPN

VPN is a virtual private network built on the internet. It uses the tunneling technology to create a virtual private tunnel between two points, ensuring communication data security.

PPTP Server PPTP/L2TP Client **OpenVPN Server**

VPN Server
Set up an OpenVPN for secure, remote access to your network.

OpenVPN Server

Service Type UDP TCP

Service Port

VPN Subnet

Subnet Mask

Client Access

*Home Network Only: The client can only access the home network, and the client's default route will not be changed.
*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.

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

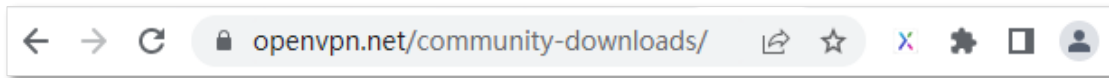
Certificate
Generate a certificate.

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

Configuration File
Export the configuration file.

II. Connect the OpenVPN server

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

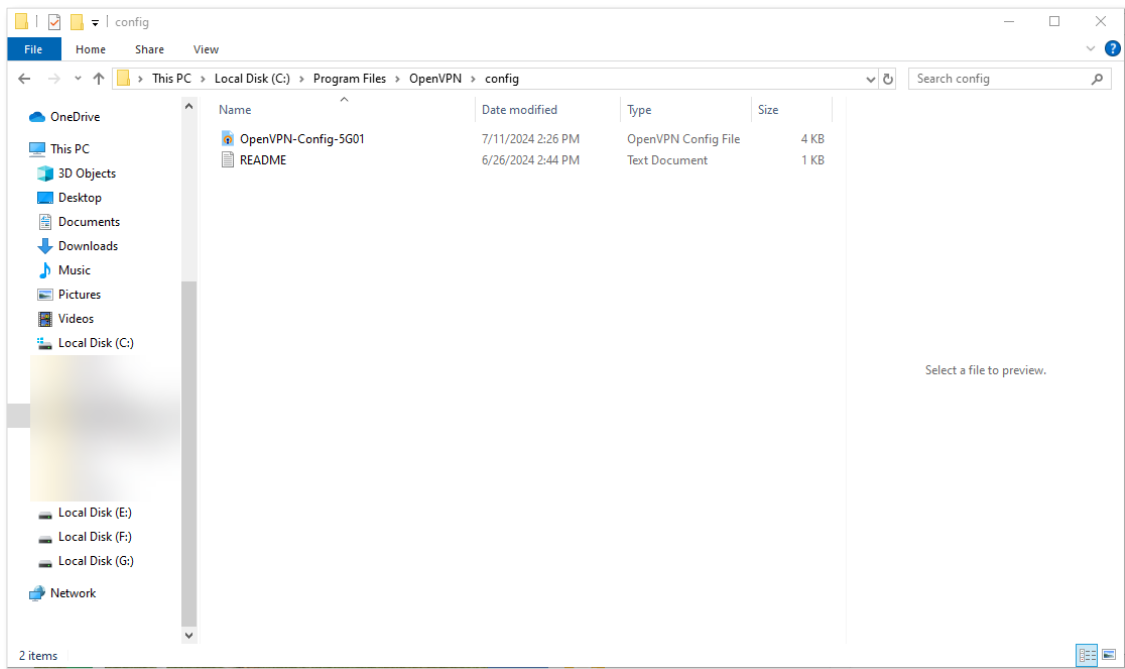



Step 2 Select a version of OpenVPN as required, and click the link corresponding to the Windows version.



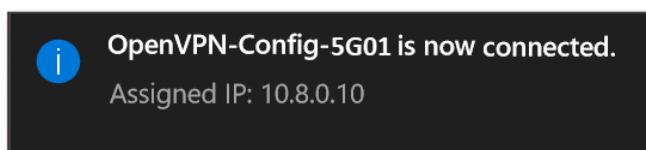
Step 3 Download and run the OpenVPN client.

Step 4 Find the Certificate in your download folder, copy the file, and paste the config file into the **config** folder located in the OpenVPN directory.



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

If connection is successful, the following figure will be displayed.



---End

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

OpenVPN connection
View the OpenVPN connections of remote clients.

No.	Online Duration	Client IP
1	3hour(s) 5min 19sec	10.8.0.10

11.2 DMZ host

11.2.1 Overview

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



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

To access the configuration page, [log in to the web UI of the router](#), and navigate to **More > Advanced > DMZ Host**.

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

DMZ Host

The DMZ host has all ports opened. You can enable this function when you need to communicate with the internet without restrictions. For example, you can set this device as the DMZ host when you are having a video conference or playing online games to improve smoothness.

DMZ Host

1. The DMZ host device will be exposed to the internet and the firewall of the router will no longer safeguard the host.
2. Hackers may use the DMZ host to attack the local network. Please use this function with caution.
3. When using this function, please disable the security software and firewall of the DMZ host temporarily.

DMZ Host IP Address

Parameter description

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

11.2.2 Example of setting DMZ host

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.

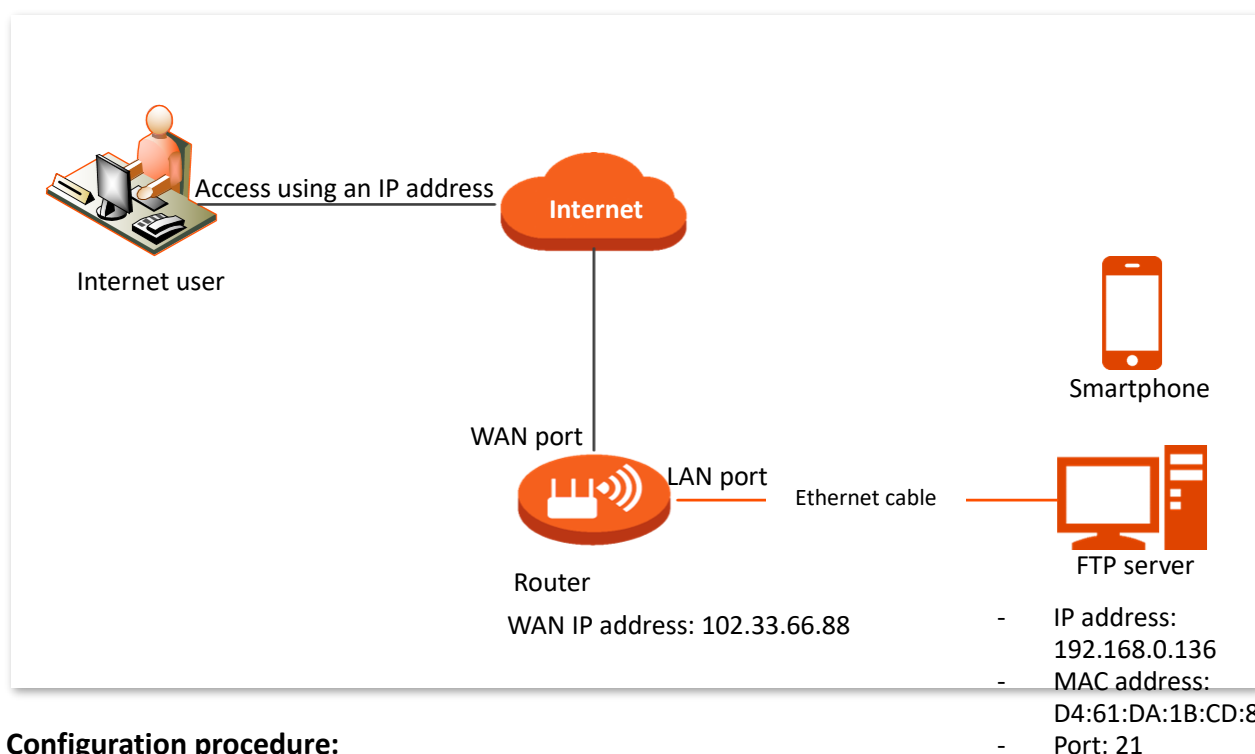
Solution: You can configure the DMZ host function to reach the requirements.

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.



Configuration procedure:

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

Step 2 Set the server host as the DMZ host.

1. Navigate to **More > Advanced > DMZ Host**.
2. Enable **DMZ Host**.

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

DMZ Host

The DMZ host has all ports opened. You can enable this function when you need to communicate with the internet without restrictions. For example, you can set this device as the DMZ host when you are having a video conference or playing online games to improve smoothness.

DMZ Host

1. The DMZ host device will be exposed to the internet and the firewall of the router will no longer safeguard the host.
2. Hackers may use the DMZ host to attack the local network. Please use this function with caution.
3. When using this function, please disable the security software and firewall of the DMZ host temporarily.

DMZ Host IP Address

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

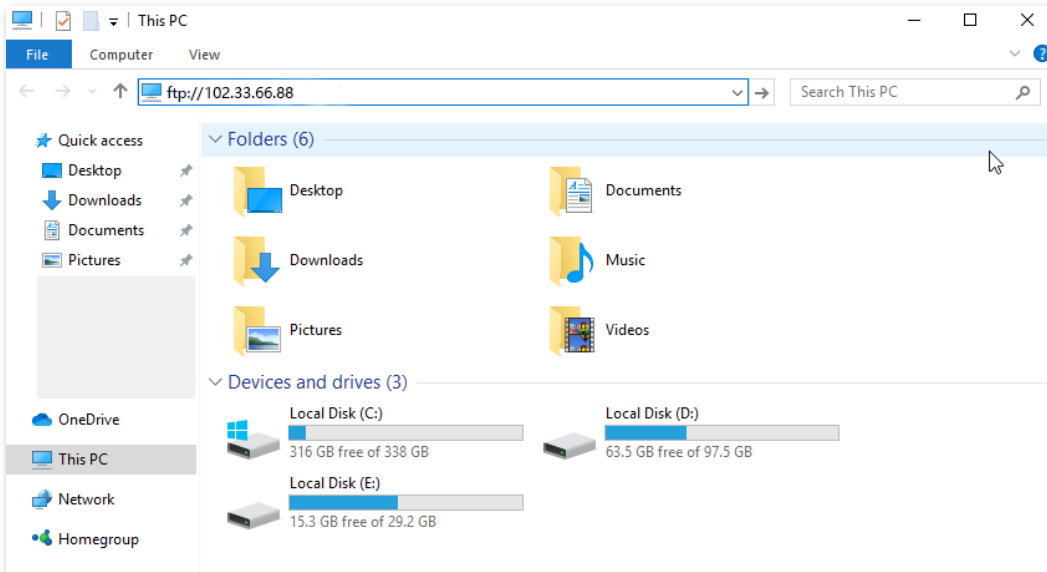
----End

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

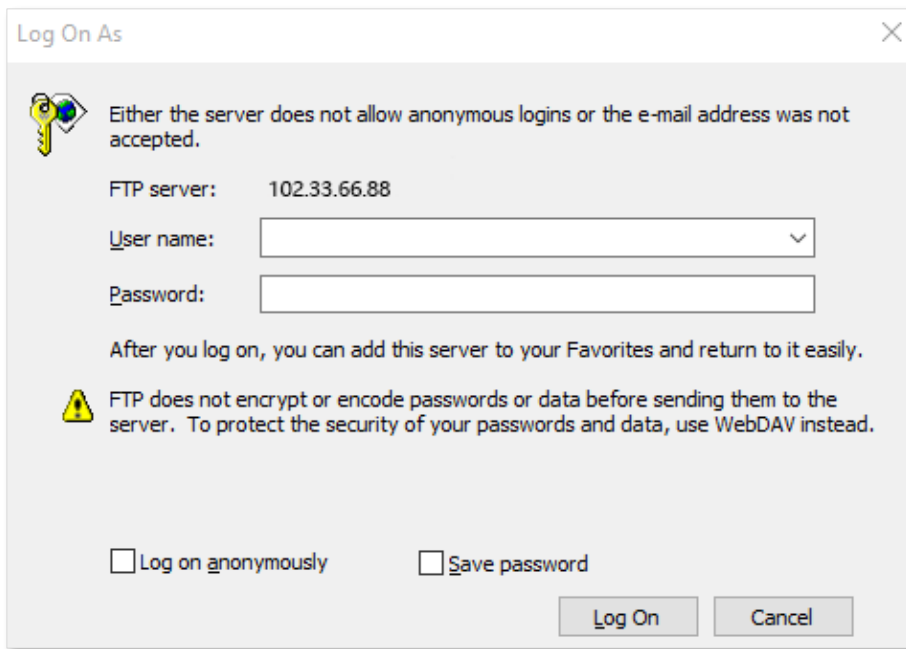
In this example, the address is **"ftp://102.33.66.88"**. You can find the WAN IP address of the router in [View WAN status](#).



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.

11.3 Remote web management

11.3.1 Overview

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

To access the configuration page, [log in to the web UI of the router](#), and navigate to **More > Advanced > Remote Web Management**.

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

Remote Web Management

Under circumstances with special need (such as remote technical support), you can enable this function to allow remote access to the web UI of the router.


Remote Web Management

Remote IP Address

Port

Parameter description

Parameter	Description
Remote Web Management	Used to enable or disable the remote web management function of the router.
Remote IP Address	<p>Specifies the IP address of the host which can access the web UI of the router remotely.</p> <ul style="list-style-type: none"> - Any IP Address: Indicates that hosts with any IP address from the internet can access the web UI of the router. It is not recommended for security. - 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	<p>Specifies the port number of the router which is opened for remote management. You can change it as required.</p> <p> TIP</p> <ul style="list-style-type: none"> The port number from 1 to 1023 has been occupied by familiar services. It is strongly recommended to enter a port number from 1024 to 65535 to prevent conflict. Remote web management can be achieved by visiting “http://WAN IP address of the router:Port number”. If the DDNS host function is enabled, the web UI can also be accessed through “http://Domain name of the router’s WAN port:Port number”.

11.3.2 Example of setting remote web management

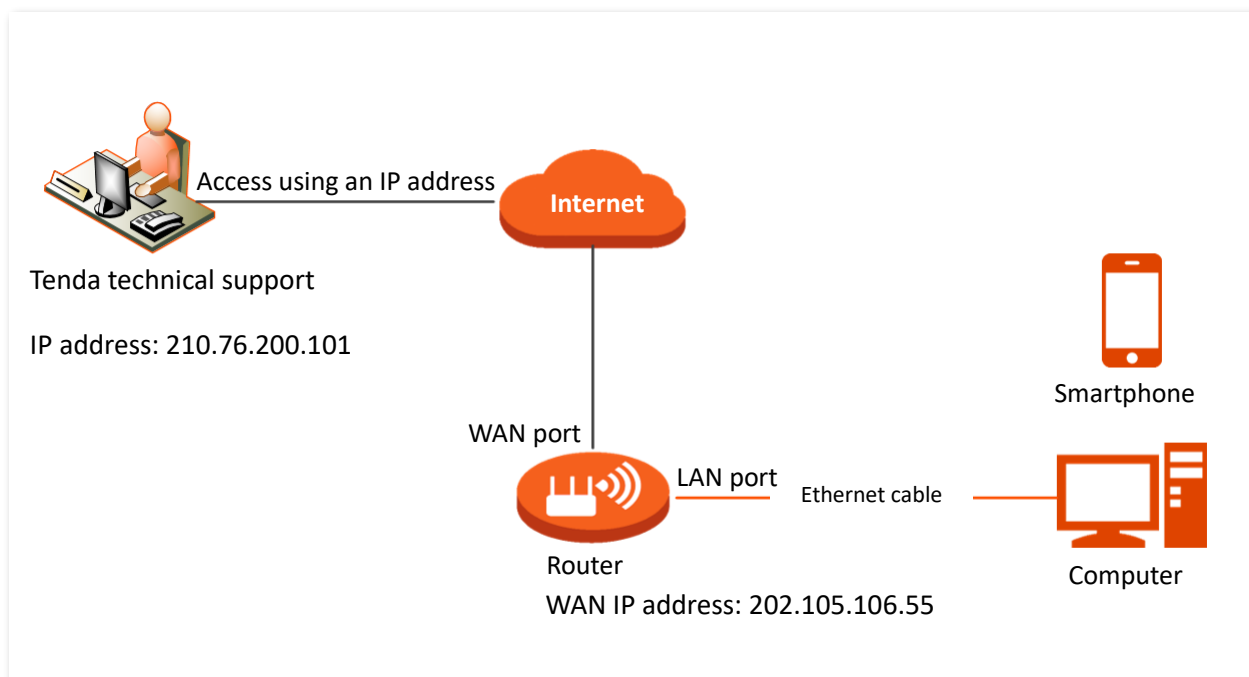
Scenario: You encounter a problem in configuring the router, and the router can access internet.

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



Configuration procedure:

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

Step 2 Navigate to **More > Advanced > Remote Web Management.**

- Step 3** Enable **Remote Web Management**.
- Step 4** Select **Specified IP Address** for **Remote IP Address**.
- Step 5** Enter the IP address that is allowed to access the web UI remotely for **Specified IP Address**, which is **210.76.200.101** in this example.
- Step 6** Click **Save**.

Remote Web Management

Under circumstances with special need (such as remote technical support), you can enable this function to allow remote access to the web UI of the router.

Remote Web Management

Remote IP Address

Specified IP Address

Port

---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.

11.4 DDNS

11.4.1 Overview

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.

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

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

DDNS

Always map the WAN IP address of the router (a public IP address) to a fixed domain name, so that internet users can access the router through this domain name.

DDNS

ISP [Register Now](#)

User Name

Password

Domain Name

Connection Status Disconnected

Parameter description

Parameter	Description
DDNS	Used to enable or disable the DDNS function.
ISP	Specifies the DDNS service provider.
User Name	Specify the user name and password registered on a DDNS service provider's website for logging in to the DDNS service.
Password	
Domain Name	Specifies the domain name registered on the DDNS service provider's website. If this field is invisible after choosing the service provider, it is not required.
Connection Status	Specifies the current connection status of the DDNS service.

11.4.2 Example of setting DDNS

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

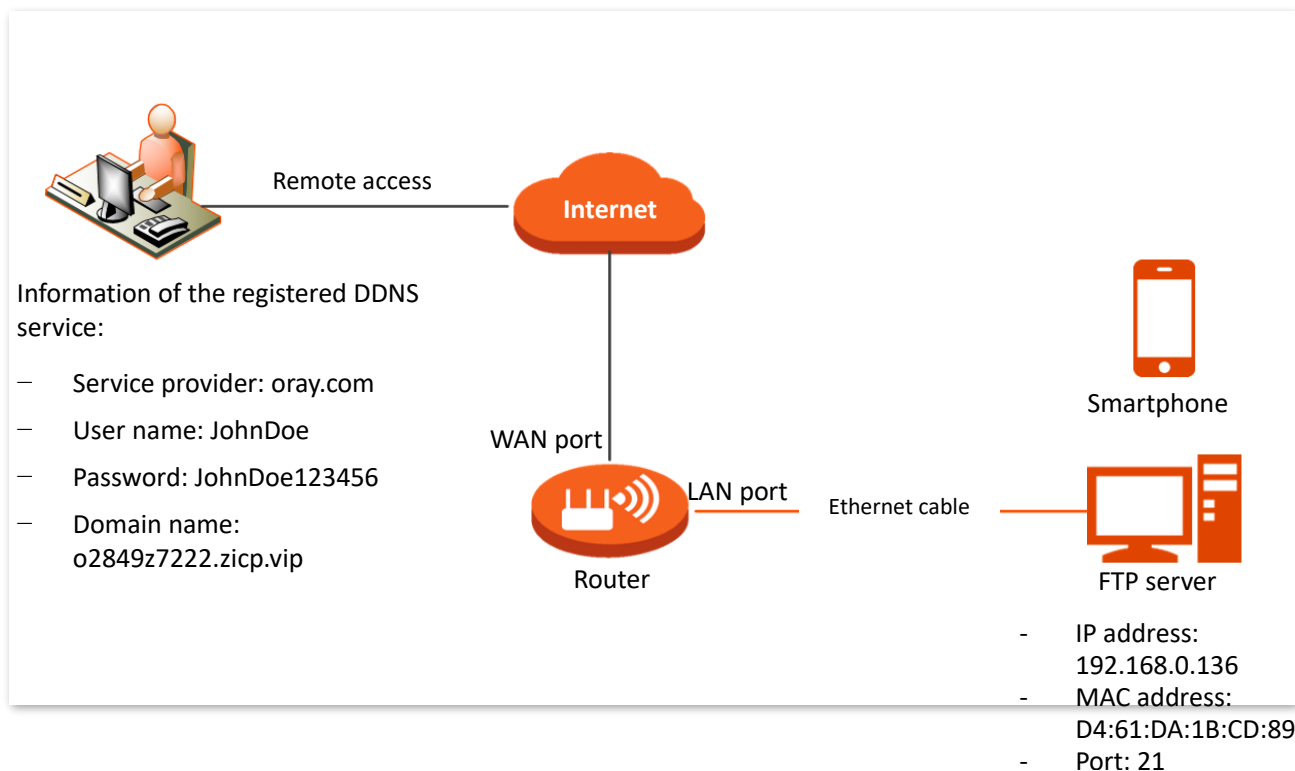
The information of the registered DDNS service:

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



TIP

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.



Configuration procedure:**Step 1** [Log in to the web UI of the router.](#)**Step 2** Configure the DDNS function.

1. Navigate to **More > Advanced > DDNS**.
2. Enable the **DDNS** function.
3. Select a service provider for **ISP**, 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**.

DDNS

Always map the WAN IP address of the router (a public IP address) to a fixed domain name, so that internet users can access the router through this domain name.

DDNS

ISP [Register Now](#)

User Name

Password

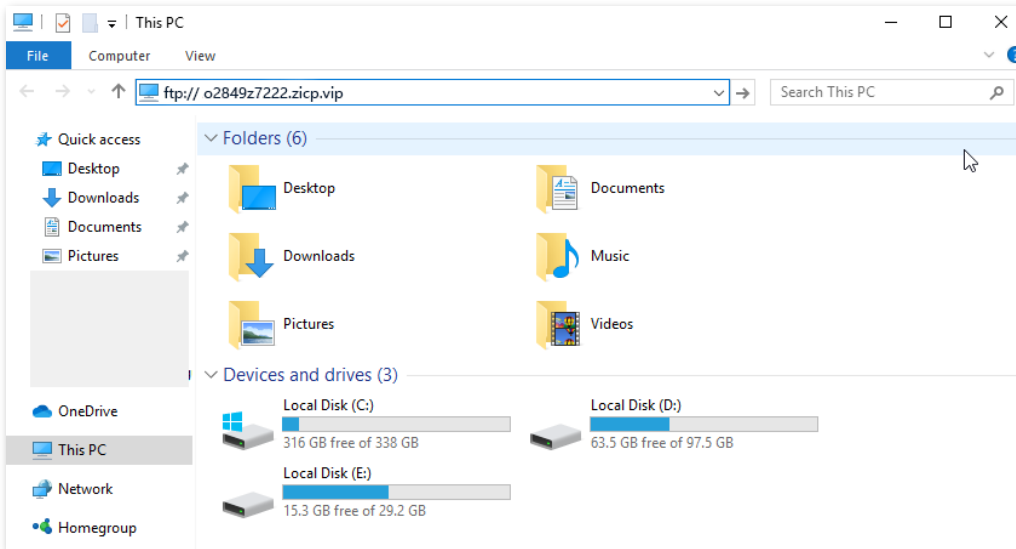
Connection Status Disconnected

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

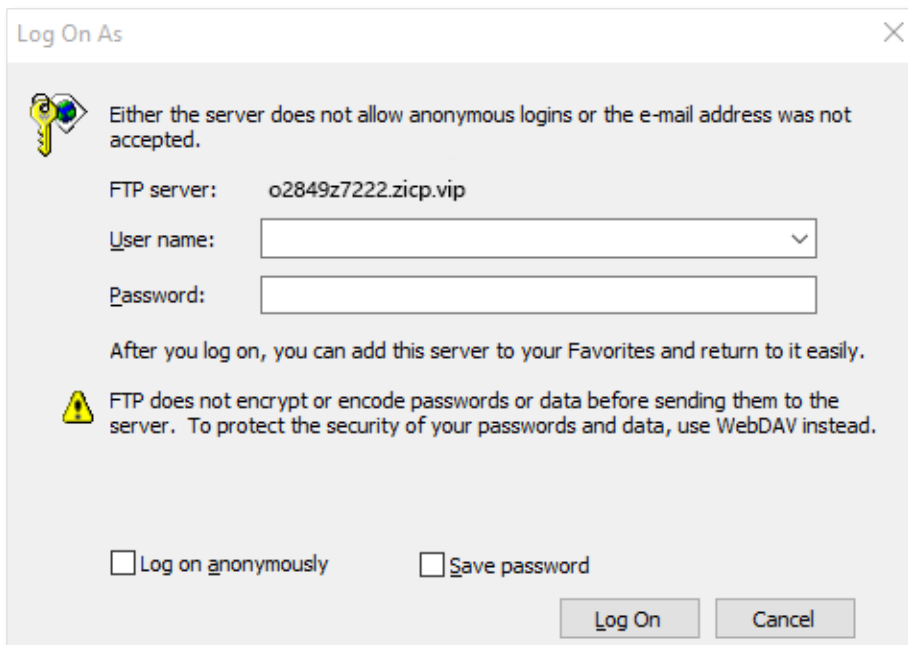
Step 3 Configure the port mapping function by following the steps in [Port mapping](#).**---End**

When completing the configurations, users from the internet can access the FTP server by visiting “*Intranet service application layer protocol name://the domain name*”. If the WAN port number is different from the default intranet service port number, the visiting address should be: “*Intranet service application layer protocol name://the domain name:WAN port number*”.

In this example, the address is **ftp://o2849z7222.zicp.vip**.



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



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.

11.5 Port mapping

11.5.1 Overview

With this function, you can map an external port to an internal port, so that applications using the internal port (such as a web server) are accessible from the internet.

To access the configuration page, [log in to the web UI of the router](#), and navigate to **More > Advanced > Port Mapping**.



Port Mapping

Port mapping opens a service port and maps it to a specified LAN server. With this function enabled, internet users can access the LAN server.

Port Mapping List +

Internal IP Address	Internal Port	External Port	Protocol	Operation
No Data				

Parameter description

Parameter	Description
Internal IP Address	Specifies the IP address of the intranet server.
Internal Port	Specifies the service port of the intranet server.
External Port	Specifies the external port for the internal port to map with.
Protocol	Specifies the mapping protocol. If you are not sure about the protocol type of the service, you are recommended to select TCP&UDP , which indicates that both TCP and UDP are selected.
Operation	The available options include: <div style="display: flex; flex-direction: column; gap: 5px;"> <div> : Used to edit a port mapping rule.</div> <div> : Used to delete a port mapping rule.</div> </div>

11.5.2 Example of setting port mapping

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

Requirements: Set up your own PC as an FTP server and let your family members who are not at home can share resources on the server.

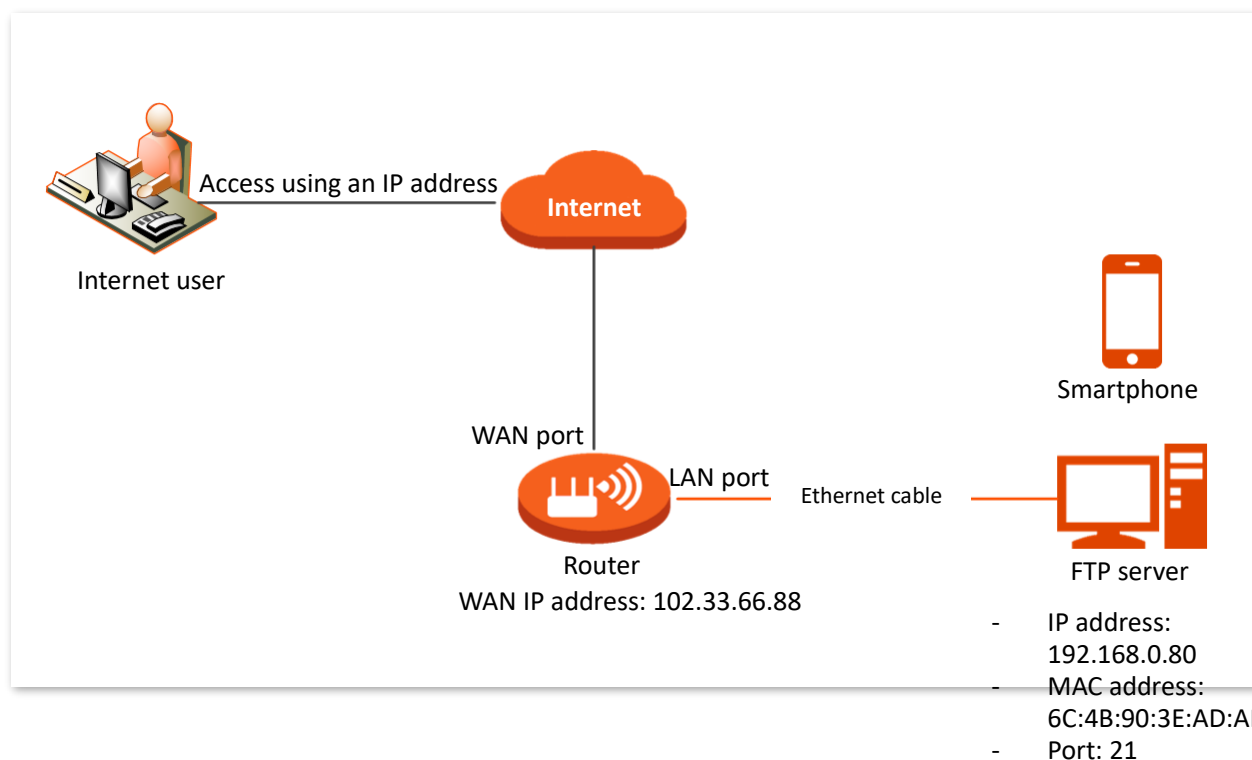
Solution: You can configure the port mapping function to reach the requirements.

Assume that:

- IP address of the FTP server: 192.168.0.80
- MAC address of the FTP server: 6C:4B:90:3E:AD:AF
- Port of the FTP server: 21




- Ensure that the router's WAN port is connected to the internet and an IP address from the public network is obtained. 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.
- The ISP may not support unreported web services accessed using the default port 80. Therefore, when setting port mapping, you are recommended to set the external port to an unfamiliar port (1024 to 65535), such as 9999, to ensure normal access.
- The internal port number and external port number can be different.



Configuration procedure:

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

Step 2 Configure port mapping rule.

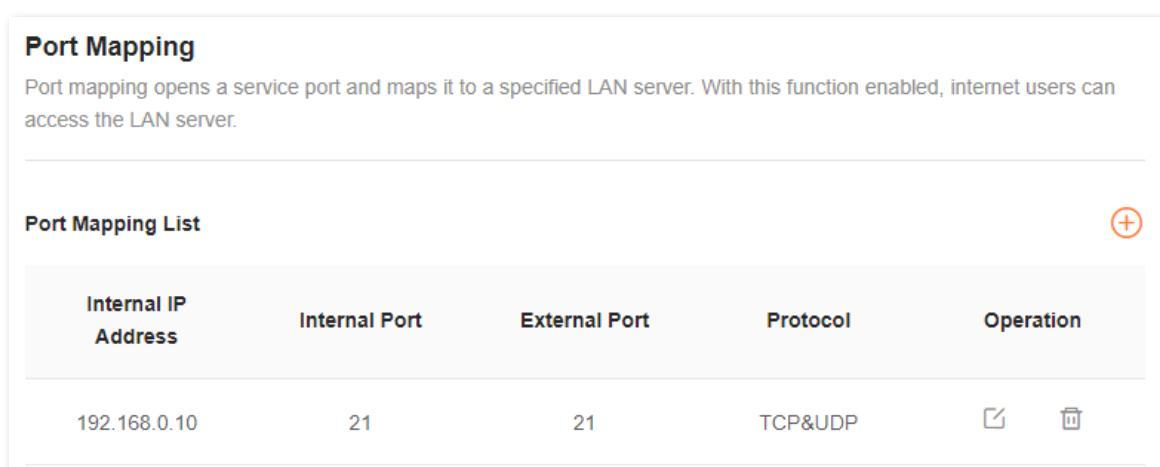
1. Navigate to **More > Advanced > Port Mapping**, and click .
2. Select the host for **Select Device**, which is **6C:4B:90:3E:AD:AF** in this example.



- You can directly select a client from the drop-down list box, which requires no further settings on **Internal IP Address**.
- If you select **Manual**, you need to set **Internal IP Address** manually.

3. Enter the IP address of internal server in **Internal IP Address**, which is **192.168.0.80** in this example.
4. Click the drop-down list of **Internal Port** and select the service port of the Intranet server, which is **21 (FTP)** in this example.
5. The **External Port** will be automatically filled, you can also customize it. Which is **21** in this example.
6. Click the drop-down list of **Protocol** and select the protocol used by the intranet service. You are recommended to select **TCP&UDP**.
7. Click **OK**.

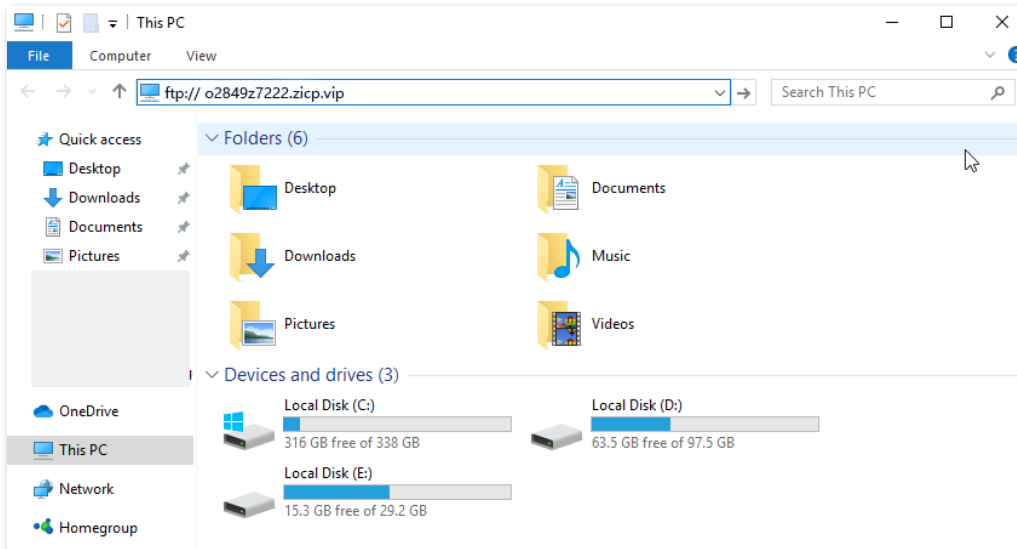
The port mapping rule is successfully added, as shown in the following figure.

**Step 3** [Assign a fixed IP address to the host where the Intranet server resides.](#)

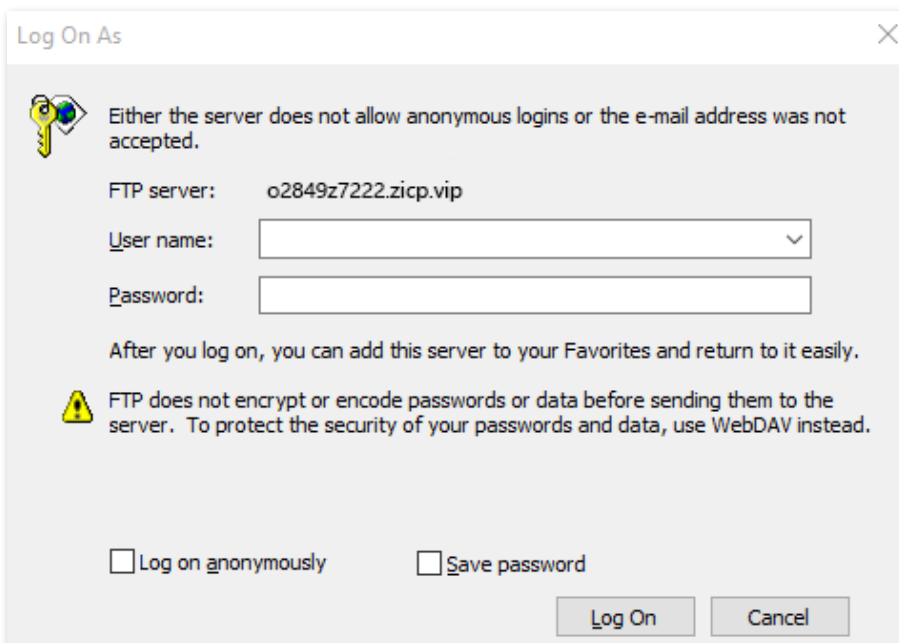
---End

Internet users can successfully access the intranet server by using the “Intranet service application layer protocol name://WAN port IP address”. If the intranet service port is not the default port number, the access address is “Intranet service application layer protocol name://WAN port IP address:External port”.

In this example, the address is **ftp://o2849z7222.zicp.vip**. You can find the current IP address of the router's WAN port on the [View WAN status](#) page.



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



If you want to access the server using a fixed domain name, refer to the solution [Port mapping + DDNS](#).



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 port mapping function is the same as the service port number set on the server.
- Close the firewall, antivirus software and security guards on the host of the FTP server and try again.

12 Network security

12.1 Change login password

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



TIP

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

Configuration procedure:

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

Step 2 Navigate to **More > System Settings > Login Password**.

Step 3 In the **Old Password**, enter the current password for logging in to the router's web UI.

Step 4 Set a new login password in the **New Password**.

Step 5 Enter the new login password again in the **Confirm Password**, and click **Save**.

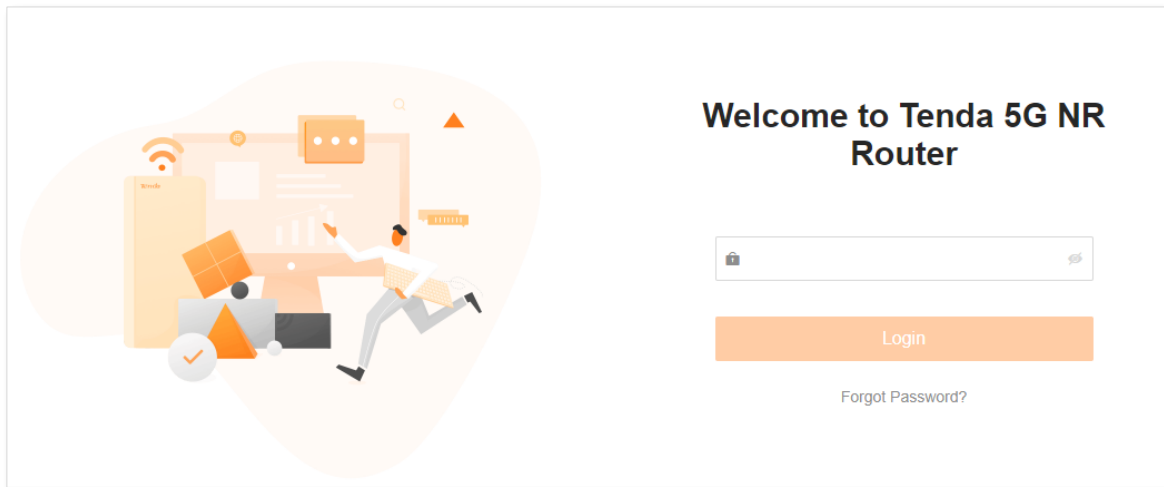
Login Password

You can modify the login password of the router here.

Old Password	<input type="password"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>

---End

The page will direct to the login page, enter the password just set, and then click **Login**. you can re-log in to the router's web UI.



12.2 Firewall

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

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

Firewall

This router can detect and defend against flooding attacks, and can also ignore the Ping packets from the WAN port.

ICMP Flood Attack Defense

TCP Flood Attack Defense

UDP Flood Attack Defense

Block Ping from WAN

[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 a large number of UDP packets to the target host, causing the target host to be busy processing these UDP packets, but unable to process normal packet requests or responses.

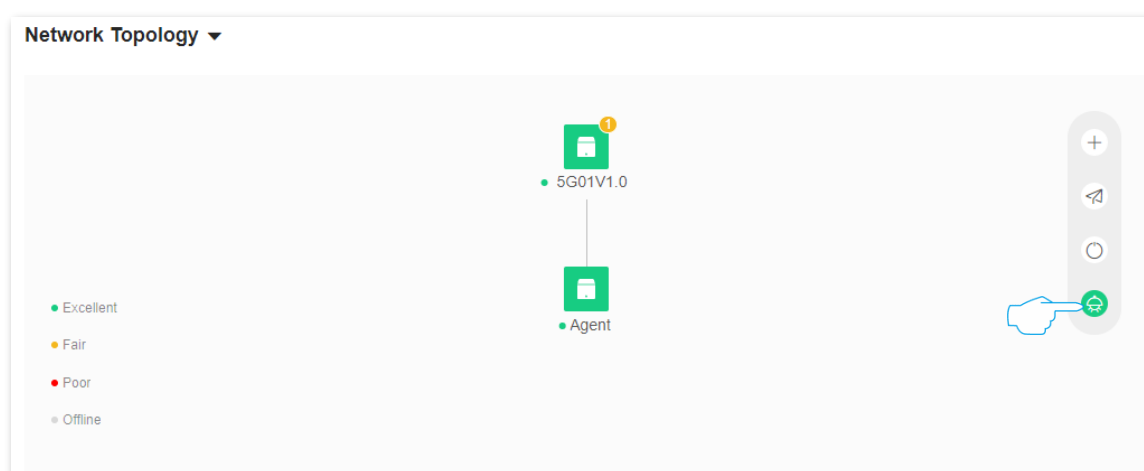
Parameter	Description
Block Ping from WAN	Used to enable or disable the Block Ping from WAN function. When it is enabled, the router automatically ignores the Ping to its WAN from hosts from the internet and prevents itself from being exposed, while preventing external Ping attacks.

13 Advanced settings

13.1 Turn on or turn off indicators

13.1.1 Turn on or turn off indicators of all nodes

To access the configuration page, [log in to the web UI of the router](#), navigate to **Network Status**, and click  or  in the **Network Topology** module.

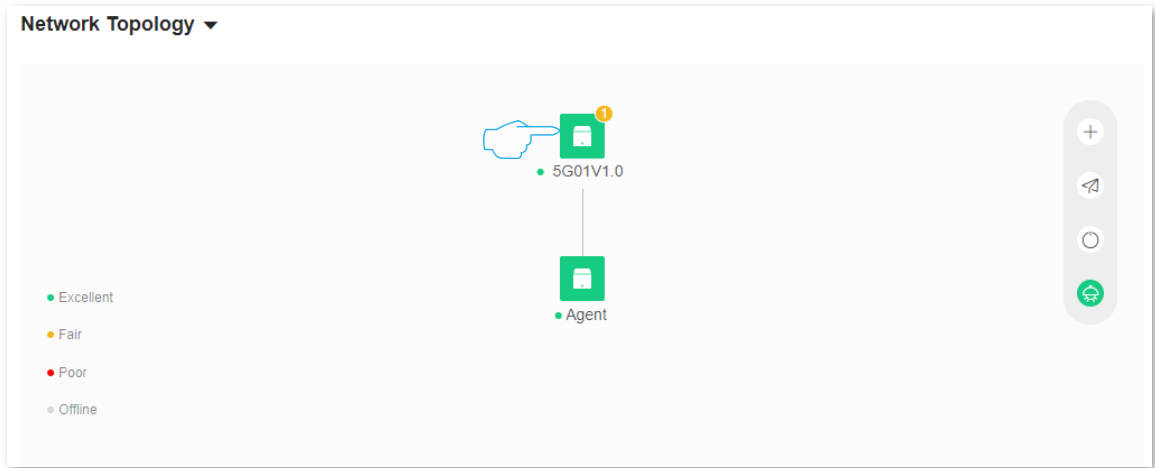


13.1.2 Turn on or turn off indicators of single node



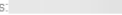




Step 1 [Log in to the web UI of the router](#).

Step 2 Navigate to **Network Status**.

Step 3 Click the node whose indicator you want to turn on or turn off. The following figure is for reference only.



Step 4 Turn on or turn off the indicator of the node as required.

Node Name	Connection Quality	LED On/Off	Operation
 5G01V1.0 Primary Node  IP Address: 192.168.0.1 MAC Address:  Uptime: 2hour(s) 10minute(s)			 

---End

13.2 Configure LAN settings

13.2.1 Overview

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

On this page, you can:

- Change the LAN IP address and subnet mask of the router.
- Change the DHCP server parameters of the router.
- Configure the DNS information assigned to clients.
- Assign static IP address to LAN client.

LAN Settings

Here, you can modify the Router LAN IP address, subnet mask and DHCP server parameters, and add static IP address rules.

LAN IP Address

Subnet Mask

DHCP Server

Once enabled, the DHCP server automatically assigns internet parameters such as IP address, subnet mask, and gateway address to the terminal device. You are recommended to enable this function.

Address Pool Range 192.168.0. -





Lease Time ⓘ


DNS

Static IP Reservation List +

Device Name	IP Address	MAC Address	Operation
No Data			

Parameter description

Parameter	Description
LAN IP Address	Specifies the LAN IP address of the router, which is also the management IP address for logging in to the web UI of the router.
Subnet Mask	Specifies the subnet mask of the LAN port. Used to identify the IP address range of the local area network.
DHCP Server	Used to enable or disable the DHCP server function. Once enabled, the DHCP server automatically assigns internet parameters such as IP address, subnet mask, and gateway address to the terminal device. This function is recommended to be enabled.
Address Pool Range	<p>Specifies the range of IP addresses that can be assigned to devices connected to the router.</p> <p> TIP</p> <p>It is available only when DHCP Server is enabled.</p>
Lease Time	<p>Specifies the valid duration of the IP address that is assigned to a client.</p> <p>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.</p> <p>The default value is recommended.</p> <p> TIP</p> <p>It is available only when DHCP Server is enabled.</p>
DNS	<p>Specifies whether to allocate another DNS address to the client. When it is disabled, the LAN port IP address of the router is used as the DNS address of the client. When it is enabled, Primary DNS must be set and Secondary DNS is optional.</p> <p> TIP</p> <ul style="list-style-type: none"> – It is available only when DHCP Server is enabled. – This router has the DNS proxy function.
Primary DNS	<p>Specifies the primary DNS address of the router, which is assigned to the clients. You can change it if necessary.</p> <p> TIP</p> <ul style="list-style-type: none"> – It is available only when DNS is enabled. – Ensure that the primary DNS server is the IP address of the correct DNS server or DNS proxy. Otherwise, you may fail to access the internet.

Parameter	Description
Secondary DNS	<p>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.</p> <p> TIP</p> <p>It is available only when DNS is enabled.</p>
Device Name	Specifies the device name of the client.
IP Address	Specifies the IP address reserved for the client.
MAC Address	Specifies the MAC address of the client.

13.2.2 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.

Configuration procedure:

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

Step 2 Navigate to **More > Network Settings > LAN Settings.**

Step 3 Change the LAN IP address in the **LAN IP Address**, which is **192.168.2.1** in this example.

Step 4 Click **Save**.

LAN Settings

Here, you can modify the Router LAN IP address, subnet mask and DHCP server parameters, and add static IP address rules.

LAN IP Address	<input type="text" value="192.168.2.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
DHCP Server	<input checked="" type="checkbox"/> Once enabled, the DHCP server automatically assigns internet parameters such as IP address, subnet mask, and gateway address to the terminal device. You are recommended to enable this function.
Address Pool Range	192.168.2. <input type="text" value="1"/> - <input type="text" value="254"/>
Lease Time ⓘ	<input type="text" value="1 day"/>
DNS	<input type="checkbox"/>

Step 5 Click **OK**.

Confirm Operation

ⓘ This IP address is also login IP address of the device. Continue?

---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.

13.2.3 Change 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.

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

LAN Settings

Here, you can modify the Router LAN IP address, subnet mask and DHCP server parameters, and add static IP address rules.

LAN IP Address	<input type="text" value="192.168.0.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
DHCP Server	<input checked="" type="checkbox"/> Once enabled, the DHCP server automatically assigns internet parameters such as IP address, subnet mask, and gateway address to the terminal device. You are recommended to enable this function.
Address Pool Range	192.168.0. <input type="text" value="1"/> - <input type="text" value="254"/>
Lease Time ⓘ	<input type="text" value="1 day"/>
DNS	<input type="checkbox"/>

13.2.4 Assign static IP address to LAN client

With the function enabled, it enables the DHCP server to always assign a fixed IP address to the client, preventing IP address-based functions, such as network bandwidth control and port mapping, from becoming invalid when the client IP address changes.



It is available only when **DHCP Server** is enabled.

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

Requirements: To prevent the failure to access the FTP server due to IP address changes, you must assign a fixed IP address to the FTP server.

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

Assume that the information of the FTP server includes:


- MAC address: 6C:4B:90:3E:AD:AF
- IP address: 192.168.1.80

Configuration procedure:

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

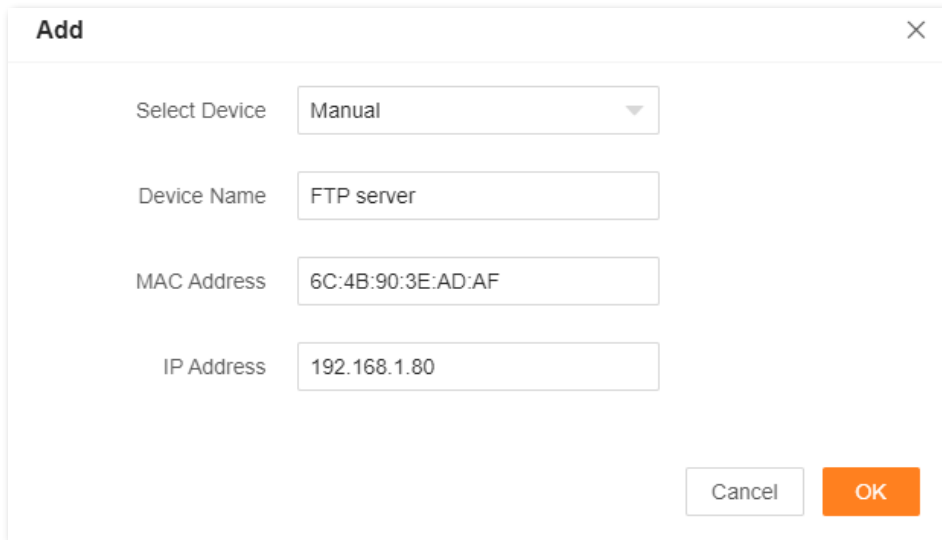
Step 2 Navigate to **More > Network Settings > LAN Settings**.

Step 3 Assign a fixed IP address to the FTP server.

1. Click  in **Static IP Reservation List**.
2. Select the host to which you want to assign a fixed IP address in **Select Device**. If the FTP server is not connected to a router, select **Manual** in the **Select Device** and set related parameters manually. The following uses **Manual** as an example.
3. Remark the device name in the **Device Name**, which is **FTP server** in this example.
4. In the **MAC Address**, enter the MAC address of the host to which a fixed IP address is to be assigned, which is **6C:4B:90:3E:AD:AF** in this example.
5. In the **IP Address**, set the IP address of the host (FTP server in this example) to **192.168.1.80**.
6. Click **OK**.



After the policy is added successfully, it takes effect the next time the device connects to the router.



The 'Add' dialog box contains the following fields:

- Select Device: Manual
- Device Name: FTP server
- MAC Address: 6C:4B:90:3E:AD:AF
- IP Address: 192.168.1.80

Buttons: Cancel, OK

---End

After the static IP reservation rule is successfully added, the following figure is displayed. After the host with the MAC address 6C:4B:90:3E:AD:AF is connected to the router, it always obtains the IP address 192.168.1.80.



Device Name	IP Address	MAC Address	Operation
FTP server	192.168.1.80	6c:4b:90:3e:ad:aF	 

13.3 Static routing

13.3.1 Overview

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

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

To access the configuration page, [log in to the web UI of the router](#), and navigate to **More > Advanced > Static Routing**.




Static Routing

After a static route is added, data whose destination address is the same as the destination network of the static route will be directly forwarded according to the specified path.

Routing Table +

Destination Network	Subnet Mask	Gateway	WAN	Operation
0.0.0.0	0.0.0.0	10.4.144.1	WAN1	System
10.4.144.0	255.255.255.0	0.0.0.0	WAN1	System
192.168.1.0	255.255.255.0	0.0.0.0	br0	System
224.0.0.0	240.0.0.0	0.0.0.0	br0	System

Parameter description

Parameter	Description
Destination Network	<p>Specifies the IP address of the destination network.</p> <p>If Destination Network and Subnet Mask are both 0.0.0.0, this is the default route.</p> <p> TIP</p> <p>When the route of packets cannot be found in the routing table, the router will forward the packets using the default route.</p>
Subnet Mask	Specifies the subnet mask of the destination network.
Gateway	<p>Specifies the ingress IP address of the next hop route after the data packet exits from the interface of the router.</p> <p>0.0.0.0 indicates that the destination network is directly connected to the router.</p>
WAN	Specifies the interface that the packet exits from.
Operation	<p>The available options include:</p> <p> : Used to modify a static routing rule.</p> <p> : Used to delete a static routing rule.</p>

13.3.2 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.

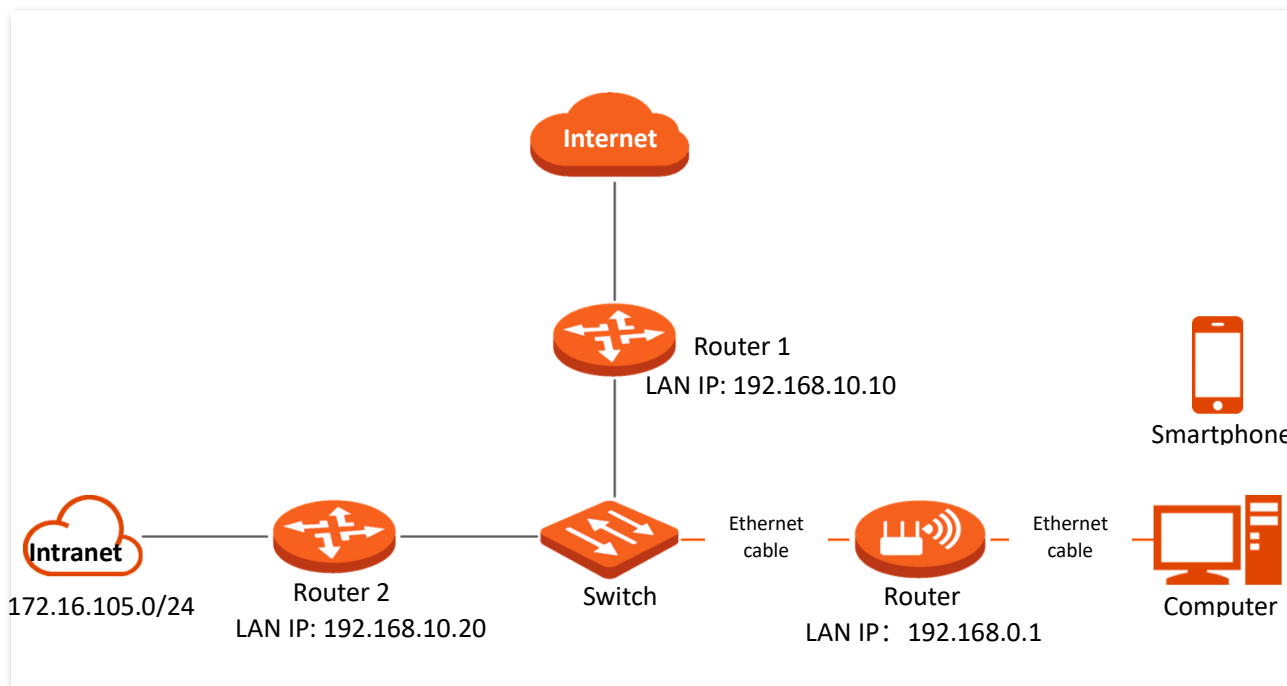
Solution: You can configure the static route function to reach the requirements.

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



Configuration procedure:

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

Step 2 Configure the router to access the internet in **Internet Settings**. For details, refer to [Access the internet through a dynamic IP address.](#)

Failover Settings

Failover ⓘ

Connection Type

DNS Settings

Step 3 Add a static route rule.

1. Navigate to **More > Advanced > Static Routing**.
2. Click .
3. Enter the IP address of the destination network, which is **172.16.105.0** in this example.
4. Enter the subnet mask of the destination network, which is **255.255.255.0** in this example.
5. Enter the ingress IP address of the next hop route, which is **192.168.10.20** in this example.
6. Click **OK**.

Edit Static Route
✕

Destination Network

Subnet Mask

Gateway

WAN
WAN1

The new static routing rule is displayed under **Routing Table**.

Static Routing

After a static route is added, data whose destination address is the same as the destination network of the static route will be directly forwarded according to the specified path.

Routing Table ⊕

Destination Network	Subnet Mask	Gateway	WAN	Operation
172.16.105.0	255.255.255.0	192.168.10.20	WAN1	✎ 🗑️

---End

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

14


System maintenance

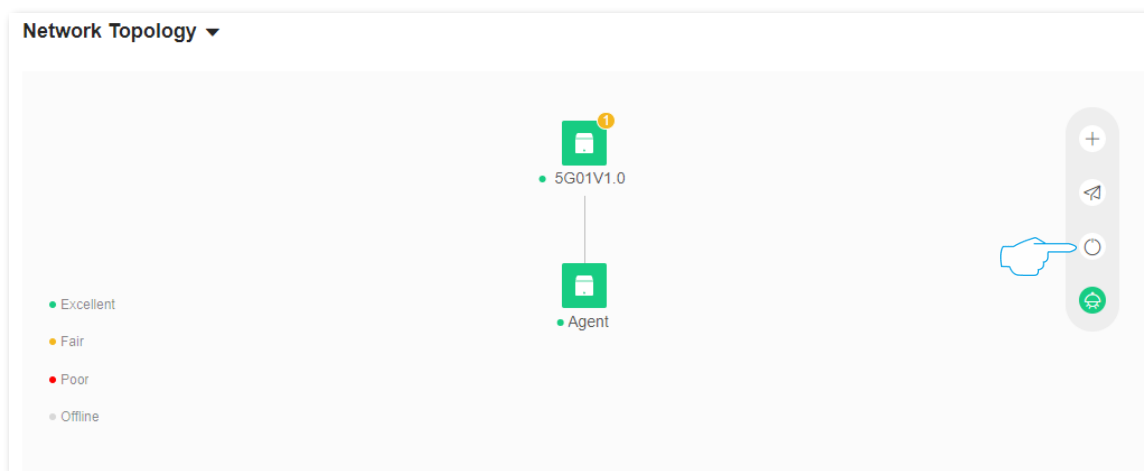
14.1 Reboot device

If a parameter you set does not take effect or a node cannot be used, you can manually reboot the node to resolve the problem. The reboot will disconnect all connections. Perform this operation when the network is relatively idle.

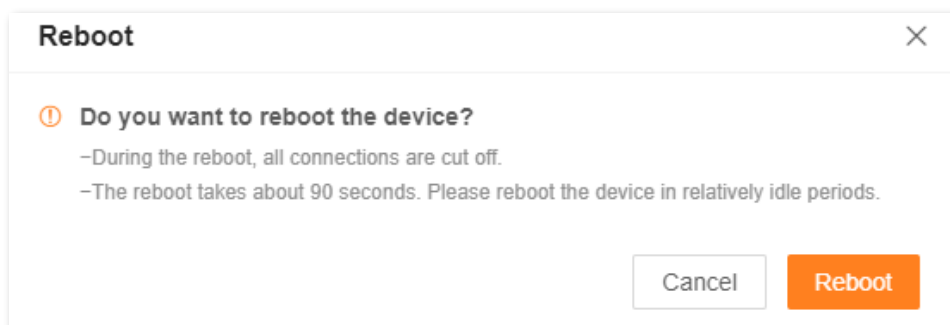
14.1.1 Reboot all nodes

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

Step 2 Navigate to **Network Status**, and click  in the **Network Topology** module.



Step 3 Click **Reboot**.



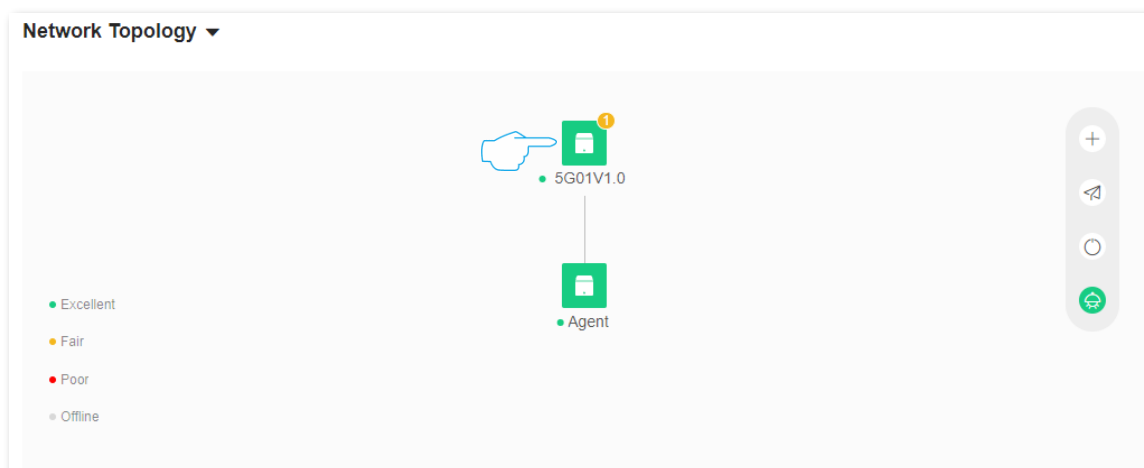
---End


Wait until the ongoing process finishes.

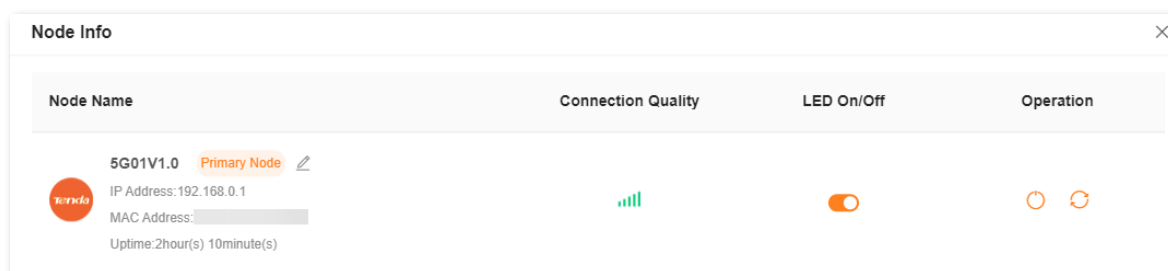
14.1.2 Reboot single node

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

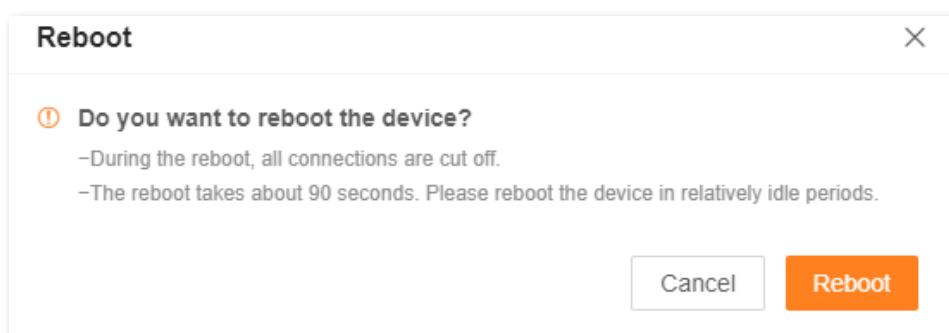
Step 2 Navigate to **Network Status**, and click the node you want to reboot. The following figure is for reference only.



Step 3 Click .



Step 4 Click **Reboot**.



---End

Wait until the ongoing process finishes.

14.2 Configure system time

To access the configuration page, [log in to the web UI of the router](#), and navigate to **More > System Settings > System Time**.

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

14.2.1 Sync system time with the internet time

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

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

System Time

Functions such as Parental Control, Smart Power Saving and Auto System Maintenance are all involve time. To make sure they take effect properly, you are recommended to select Sync with internet time.

System Time	2024-07-10 08:57:31		
Sync Status	Synced		
Sync Mode	Sync with internet time ▼		
Time Zone	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urur ▼		
DST	<input checked="" type="checkbox"/>		
Start 2024	Mar. ▼	2nd ▼	
	Sun. ▼	02:00 ▼	
End 2024	Nov. ▼	1st ▼	
	Sun. ▼	02:00 ▼	
Status	DST not use		

Parameter description

Parameter	Description
System Time	Specifies the current system time.
Sync Status	Specifies whether the system is synced.
Sync Mode	<p>Specifies the sync mode of the system time.</p> <ul style="list-style-type: none"> - Sync with internet time: Indicates that the system time is synced with the internet time. Time Zone must be set when this option is selected. - Sync with local time: Indicates that the system time is automatically synced with the local time on your host, and you do not need to select a time zone.
Time Zone	<p>Specifies the time zone used for the system time. Select one option as required.</p> <p>It is available only when Sync with internet time is selected for Sync Mode.</p>
Local Time	<p>Specifies the local time set on your host.</p> <p>It is available only when Sync with local time is selected for Sync Mode.</p>
DST	Used to enable or disable the Daylight Saving Time (DST) function. It is disabled by default.
Start 2024	<p>It specifies the start time of DST.</p> <p>It is available only when DST is enabled.</p>
End 2024	<p>It specifies the end time of DST.</p> <p>It is available only when DST is enabled.</p>
Status	<p>It specifies whether the DST is used.</p> <p>It is available only when DST is enabled.</p>

14.2.2 Synchronize with local time

In this mode, the system time is synchronized with the system time of the device that is managing the router. You need to reconfigure the system time every time your router reboots.

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

System Time

Functions such as Parental Control, Smart Power Saving and Auto System Maintenance are all involve time. To make sure they take effect properly, you are recommended to select Sync with internet time.

System Time	2024-07-10 09:08:55		
Sync Status	Synced		
Sync Mode	<input type="text" value="Sync with local time"/>		
Local Time	2024-7-9 20:51:20		
DST	<input checked="" type="checkbox"/>		
Start 2024	<input type="text" value="Mar."/>	<input type="text" value="2nd"/>	
	<input type="text" value="Sun."/>	<input type="text" value="02:00"/>	
End 2024	<input type="text" value="Nov."/>	<input type="text" value="1st"/>	
	<input type="text" value="Sun."/>	<input type="text" value="02:00"/>	
Status	DST not use		

14.3 Upgrade firmware

With this function, 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.

14.3.1 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.

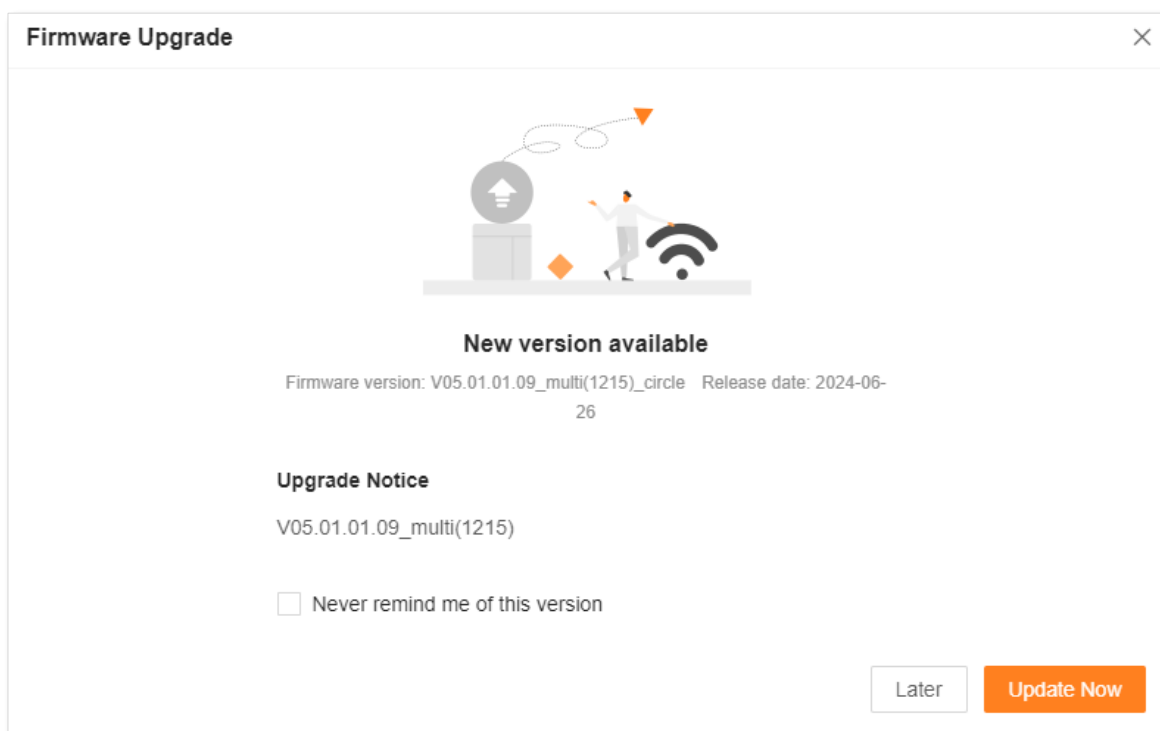


Do not disconnect the device from power or internet during this process. Otherwise, the upgrade may fail or the router may be damaged.

Method 1

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

Step 2 After detecting the new firmware version, the router will display a pop-up window. Click **Update Now**. The following figure is for reference only.



---End

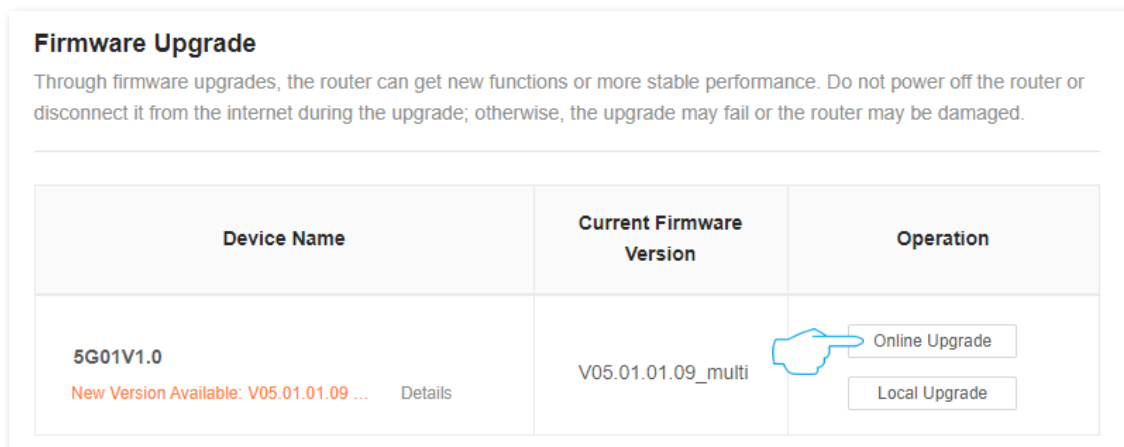
The system will download the upgrade firmware from the cloud and upgrade automatically. Please wait with patience. After the upgrade is completed, access the **Firmware Upgrade** page again and check whether the upgrade is successful based on **Current Firmware Version**.

Method 2

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

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

Step 3 If a new firmware version is detected, click **Online Upgrade**. The following figure is for reference only.



---End

The system will download the upgrade firmware from the cloud and upgrade automatically. Please wait with patience. After the upgrade is completed, access the **Firmware Upgrade** page again and check whether the upgrade is successful based on **Current Firmware Version**.

14.3.2 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**.
- When you are upgrading the firmware, do not power off the router.

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

Step 2 [Log in to the web UI of the router.](#)

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

Step 4 Click **Local Upgrade** in the line of the router to be upgraded. The following figure is for reference only.

Firmware Upgrade

Through firmware upgrades, the router can get new functions or more stable performance. Do not power off the router or disconnect it from the internet during the upgrade; otherwise, the upgrade may fail or the router may be damaged.

Device Name	Current Firmware Version	Operation
5G01V1.0 New Version Available: V05.01.01.09 ... Details	V05.01.01.09_multi	<input type="button" value="Online Upgrade"/> <input type="button" value="Local Upgrade"/>

Step 5 Click **Select File**. Find the firmware file downloaded previously (suffixed with **.bin**).

Local Upgrade ×

ⓘ **The device will reboot after the upgrade completes. The whole process takes about 3 minutes. Continue?**

The upgrade file is a BIN file

No file chosen

Step 6 Click **Upgrade**.

---End

Wait until the upgrade completes. Access the **Firmware Upgrade** page again and check whether the upgrade is successful based on **Current Firmware Version**.

14.4 Backup & Restore

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

If you forgot your WiFi password or fail to fix network connection problems with other solutions, you can reset the router to factory settings.

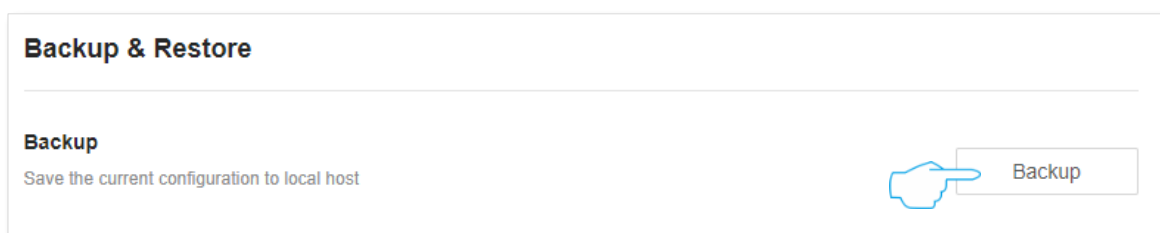
After you restore the router to factory settings or upgrade it, you can use the Backup function to restore the configurations that have been backed up.

14.4.1 Backup the configurations of the router

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

Step 2 Navigate to **More > System Settings > Backup & Restore.**

Step 3 Click **Backup.**



---End

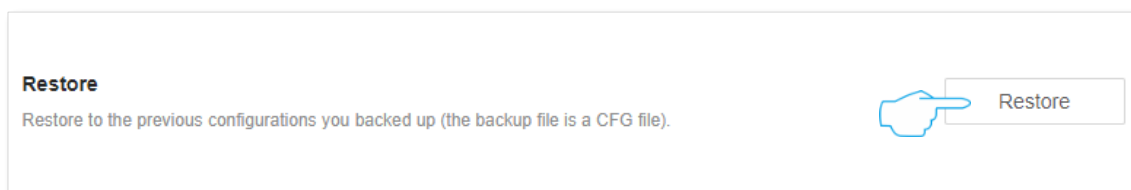
A file named **RouterCfm.cfg** will be downloaded to your local host.

14.4.2 Restore previous configurations of the router

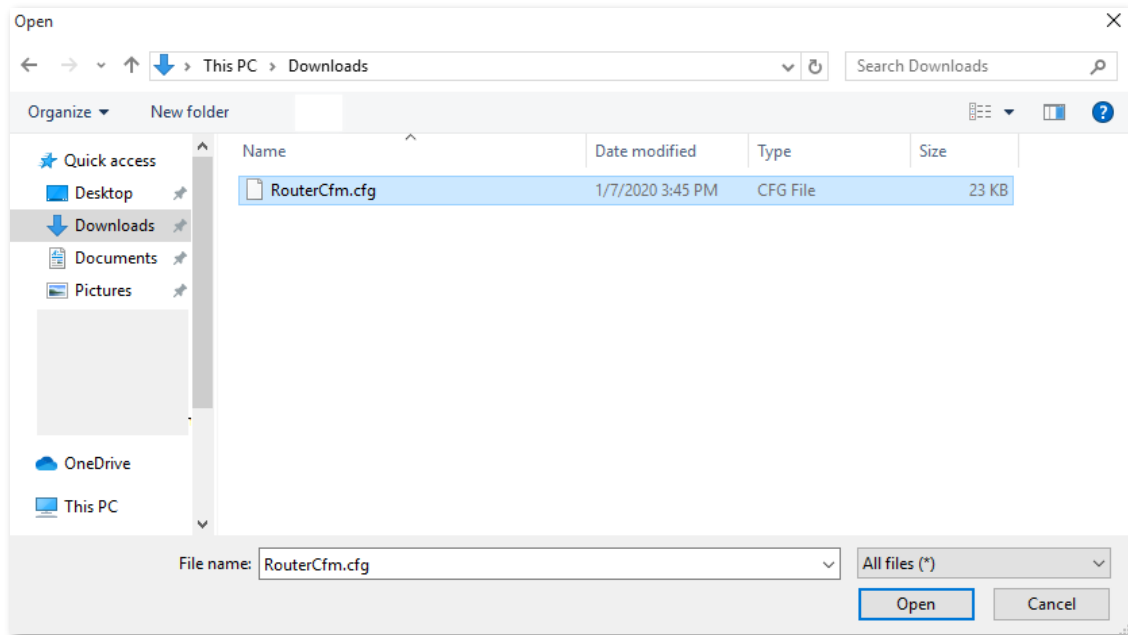
Step 1 [Log in to the web UI of the router.](#)

Step 2 Navigate to **More > System Settings > Backup & Restore.**

Step 3 Click **Restore.**



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



---End

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

14.4.3 Reset

When the network cannot locate the problem or you want to log in to the web UI of the router but forgot the login password, you can restore the router to factory settings and reconfigure.



- Resetting clears all configurations and restores the router to factory settings. You need to reconfigure the router. You are recommended to back up the configuration before restoring the factory settings.
- During the process of restoring factory settings, ensure that the router is powered properly to avoid damage to the router.
- After the router is restored to factory settings, the default login IP address of the router is 192.168.0.1.

Reset all modes

You can restore the entire network to factory settings by restoring all nodes to factory settings.


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

Step 2 Navigate to **More > System Settings > Backup & Restore.**

Step 3 Click **Restore to Factory Settings** in **Reset.**

Reset
Resetting clears all configurations and restores the device to factory settings. Please operation with caution.

Device Name	Operation
5G01V1.0	<input type="button" value="Reset"/>
Agent	<input type="button" value="Reset"/>



Step 4 Click **Reset**. Wait until the reset completes.

Reset ✕

ⓘ Are you sure you want to reset the whole network?
After the whole network is reset, devices cannot access the internet and you need to configure the network again. It is recommended that the configurations be backed up first. Do not cut off the power supply of the device during the reset. Otherwise, the device may be damaged.

---End

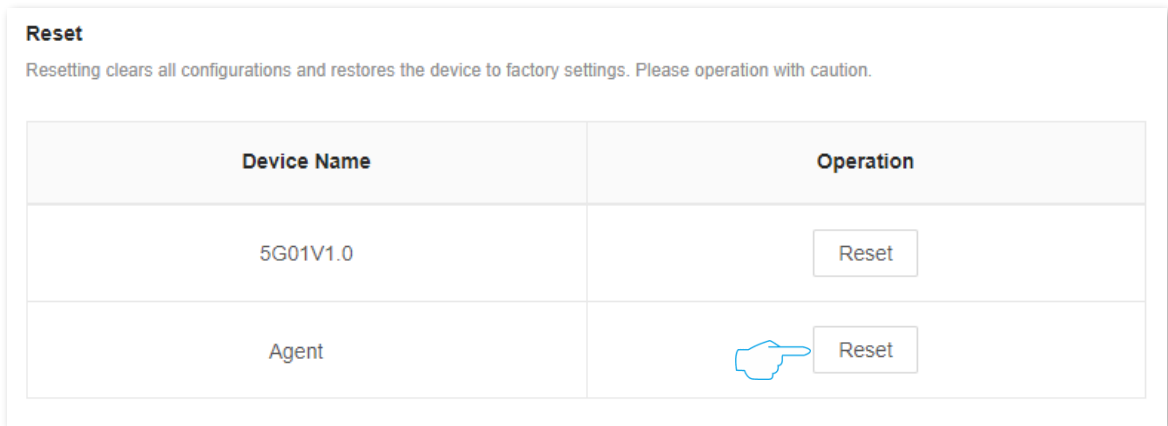
Reset a node



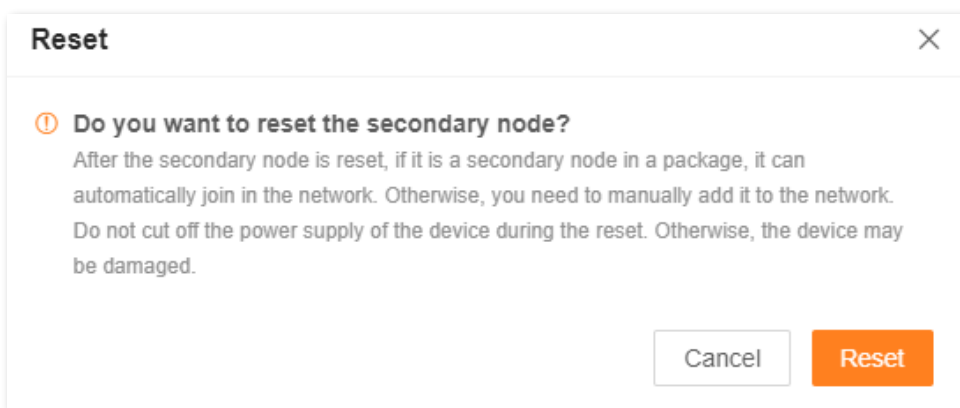
Resetting clears all configurations and restores the router to factory settings. Please operate with caution. You are recommended to [back up the configurations](#) first.

Method 1

- Step 1** [Log in to the web UI of the router.](#)
- Step 2** Navigate to **More > System Settings > Backup & Restore.**
- Step 3** Click **Reset.**



Step 4 Click **Reset**. Wait until the reset completes.



---End

Method 2

Use the reset button on the device body to restore the router to factory settings.

Method: When the device completes startup, press the reset button (**RST**) 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.

14.5 Automatic system maintenance

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

To access the configuration page, [log in to the web UI of the router](#), and navigate to **More > System Settings > Auto System Maintenance**.

Auto System Maintenance

Here, you can set a auto reboot time point for the router to improve the lifetime and system stability.


Auto System Maintenance

Reboot at

Delay Reboot

Delay the reboot if a client is connected and the traffic is higher than 3 KB/s

Parameter description

Parameter	Description
Auto System Maintenance	Used to enable or disable the auto system maintenance function.
Reboot at	Specifies the time when the router reboots automatically every day.
Delay Reboot	<p>Used to enable or disable the reboot delay function.</p> <ul style="list-style-type: none"> - 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. <p> TIP</p> <p>After Delay Reboot function is enabled, the router continuously detects traffic within 2 hours after reboot time, and reboots once the conditions are met.</p>

14.6 System log

To access the configuration page, [log in to the web UI of the router](#), and navigate to **More > System Settings > System Log**.

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

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 [System time](#) page to calibrate the router's system time.

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



Rebooting the router will clear all previous system logs. Power-on after a power failure, firmware upgrade, restore settings, or reset may cause the system to reboot.

System Log

The system logs record the events of the system. You can check them for troubleshooting in case of network failure.

Export to Local

No.	Time	Type	Log Content
1	2024-07-10 10:42:51	system	USER(192.168.0.173) LOGIN SUCCESS !
2	2024-07-10 10:04:51	system	USER(192.168.0.173) LOGIN SUCCESS !
3	2024-07-10 09:53:31	system	USER(192.168.0.173) LOGIN SUCCESS !
4	2024-07-10 09:42:07	system	Sync time success!
5	2024-07-10 09:41:58	system	Sync time success!
6	2024-07-10 09:41:57	system	WAN1 up
7	2024-07-10 09:41:54	system	WAN1 down
8	2024-07-10 09:21:21	system	USER(192.168.0.173) LOGIN SUCCESS !
9	2024-07-10 09:13:12	system	USER(192.168.0.173) LOGIN SUCCESS !
10	2024-07-10 09:06:04	system	USER(192.168.0.173) LOGIN SUCCESS !

299 items in total


<
1
2
3
4
5
6
7
...
30
>


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 WiFi network adapter are similar.

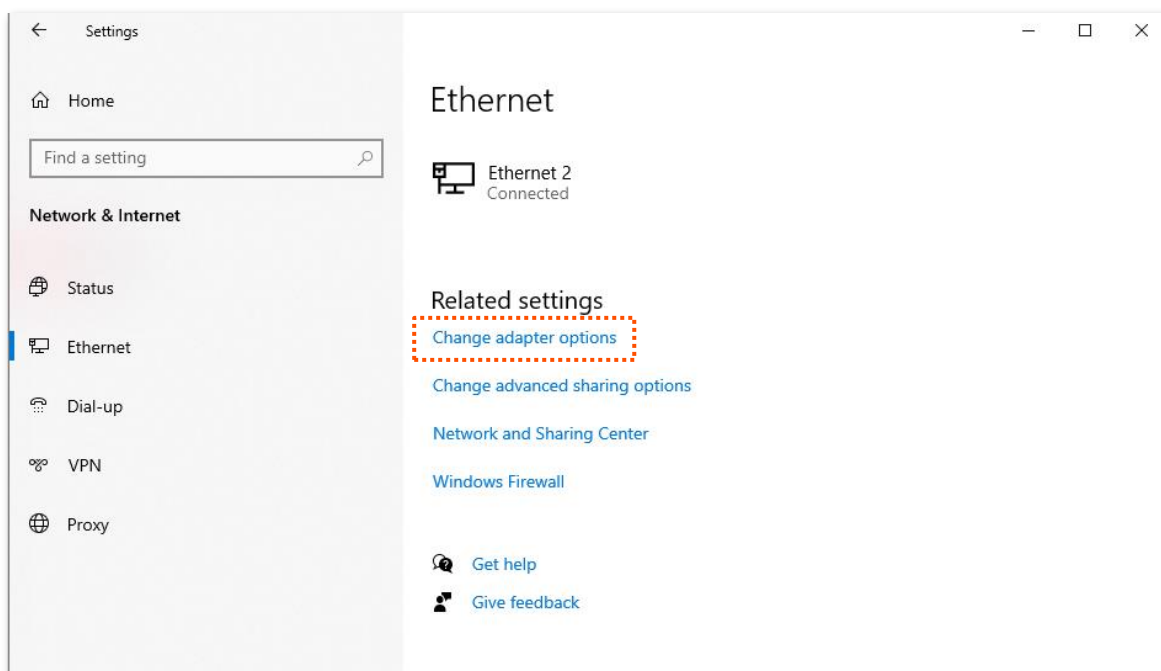
A.1.1 Windows 10

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

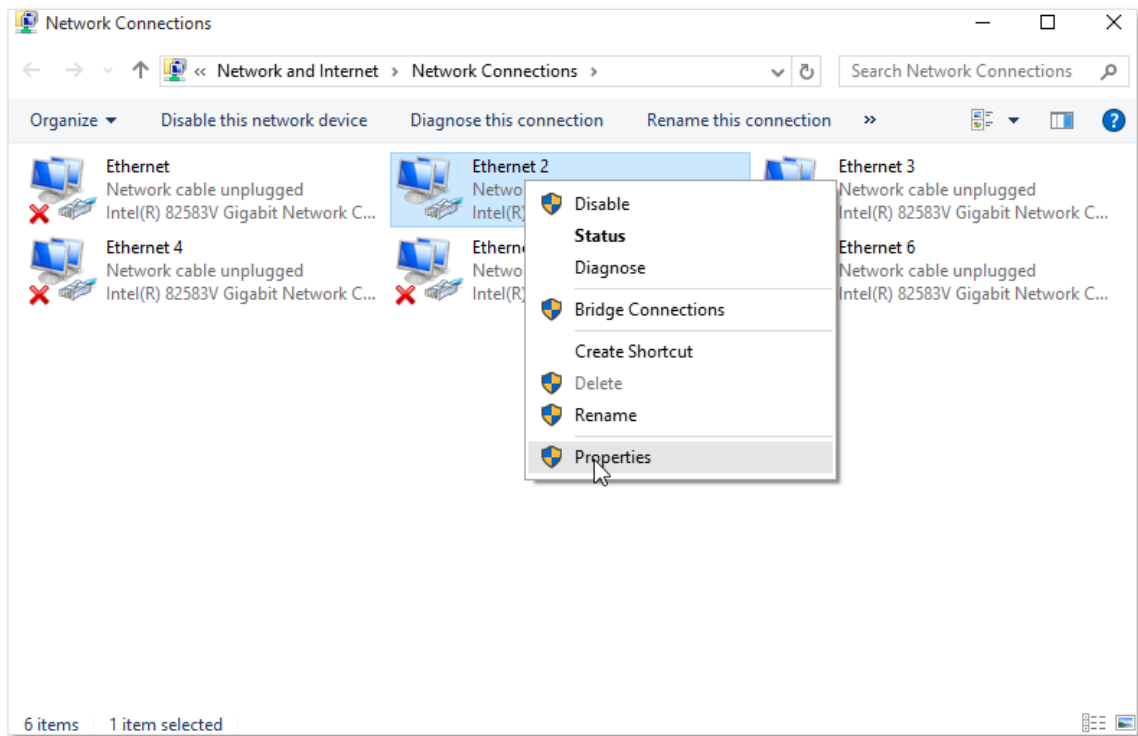


Network & Internet settings

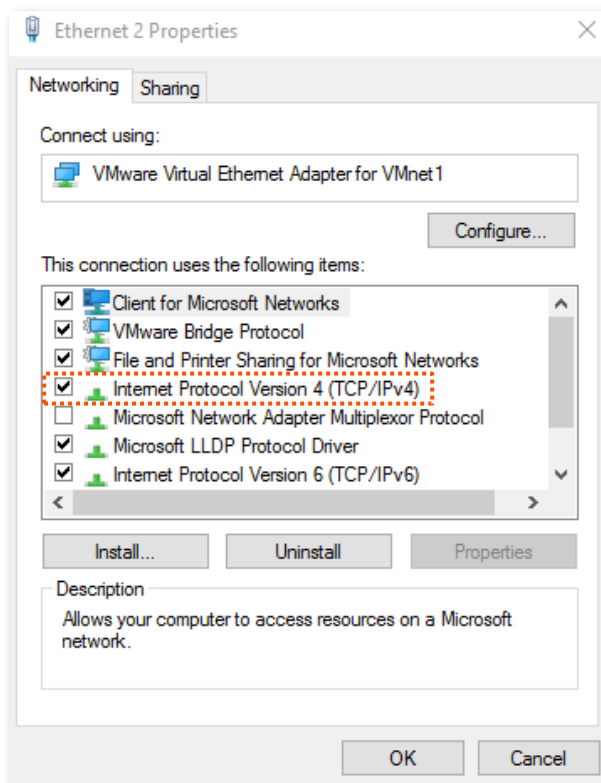
Step 2 Click **Change adapter options**.



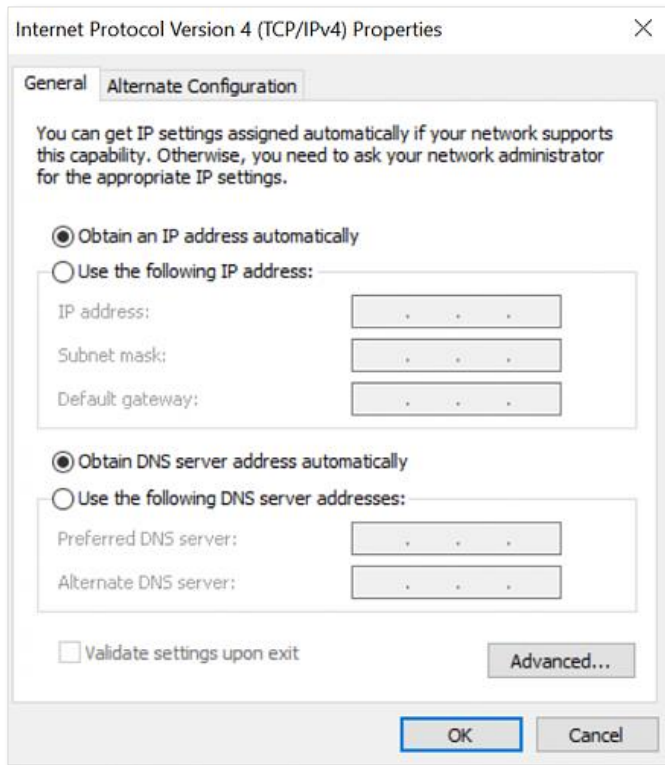
Step 3 Right-click on the connection which is being connected, and then click **Properties**.



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




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

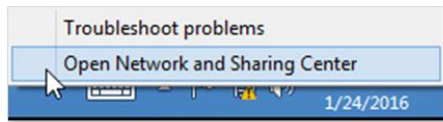


- Step 6** Click **OK** in the **Ethernet Properties** window.

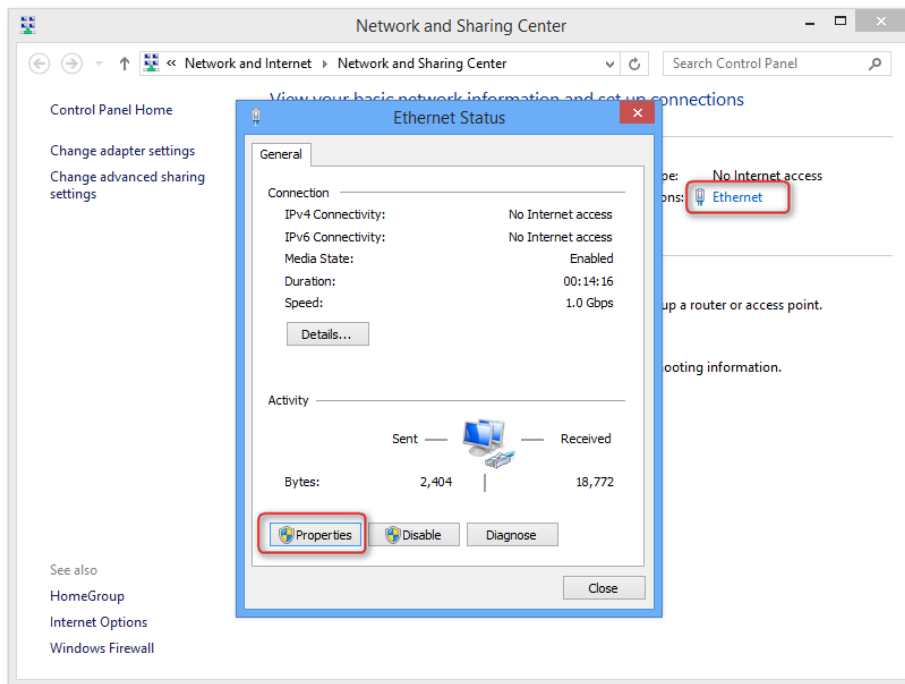
---End

A.1.2 Windows 8

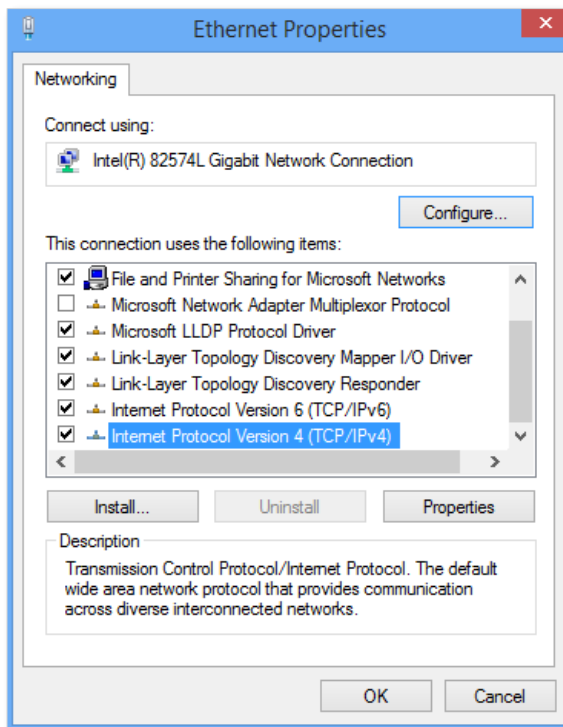
Step 1 Right-click  in the bottom right corner of the desktop and choose **Open Network and Sharing Center**.



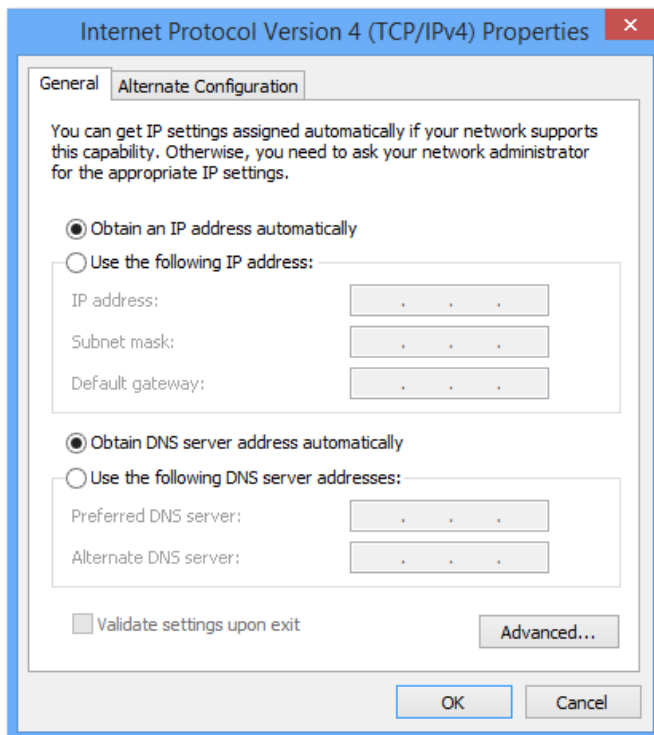
Step 2 Click **Ethernet** and then **Properties**.



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




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

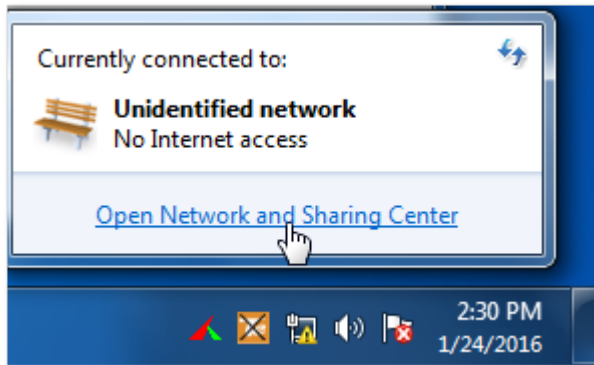


Step 5 Click **OK** in the **Ethernet Properties** window.

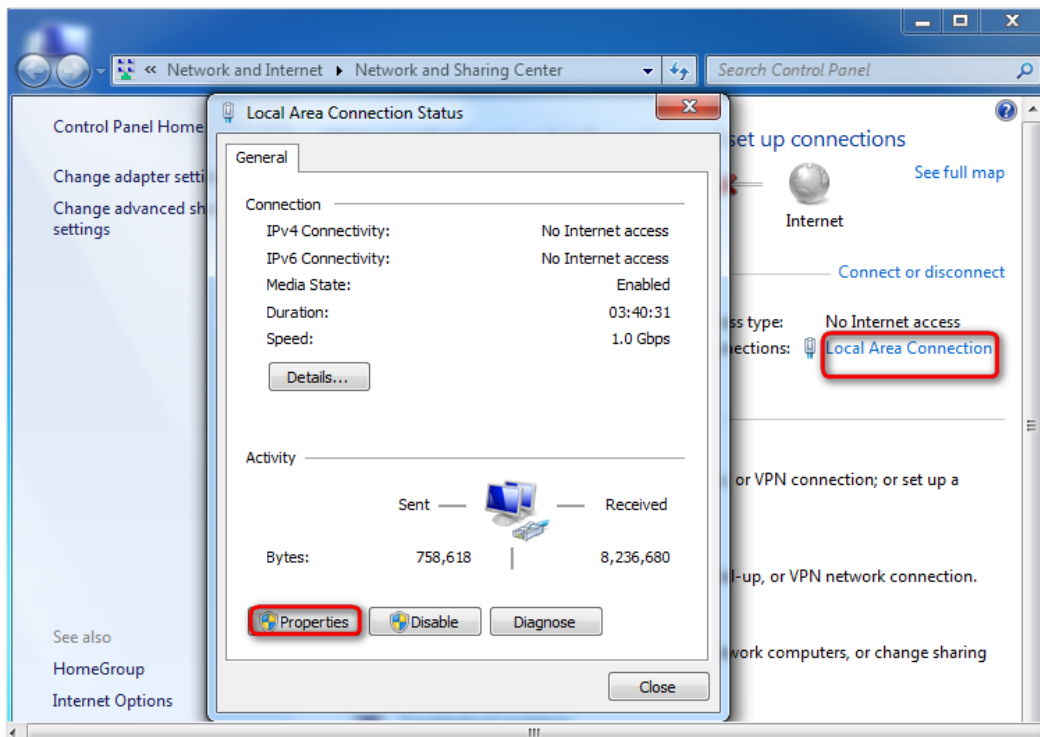
---End

A.1.3 Windows 7

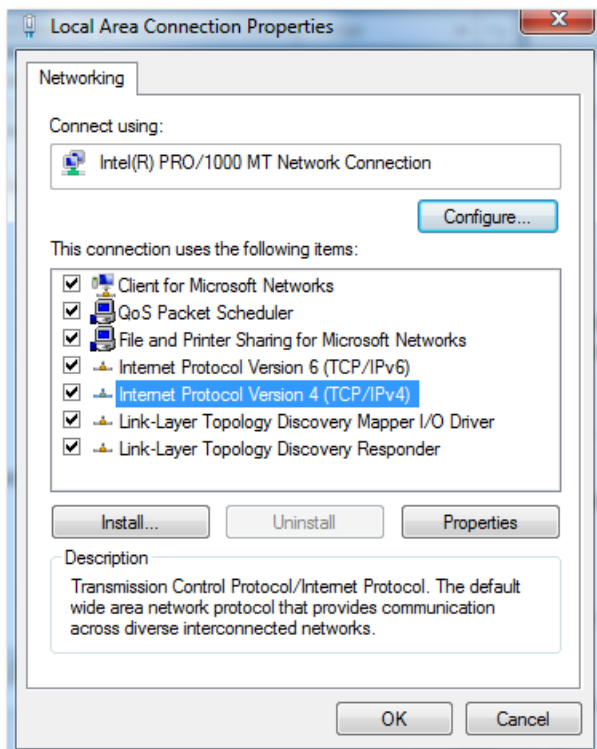
Step 1 Click  in the bottom right corner of the desktop and choose **Open Network and Sharing Center**.



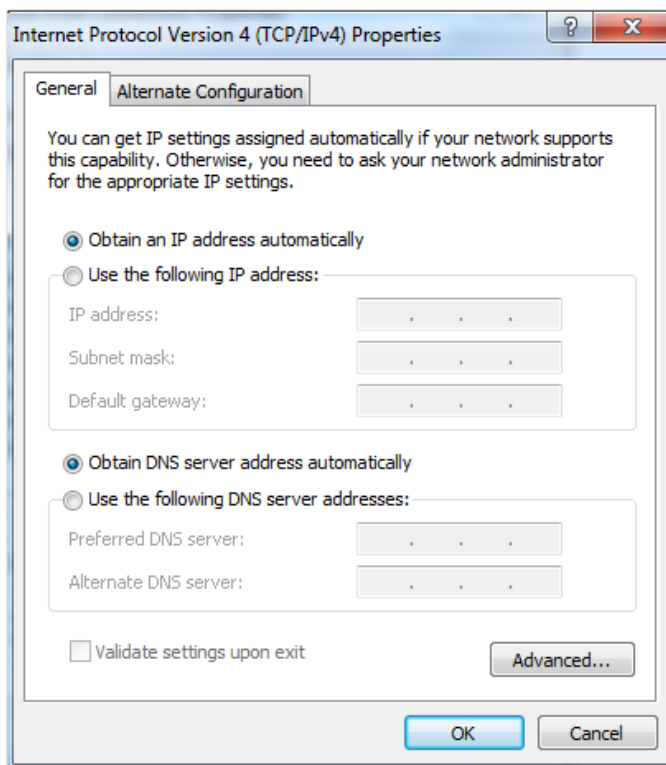
Step 2 Click **Local Area Connection** and then **Properties**.



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



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



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

---End

A.2 Acronyms and abbreviations

Acronym or Abbreviation	Full Spelling
AES	Advanced Encryption Standard
BR	Border Relay
CE	Customer Edge
DDNS	Dynamic Domain Name System
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
GMT	Greenwich Mean Time
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
SIM	Subscriber Identity Module
SMS	Short Message Service

Acronym or Abbreviation	Full Spelling
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