

Tenda

Web User Guide

Wi-Fi 7 Dual-band Wireless Router



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, and this guide demonstrates how to configure functions by logging in to the device's web UI with the PC.

Applicable model

This user guide walks you through all functions on the Tenda Wi-Fi 7 Routers. The "router", "product", "node" and "node device" mentioned in this guide all refer to Wi-Fi 7 dual-band wireless routers. All the screenshots and product figures herein, unless otherwise specified, are taken from RE6L Pro.

Conventions

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



In this guide, unless otherwise specified:

- The firmware version uses V16.03.06.11 of RE6L Pro as an example.
- The screenshots use the router mode as an example. For other working modes, the actual web UI prevails.

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

For more documents

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

Technical support

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

Email address: support@tenda.cn

Website: www.tendacn.com

Revision history

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

Version	Date	Description
V1.0	2024-09-26	Original publication.

Contents

Mesh networking	1
1.1 Overview	1
1.2 Set up as an add-on node	2
Connect the client to the router's network	8
2.1 Wired connection	9
2.2 Wireless connection	10
2.3 WPS connection	11
Web UI 15	
3.1 Log in to the web UI	15
3.2 Log out of the web UI	16
3.3 Change the language	17
3.4 Web UI layout	18
Internet settings	19
4.1 Modify IPv4 internet settings	20
4.2 IPv6 settings	26
4.3 Modify MTU	35
4.4 Clone MAC address	37
4.5 Modify WAN speed	38
4.6 Change the device working mode	39
Wi-Fi settings	54
5.1 Change Wi-Fi name and Wi-Fi password	55
5.2 Guest WiFi Settings	56
5.3 Schedule disable Wi-Fi	58
5.4 Change the Wi-Fi signal strength	59
Network status	60
6.1 View network status	61
6.2 View Wi-Fi name	64
6.3 View the number of Mesh nodes and clients	65
6.4 View network status, node and client details	68
6.5 View system information	69
Client management	70
7.1 Add the client to the blacklist	71
7.2 Add the client to the whitelist	75
7.3 Remove a client from the blacklist	79
7.4 Internet access speed control	81
7.5 Only prohibit specified clients from accessing the internet	82
7.6 Internet access rule control	84

Optimize network performance	87
8.1 One-click optimization	88
8.2 Network diagnosis	89
8.3 Change channel and bandwidth	90
8.4 Enable or disable MLO function	92
8.5 Enable or disable OFDMA function	93
8.6 UPnP	95
Remote access	96
9.1 Remote web management	97
9.2 DDNS	100
9.3 Port mapping	104
9.4 DMZ host	109
9.5 VPN	113
Network security	124
10.1 Hide the Wi-Fi network	125
10.2 Enable or disable MESH/WPS button	126
10.3 Change the login password	127
10.4 Firewall	128
Advanced	130
11.1 Turn on or turn off the indicator of router	131
11.2 Enable or disable TWT function	134
11.3 IPTV	135
11.4 Enable or disable router's WAN/LAN auto-negotiation function	140
11.5 Change LAN IP address	141
11.6 Change DHCP server	143
11.7 Assign static IP address to LAN client	145
11.8 Static routing	147
System maintenance	151
12.1 Reboot device	152
12.2 Auto system maintenance	154
12.3 Firmware upgrade	155
12.4 Backup & restore	157
12.5 System time	164
12.6 View or export the system log	167
Appendixes	168
A.1 FAQ	168
A.2 Connect to a hidden Wi-Fi network	173
A.3 Acronyms and Abbreviations	174

1 Mesh networking

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

This chapter introduces Mesh networking methods in the following sections:

[Overview](#)

[Set up as an add-on node](#)

1.1 Overview

Tenda WiFi+ routers 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.

1.2 Set up as an add-on node

This section describes how to add a new router to extend the wireless 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 corresponding router model to configure the router to the internet.



TIP

- If there are more than two secondary nodes, place the primary node in the key area and ensure that no more than one node is between the primary node and the secondary node.
- Before using a new router to extend the network, ensure that the existing router (primary node) has been connected to the internet and the new router (secondary node) is restored to the factory settings.
- The router can be networked with **Tenda WiFi+** routers. If the router fails to be added to an existing network, contact Tenda customer service for help. The following uses two RE6L Pro routers as an example.

1.2.1 MESH button networking



TIP

Before using the new router to extend the network, ensure that the [MESH/WPS button](#) function is enabled on the existing router (primary node).

Step 1 Add to the existed network.

1. Place the new router 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.
2. Press (1 to 3 seconds) the networking button (WPS or MESH) on the existing router. The indicator blinks green fast.
3. Press (1 to 3 seconds) the networking button (WPS or MESH) of the new router within 2 minutes. The indicator blinks green fast.



Observe the indicator of the new router. When the indicator turns **solid green**, it indicates that the router is added to the existing network and 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
If the indicator of the new router is still blink green slowly (indicates not connected to the internet) after 3 minutes. 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:

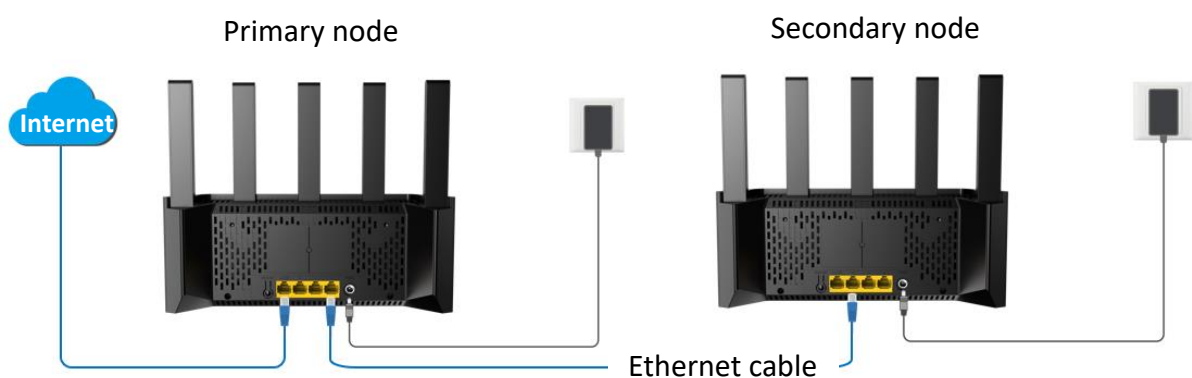
- **Wired devices:** Connect to the Ethernet port of any node using an Ethernet cable.
- **Wi-Fi-enabled devices:** Reconnect to the Wi-Fi network of the node. (The Wi-Fi name and Wi-Fi password of all nodes are the same.)

1.2.2 Wired networking

Assume that the Ethernet cable has been deployed in advance between the living room and the bedroom at home, the router RE6L Pro (primary node) placed in the living room has been connected to the internet, and now you need to deploy a router RE6L Pro (planned as a secondary node) in the bedroom to extend the wireless network.

Step 1 Place the new router (RE6L Pro) where you want to deploy it, which is **bedroom** in this example. Power on the new router (RE6L Pro). Wait until the startup of the new router (RE6L Pro) is complete (the indicator blinks green slowly).

Step 2 Connect the Ethernet port of the primary node to the Ethernet port of the new router (RE6L Pro) using an Ethernet cable.



---End

The router will automatically network. Please wait about 1 minute. When the indicator of the new router (RE6L Pro) turns **solid green**, the networking is successful. The RE6L Pro becomes a secondary node in the network.

To access the internet with:

- **Wired devices:** Connect to an Ethernet port of any node using an Ethernet cable.
- **Wi-Fi-enabled devices:** Reconnect to the Wi-Fi network of the node. (The Wi-Fi name and Wi-Fi password of all nodes are the same.)



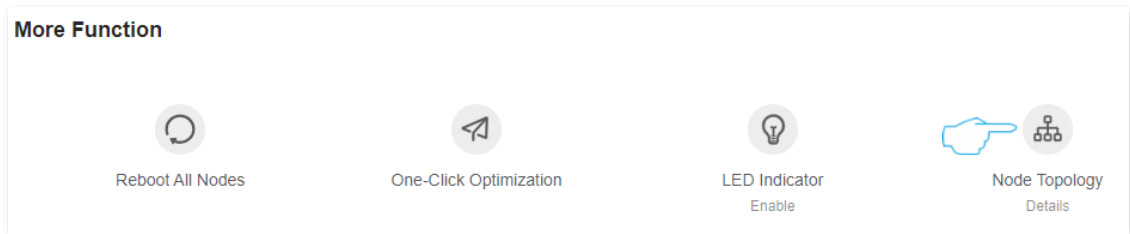
TIP

- After the wired networking is successful, if the Ethernet cable connecting the two RE6L Pro routers are removed, the system automatically switches to the wireless networking. To obtain better internet access experience after switching to a wireless network, go to [select an appropriate position for the new router](#).
- To obtain a better wireless internet experience, keep your nodes away from electronics with strong interference, such as microwave ovens, induction cookers, and refrigerators.

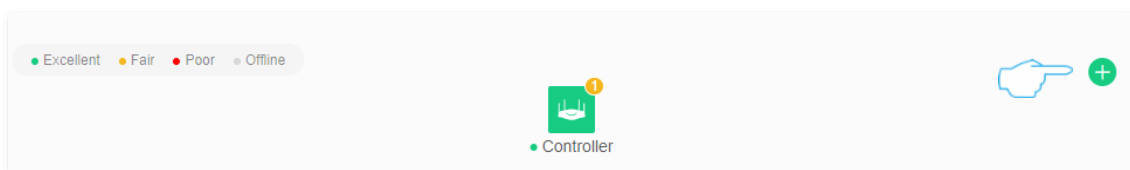
1.2.3 Scanning networking

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

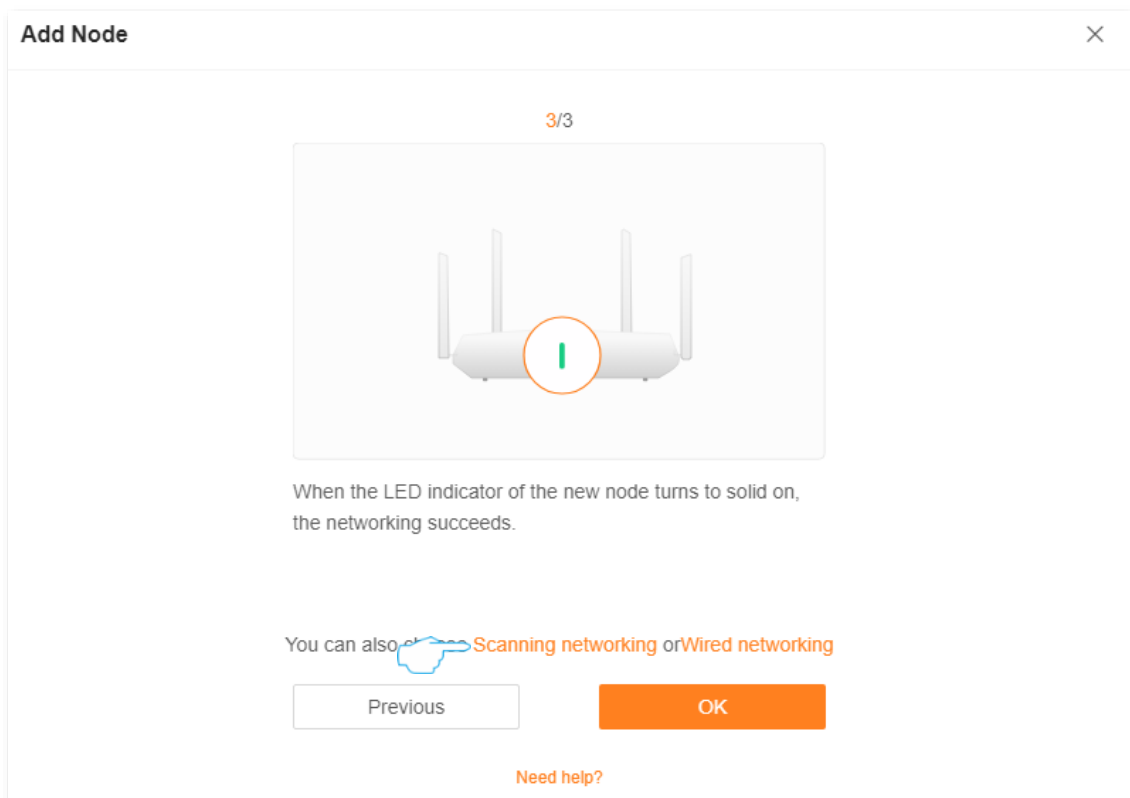
Step 2 Navigate to **Network Status**, click  (**Node Topology**) in the **More Function** module.



Step 3 Click .



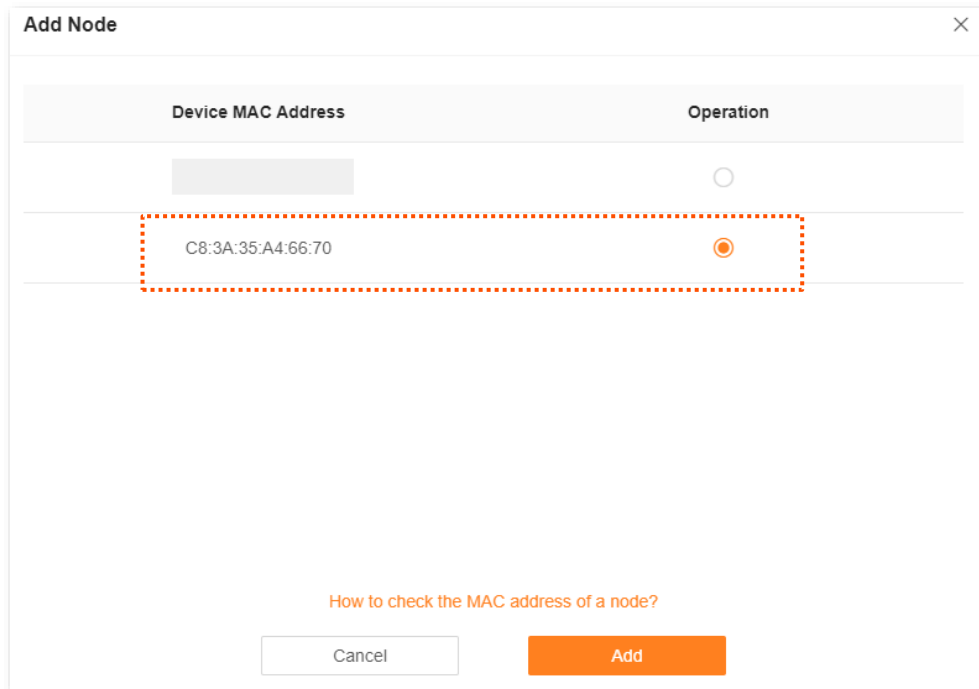
Step 4 Click **Next > Next**, ignore the MESH button networking guidance, and click **Scanning networking**.



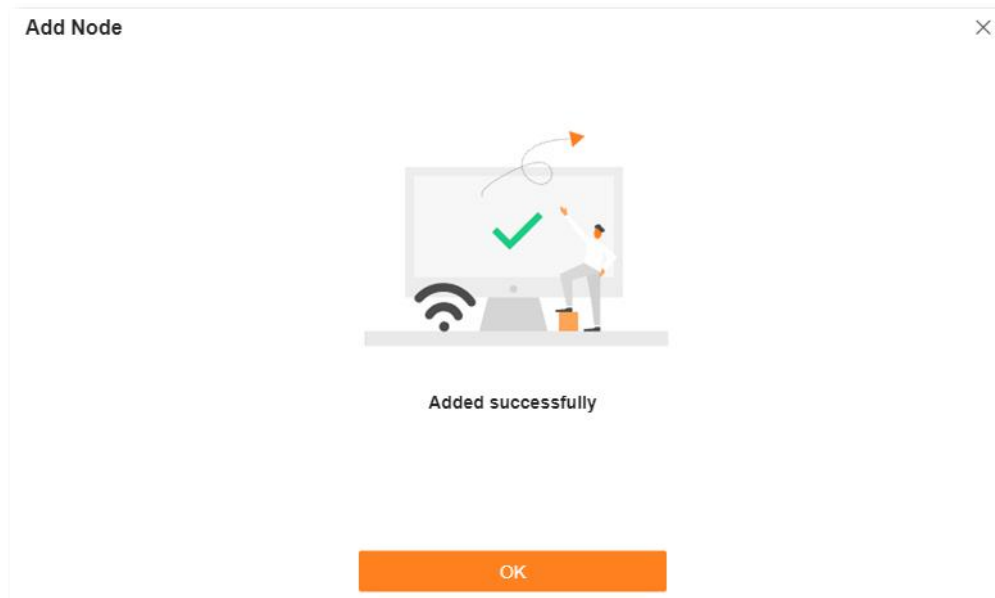
Step 5 The system discovers new nodes, ensure that the MAC address or SN is the same as the MAC address or SN on the bottom label of the new router, select a node, and click **Add**. The MAC address is taken as an example here. The following figure is for reference only.



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



Wait until the ongoing process is complete.



---End

Back to the **Node Topology** module, you can see that the newly added RE6L Pro router has successfully joined the network as a secondary node.



To access the internet with:

- **Wired devices:** Connect to an Ethernet port of any node using an Ethernet cable.
- **Wi-Fi-enabled devices:** Reconnect to the Wi-Fi network of the node. (The Wi-Fi name and Wi-Fi password of all nodes are the same.)

2

Connect the client to the router's network

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

This chapter introduces how to connect the clients to the router's network in the following sections:

[Wired connection](#)

[Wireless connection](#)

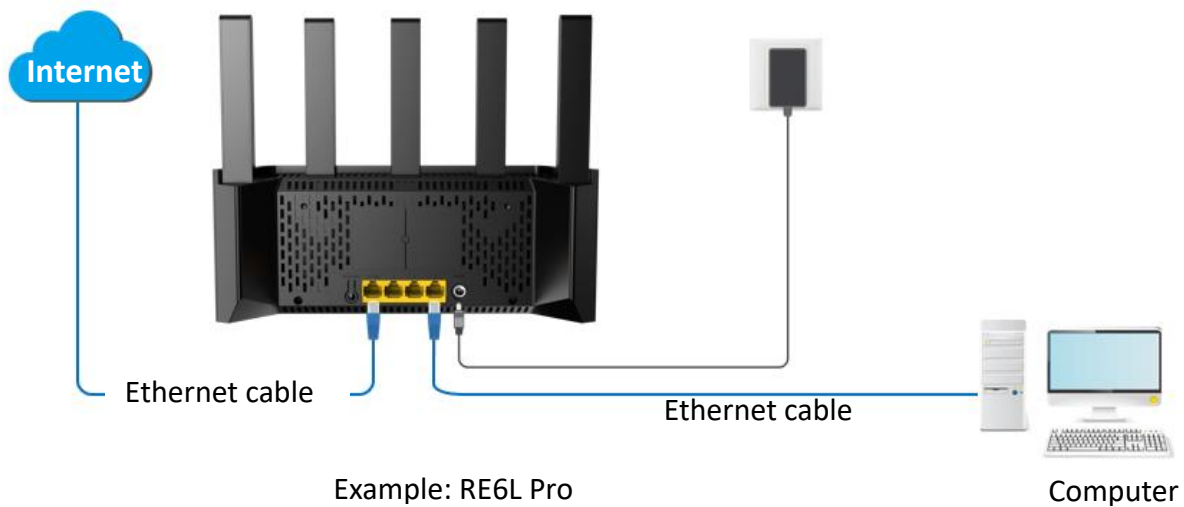
[WPS connection](#)

2.1 Wired connection

Connect the computer to any Ethernet port of the router. If the [WAN/LAN auto-negotiation](#) function is disabled, connect the computer to any Ethernet port 2/3/4 of the router.



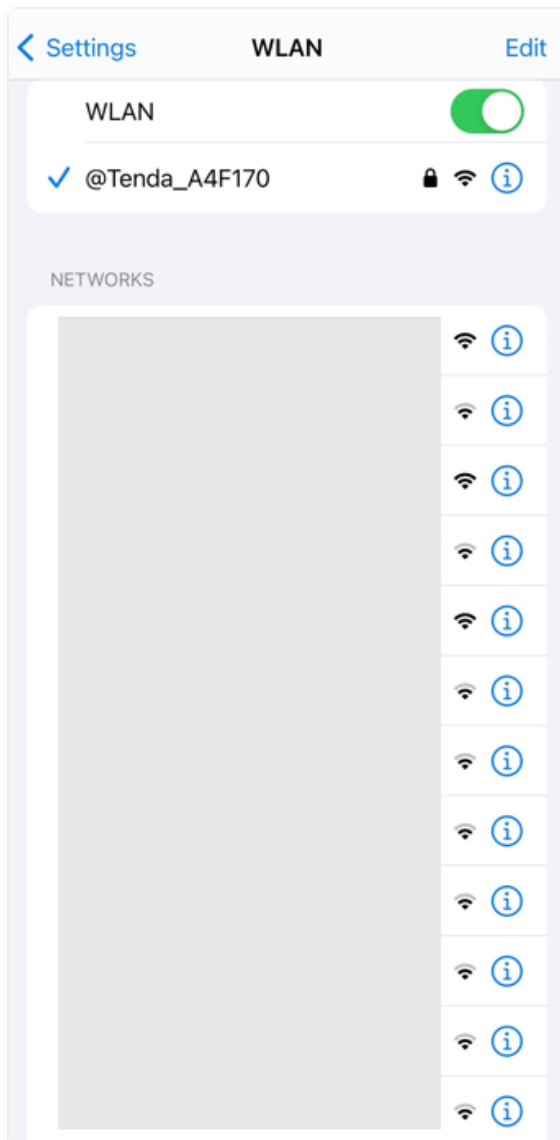
After the IPTV function is enabled on the router, the Ethernet port 4 on the primary node only functions as the IPTV port to connect to the set-top box. If you want to modify the IPTV bound Ethernet port, refer to the [IPTV](#) settings.



2.2 Wireless connection

The smartphone is taken as an example.

Connect the smartphone to the router's wireless network. The **@Tenda_A4F170** is taken as an example here.



- At the first login, connect the SSID (Wi-Fi name) on the label of the device.
 - When you log in to the router again, use the new Wi-Fi name and Wi-Fi password to connect to the wireless network.
-

2.3 WPS connection

The WPS function enables Wi-Fi-enabled devices, such as smartphones, to connect to Wi-Fi networks of the router without entering the password.



The wireless network whose encryption mode is WPA3 does not support WPS connection. To use the WPS function of the router, you are recommended to set the encryption mode of the router's wireless network to **WPA2-PSK**.

2.3.1 Method 1: Connect to the router's Wi-Fi through PBC

Step 1 Enable the WPS-PBC function on the router.

Method 1: Through MESH button on the router body.


Press the **MESH** button on the router body.



Example: RE6L Pro


Method 2: Through WPS button on the router's web UI.

Procedure:

1. [Log in to the web UI of the router.](#)
2. Navigate to **More > WiFi Settings > WPS**.
3. Locate the device you want to connect to Wi-Fi and click . The **Router** is used as an example here.


WPS

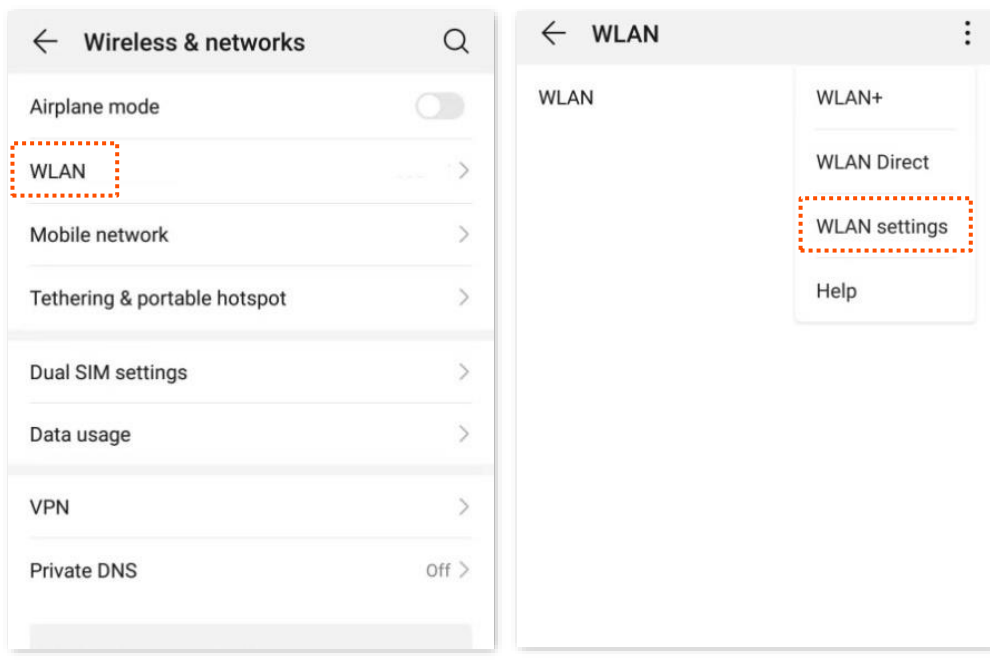
With this function enabled, wireless clients, such as mobile phones, can connect to the router's WiFi network of the router easily.

Node Name	Operation
Router	

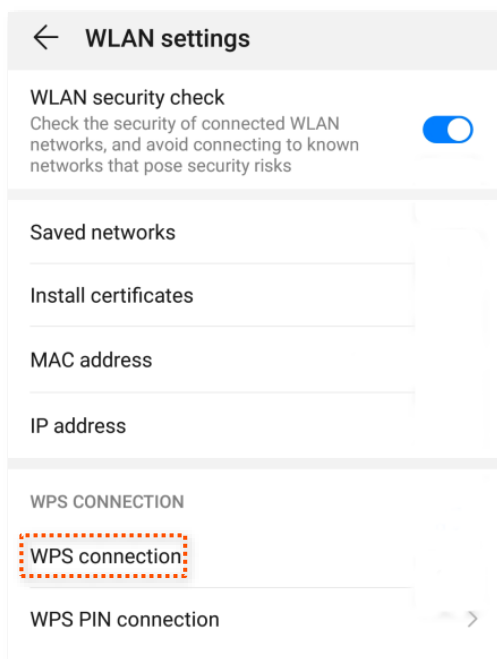
The indicator blinks fast.

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

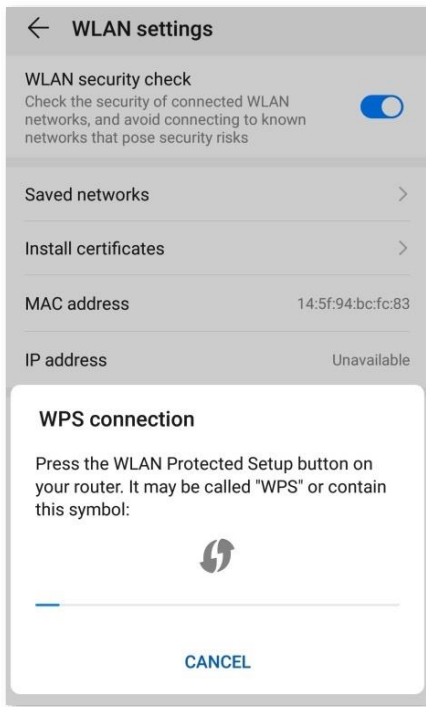
1. Find WLAN settings on your phone.
2. Tap , and choose **WLAN settings**.



3. Choose WPS connection.



Wait until the WPS negotiation completes. Now the phone is connected to the Wi-Fi network.



---End

2.3.2 Method 2: Connect to the router's Wi-Fi through PIN code



This method only supports entering the WPS PIN code of the router on the wireless clients to connect to the router's Wi-Fi. It is usually used for wireless network adapter to connect to the router's Wi-Fi. For details, see the user guide of the corresponding wireless network adapter.

Step 1 Check and record the WPS PIN code (Pin No) on the label of the router.

Step 2 Enter the WPS PIN code of the router on the wireless clients for connection. The connection is successful within 2 minutes.

---End

3 Web UI

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

This chapter introduces basic information of the web UI in the following sections:

[Log in to the web UI](#)

[Log out of the web UI](#)

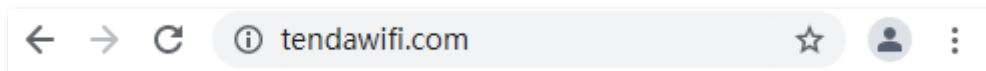
[Change the language](#)

[Web UI layout](#)

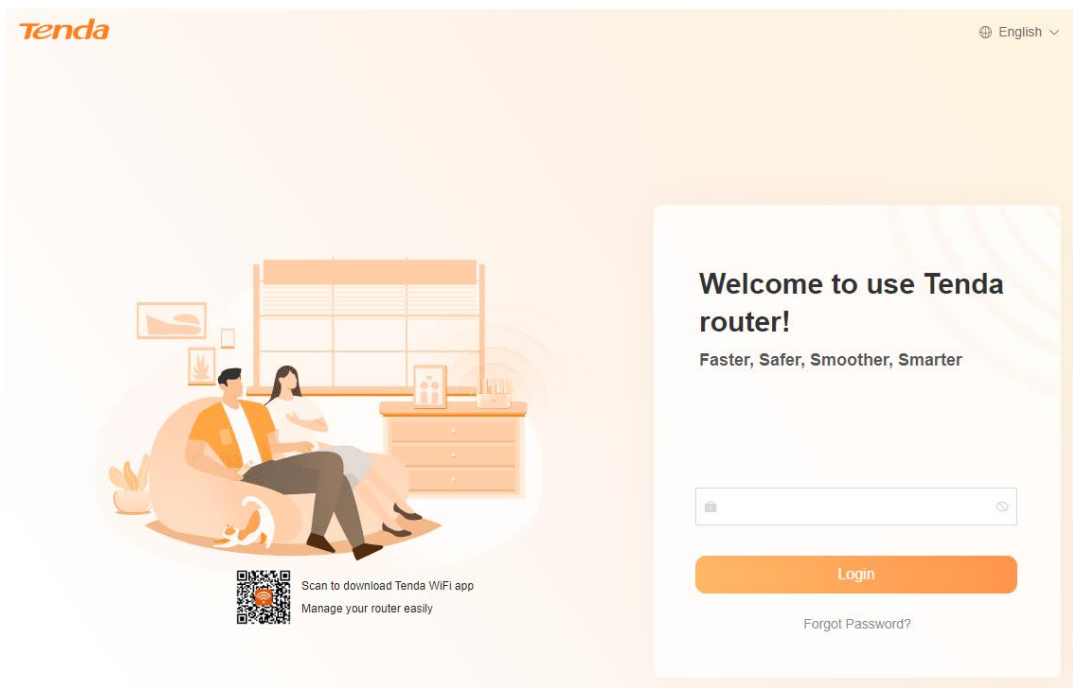
3.1 Log in to the web UI

To log in to the web UI, perform the following steps:

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



Step 2 Enter the login password, and click **Login**.



---End

After logging in to the router's web UI, you can configure the router as required.



TIP

If the login page does not appear, try the following solutions.

- Ensure that the router is powered on properly.
- Use the default IP address (**<http://tendawifi.com>** or **<http://192.168.0.1>**) to log in to the router.
- Ensure that the computer is connected to the router's Ethernet port, and the Ethernet cable is connected properly. If the [WAN/LAN auto-negotiation](#) function is disabled, connect the computer to any Ethernet port 2/3/4 of the router.
- Ensure that the computer is set to **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
- [Restore the router to factory settings](#) and try again.

If you forgot the login password, try the following solutions.

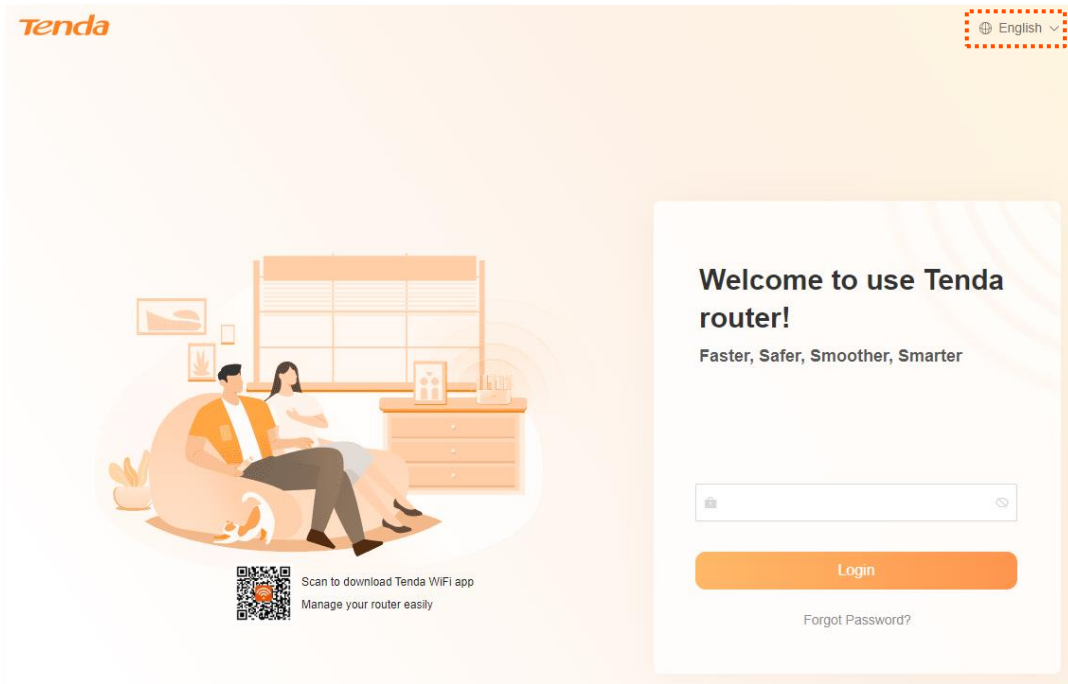
- The Wi-Fi password is set to the login password of the router by default. Try to use the Wi-Fi password to log in to the router.
- If the problem persists, [restore the router to factory settings](#) and try again.

3.2 Log out of the web UI

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

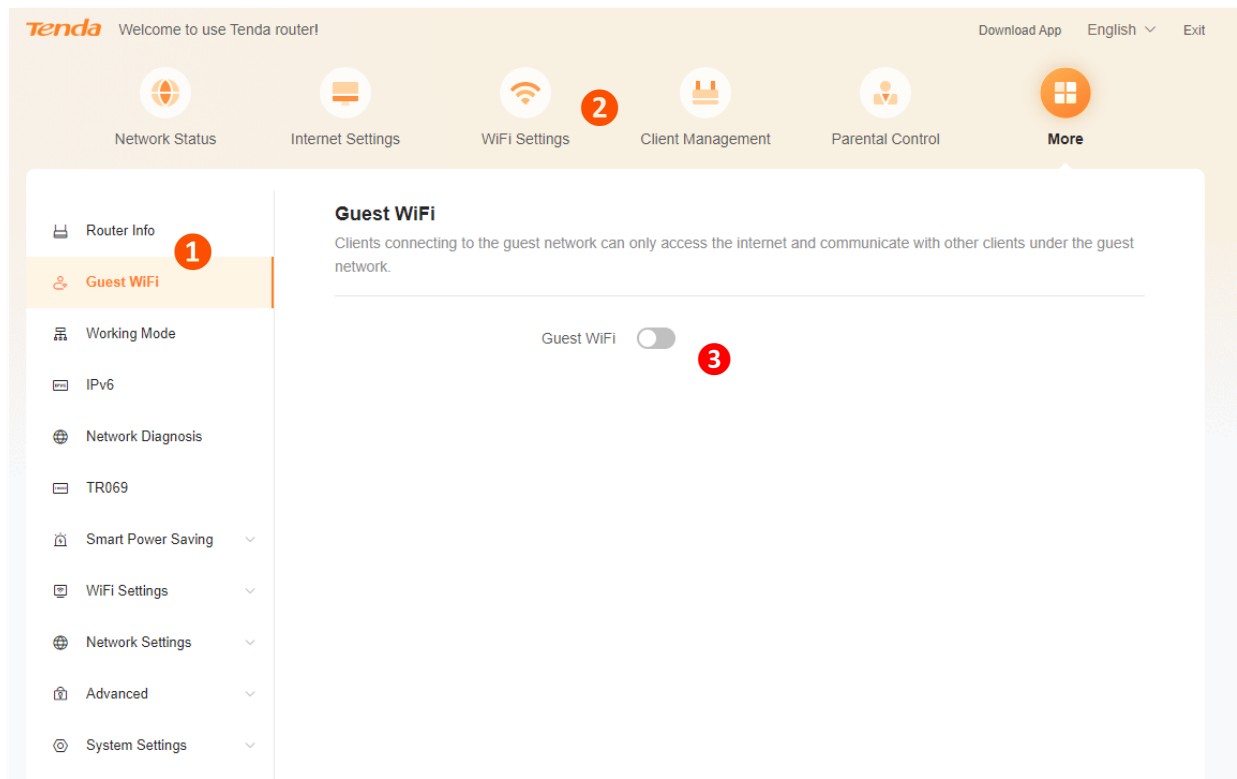
3.3 Change the language

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



3.4 Web UI layout

The web UI of the router consists of two sections, including the navigation bar and the configuration area. See the following figure.



TIP

Features displayed in gray are not available or cannot be configured under the current condition.

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

4 Internet settings

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

This chapter includes the following parts:

[Modify IPv4 internet settings](#)

[IPv6 settings](#)

[Modify MTU](#)

[Clone MAC address](#)

[Modify WAN speed](#)

[Change the device working mode](#)

4.1 Modify IPv4 internet settings

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

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

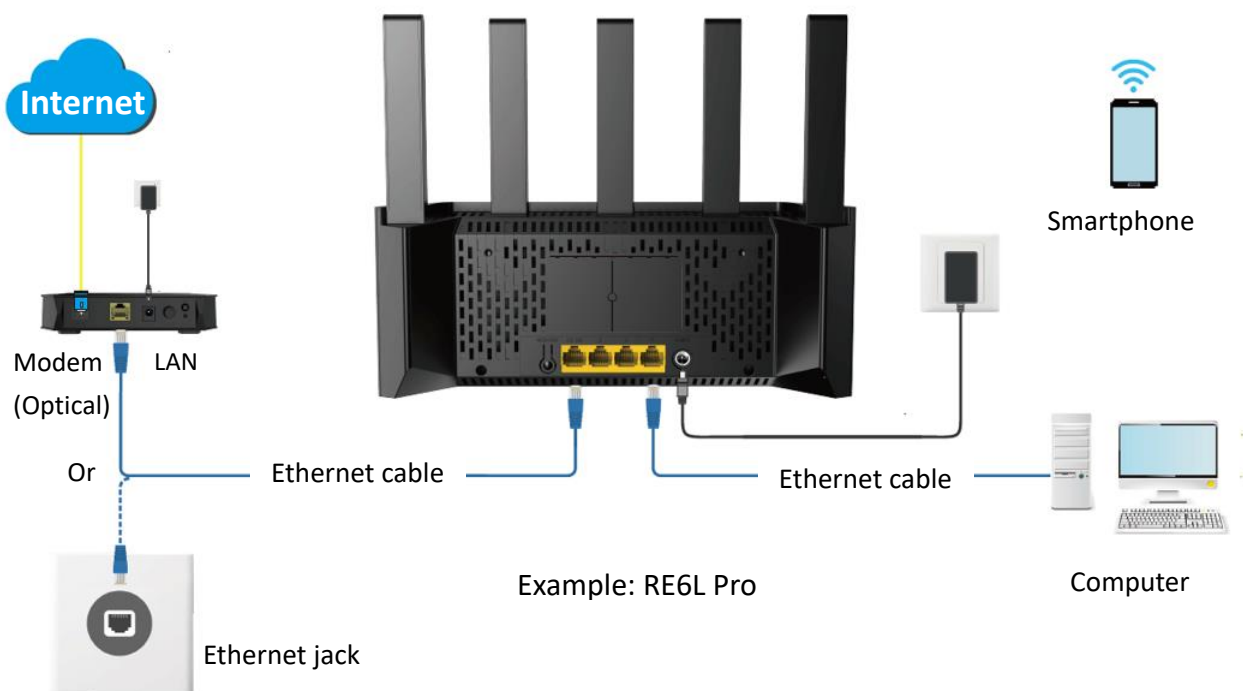


TIP

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

4.1.1 Access the internet with a PPPoE account

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



TIP

By default, the [WAN/LAN auto-negotiation](#) function of the router is enabled, and the Ethernet cable connected to the internet can be connected to any Ethernet port. If the WAN/LAN auto-negotiation function is disabled, connect the Ethernet cable connected to the internet to Ethernet port 1 (WAN port).

To access the internet with a PPPoE account:

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

Step 2 Set **ISP Type**.



If you select **Manual** for **ISP Type**, enter **Internet VLAN ID** and **IPTV VLAN ID** (if any) provided by your ISP. Blank VLAN ID indicates that the IPTV function is disabled.

Step 3 Set **Internet Connection Type** to **PPPoE**.

Step 4 Enter the **PPPoE Username** and **PPPoE Password** provided by your ISP.

Step 5 Perform advanced settings as required.

- If the ISP provides **Server Name** and **Service Name**, input the corresponding parameters in the corresponding field. If not, leave it as default.
- DNS settings, in general, can be left as default. If your ISP provides a DNS address, change the DNS settings to **Manual** and fill in the correct DNS address. If there is only one DNS address, fill in the **Primary DNS**.

Step 6 Click **Connect**.

Internet Settings

Network Status: Disconnected

ISP Type: Normal

Internet Connection Type: PPPoE
Select this type if you access the internet using the PPPoE account and PPPoE password.

PPPoE Username:

PPPoE Password:

Advanced v

Connect

---End

Wait until the network status changes to **Connected**, then you can access the internet.

Internet Settings

Network Status: **Connected**

If you cannot access the internet, try the following solutions:

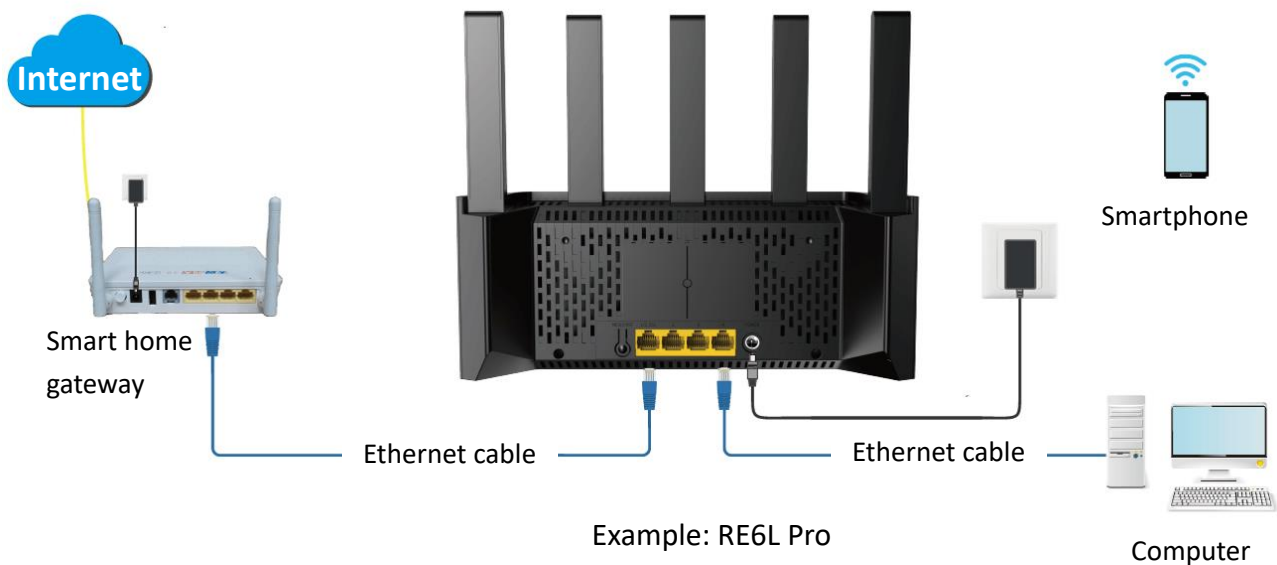
- If **No response from the remote server** displays in **Network Status**, you are recommended to set the router to [Dynamic IP address](#) for internet access.
- If the problem persists, refer to [Router disconnected from the internet](#) to resolve the problem.

4.1.2 Access the internet through a dynamic IP address

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

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

The application scenario is shown below.



By default, the [WAN/LAN auto-negotiation](#) function of the router is enabled, and the Ethernet cable connected to the internet can be connected to any Ethernet port. If the WAN/LAN auto-negotiation function is disabled, connect the Ethernet cable connected to the internet to Ethernet port 1 (WAN port).

To access the internet through dynamic IP address:

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

Step 2 Set **ISP Type**.



If you select **Manual** for **ISP Type**, enter **Internet VLAN ID** and **IPTV VLAN ID** (if any) provided by your ISP. Blank VLAN ID indicates that the IPTV function is disabled.

Step 3 Set **Internet Connection Type** to **Dynamic IP**.

Step 4 Perform advanced settings as required.

DNS settings, in general, can be left as default. If your ISP provides a DNS address, change the DNS settings to **Manual** and fill in the correct DNS address. If there is only one DNS address, fill in the **Primary DNS**.

Step 5 Click **Connect**.

The screenshot shows the 'Internet Settings' interface. At the top, it says 'Internet Settings'. Below that, 'Network Status' is 'Disconnected'. There are two dropdown menus: 'ISP Type' set to 'Normal' and 'Internet Connection Type' set to 'Dynamic IP'. A note below the second dropdown says: 'Select this type if you can access the internet simply by plugging in an Ethernet cable for internet connection.' There is an 'Advanced' link with a dropdown arrow. At the bottom, there is a large orange 'Connect' button.

---End

Wait until the network status changes to **Connected**, then you can access the internet.

The screenshot shows the 'Internet Settings' interface. At the top, it says 'Internet Settings'. Below that, 'Network Status' is 'Connected'.

If you cannot access the internet, refer to [Router disconnected from the internet](#) to resolve the problem.

4.1.3 Access the internet with a set of 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.

To access the internet with a set of static IP address information:

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

Step 2 Set **ISP Type**.



If you select **Manual** for **ISP Type**, enter **Internet VLAN ID** and **IPTV VLAN ID** (if any) provided by your ISP. Blank VLAN ID indicates that the IPTV function is disabled.

Step 3 Set **Internet Connection Type** to **Static IP**.

Step 4 Set **IP Address**, **Subnet Mask**, **Default gateway** and **Primary DNS**, and **Secondary DNS**

with the information provided by your ISP.

If your ISP provides only one DNS address, fill in the **Primary DNS**.

Step 5 Click **Connect**.

Internet Settings

Network Status Verifying your PPPoE user name and password... Please wait

ISP Type

Internet Connection Type
Select this type if you access the internet using the fixed IP address information.

IP Address

Subnet Mask

Default gateway

Primary DNS

Secondary DNS

Advanced

---End

Wait until the network status changes to **Connected**, then you can access the internet.

Internet Settings

Network Status **Connected**

If you cannot access the internet, refer to [Router disconnected from the internet](#) to resolve the problem.

4.1.4 Set up dual access connection

In countries like Russia, the ISP may require you to set up dual access. One is for access to the internet through PPPoE, PPTP or L2TP, and the other is for access to the “local” resources where the ISP is located through DHCP or static IP address. If your ISP provides such connection information, you can set up dual access to access the internet.

To set up dual access connection:

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

Step 2 Set **ISP Type** to **Russia**.

Step 3 Set **Internet Connection Type**, which is **Russia PPTP** in this example, and fill in required parameters.

The screenshot shows the 'Internet Settings' configuration page. The fields are as follows:

- ISP Type: Russia
- Internet Connection Type: Russia PPTP
- Server IP Address/Domain Name: (empty)
- User Name: (empty)
- Password: (empty)
- Address Type: Dynamic IP Address, Static IP Address
- DNS Settings: Auto

Below the DNS Settings, there is an 'Advanced' dropdown menu. At the bottom of the form is a large orange 'Connect' button.

Step 4 Set **Address type**, and fill in required parameters.

Step 5 Click **Connect**.

---End

Wait until the network status changes to **Connected**, then you can access the internet.

The screenshot shows the 'Internet Settings' page with the 'Network Status' displayed as 'Connected' in green text.

4.2 IPv6 settings

4.2.1 Overview

IPv6, abbreviated for Internet Protocol Version 6, is the second-generation network layer protocol. IPv6 is an upgraded version of Internet Protocol version 4 (IPv4), which is the solution that addresses the relatively limited number of IP addresses possible under IPv4.

An IPv6 address is 128 bits long and is arranged in eight groups, each of which is 16 bits. Each group is expressed as four hexadecimal digits and the groups are separated by colons. An IPv6 address is split into two parts:

- Network Prefix: n bits, equivalent to the network ID in the IPv4 address.
- Interface Identifier: 128-n bits, equivalent to the host ID in the IPv4 address.

This router supports IPv4 and IPv6. You can connect to the IPv6 network of ISPs through IPv6 WAN settings.

The router can access the IPv6 network of ISPs through three connection types. Choose the connection type by referring to the following chart.

Scenario	Connection Type
<ul style="list-style-type: none"> • The ISP does not provide any PPPoEv6 user name and password and information about the IPv6 address. • You have a router that can access the IPv6 network. 	DHCPv6
IPv6 service is included in the PPPoE user name and password.	PPPoEv6
The ISP provides you with a set of information including IPv6 address, subnet mask, default gateway and DNS server.	Static IPv6 address



- Before configuring the IPv6 function, ensure that you are within the coverage of the IPv6 network and already subscribe to the IPv6 internet service. Contact your ISP for any doubt about it.
- The router supports automatic NAT66. If the LAN port cannot obtain a prefix after IPv6 is configured, the upstream device may not support PD prefix delivery. In this case, the router automatically enables the NAT66 function.

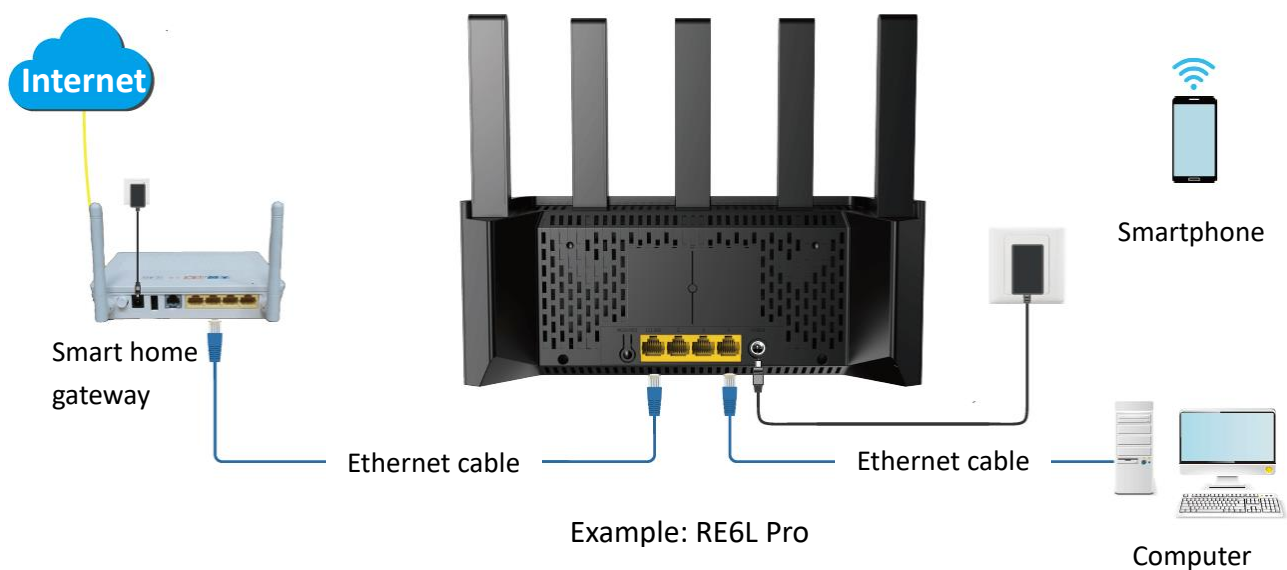
4.2.2 IPv6 WAN settings

DHCPv6

DHCPv6 enables the router to obtain an IPv6 address from the DHCPv6 server to access the internet. It is applicable in the following scenarios:

- The ISP does not provide any PPPoEv6 user name and password and information about the IPv6 address.
- You have a router that can access the IPv6 network, and this router is used as a new router.

The application scenario is shown below.



By default, the [WAN/LAN auto-negotiation](#) function of the router is enabled, and the Ethernet cable connected to the internet can be connected to any Ethernet port. If the WAN/LAN auto-negotiation function is disabled, connect the Ethernet cable connected to the internet to Ethernet port 1 (WAN port).

Configuration procedure:

- Step 1** [Log in to the web UI of the router.](#)
- Step 2** Navigate to **More > IPv6**.
- Step 3** Enable the **IPv6** function.
- Step 4** Set **Internet Connection Type** to **DHCPv6**.
- Step 5** Click **Save**.

IPv6

This device supports IPv6 and can access IPv6 network.

IPv6

IPv6 WAN

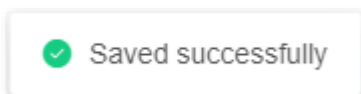
Internet Connection Type

IPv6 LAN

Assignment Method Auto
 SLAAC
 SLAAC+RDNSS
 DHCPv6

---End

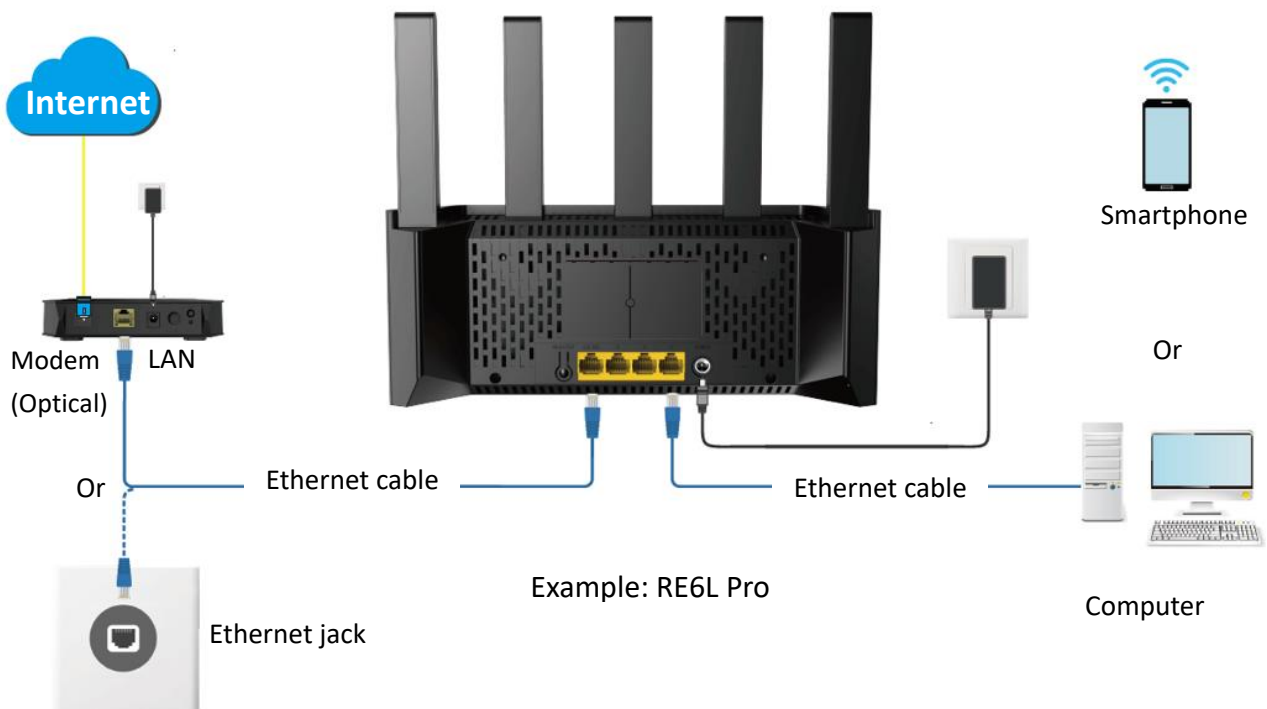
The following message is displayed, indicating that the settings are saved successfully.



After the settings are completed, you can perform [IPv6 network test](#) to check whether IPv6 network settings are successful.

PPPoEv6

If your ISP provides you with the PPPoE user name and password with IPv6 service, you can choose PPPoEv6 to access the internet.



By default, the [WAN/LAN auto-negotiation](#) function of the router is enabled, and the Ethernet cable connected to the internet can be connected to any Ethernet port. If the WAN/LAN auto-negotiation function is disabled, connect the Ethernet cable connected to the internet to Ethernet port 1 (WAN port).

Configuration procedure:

- Step 1** [Log in to the web UI of the router.](#)
- Step 2** Navigate to **More > IPv6**.
- Step 3** Enable the **IPv6** function.
- Step 4** Set **Internet Connection Type** to **PPPoEv6**.
- Step 5** Set **PPPoE Username** and **PPPoE Password**.
- Step 6** Click **Save**.

IPv6
This device supports IPv6 and can access IPv6 network.

IPv6

IPv6 WAN

Internet Connection Type ▼

PPPoE Username

PPPoE Password 🗨

IPv6 LAN

Assignment Method Auto
 SLAAC
 SLAAC+RDNSS
 DHCPv6

---End

The following table describes the parameters displayed on this page.

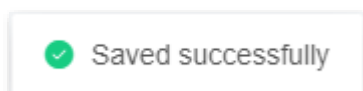
Parameter description

Parameter	Description
PPPoE Username	Specify the PPPoE user name and password provided by your ISP.
PPPoE Password	IPv4 and IPv6 services share the same PPPoE account.



TIP

The following message is displayed, indicating that the settings are saved successfully.



After the settings are completed, you can perform [IPv6 network test](#) to check whether IPv6 network settings are successful.

Static IPv6 address

When your ISP provides you with information including IPv6 address, subnet mask, default gateway and DNS server, you can choose this connection type to access the internet with IPv6.

Configuration procedure:

- Step 1** [Log in to the web UI of the router.](#)
- Step 2** Navigate to **More > IPv6**.
- Step 3** Enable the **IPv6** function.
- Step 4** Set the **Internet Connection Type** to **Static IPv6 Address**.
- Step 5** Enter the required parameters under **IPv6 WAN**.
- Step 6** Click **Save**.

IPv6
This device supports IPv6 and can access IPv6 network.

IPv6

IPv6 WAN

Internet Connection Type: Static IPv6 Address ▾

IPv6 Address: /

Default IPv6 Gateway:

Primary IPv6 DNS:

Secondary IPv6 DNS:

IPv6 LAN


Assignment Method: Auto
 SLAAC
 SLAAC+RDNSS
 DHCPv6

LAN Prefix: /

---End

The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
IPv6 Address	Specify the fixed IPv6 address information provided by your ISP.
Default IPv6 Gateway	 TIP
Primary IPv6 DNS	If your ISP only provides one DNS address, leave the secondary IPv6
Secondary IPv6 DNS	DNS blank.

The following message is displayed, indicating that the settings are saved successfully.



After the settings are completed, you can perform [IPv6 network test](#) to check whether IPv6 network settings are successful.

IPv6 network test:

You can ping an IPv6 website (240c::6666 for example) to check whether the router accesses the IPv6 network successfully. The following steps are for your reference.

Step 1 On a computer connected to the router, press **Windows + R** to open the **Run** dialog box.

Step 2 Type **cmd** and then click **OK** to open a regular Command Prompt.

Step 3 Enter ping **240c::6666** and press **Enter**.

---End

As shown in the following figure, if the number of packets received is not 0, the router accesses the IPv6 network successfully.

```
C:\Users\user>ping 240c::6666

Pinging 240c::6666 with 32 bytes of data:
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Reply from 240c::6666 bytes=32 time<1ms TTL=128

Ping statistics for 240c::6666:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss):
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

If the IPv6 network test fails, try the following solutions:

- Ensure that the IPv6 address obtaining type of Wi-Fi-enabled devices such as smartphones or computers is set to **Obtain an IPv6 address automatically** and **Obtain DNS server address automatically**.
- If the internet connection type is static IPv6 address, ensure that the IPv6 address of the WAN port, subnet prefix length, default gateway, and DNS are correct.
- Consult your ISP for help.


4.2.3 IPv6 LAN settings

To access the configuration page, [log in to the web UI of the router](#), and navigate to **More > IPv6**. Locate the **IPv6 LAN** module, you can configure the method for LAN IPv6 clients to obtain IPv6 addresses, and LAN port prefix addresses, to achieve multiple clients in the LAN to share your broadband service to access internet.

The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description	
Assignment Method	Auto	Specifies the stateful configuration and stateless configuration. The IPv6 prefix address, and DNS server address of the client can be obtained from the DHCPv6 server or through Route Advertisement (RA). The gateway address can be obtained from RA.
	SLAAC	Specifies the DHCPv6 stateless configuration. The IPv6 prefix address and gateway address of the client are obtained through RA, the interface address is generated based on the standard, and the DNS server address is obtained from the DHCPv6 server.
	SLAAC+RDNSS	Specifies the stateless address automatic configuration. The IPv6 prefix address and gateway address of the client are obtained through RA, the interface address is generated based on the standard, and the DNS server address is obtained from the RDNSS option in the RA packet.
	DHCPv6	Specifies the stateful configuration of Dynamic Host Configuration Protocol for IPv6 (DHCPv6). The client obtains the complete IPv6 address information, including the DNS server address, from the DHCPv6 server. The gateway address is obtained through RA.

Parameter	Description
LAN Prefix	<p>Specifies the IPv6 address prefix of LAN port.</p> <p> TIP</p> <p>It can be configured only when the Internet Connection Type of IPv6 WAN is Static IPv6 Address.</p> <hr/>

4.3 Modify MTU

Maximum Transmission Unit (MTU) is the largest data packet that a network device transmits.

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

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

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

MTU application description

MTU	Application
1500	Used for the most common settings in non-PPPoE connections and non-VPN connections.
1492, 1480	Used for PPPoE connections.
1472	It is the maximum value for the ping command. A packet with a larger size is fragmented.
1468	Used for DHCP connections.
1436	Used for VPN connections.

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

When the internet connection type is **PPPoE**, the default MTU value is **1480**. If the internet connection type is set to **Dynamic IP** or **Static IP**, the default MTU value is **1500**.

Internet Settings

Network Status Connected

Connected time 19hour(s) 13minute(s)

ISP Type Normal

Internet Connection Type PPPoE

Select this type if you access the internet using the PPPoE account and PPPoE password.

PPPoE Username

PPPoE Password

Advanced

Server Name Default setting is recommended

Service Name Default setting is recommended

MTU 1480

MAC Address Clone Default MAC

Default MAC Address:C8:3A:35:A3:75:31

DNS Settings Auto

4.4 Clone MAC address

When the internet settings are completed, if the router is still cannot be connected to the internet, it is possible that the ISP is bound to a certain MAC address (physical address). You can try to solve the problem through MAC address cloning.

Clone WAN MAC address



Use the correct MAC address to clone. The correct MAC address is the MAC address of the computer that can access the internet when the router is not in use, or the MAC address of the router's WAN port that can access the internet before.

Configuration procedure:

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

Step 2 Navigate to **Internet Settings**, and click **Advanced**.

Step 3 Click the drop-down menu of **MAC Address Clone** to change the MAC address.

- If you are using "a computer that can access the internet when the router is not in use to configure the router", select **Clone Local Host MAC**.
- If you are using another computer to configure the router, select **Custom** and fill in the correct MAC address (this could be "MAC address of the computer that successfully connected to the internet when connected directly to the Ethernet cable" or "MAC address of the router's WAN port that was previously connected to the internet").



To restore the MAC address of the WAN port to the factory MAC address, set **MAC Address Clone** to **Default MAC**.

Step 4 Click **Connect**. The following figure uses **Custom** as an example.

Advanced ^

Server Name	<input type="text" value="Default setting is recommended"/>
Service Name	<input type="text" value="Default setting is recommended"/>
MTU	<input type="text" value="1480"/>
MAC Address Clone	<input type="text" value="Custom"/>
Custom MAC Address	<input type="text" value="c8 : 3a : 35 : a3 : 75 : 31"/>
DNS Settings	<input type="text" value="Auto"/>

---End

4.5 Modify WAN speed

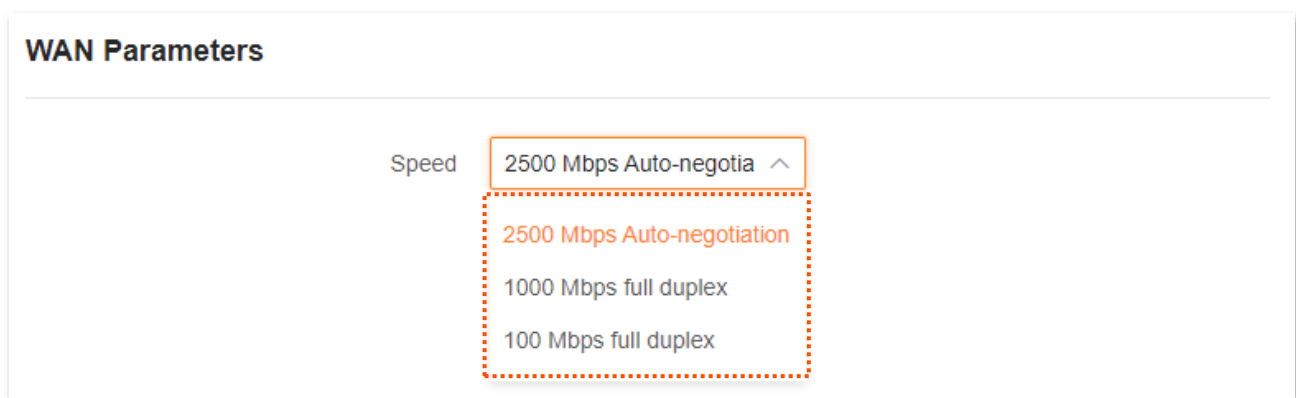
When the Ethernet cable is intact and connected to the WAN port properly, but **Disconnected** is still shown on the **Network Status** page, you can try to change the WAN port speed to solve the problem. Otherwise, keep the default settings.

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



TIP

WAN port negotiation speed cannot be configured if the [WAN/LAN auto-negotiation](#) function is enabled.



The following table describes the parameters displayed on this page.

Parameter description

Speed	Application
2500 Mbps Auto-negotiation	Indicates that the speed and duplex mode are determined through the negotiation with the peer port. The maximum negotiation speed is up to 2500 Mbps.
1000 Mbps full duplex	Indicates that the WAN port is working at the speed of 1000 Mbps, and the port can receive and send data packets at the same time.
100 Mbps full duplex	Indicates that the WAN port is working at the speed of 100 Mbps, and the port can receive and send data packets at the same time.

4.6 Change the device working mode

You can select a working mode for the router on this page. The router can work in the router mode, access point (AP) mode, Wireless Internet Service Provider (WISP) mode and Client+AP mode.

Current Mode is displayed after the working mode currently adopted by the router, as shown in the following figure. In this example, the current working mode is router mode.

You can select a working mode based on the following scenarios:

- To specify the network connection mode, select the [Router mode](#).
- To use an upstream router, select the [AP mode](#).
- To bridge the hotspot of ISPs, select the [WISP mode](#).
- To bridge all kinds of Wi-Fi networks, select the [Client+AP mode](#).

4.6.1 AP mode

When you have a smart home gateway that only provides wired internet access, you can set the router to work in AP mode to provide wireless coverage.



When the router is set to AP mode:

- Every physical port can be used as a LAN port.
 - Functions, such as bandwidth control and port mapping will be unavailable. Refer to the web UI for available functions.
-

To switch the working mode to AP mode:

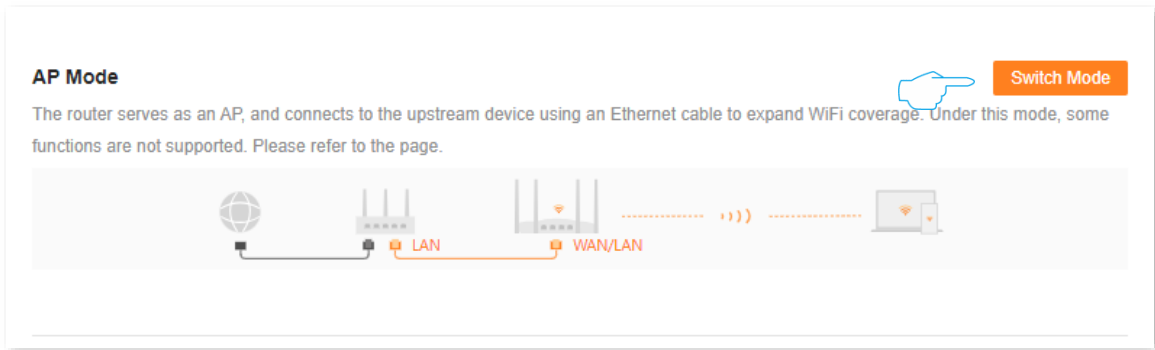
Step 1 Power on the router.

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

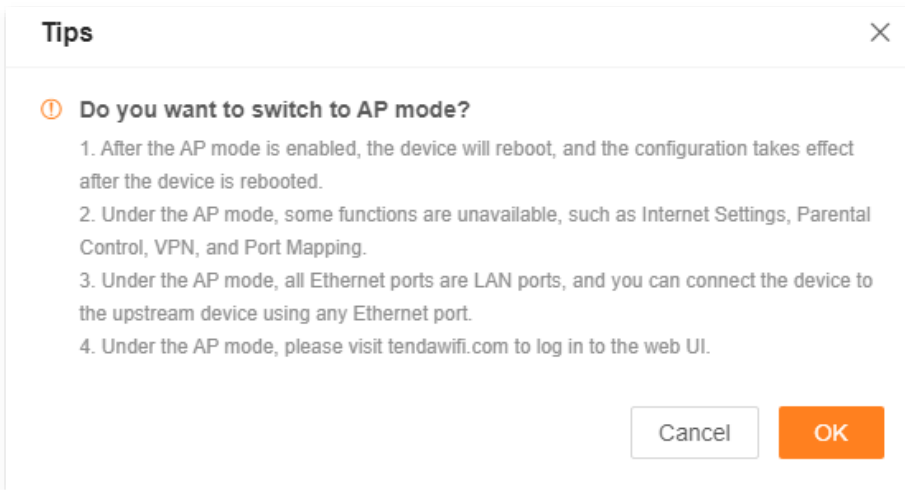
If you are setting the router for the first time or have restored the router to factory settings. Refer to [log in to the web UI of the router and complete the initial configuration](#).

Step 3 Set the router to **AP Mode**.

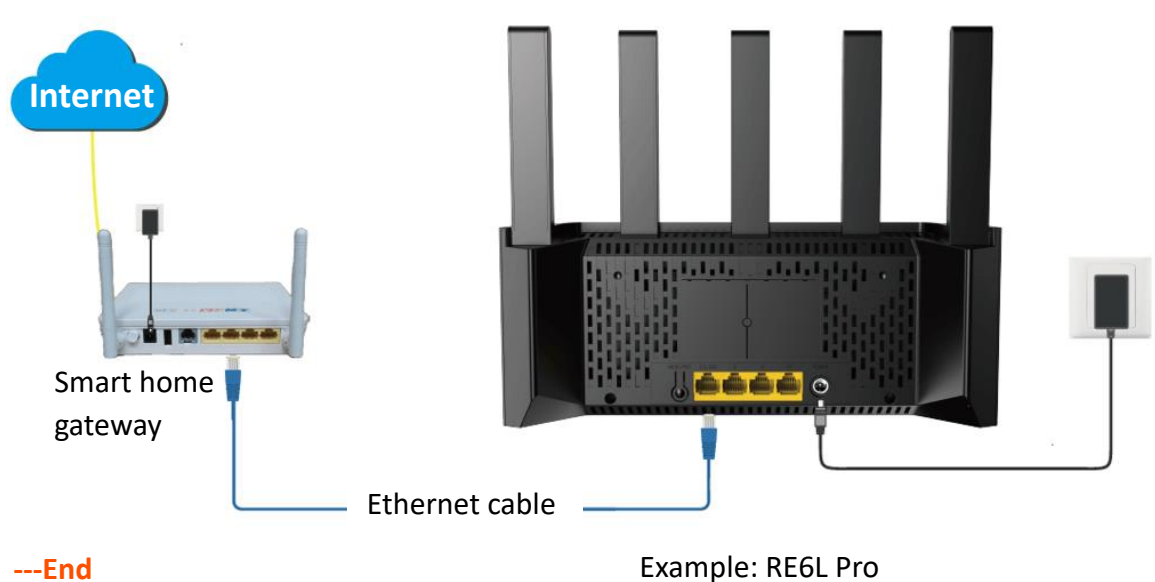
1. Navigate to **More > Working Mode**.
2. Click **Switch Mode** after **AP Mode**.



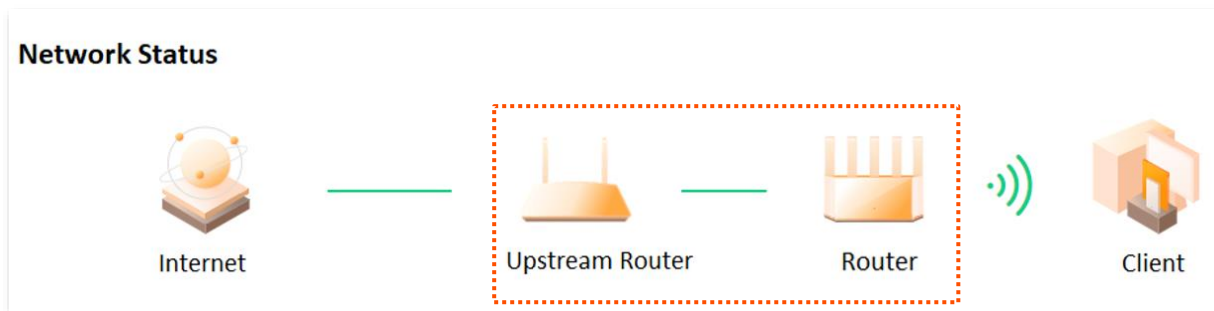
3. Click **OK**.



Step 4 Connect the upstream device, such as a gateway, to any port of the router.



[Log in to the web UI of the router](#) again, and navigate to **Network Status** to check whether the AP mode is configured successfully as shown below.



If there is another network device with the same login domain name (**tendawifi.com**) as the router, log in to the upstream router and find the IP address obtained by the router in the client list. Then you can log in to the web UI of the router by visiting the IP address.

To access the internet, connect your computer to a physical port, or connect your smartphone to the Wi-Fi network.

You can find the Wi-Fi name and Wi-Fi password on the **WiFi Settings** page. If the network is not encrypted, you can also set a Wi-Fi password on this page for security.



If you cannot access the internet, try the following solutions:

- Ensure that the existing router is connected to the internet.
- Ensure that your Wi-Fi-enabled clients are connected to the correct Wi-Fi network of the router.
- If the computer connected to the router cannot access the internet, ensure that the computer is set to **Obtain an IP address automatically** and **Obtain DNS server address automatically**.

4.6.2 Router mode

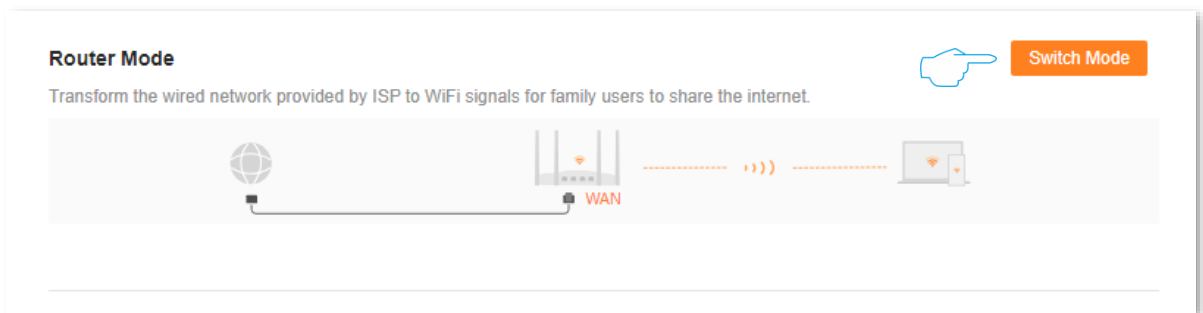
Scenario: The router is working in AP mode.

Goal: Now you have moved to a new home, the ISP provides a PPPoE username and password for internet access, or provides internet access information such as an IP address, subnet mask, default gateway, and DNS server.

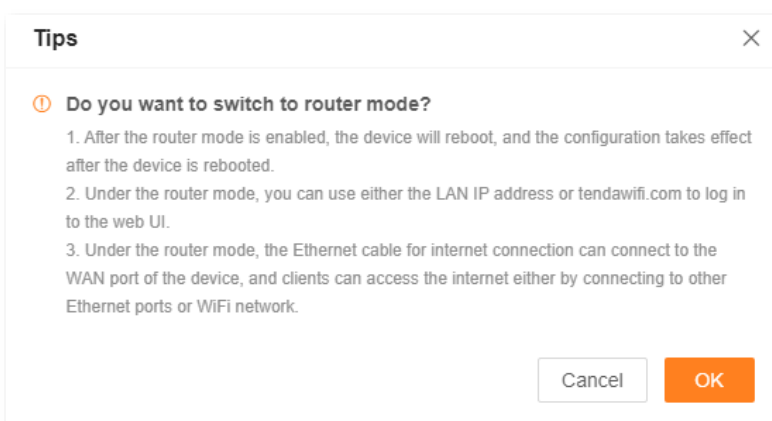
Solution: Reconfigure the router and set its working mode to **Router Mode**.

To switch the working mode from the other modes to router mode:

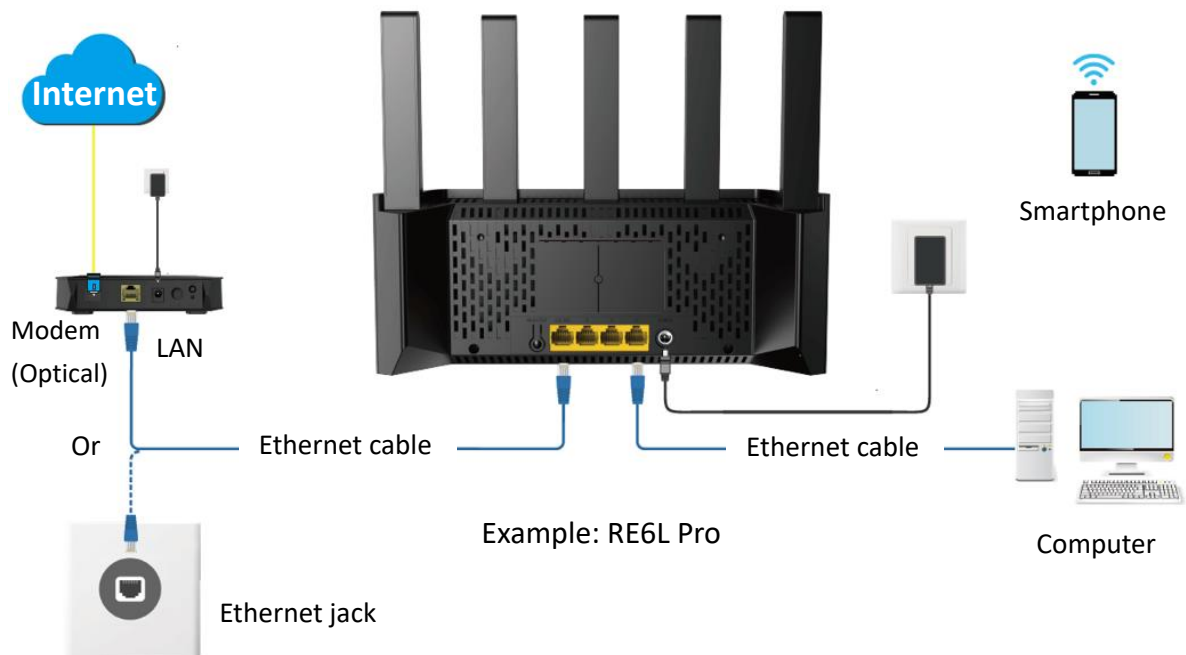
- Step 1** Power on the router.
- Step 2** [Log in to the web UI of the router.](#)
- Step 3** Set the router to **Router Mode**.
 1. Navigate to **More > Working Mode**.
 2. Click **Switch mode**.



3. Click **OK**. Wait until the device is rebooted for the configuration to take effect.



Step 4 Connect the Ethernet port of the router to the Ethernet jack or the LAN port of the Modem using an Ethernet cable.

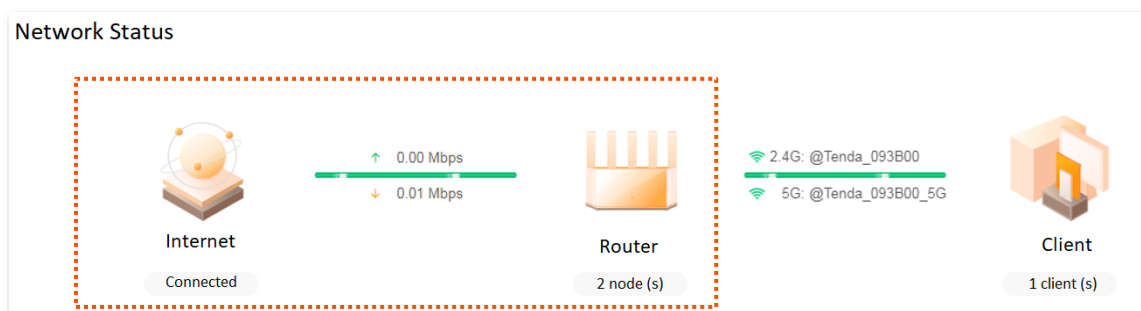


By default, the [WAN/LAN auto-negotiation](#) function of the router is enabled, and the Ethernet cable connected to the internet can be connected to any Ethernet port. If the WAN/LAN auto-negotiation function is disabled, connect the Ethernet cable connected to the internet to Ethernet port 1 (WAN port).

Step 5 Configure the router to the internet. For details, see [Modify IPv4 internet settings](#).

---End

[Log in to the web UI of the router](#) again, and navigate to **Network Status** to check whether the router mode is configured successfully as shown below.



To access the internet, connect your computer to an Ethernet port (If the [WAN/LAN auto-negotiation](#) function is disabled, connect the computer to any Ethernet port 2/3/4 of the router.), or connect your smartphone to the Wi-Fi network.

You can find the Wi-Fi name and Wi-Fi password on the **WiFi Settings** page.



If you cannot access the internet, try the following solutions:

- Ensure that your Wi-Fi-enabled clients are connected to the correct Wi-Fi network of the router.
- If the computer connected to the router's Ethernet port (If the [WAN/LAN auto-negotiation](#) function is disabled, connect the computer to any Ethernet port 2/3/4 of the router.) cannot access the internet, ensure that the computer is set to **Obtain an IP address automatically** and **Obtain DNS server address automatically**.

4.6.3 Wireless repeating



In wireless repeating mode:

- Some functions, such as smart power saving, IPTV, WPS, and Wi-Fi schedule, are unavailable. For details, see functions displayed on the device web UI.
- When WISP mode is chosen and the LAN IP of the router is at the same network segment as that of the upstream device, the router will change the LAN IP address to a different network segment to avoid conflict.
- When Client+AP mode is chosen and the LAN IP of the router, the LAN IP address of this device may change. Visit tendawifi.com to log in to the web UI of this device.

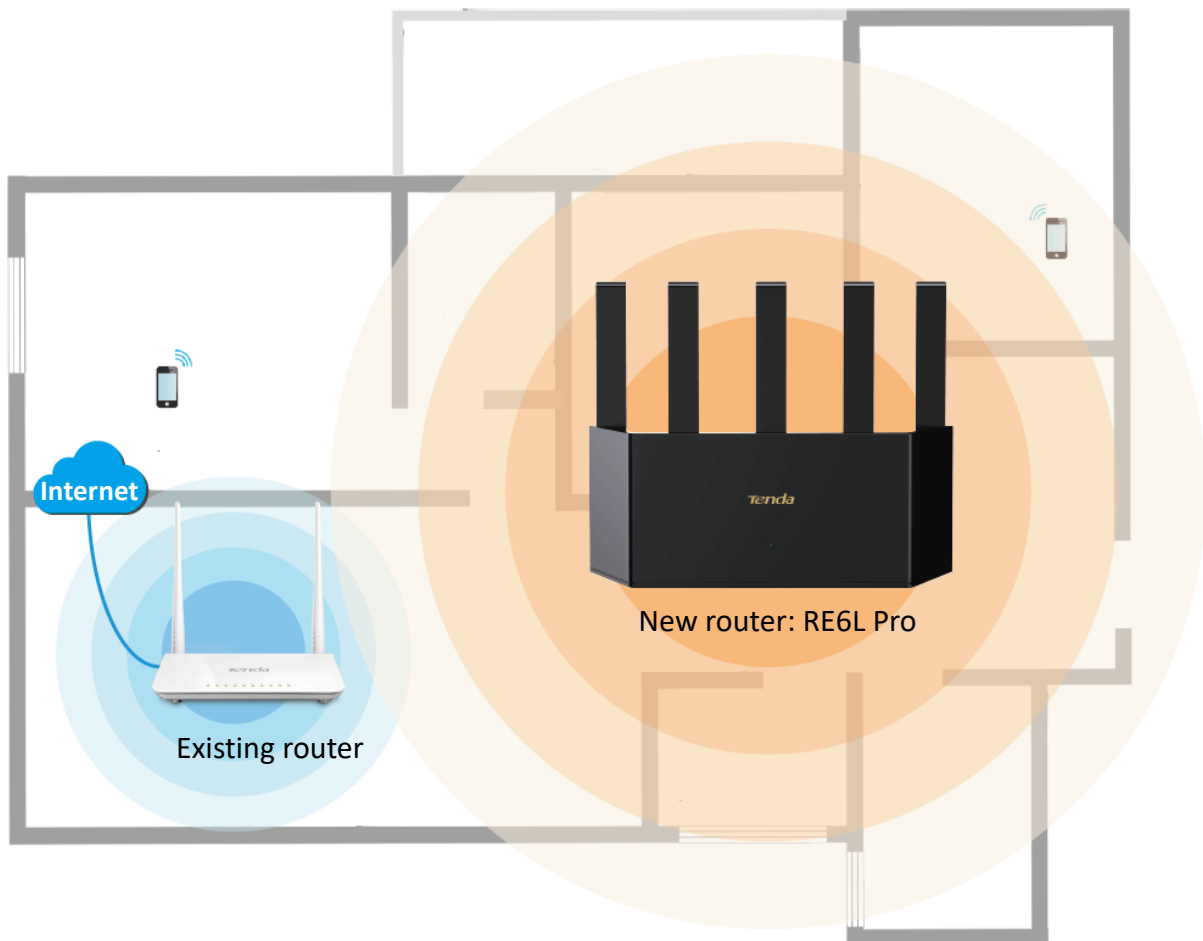
Scenario: You have a wireless router at home and it has been successfully connected to the internet.

Goal: The signal is weak in the room far from the router. Now a new wireless router is added to extend the wireless network coverage at home.

Solution: The new router can be set to the WISP or Client+AP to reach the goal.

Assume that the wireless network information of the existing router is as follows:

- Wi-Fi name: My Wi-Fi
- Wi-Fi password: UmXmL9UK

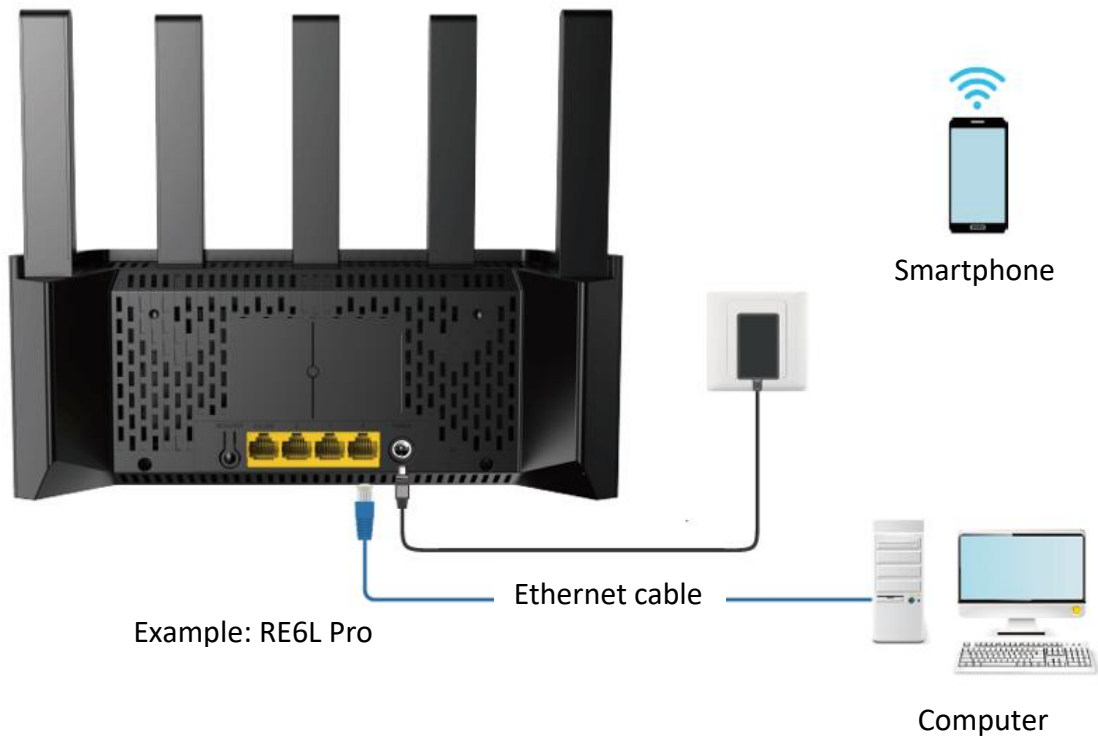


Set the router to WISP mode

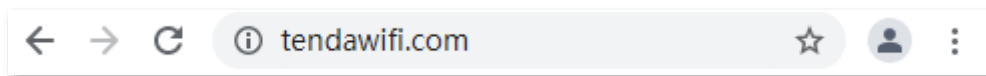
Step 1 Place the new router near the existing router and power it on.

Step 2 Log in to the web UI of the new router and complete the initial configuration.

1. Connect your Wi-Fi-enabled device to the Wi-Fi network of your new router, or connect a computer to an Ethernet port (If the [WAN/LAN auto-negotiation](#) function is disabled, connect the computer to any Ethernet port 2/3/4 of the router.) of the router.

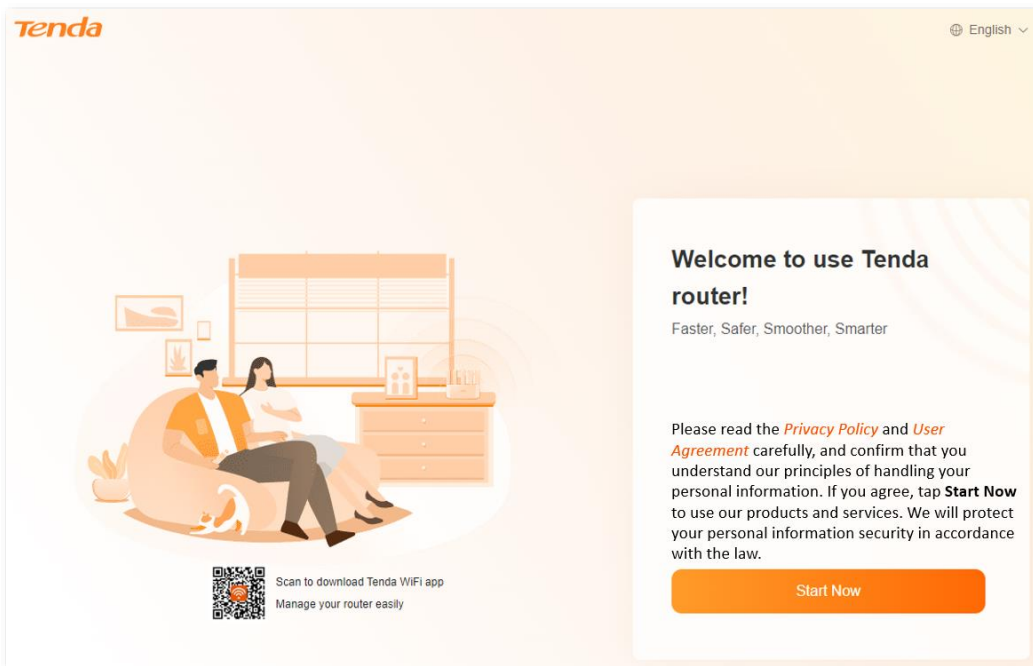


2. On the smartphone or computer connected to the router, start the browser and enter **tendawifi.com** to access the web UI of the router. The following uses computer settings as an example.

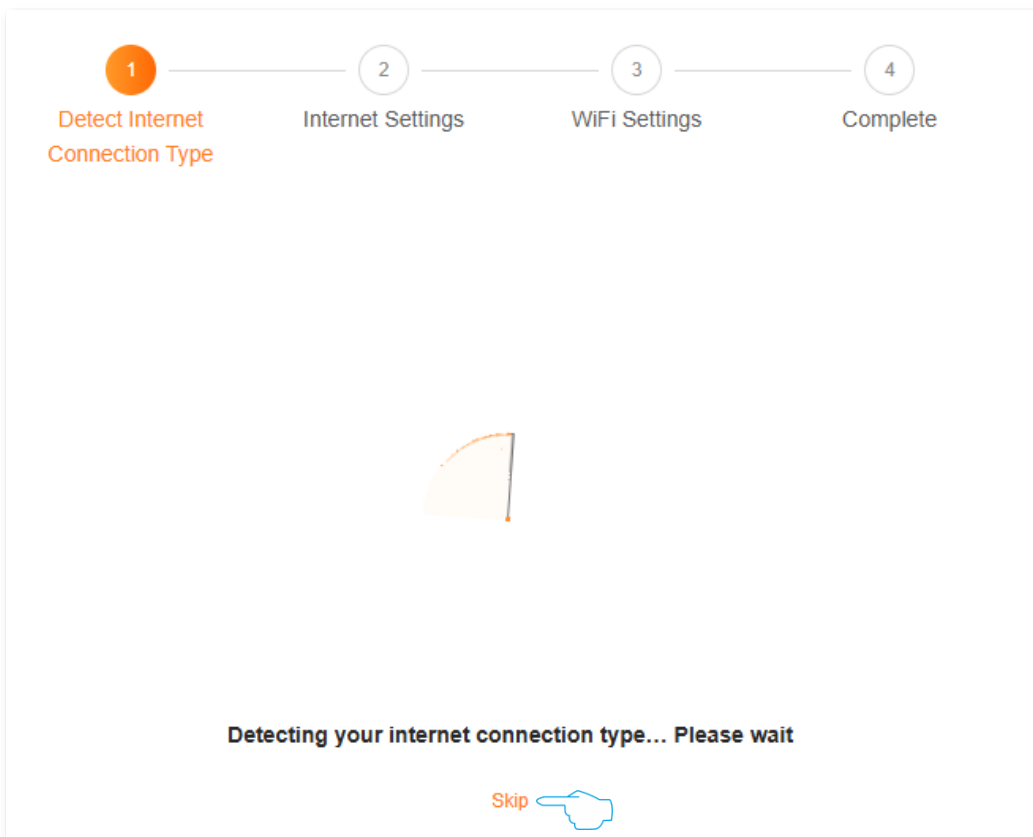


If you are setting up the router for the first time or have restored the router to factory settings, please refer to the following to continue setting. If you have finished the quick setup wizard before, start a web browser and visit **tendawifi.com** on a connected client, then start from [Step 3](#).

3. Click **Start Now**.



4. Click **Skip**.



5. Click **Skip**.

✓ — 2 — 3 — 4
 Detect Internet Connection Type Internet Settings WiFi Settings Complete

✓ Detection succeeded. Recommended internet connection type: Dynamic IP
 or [Set the current router as an extender](#) ⓘ

ISP Type

Internet Connection Type

Select this type if you can access the internet simply by plugging in an Ethernet cable for internet connection.

Next

Skip

6. Set the **WiFi Name**, **WiFi Password** and **Login Password**, and click **Next**.



TIP

The Wi-Fi password is set as the login password by default. If you want to customize the login password, deselect **Set WiFi password to router login password** and set the password.

✓ — ✓ — 3 — 4
 Detect Internet Connection Type Internet Settings WiFi Settings Complete

WiFi Name

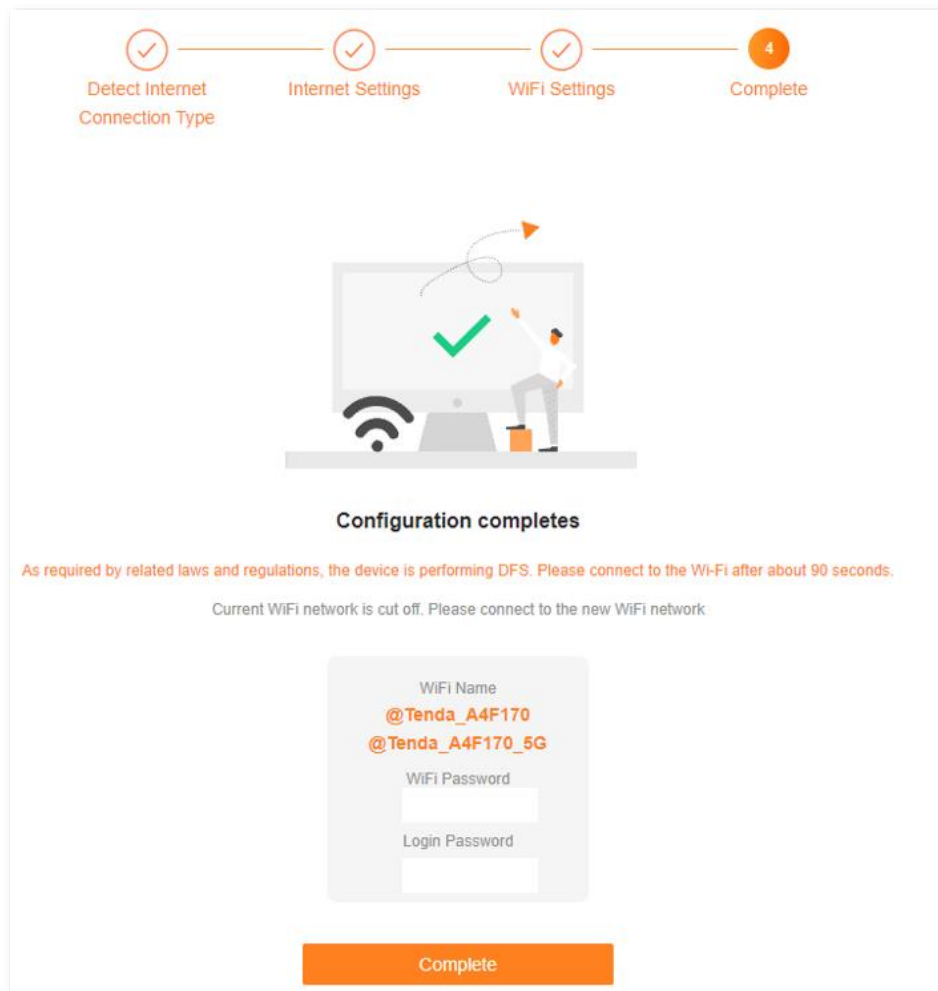
WiFi Password Not encrypted

Set WiFi password to router login password ⓘ

Next

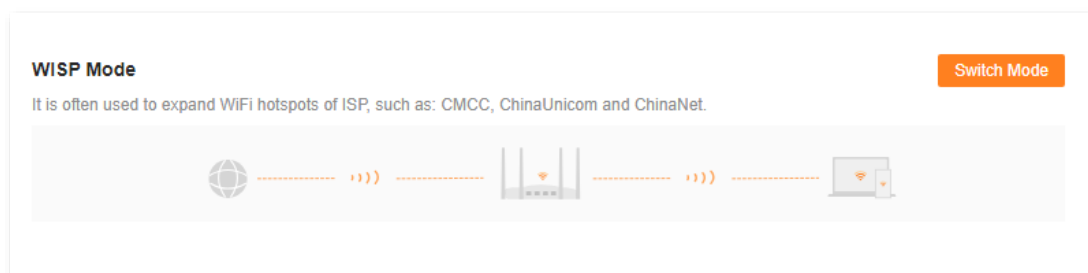
Previous

- Click **Complete**. The login page is displayed. Enter the login password to log in to the web UI.

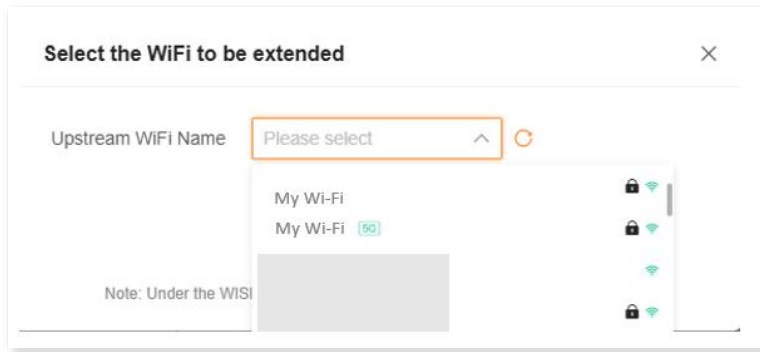


Step 3 Set the new router to **WISP Mode**.

- Navigate to **More > Working Mode**.
- Click **Switch Mode** after **WISP Mode**.



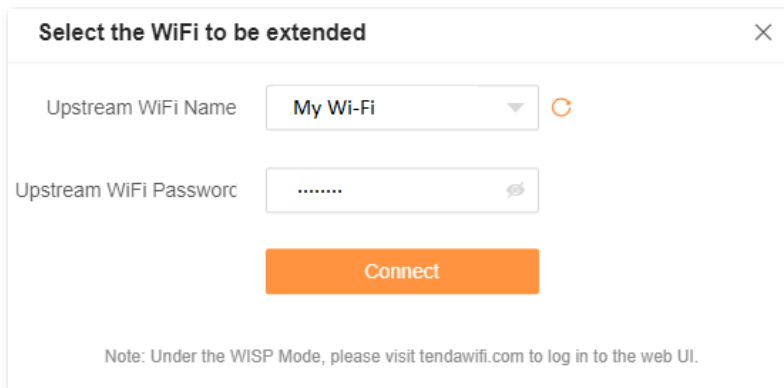
- Confirm the prompt message and click **OK**.
- Select the Wi-Fi to be extended from the **Upstream WiFi Name** drop-down list box, which is **My Wi-Fi** in this example. If the 2.4 GHz Wi-Fi name and 5 GHz Wi-Fi name is the same, select it as required.



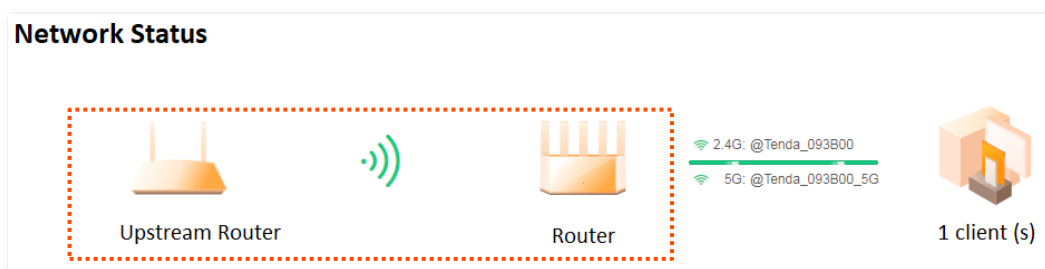
5. Set **Upstream WiFi Password**, which is **UmXmL9UK** in this example, and click **Connect**. Wait until the device is restarted.



Click  at the end of the **Upstream Wi-Fi Password** input box to display the Wi-Fi password in plain text.



6. [Log in to the web UI of the router](#) again, and navigate to **Network Status** to check whether the WISP mode is configured successfully as shown below.



If the connection between the **Upstream router** and **Router** failed, try the following solutions:

- Ensure that you have entered the correct Wi-Fi password of the Wi-Fi network, and mind case sensitivity.
- Ensure that **Router** is within the wireless coverage of the **Upstream Router**.

Step 4 Relocate the new router by referring to the following suggestions and power it on.

- Between the existing router and the uncovered area, but within the coverage of the existing router.
- Away from microwave ovens, electromagnetic ovens, and refrigerators.
- Above the ground with few obstacles.

---End

To access the internet, connect your computer to an Ethernet port of the new router, or connect your smartphone to the Wi-Fi network of the new router.

You can find the Wi-Fi name and password on the **WiFi Settings** page. If the network is not encrypted, you can also set a Wi-Fi password on this page for security.



TIP

If you cannot access the internet, try the following solutions:

- Ensure that the existing router is connected to the internet successfully.
- Ensure that your Wi-Fi-enabled devices are connected to the Wi-Fi network of the new router.
- If the computer connected to the router for repeating cannot access the internet, ensure that the computer is set to **Obtain an IP address automatically** and **Obtain DNS server address automatically**.

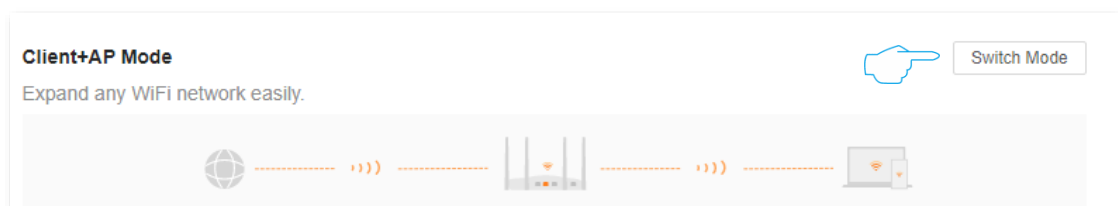
Set the router to Client+AP mode

Step 1 Place the new router near the existing router and power it on.

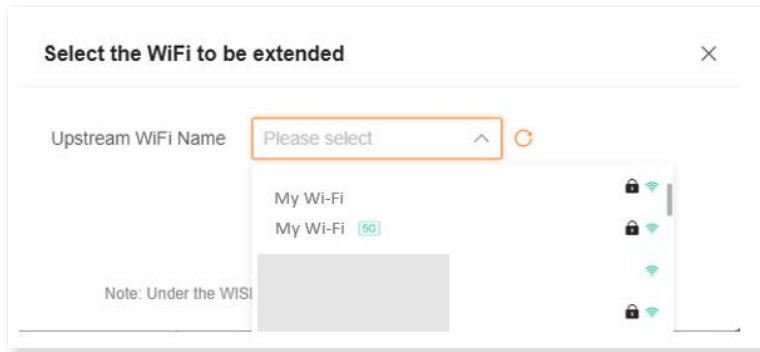
Step 2 [Log in to the web UI of the new router and complete the initial configuration.](#)

Step 3 Set the new router to **Client+AP Mode**.

1. Navigate to **More > Working Mode**.
2. Click **Switch Mode** after **Client+AP Mode**.




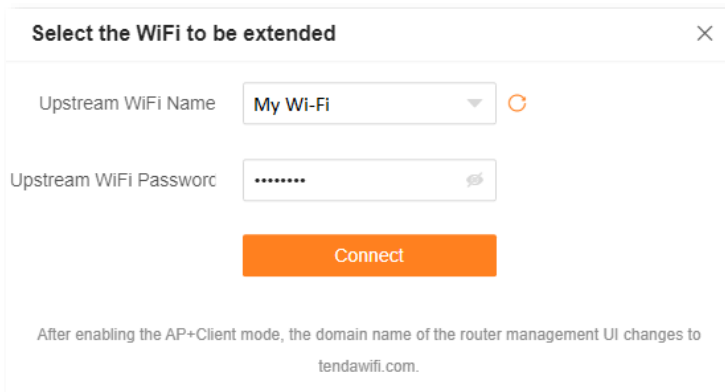
3. Confirm the prompt message and click **OK**.
4. Select the Wi-Fi to be extended from the **Upstream WiFi Name** drop-down list box, which is **My Wi-Fi** in this example. If the 2.4 GHz Wi-Fi name and 5 GHz Wi-Fi name is the same, select it as required.



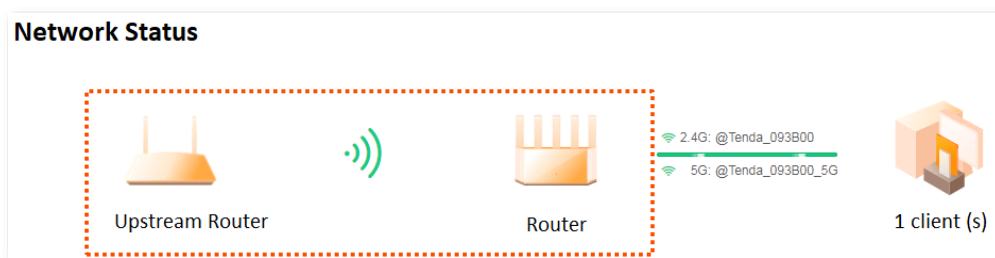
- Set **Upstream WiFi Password**, which is **UmXmL9UK** in this example, and click **Connect**. Wait until the device is restarted.



Click  at the end of the **Upstream WiFi Password** input box to display the Wi-Fi password in plain text.



- [Log in to the web UI of the router](#) again, and navigate to **Network Status** to check whether the **Client+AP** mode is configured successfully as shown below.



If there is another network device with the same login domain name (tendawifi.com) with the router, log in to the upstream router and find the IP address obtained by the new router in the client list. Then you can log in to the web UI of the router by visiting the IP address.

Step 4 Relocate the new router by referring to the following suggestions and power it on.

- Between the existing router and the uncovered area, but within the coverage of the existing router.
- Away from microwave ovens, electromagnetic ovens, and refrigerators.
- Above the ground with few obstacles.

---End

To access the internet, connect your computer to an Ethernet port of the new router, or connect your smartphone to the Wi-Fi network of the new router.

You can find the Wi-Fi name and password on the **WiFi Settings** page. If the network is not encrypted, you can also set a Wi-Fi password on this page for security.



If you cannot access the internet, try the following solutions:

- Ensure that the existing router is connected to the internet successfully.
 - Ensure that your Wi-Fi-enabled devices are connected to the Wi-Fi network of the new router.
 - If the computer connected to the router for repeating cannot access the internet, ensure that the computer is set to **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
-

5 Wi-Fi settings

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

This chapter includes the following sections:

[Change Wi-Fi name and Wi-Fi password](#)

[Guest WiFi Settings](#)

[Schedule disable Wi-Fi](#)

[Change the Wi-Fi signal strength](#)

5.1 Change Wi-Fi name and Wi-Fi password

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

Step 2 Click **WiFi Settings**.

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

- Enable **Unify 2.4 GHz & 5 GHz**: The Wi-Fi name and password of the 2.4 GHz and 5 GHz network on the router are the same, and only one Wi-Fi name is displayed. When you connect to your router's wireless network, you will automatically connect to the best quality Wi-Fi.
- Disable **Unify 2.4 GHz & 5 GHz**: The 2.4 GHz and 5 GHz networks on the router are displayed separately. You can access the internet through either wireless network. If you have wireless devices that only support 2.4GHz networks, you need to connect to the router's Wi-Fi network, such as security cameras, you are recommended to disable the **Unify 2.4 GHz & 5 GHz**.

Step 4 Set **WiFi Name**, **Security**, and **WiFi Password** as required.

Step 5 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.

MLO

When enabled, the terminal can establish multiple connections with the router to improve speed and reduce latency.
This function can only work when the Wi-Fi name and Wi-Fi password of at least two bands are the same and the network mode supports 802.11be.

WiFi Enable

WiFi Name

Hide (After it is enabled, clients such as smartphones cannot find the Wi-Fi name and networking through the button is not supported for the frequency range.)

Security

WiFi Password ⓘ

---End

After the settings are completed, your Wi-Fi-enabled devices (such as smartphone) need to connect to the new wireless network to access the internet.

5.2 Guest WiFi Settings

The router's guest Wi-Fi is isolated from other networks. The clients connected to the guest Wi-Fi can access the internet, but cannot access the router's web UI or other networks.

When you need to open a wireless network for guests, you can enable guest Wi-Fi to meet the internet requirements of guests. It protects the security of the main network to prevent personal information disclosure.

This function is disabled by default. Assume that:

- Wi-Fi names for the networks: **Tom**.
- Wi-Fi password for the networks: **Tenda+245**.

Configuration procedure:

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

Step 2 Enter the **Guest WiFi** configuration page.

Method 1: Click **Go to Settings** in the **Guest Networks** section of the **Network Status** page.

Method 2: Navigate to **More > Guest Wi-Fi**.

Step 3 Enable **Guest WiFi**.

Step 4 Set **WiFi Name**, which is **Tom** in this example.

Step 5 Set **WiFi Password**, which is **Tenda+245** in this example.

Step 6 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

WiFi Name

WiFi Password

Validity



Shared Bandwidth

---End

After the settings are completed, the guest's smartphone and other Wi-Fi-enabled devices can connect to the guest Wi-Fi for internet access you set, and the validity period is 8 hours.

The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
Guest WiFi	Used to enable or disable the guest network function.
WiFi Name	<p>Specify the Wi-Fi name of the router's guest network.</p> <p> TIP</p> <p>You can change the Wi-Fi names (SSIDs) as required. To distinguish the Wi-Fi name of the router's primary network, it is recommended that the guest network's Wi-Fi name is not set the same as the router's primary network's Wi-Fi name.</p>
WiFi Password	<p>Specifies the password for the router's guest network.</p> <p> TIP</p> <p>A Wi-Fi password that contains multiple characters, such as digits, uppercase and lowercase letters, can improve Wi-Fi security.</p>
Validity	<p>Specifies the validity period of the guest networks.</p> <p>The guest network function will be disabled automatically (The Wi-Fi enabled devices cannot scan the router's guest Wi-Fi.) out of the validity period. If the guest's visit is 8 hours, it can be set to 8 hours.</p>
Shared Bandwidth	Allows you to specify the maximum upload and download speed for all clients connected to the guest networks. By default, the bandwidth is Unlimited . You can modify it as required.

5.3 Schedule disable Wi-Fi

With the **Wi-Fi Schedule** function, you can set the router to disable the Wi-Fi for a specified period, leaving the router in a power-saving state. At other times, Wi-Fi is restored. This function is disabled by default.

Assume that you want to enable the router's Wi-Fi from 22:00 to 7:00 each day.

Configuration procedure:

- Step 1** [Log in to the web UI of the router.](#)
- Step 2** Navigate to **More > Smart Power Saving > WiFi Schedule.**
- Step 3** Enable the **WiFi Schedule** function.
- Step 4** Set a period, which is **22:00-07:00** in this example.
- Step 5** Choose a date, which is **Every Day** in this example.
- Step 6** Click **Save.**

WiFi Schedule

Disable the WiFi network in a specified period, and enable at other times.

WiFi Schedule

Time 1 → ⓘ The Schedule Disable time takes effect based on the system time

Repeat Every Day Mon. Tues. Wed. Thur.
 Fri. Sat. Sun.

Add Period

---End

After the setup is completed, the router's Wi-Fi is not available from 22:00 to 07:00 every day, and the wireless devices such as a smartphone cannot search the router's Wi-Fi and cannot connect to the router's Wi-Fi to surf the internet.



If you want to disable the router's Wi-Fi for multiple periods, click **Add Period** and set the relevant parameters.

5.4 Change the Wi-Fi signal strength

The Wi-Fi signal strength function regulates the through-the-wall capability and coverage of the router's wireless network.

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

Wi-Fi signal strength mode description:

- **Energy-saving mode:** Routers use lower wireless transmit power, which is usually used to meet the wireless coverage requirements of small area or obstacle-free environments.
- **Standard mode:** Routers use standard wireless transmit power, which is usually used to meet the wireless coverage requirements of medium area or few obstacles environments.
- **Through-wall mode:** Routers use higher wireless transmit power, which is usually used to meet the wireless coverage requirements of large areas or multi-obstacle environments.

Wi-Fi Signal Strength

The Wi-Fi signal strength mode can be switched as required.

- Wi-Fi Signal Strength
- Energy-saving Mode
(Reduce Wi-Fi signal strength to be more energy efficient)
 - Standard Mode
(Wi-Fi coverage is average)
 - Through-wall Mode
(Improved Wi-Fi signal strength and through-wall capacity)

6 Network status

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

This chapter includes the following sections:

[View network status](#)

[View Wi-Fi name](#)

[View the number of Mesh nodes and clients](#)

[View network status, node and client details](#)

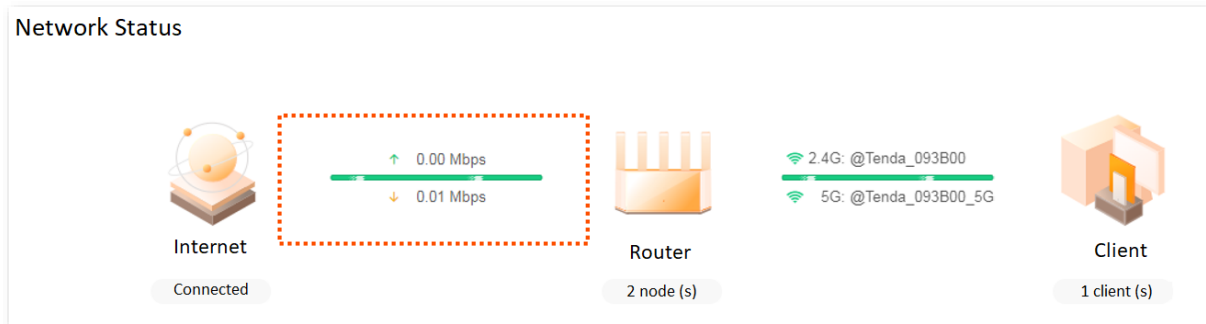
[View system information](#)

6.1 View network status

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

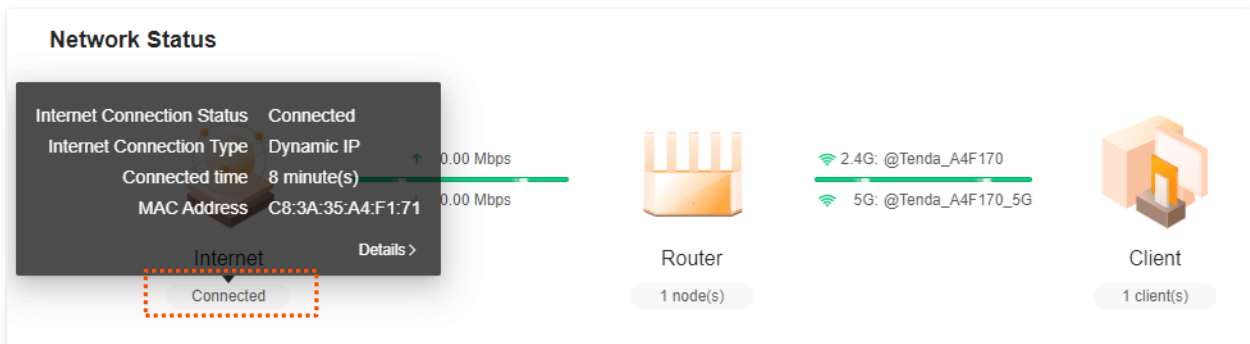
6.1.1 Router connected to internet

If the connection between **Internet** and **Router** is normal, as shown in the following figure, the router is successfully connected. You can connect to the router for internet access.



Hover the mouse over **Connected**, you can view the basic internet information of the router, including internet status, internet connection mode, duration and WAN port MAC address. The following figure is for reference only.

Click the **Details** or internet icon, and enter the **Internet Settings** page to view or set more information.



6.1.2 Router disconnected from the internet

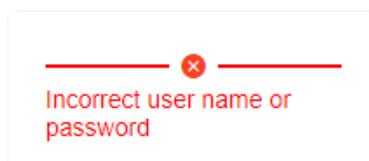
No Ethernet cable is connected to the WAN port

If **No Ethernet cable is connected to the WAN port** is displayed in the **Network Status**, indicates that the Ethernet cable is improperly connected to the Ethernet port, as shown in the following figure. Check whether both ends of the Ethernet cable at the Ethernet port are tightly connected. If the Ethernet cable is tightly connected but the problem persists, [Modify WAN speed](#) to solve the problem. If the problem persists, contact Tenda technical support for help.



Incorrect PPPoE username or password

If **Incorrect user name or password** is displayed in the **Network Status**, it indicates that the PPPoE username or password you entered is incorrect, as shown in the following figure. Click the error message to direct to the **Internet Settings** page, re-enter the correct PPPoE username and password for internet access.

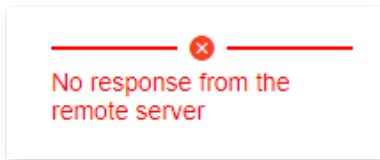


NOTE

- Note the following when entering the PPPoE username and password:
 - Case sensitive, such as "Z" and "z".
 - Distinguish between similar letters and numbers, such as the letter "l" and the number "1".
 - Enter the complete PPPoE username.
 - If the PPPoE username and password are entered correctly, but the problem persists, you are recommended to click **Advanced** to change the WAN MAC address and try again. For details, see [Modify WAN MAC Address](#). If the problem persists, contact your ISP for help.
-

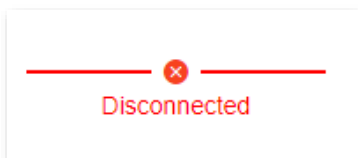
No response from the remote server

If the **No response from the remote server** is displayed in **Network Status**, as shown in the following figure. Click the error message to direct to the **Internet Settings** page, and try to solve the problem according to the on-screen prompts.



Disconnected

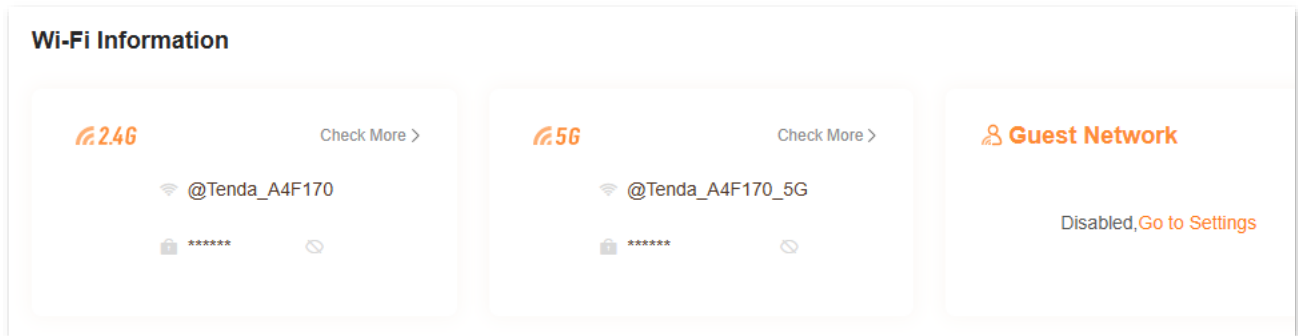
If the **Disconnected** is displayed in **Network Status**, as shown in the following figure. Click the error message to direct to the **Internet Settings** page, and try to solve the problem according to the on-screen prompts.



6.2 View Wi-Fi name

After [logging in to the web UI of the router](#), on the **Network Status** page, you can view the Wi-Fi name and Wi-Fi password of the primary network and guest network in the **Wi-Fi Information** module.

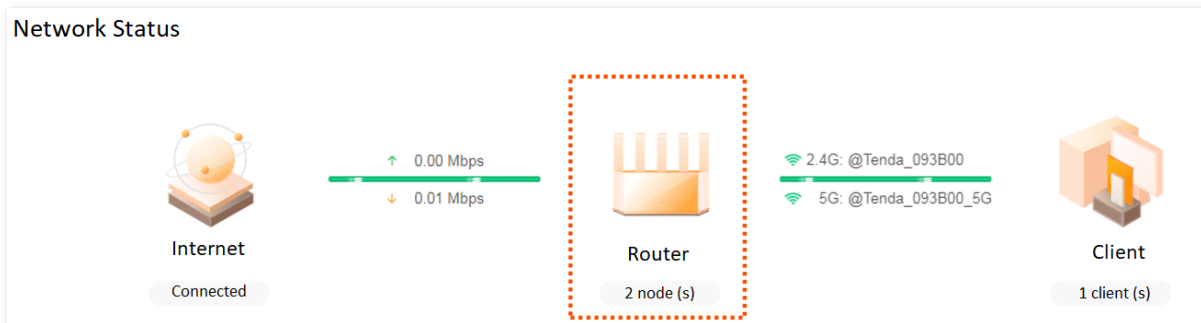
Click **Check More** to view or set more wireless information. The following figure is for reference only.




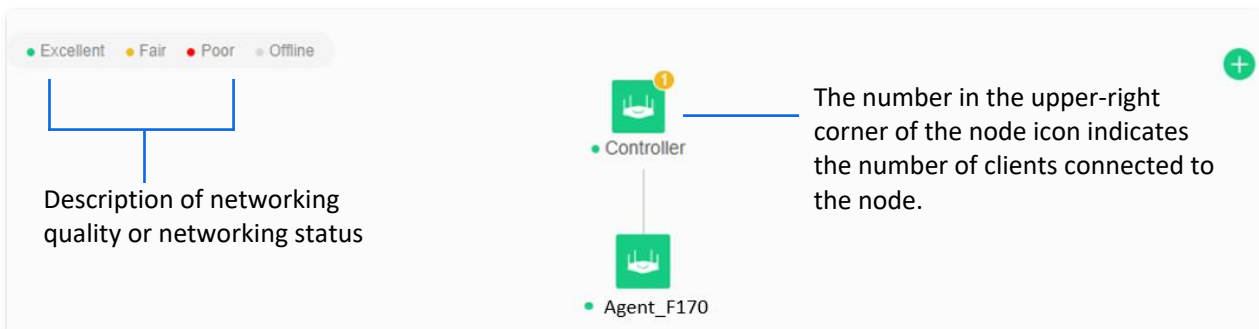
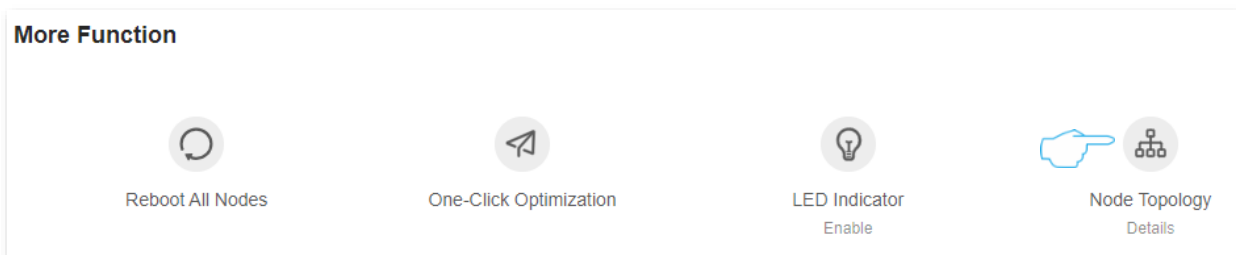
6.3 View the number of Mesh nodes and clients


After [logging in to the web UI of the router](#), 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](#).



Navigate to **Network status**, click  (**Node Topology**) in the **More Function** module to view the networking situation, the number of Mesh nodes, the quality of networking connections, and the number of clients connected to a node.



Click the node icon  to view the details of the node, including IP address, MAC address, online duration, and client device information connected to the node. The following figure is for reference only.






The screenshot shows the 'Node Info' interface. At the top, there's a 'Node Name' section for the 'Controller' (Primary Node) with IP 192.168.1.1 and a 2.5GE Ethernet port status diagram. Below that is a table for 'Main Network Device(2)' with columns for device name, current speed, negotiation speed, bandwidth control, and operation. Two devices are listed: 'DESKTOP-R8R80TU' (100 Mbps) and '123' (206 Mbps).

Node Name	Ethernet Port Status	LED On/Off	Operation	
Controller Primary Node IP Address: 192.168.1.1 MAC Address: [Redacted] Uptime: 2 hour(s) 53 minute(s)	2.5GE WAN LAN 1 2 3 4	<input checked="" type="checkbox"/>		
Main Network Device(2)	Current Speed	Negotiation Speed	Bandwidth Control	Operation
DESKTOP-R8R80TU IP Address: 192.168.1.183 MAC Address: [Redacted] Uptime: 2 hour(s) 37 minute(s) Wired	↑ 0 KB/s ↓ 0 KB/s	100 Mbps	Upload: Unlimited Download: Unlimited	Local Host
123 IP Address: 192.168.1.249 MAC Address: [Redacted] Uptime: 0 minute(s) 2.4G	↑ 0 KB/s ↓ 0 KB/s	206 Mbps	Upload: Unlimited Download: Unlimited	<input type="button" value="Add to blacklist"/>

The following table describes the parameters displayed on this page.

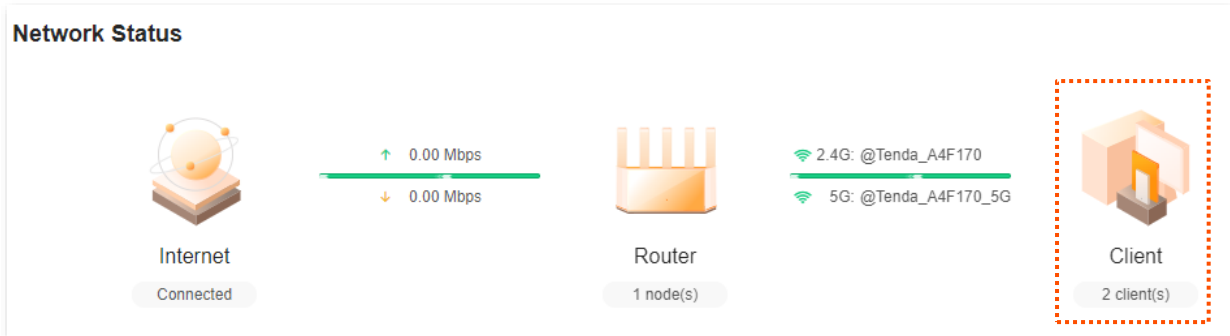
Parameter description

Parameter	Description
Controller	Specifies the default name of the primary node. You can customize it on the Node Info page.
Agent_XXXX	Specifies the default name of the secondary node. You can customize it on the Node Info page.
	Used to scan networking, view button networking or wired networking methods, or see recommended solutions for networking anomalies. If you want to network, detailed steps can refer to the MESH networking .
	Used to reboot all nodes. TIP Rebooting the node will disconnect all connections. Perform this operation when the network is relatively idle.
	Used to optimize wireless networks with one click. TIP When your clients are stuck for internet access or cannot receive Wi-Fi signals, you can optimize the wireless network with one click.
/	Used to turn on or turn off indicators on all nodes.
	Used to view the network topology and networking, or enter the adding node device page.

Parameter	Description
Node Name	<p>Displays the Mesh node name, IP address, MAC address, and uptime.</p> <ul style="list-style-type: none"> – Controller: Specifies the default name of the primary node. You can customize it as required. – Agent_XXXX: Specifies the default name of the secondary node. You can customize it as required.
Ethernet Port Status	<p>The role and connection status of each physical Ethernet port of the primary node device. Hover the mouse over the icon  next to Ethernet Port Status to view the role description of Ethernet port.</p>
Connection Quality	<p>Specifies the network quality of the secondary nodes.</p> <p> TIP</p> <p>If the secondary node is wired networking, the connection quality is Excellent.</p>
LED On/Off	Used to turn on or turn off the indicator display of the node.
Main Network Device	<p>Specifies the name, IP address, MAC address, uptime, and access mode of the clients currently connected to the node.</p> <p>You can customize the clients name as required.</p>
Offline Device	<p>Specifies the offline clients. Including the name and MAC address of the clients.</p> <p>You can customize the clients name as required.</p>
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.
Operation	<p>Perform operations on nodes or clients.</p> <ul style="list-style-type: none"> – : Used to reboot the node. During the reboot, all connections will be disconnected. Therefore, perform this operation when the network is relatively idle. – : 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. – : Used to remove a secondary node. Removing a node narrow the Wi-Fi coverage, and the removed node will no longer join the current network automatically. – 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. – Delete: Used to delete selected offline devices.

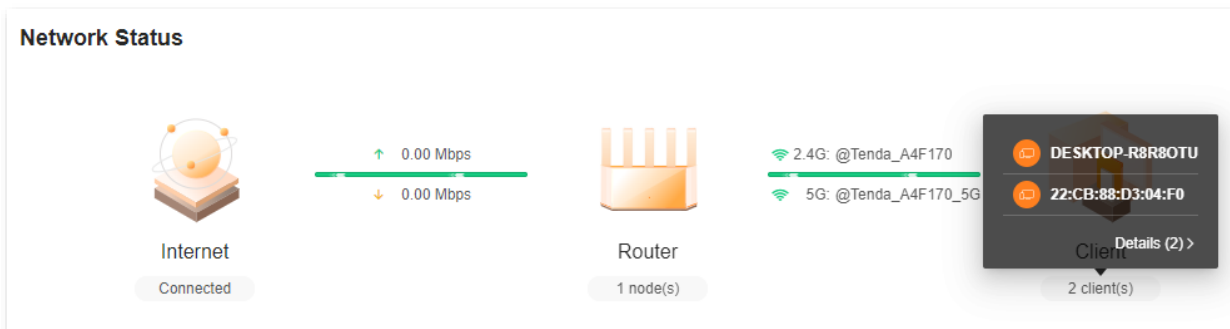
6.4 View network status, node and client details

After [logging in to the web UI of the router](#), navigate to the **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.



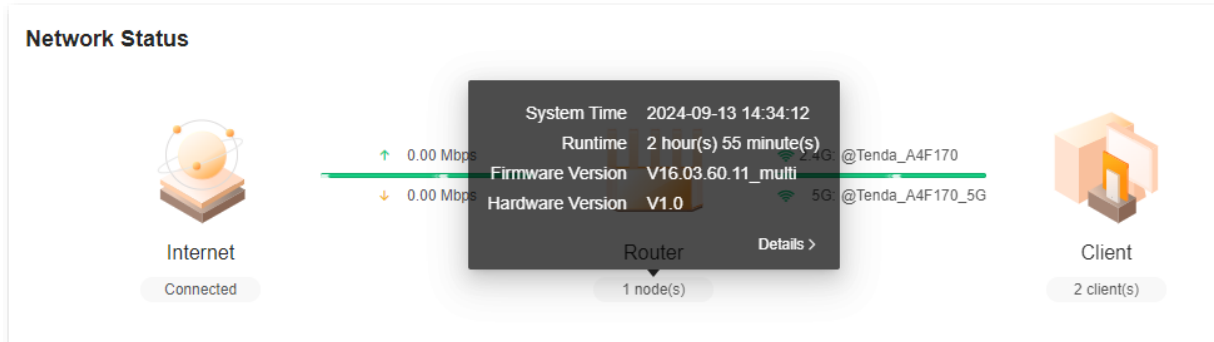
The mouse hover over the **X client(s)**, you can view the basic information of the online client. The following figure is for reference only.

Click **Details** or client device icon to enter the **Device Management** page to view or configure more information.



6.5 View system information

After [logging in to the web UI of the router](#), hover the mouse over **X node(s)** in **Network Status** page to view the basic information of the router, including system time, running time, firmware version, and hardware version. The following figure is for reference only.



Click **Details** or router icon, and navigate to **More > Router Info**. You can view the system information about the router. The details are as follows:

- Basic information: Displays the system time, running time, firmware version, and hardware version of the router.
- WAN port status: Displays the IPv4 internet connection type, connection status, and IP address of the current WAN port on the router.
- LAN status: Displays the IPv4 address, subnet mask, and MAC address of the router's LAN port.
- Wireless status: Displays basic information about the 2.4 GHz and 5 GHz wireless networks, including wireless network status, Wi-Fi name, and security.
- IPv6 status: Displays the IPv6 internet connection type, IP address, and DNS information of the current WAN port on the router.

7 Client management

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

This chapter describes how to manage your clients, including:

[Add a client to the blacklist](#)

[Add the client to the whitelist](#)

[Remove a client from the blacklist](#)

[Internet access speed control](#)

[Only prohibit specified clients from accessing the internet](#)

[Internet access rule control](#)

7.1 Add the client to the blacklist

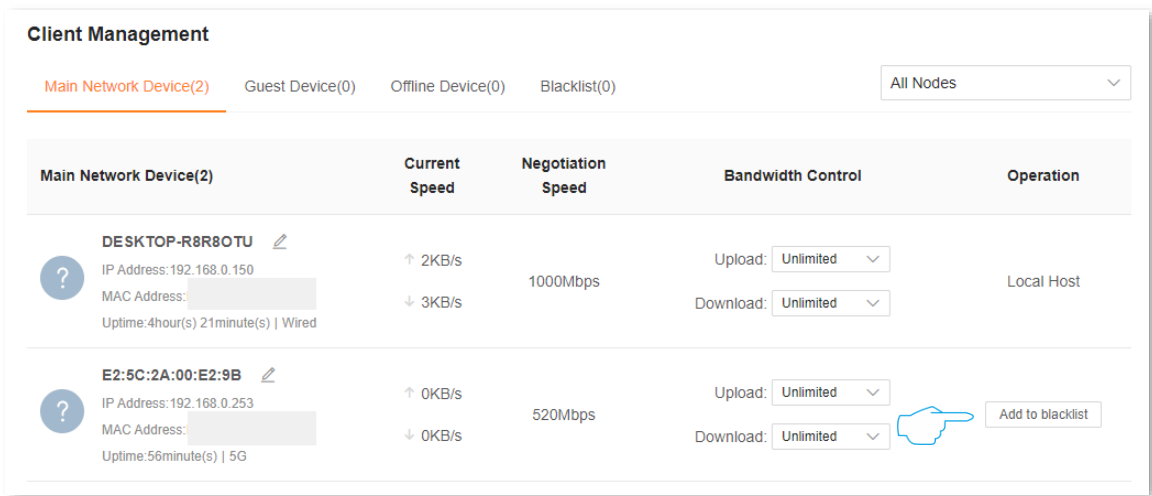
The blacklisted devices cannot access the internet through the router.

7.1.1 Method 1

To blacklist a client:

Step 1 [Log in to the web UI of the router](#), and navigate to **Client Management**.

Step 2 Locate the device that not allowed to access the internet and click **Add to blacklist**. The following figure is for reference only.

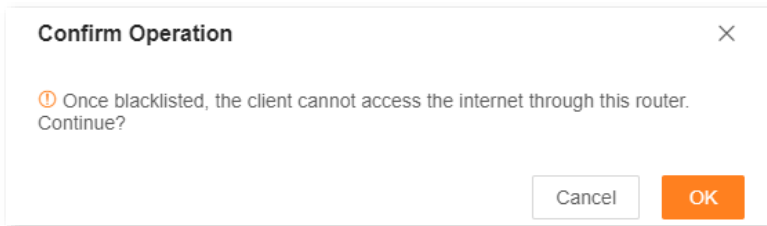


The following table describes the parameters displayed on this page.

Parameter description

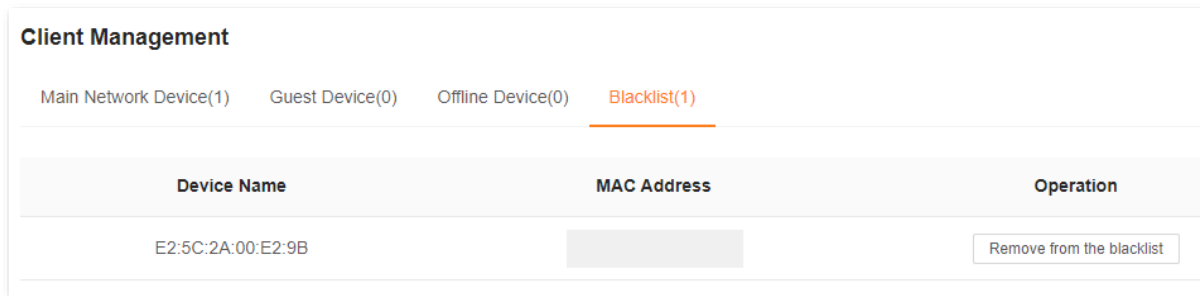
Parameter	Description
All Nodes	Used to filter the clients connected to each node. When a router is networked with other routers through Mesh networking, you can click the primary node name or other node name to display only the devices under the corresponding node.
Main Network Device	Specifies the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

Step 3 Confirm the prompt message, and click **OK**.



---End

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

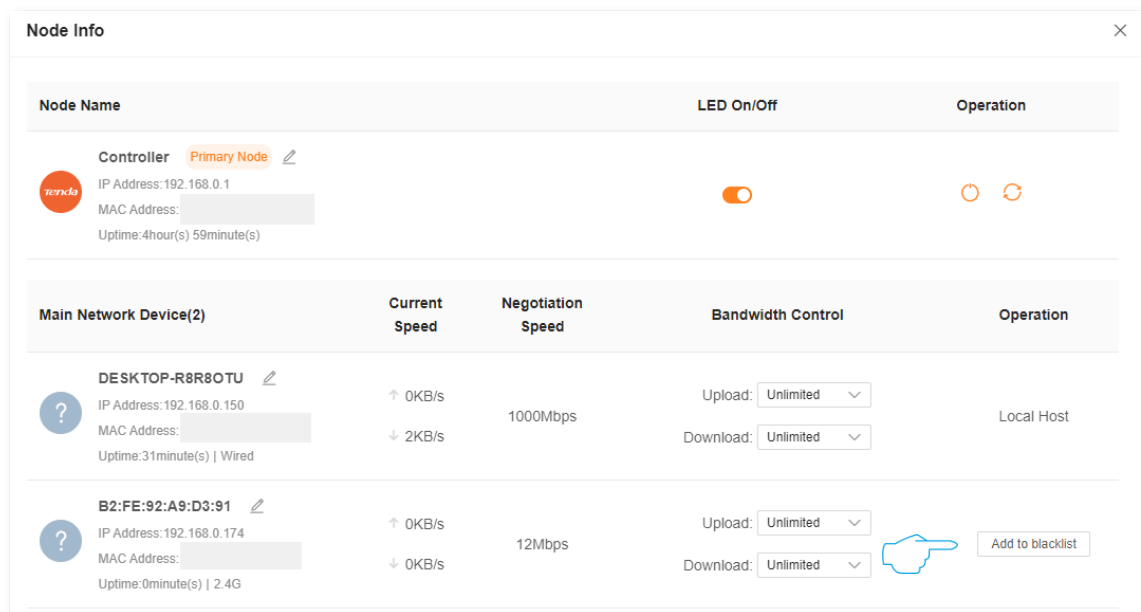


7.1.2 Method 2

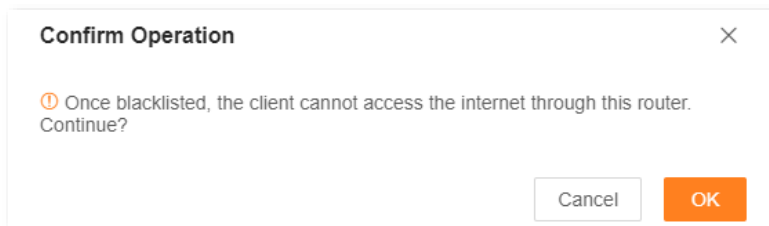
Step 1 [Log in to the web UI of the router.](#)

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

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



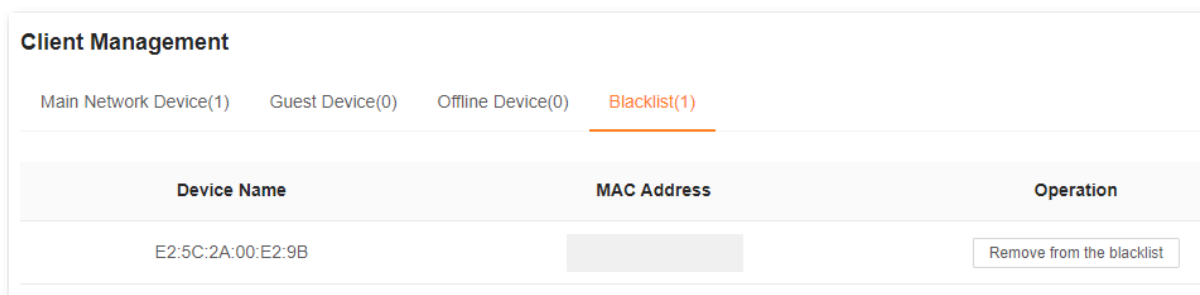
Step 4 Confirm the prompt message, and click **OK**.



---End

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

A blacklisted device cannot access the internet through a router.



7.1.3 Method 3

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

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

Step 3 Enable the **MAC Address Filter** function, and set **Filter mode** to **Blacklist**.

Step 4 Add the clients to the blacklist.

1. Click **Add**.
2. Select a client, and click **OK**. The following figure is for reference only.
 - Method 1: Select the clients that is currently connected to the router in the **Select Device** bar.
 - Method 2: Select **Manual** in the **Select Device** bar, and enter the MAC address of the client to be added to the blacklist, and the device name can be customized.

Add Blacklist

Select Device

Device Name

MAC Address

Step 5 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)

Whitelist
(Only users with listed MAC addresses are allowed to access the internet)

Blacklist Device

Device Name	MAC Address	Operation
Kid's computer	98:9C:57:19:D0:1B	<input type="button" value="Delete"/>

1 items in total < **1** >

---End

7.2 Add the client to the whitelist

Devices that add to the whitelist can access the internet through the router, while other devices cannot access the internet through the router.

7.2.1 Add online clients to the whitelist

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

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

Step 3 Enable the **MAC Address Filter** function, and set **Filter mode** to **Whitelist.**

Step 4 Click **Add all online devices to the whitelist**, and all currently online devices will be added to the whitelist. The following figure is for reference only.

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)

Whitelist
(Only users with listed MAC addresses are allowed to access the internet)

Before the whitelist function is enabled, you are recommended to disable the "Private WLAN Address" or "Use randomized MAC" function of the smartphone Wi-Fi for better network connection.

Whitelist Add all online devices to the whitelist Add

Device Name	MAC Address	Operation
DESKTOP-R8R8OTU	6C:4B:90:41:E2:AD	Local Host

1 items in total < 1 >

Save

Step 5 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)

Whitelist
(Only users with listed MAC addresses are allowed to access the internet)

Before the whitelist function is enabled, you are recommended to disable the "Private WLAN Address" or "Use randomized MAC" function of the smartphone Wi-Fi for better network connection.

Whitelist [Add](#)

Device Name	MAC Address	Operation
DESKTOP-R8R80TU	6C:4B:90:41:E2:AD	Local Host
22:CB:88:D3:04:F0	22:CB:88:D3:04:F0	

2 items in total < 1 >

[Save](#)

---End

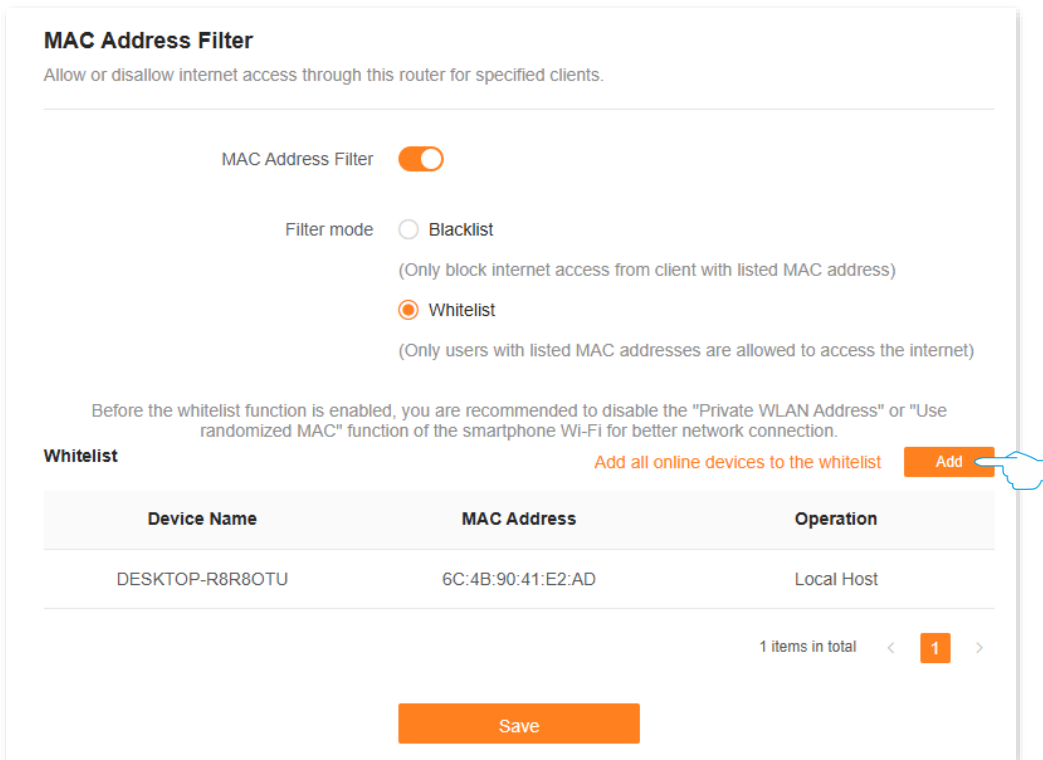
7.2.2 Add the clients to whitelist that are not connected to the internet

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

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

Step 3 Enable the **MAC Address Filter** function, and set **Filter mode** to **Whitelist.**

Step 4 Click **Add.**



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)

Whitelist
(Only users with listed MAC addresses are allowed to access the internet)

Before the whitelist function is enabled, you are recommended to disable the "Private WLAN Address" or "Use randomized MAC" function of the smartphone Wi-Fi for better network connection.

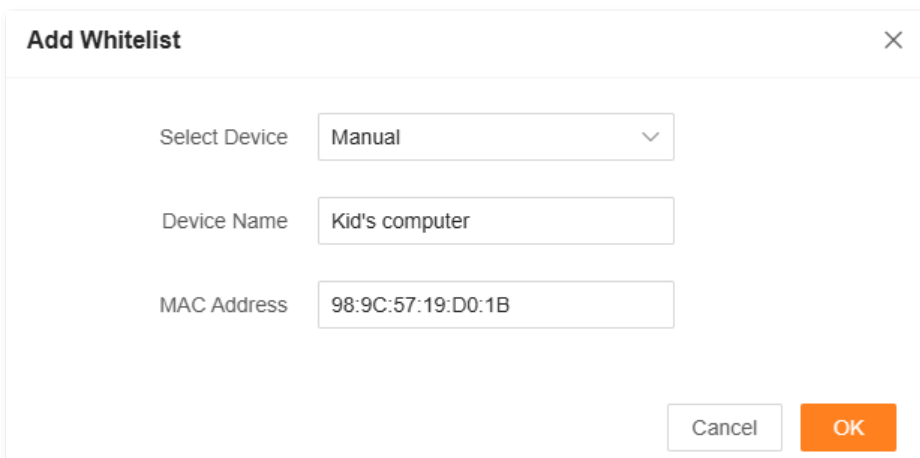
Whitelist Add all online devices to the whitelist **Add**

Device Name	MAC Address	Operation
DESKTOP-R8R8OTU	6C:4B:90:41:E2:AD	Local Host

1 items in total < **1** >

Save

Step 5 Select **Manual** in the **Select Device** bar, and enter the MAC address of the clients to be added to the whitelist, and the device name can be customized.



Add Whitelist [Close]

Select Device

Device Name

MAC Address

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)

Whitelist
(Only users with listed MAC addresses are allowed to access the internet)

Before the whitelist function is enabled, you are recommended to disable the "Private WLAN Address" or "Use randomized MAC" function of the smartphone Wi-Fi for better network connection.

Whitelist Add

Device Name	MAC Address	Operation
DESKTOP-R8R8OTU	6C:4B:90:41:E2:AD	Local Host
22:CB:88:D3:04:F0	22:CB:88:D3:04:F0	
Kid's computer	98:9C:57:19:D0:1B	

3 items in total < 1 >

Save

---End

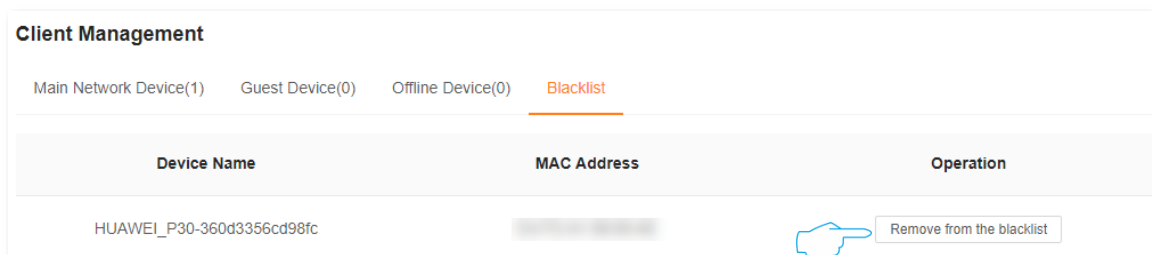
7.3 Remove a client from the blacklist

7.3.1 Method 1 (For blacklist only)

Step 1 [Log in to the web UI of the router](#), and navigate to **Client Management**.

Step 2 Choose **Blacklist** on the right.

Step 3 Click **Remove from the blacklist** under **Operation** in the line of the client to be removed from the blacklist.



Step 4 Confirm the prompt message, and click **OK**.


---End

The client is removed from the blacklist and displayed in **All Devices** now. It can access the internet upon the next connection.

7.3.2 Method 2

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

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

Step 3 Locate the device you want to remove from the blacklist in the **Blacklist**, and click  (**Delete**).

Step 4 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)

Whitelist
(Only users with listed MAC addresses are allowed to access the internet)

Blacklist Device

Device Name	MAC Address	Operation
Kid's computer	98:9C:57:19:D0:1B	 

1 items in total < 1 >

---End

7.4 Internet access speed control

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

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**.

Set **Download** to **512KB/s** in this example: 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 with a dropdown menu set to 'All Nodes'. Below the navigation tabs, there are two device entries under 'Main Network Device(2)'. The first device, 'DESKTOP-R8R80TU', has a current speed of 0 KB/s, a negotiation speed of 100 Mbps, and bandwidth control set to 'Unlimited' for both upload and download. The second device, '6E:ED:56:D7:E3:F0', has a current speed of 0 KB/s, a negotiation speed of 1201 Mbps, and bandwidth control set to 'Unlimited' for upload and '512 KB/s' for download. An 'Add to blacklist' button is visible next to the second device.

Main Network Device(2)	Current Speed	Negotiation Speed	Bandwidth Control	Operation
DESKTOP-R8R80TU IP Address: 192.168.0.183 MAC Address: [REDACTED] Uptime: 5 minute(s) Wired	↑ 0 KB/s ↓ 0 KB/s	100 Mbps	Upload: Unlimited Download: Unlimited	Local Host
6E:ED:56:D7:E3:F0 IP Address: 192.168.0.120 MAC Address: [REDACTED] Uptime: 0 minute(s) 5G	↑ 0 KB/s ↓ 0 KB/s	1201 Mbps	Upload: Unlimited Download: 512 KB/s	Add to blacklist

---End

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

The following table describes the parameters displayed on this page.

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.

7.5 Only prohibit specified clients from accessing the internet

With the MAC address filter function, you can:

- Add the client to the blacklist: Prohibits the specified client from accessing the internet through the router.
- Add the client to the whitelist: Only the specified client can access the internet through the router. Other devices cannot access the Internet through the router.

This section uses adding the clients to blacklist as an example.

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 goal.

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 **Add.**
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 **Add.**
2. Select the kid's phone name in the **Select Device**, and 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)
 Whitelist
(Only users with listed MAC addresses are allowed to access the internet)

Blacklist Device Add

Device Name	MAC Address	Operation
Kid's computer	98:9C:57:19:D0:1B	
42:c6:4d:2b:d8:16	42:C6:4D:2B:D8:16	

2 items in total < 1 >

Save

---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.

7.6 Internet access rule control

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

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.

Goal: Devices cannot access to websites include kid's phones and computers.

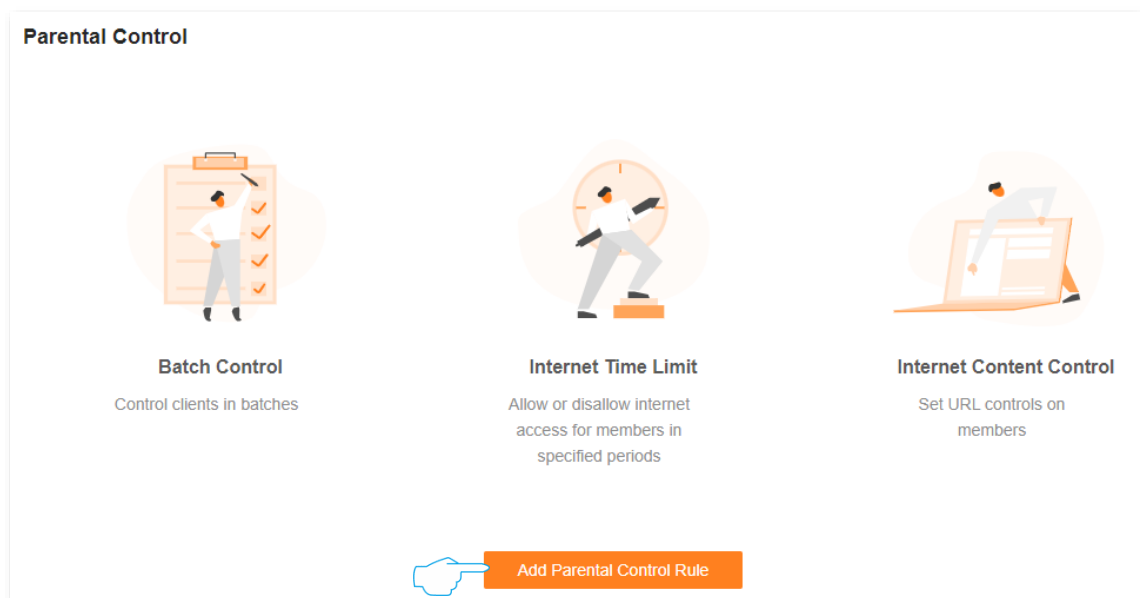
Solution: You can configure a parental control rule to reach the goal.

To add such a rule:

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

Step 2 Set parental control rule.

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



2. Set **Group Name**, which is **Kid's phone and computer** in this example.
3. Click **+** beside **Selected clients**.
4. Enable **Time 1**, and set control period of the client, which are **08:00-22:00** and **Sun.** in this example.



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 the listed URLs**.


7. Enter **Facebook**, **Twitter**, **Youtube**, and **Instagram** for URL.


8. Click **Save**.

---End

The following table describes the parameters displayed on this page.

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	Time 1	Used to enable or disable the internet access control period function and 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	Specifies whether the URL filter rule is applied.

Parameter	Description
Filter mode	Specifies the website filter mode.
	Specifies the websites that the Selected clients are blocked from accessing or allowed to access.
	 TIP
URL	<ul style="list-style-type: none">• 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: <code>www.google.com</code>.

After the settings are completed, your kid's phone and computer can access any websites except for Facebook, Twitter, Youtube and Instagram from 8:00 to 22:00 on Sunday.

8 Optimize network performance

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

This chapter includes the following sections:

[One-click optimization](#)

[Network diagnosis](#)

[Change channel and bandwidth](#)

[Enable or disable MLO function](#)

[Enable or disable OFDMA function](#)


[UPnP](#)

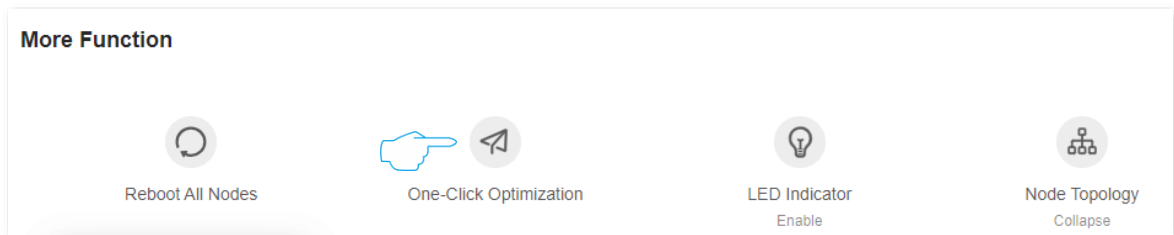
8.1 One-click optimization

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

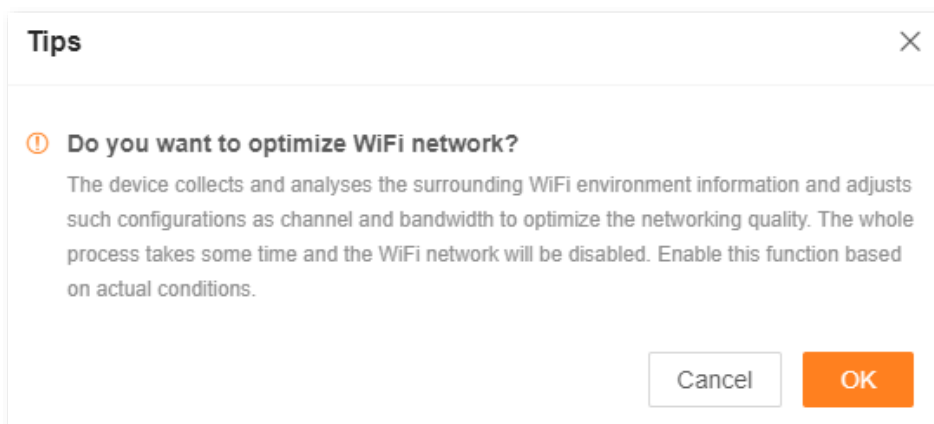
Configuration procedure:

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

Step 2 Navigate to **Network Status**. Then, click  (**One-Click Optimization**) under **More Function**.



Step 3 Confirm the prompt message, and click **OK**.



---End

8.2 Network diagnosis

If you cannot access the internet or the internet lag is severe, you can use network diagnosis function, and solve the problem according to the system's suggestions.


Configuration procedure:

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

Step 2 Navigate to **More > Network Diagnosis**.

Step 3 Click **Diagnose**.

Network Diagnosis



If the internet access failed or the internet lag is severe, network diagnosis is recommended.

[Diagnose](#)

WiFi Status	Checks the WiFi interference, air interface usage and packet error rate.	Not diagnosed
WAN Port Connection	Checks whether the WAN port is connected with an Ethernet cable and whether an IP address is obtained.	Not diagnosed
Ping Detection	Checks the connection between the device and internet/gateway.	Not diagnosed
DNS Parse	Checks whether the DNS is normal.	Not diagnosed
IPv6 Detection	Checks whether an IPv6 address is obtained, external network or gateway is pinged, and DNS is parsed successfully.	Not diagnosed
Router Status	Checks the memory and CPU usage.	Not diagnosed

---End

8.3 Change channel and bandwidth

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

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



To ensure 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	<input type="text" value="802.11b/g/n/ax"/>
Channel	<input type="text" value="Auto"/> <small>Current Channel:1</small>
Bandwidth	<input type="text" value="20/40MHz"/> <small>Current Bandwidth:20</small>

5 GHz WiFi

Network Mode	<input type="text" value="802.11a/n/ac/ax"/>
Channel	<input type="text" value="Auto"/> <small>Current Channel:48</small>
Bandwidth	<input type="text" value="20/40/80MHz"/> <small>Current Bandwidth:80</small>

The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
Network Mode	<p>Specifies various protocols used for wireless transmission. The maximum wireless rate varies from different standards. In general, it is recommended to keep the default setting. If you need to be compatible with some old devices, you can modify the corresponding network mode.</p> <p> TIP</p> <p>For the maximum wireless transmission speed, please visit www.tendacn.com and refer to the Datasheet of the corresponding product.</p>
Channel	<p>Specifies the channel in which the Wi-Fi network works.</p> <p>By default, the wireless channel is Auto, which indicates that the router selects a channel for the Wi-Fi network automatically.</p> <p>You are recommended to choose a channel with less interference for better wireless transmission efficiency. You can use a third-party tool to scan the Wi-Fi signals nearby to understand the channel usage situations.</p>
Bandwidth	<p>Specifies the bandwidth of the wireless channel of a Wi-Fi network. Please change the default settings only when necessary.</p> <ul style="list-style-type: none"> • 20MHz: Indicates that the channel bandwidth used by the router is 20 MHz. • 40MHz: Indicates that the channel bandwidth used by the router is 40 MHz. • 20/40MHz: 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: Indicates that the channel bandwidth used by the router is 80 MHz. This option is available only at 5 GHz. • 160MHz: Indicates that the channel bandwidth used by the router is 160 MHz. This option is available only at 5 GHz. • 20/40/80/160MHz: Specifies that a router can switch its channel bandwidth among 20 MHz, 40 MHz, 80 MHz and 160 MHz based on the ambient environment. This option is available only at 5 GHz.

8.4 Enable or disable MLO function

With Wi-Fi 6 and earlier routers, end devices can only have one connection to the router at a time. With Multi-Link Operation (MLO) enabled on a Wi-Fi 7 router, end devices can establish multiple connections to the router at the same time, increasing speed and reducing latency.



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

This function is disabled by default. When it is enabled, the page is displayed as follows.



TIP

MLO will only work if the Wi-Fi name and Wi-Fi password are the same for both bands and the network mode supports 802.11be.

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.

MLO

When enabled, the terminal can establish multiple connections with the router to improve speed and reduce latency.
This function can only work when the Wi-Fi name and Wi-Fi password of at least two bands are the same and the network mode supports 802.11be.

WiFi Enable

WiFi Name

Hide (After it is enabled, clients such as smartphones cannot find the Wi-Fi name and networking through the button is not supported for the frequency range.)

Security

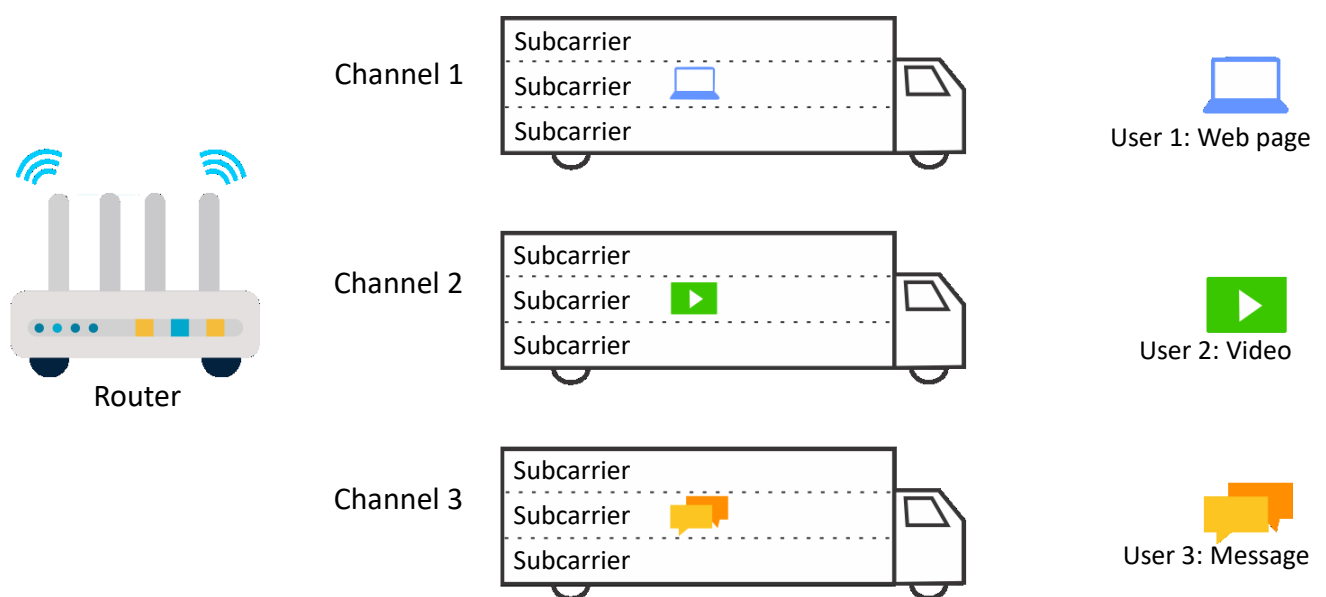
WiFi Password

8.5 Enable or disable OFDMA function

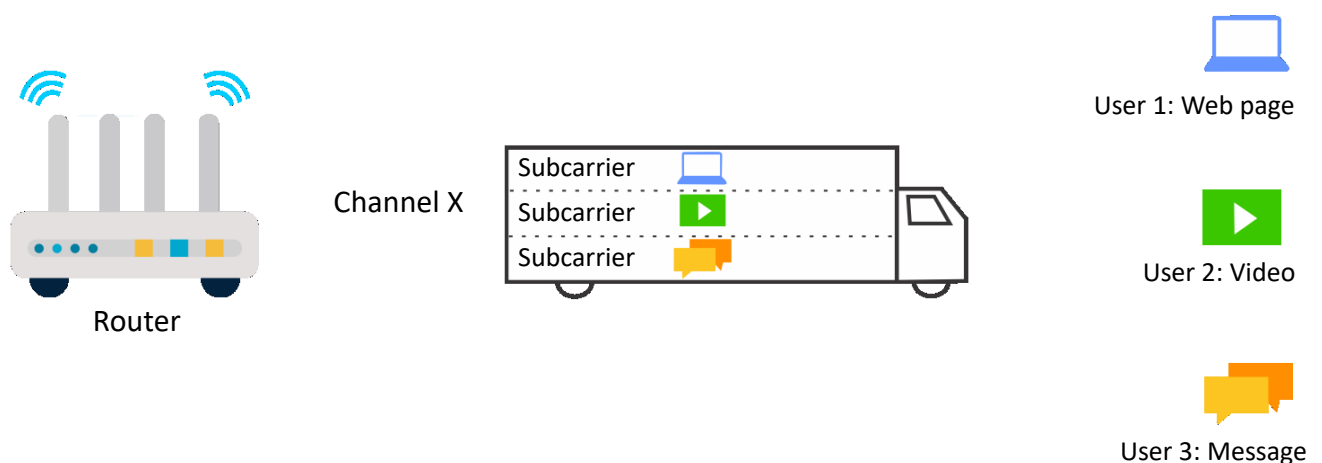
In telecommunications, Orthogonal Frequency-division Multiplexing (OFDM) is a type of digital transmission and a method of encoding digital data on multiple carrier frequencies. OFDM divides a channel into subcarriers, but only a single user can transmit on all of the sub-carriers at any given time.

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

OFDM data transmission mode:

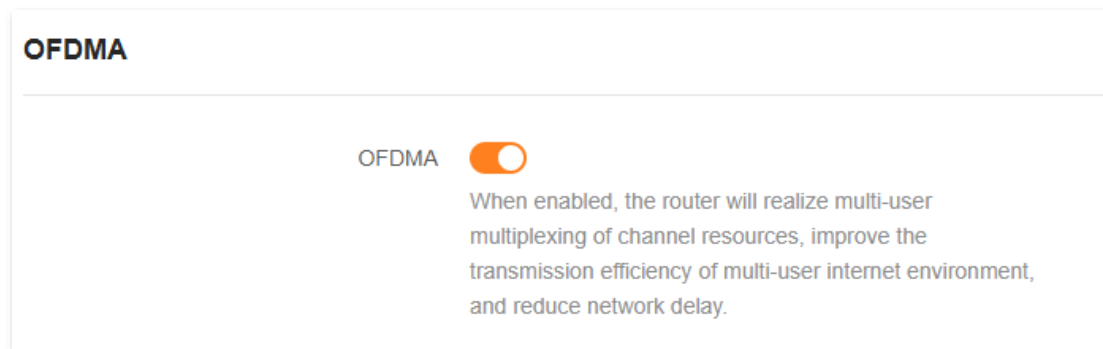


OFDMA data transmission mode:



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

This function is disabled by default. When it is enabled, the page is displayed as follows.



8.6 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
anywhere	64476	192.168.0.103	64476	UDP

9 Remote access

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

This chapter includes the following sections:

[Remote web management](#)

[DDNS](#)

[Port mapping](#)

[DMZ host](#)

[VPN](#)

9.1 Remote web management

9.1.1 Overview

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

9.1.2 Internet users access the router's web UI

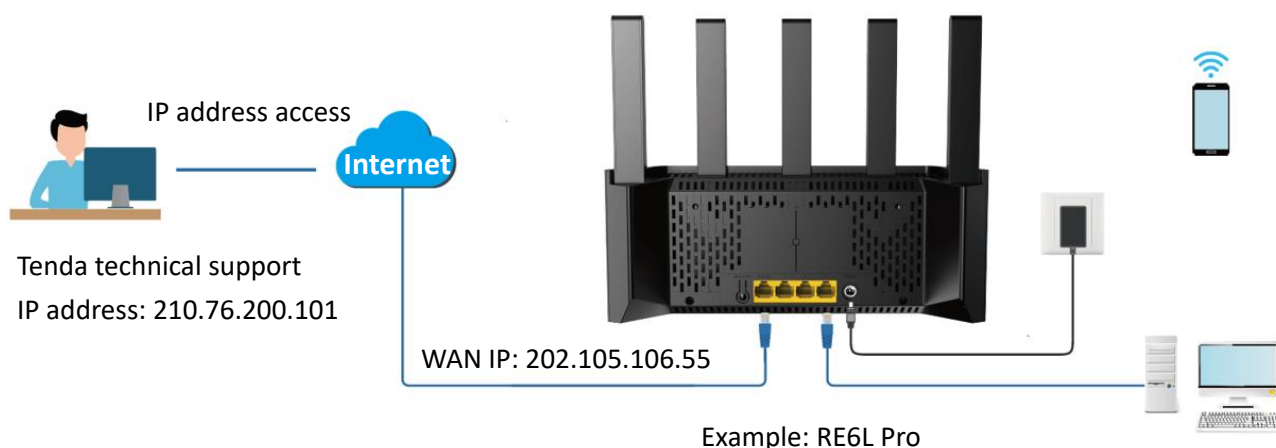
Scenario: You encounter a problem in configuring the router, and the router can access the internet.

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

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

Assume that:

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



By default, the [WAN/LAN auto-negotiation](#) function of the router is enabled, and the Ethernet cable connected to the internet can be connected to any Ethernet port. If the WAN/LAN auto-negotiation function is disabled, connect the Ethernet cable connected to the internet to Ethernet port 1 (WAN port).

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 ▼

Specified IP Address 210.76.200.101

Port 8888

Save

---End

The following message is displayed, indicating that the settings are saved successfully.


✔ Saved successfully. The configurations will take effect when the client connects to the WiFi network the next time

When the configuration is complete, 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 (IP address is **210.76.200.101**). You can find the current IP address of the router's WAN port on the [router information](#) page.

The following table describes the information displayed on this page.

Parameter description

Parameter	Description
Remote Web Management	Used to enable or disable the remote web management function of the router.

Parameter	Description
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).
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 “<i>http://WAN IP address of the router:Port number</i>”. If the DDNS host function is enabled, the web UI can also be accessed through “<i>http://Domain name of the router’s WAN port:Port number</i>”.

9.2 DDNS

9.2.1 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.

9.2.2 Internet users to access LAN resources using a domain name

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

Goal: 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 with a domain name.

Solution: You can configure the DDNS plus port mapping functions to reach the goal.

Assume that the information of the FTP server includes:

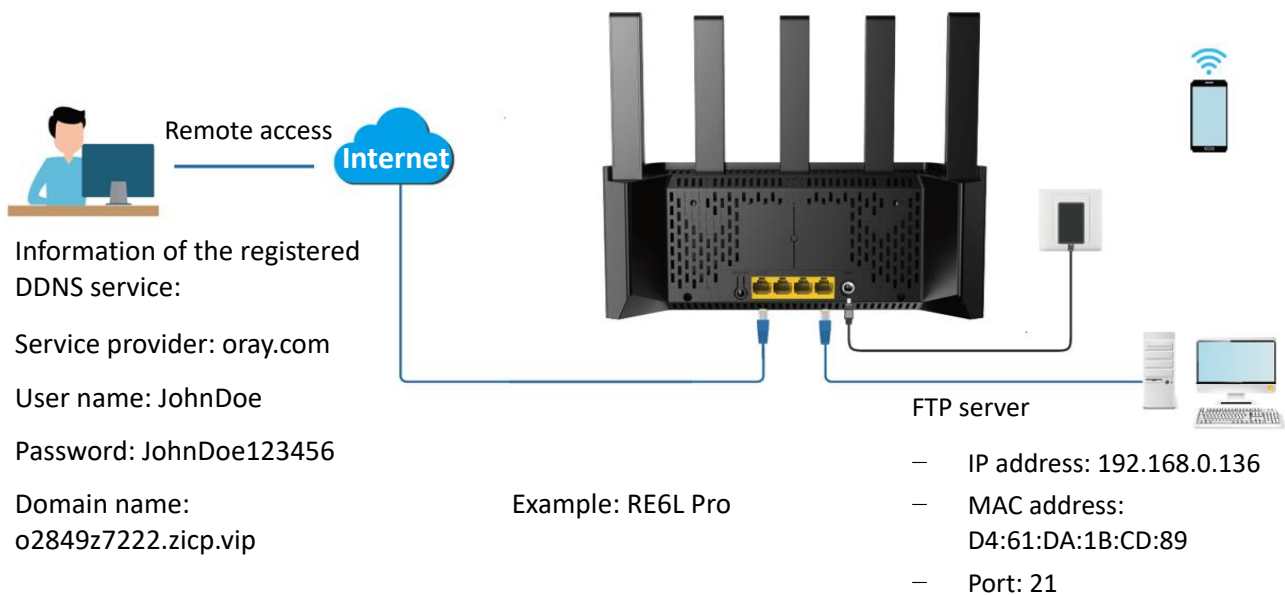
- IP address: **192.168.0.136**
- MAC address of the host: **D4:61:DA:1B:CD:89**
- Service port: **21**

Information of the registered DDNS service:

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



Ensure that the router obtains an IP address from the public network. This function may not work on a host with an IP address of a private network 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.



By default, the [WAN/LAN auto-negotiation](#) function of the router is enabled, and the Ethernet cable connected to the internet can be connected to any Ethernet port. If the WAN/LAN auto-negotiation function is disabled, connect the Ethernet cable connected to the internet to Ethernet port 1 (WAN port).

Log in to the web UI

Configure DDNS

Configure port mapping rule

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 **DDNS**.
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**

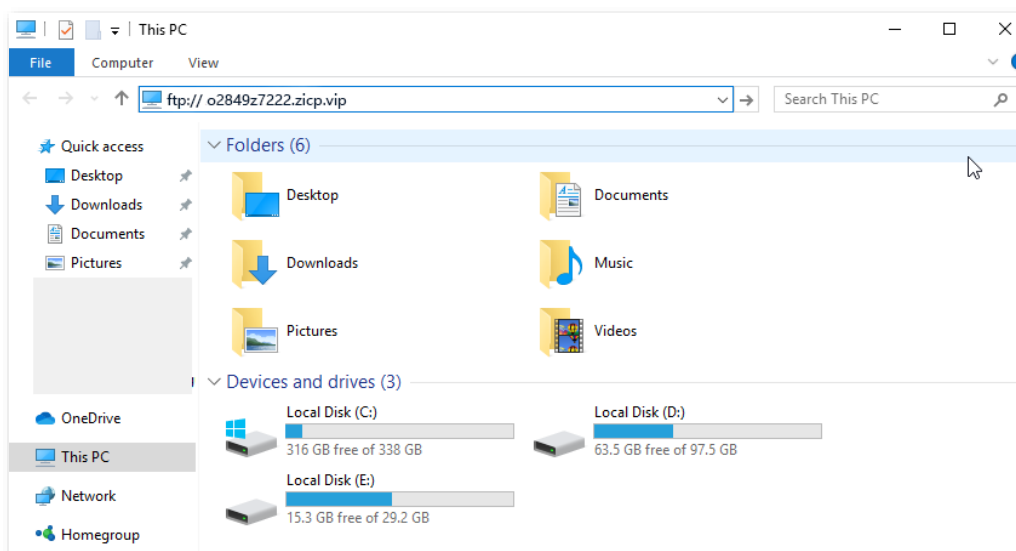
Wait until **Connected** is displayed after **Connection Status**, which indicates that the configuration is successful.

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

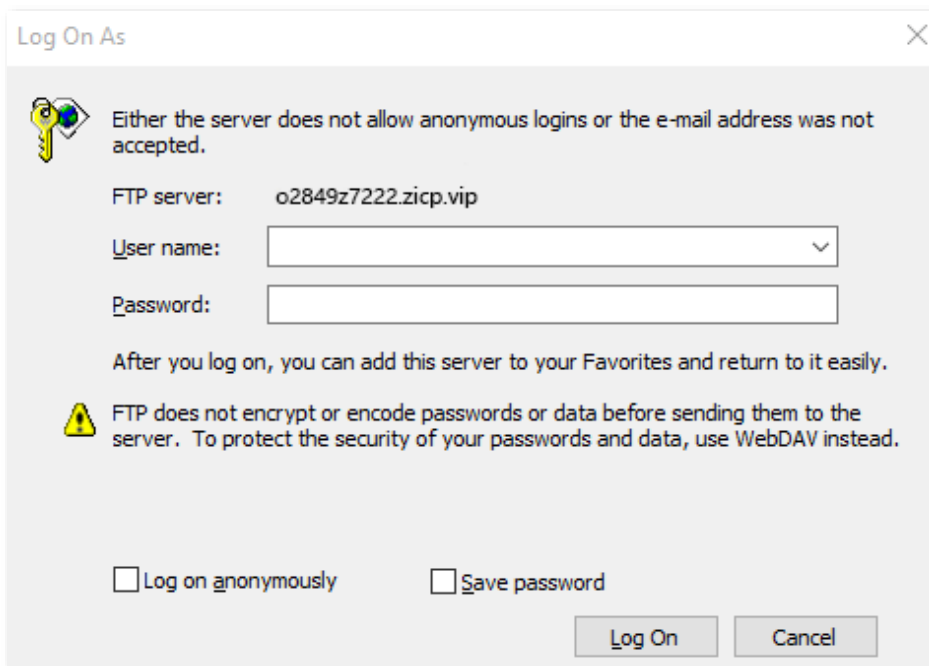
---End

When completing the configuration, users from the internet can access the FTP server by visiting “*Intranet service application layer protocol name://Domain name*”. If the WAN port number is not the same as the default intranet service port number, the visiting address should be: “*Intranet service application layer protocol name://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.



Log On As


Either the server does not allow anonymous logins or the e-mail address was not accepted.

FTP server: o2849z7222.zicp.vip

User name:

Password:

After you log on, you can add this server to your Favorites and return to it easily.

 FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use WebDAV instead.

Log on anonymously Save password



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



- Ensure that the Intranet port you fill in is the correct corresponding service port.
 - Close the firewall, antivirus software and security guards on the host of the FTP server and try again.
-

9.3 Port mapping

9.3.1 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
192.168.0.103	21	21	TCP&UDP	 

The following table describes the parameters displayed on this page.

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. You can click the drop-down menu and select the corresponding service port number. You can also select Custom and manually enter the corresponding service port number.
External Port	Specifies the external port for the internal port to map with. After selecting the internal port, the external port will be filled automatically, or you can enter it manually.
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:  : Used to edit a port mapping rule.  : Used to delete a port mapping rule.

9.3.2 Internet users access LAN resources

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

Goal: 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.

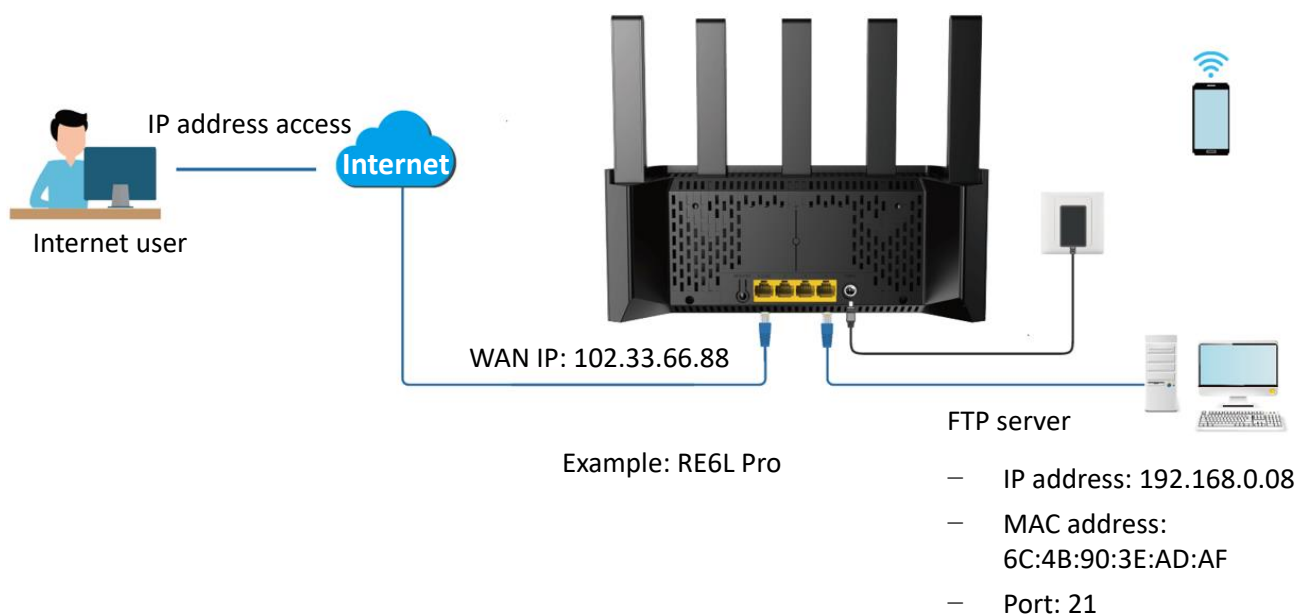
Solution: You can configure the port mapping function to reach the goal.

Assume that:

- IP address of the FTP server: 192.168.0.08
- 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.





By default, the [WAN/LAN auto-negotiation](#) function of the router is enabled, and the Ethernet cable connected to the internet can be connected to any Ethernet port. If the WAN/LAN auto-negotiation function is disabled, connect the Ethernet cable connected to the internet to Ethernet port 1 (WAN port).

Log in to the web UI

Configure port mapping rule

Assign a fixed IP address to the host where the intranet server resides

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 **Add**.
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 **Intranet 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.

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 Add

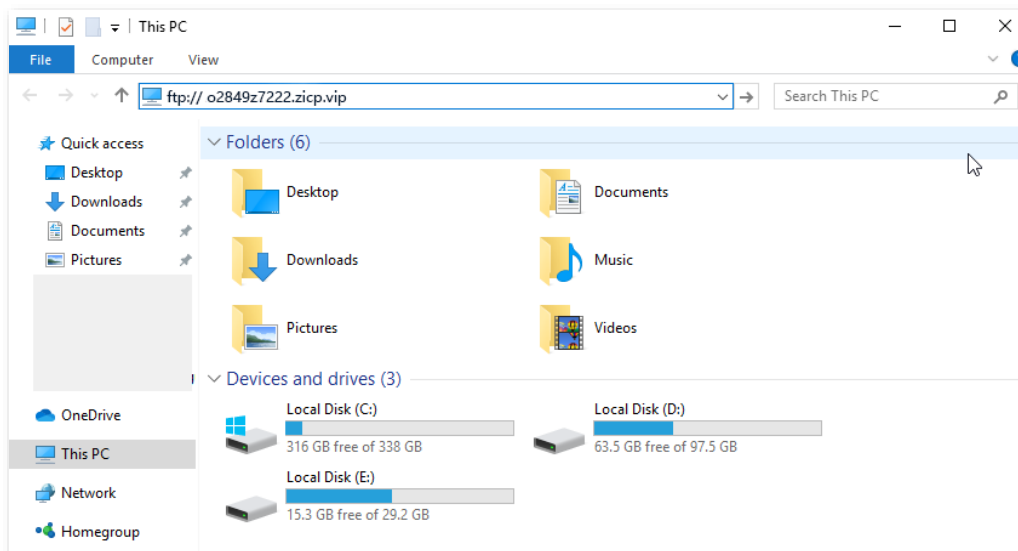
Internal IP Address	Internal Port	External Port	Protocol	Operation
192.168.0.80	21	21	TCP&UDP	 

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

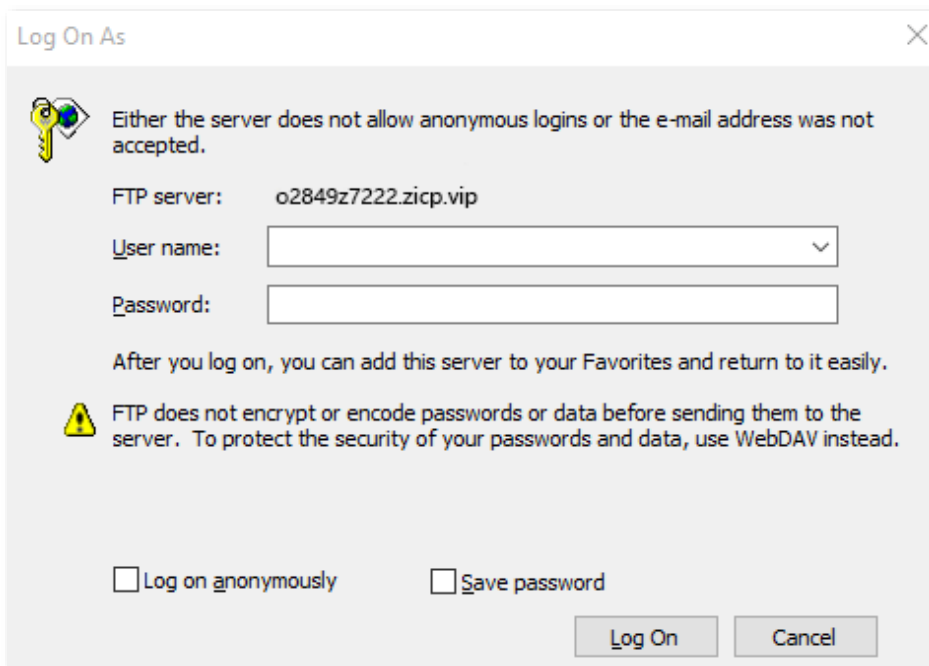
---End

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 [System information](#) page.



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



Log On As


Either the server does not allow anonymous logins or the e-mail address was not accepted.

FTP server: o2849z7222.zicp.vip

User name:

Password:

After you log on, you can add this server to your Favorites and return to it easily.

 FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use WebDAV instead.

Log on anonymously Save password

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



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

- Ensure that the Intranet port you fill in is the correct corresponding service port.
 - Close the firewall, antivirus software and security guards on the host of the FTP server and try again.
-

9.4 DMZ host

9.4.1 Overview

A DMZ host on a LAN is free from restrictions in communicating with the internet. It is useful for getting better and smoother experiences 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.
-

9.4.2 Internet users access LAN resources

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

Goal: 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.

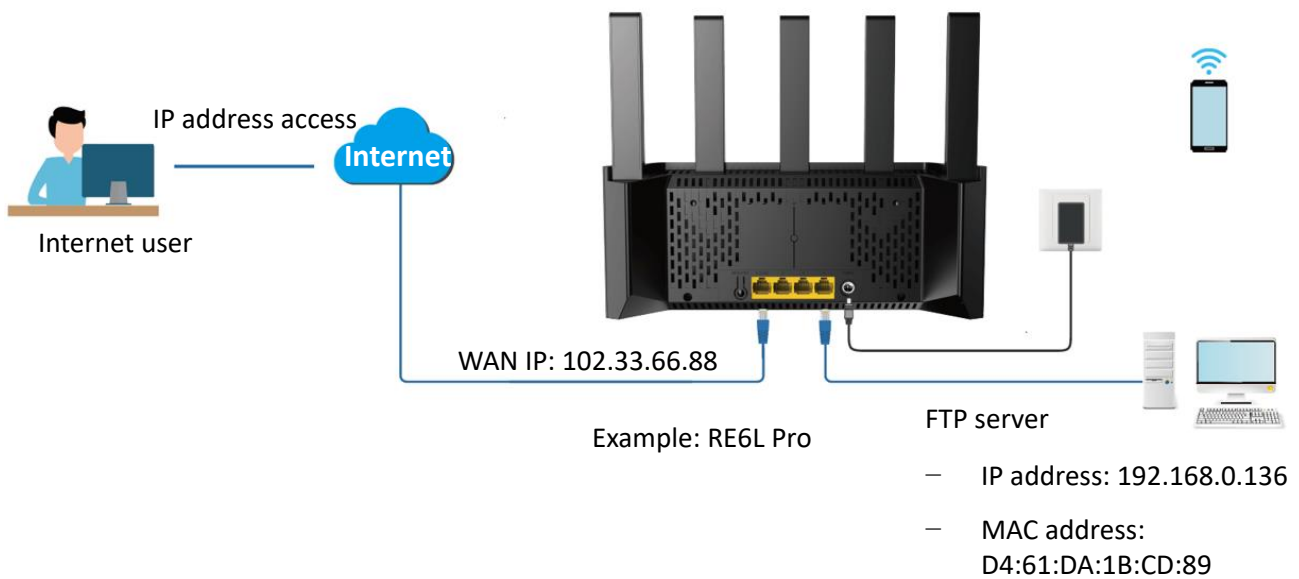
Solution: You can configure the DMZ host function to reach the goal.

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**



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



By default, the [WAN/LAN auto-negotiation](#) function of the router is enabled, and the Ethernet cable connected to the internet can be connected to any Ethernet port. If the WAN/LAN auto-negotiation function is disabled, connect the Ethernet cable connected to the internet to Ethernet port 1 (WAN port).

Log in to the web UI

Configure DMZ host

Assign a fixed IP address to a DMZ host

Configuration procedure:

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

Step 2 Set 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

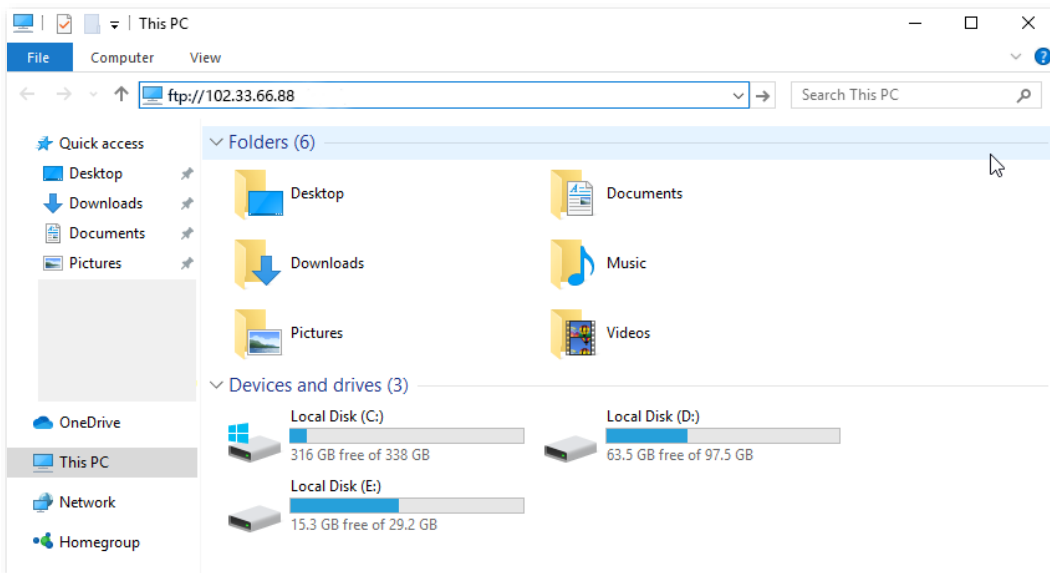
When the configuration is complete, users from the internet can access the DMZ host by visiting “*Intranet service application layer protocol name://WAN IP address of the router*”. If the intranet service port number is not the default number, the visiting address should be: “*Intranet service application 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 on the [router information](#) page.

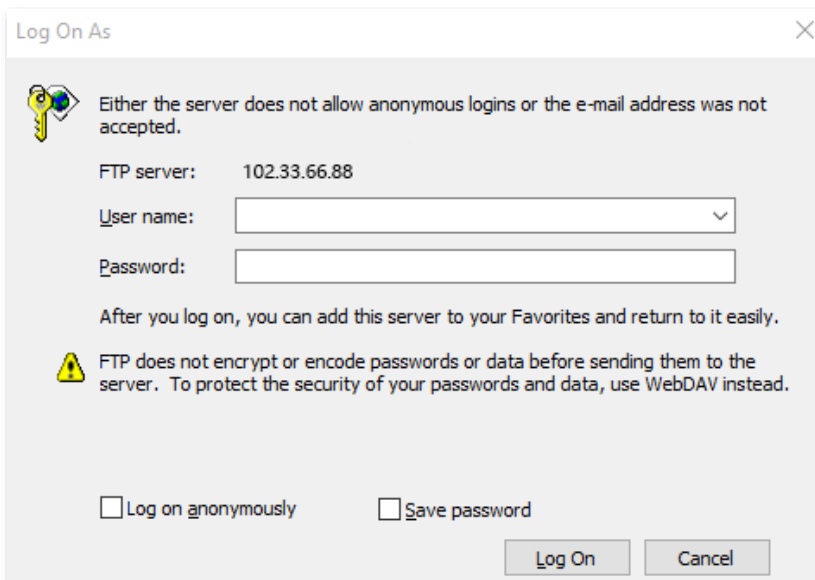


TIP

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](#).



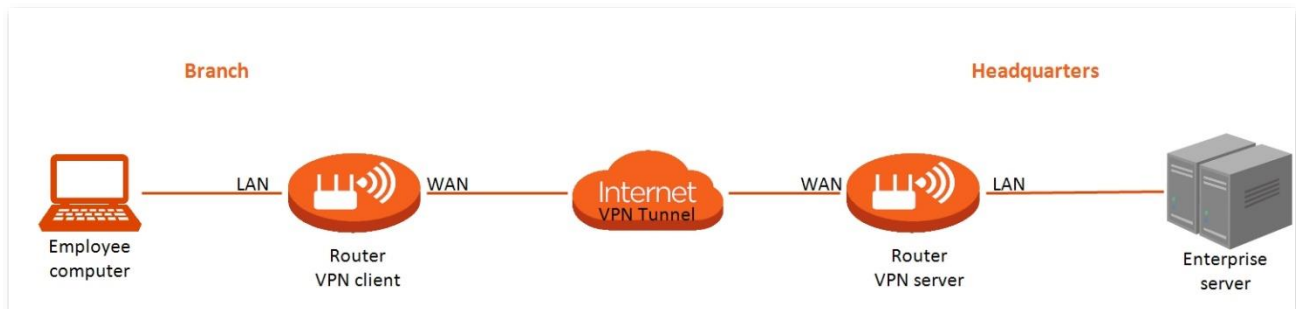
After the configuration, if internet users still cannot access the FTP server, close the firewall, antivirus software and security guards on the host of the FTP server and try again.

9.5 VPN

9.5.1 Overview

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.



The router supports Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP).

- PPTP encapsulates link-layer PPP frames in IP packets to transmit data over the IP network.
- L2TP encapsulates link-layer PPP frames in different packets for transmission based on different network types.

9.5.2 PPTP server

The routers 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 > Network Settings > VPN**. 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

PPTP Server

Address Pool Range . . . -

MPPE Encryption

The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
PPTP Server	Used to enable or disable the PPTP server. When it is enabled, the router functions as a PPTP server, which can accept the connections from PPTP clients.
Address Pool Range	Specifies the IP address range within which the PPTP server can assign to PPTP clients. It is recommended to keep the default settings.
MPPE Encryption	Used to enable or disable 128-bit data encryption. The encryption settings should be the same between the PPTP server and PPTP clients. Otherwise, communication cannot be achieved normally.





Add PPTP user account

To access the configuration page, [log in to the web UI of the router](#), and navigate to **More > Network Settings > VPN**. Click **Add**, set the user name and password, and click **OK**.

PPTP Account			
User Name	Password	Connection Status	Operation
No Data			

The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
User Name	Specify the VPN user name and password, which the VPN user needs to enter when making PPTP dial-ups (VPN connections).
Password	
Connection Status	Specifies the connection status of the VPN connection.
	The available operations include:
	 : Indicates that the PPTP user account is available. You can click it to disable the account.
Operation	 : 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 > Network Settings > VPN > PPTP Server**.

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

The following table describes the parameters displayed on this page.

Parameter description

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

Internet users access resources

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

Goal: 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 goal. 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**.



Ensure that the WAN IP address of router is public. This function may not work on a host with a private IP address. 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 Enable **PPTP Server**.

1. Navigate to **More > Network Settings > 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 user name and password for the PPTP server.

Click **Add**, and set the user name and password for the PPTP server, which are both **admin1** in this example. Then, 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

PPTP Server

Address Pool Range -

MPPE Encryption

[Save](#)


PPTP Account [Add](#)

User Name	Password	Connection Status	Operation
admin1	admin1	• Offline	✔ ✎ 🗑

---End

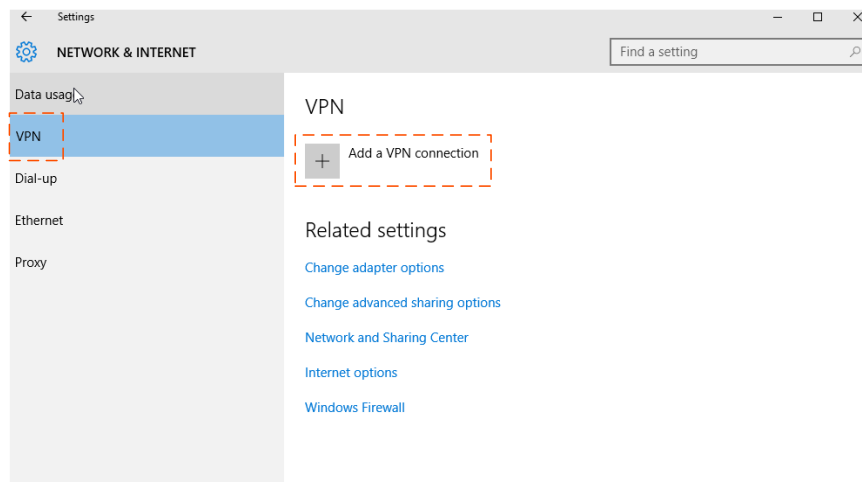
After the settings are completed, internet users can access the FTP server by following these steps:

Step 1 Perform VPN dial-up.

1. Click the  icon at the bottom right corner on the desktop of another computer with internet access, and then click **Network settings**.

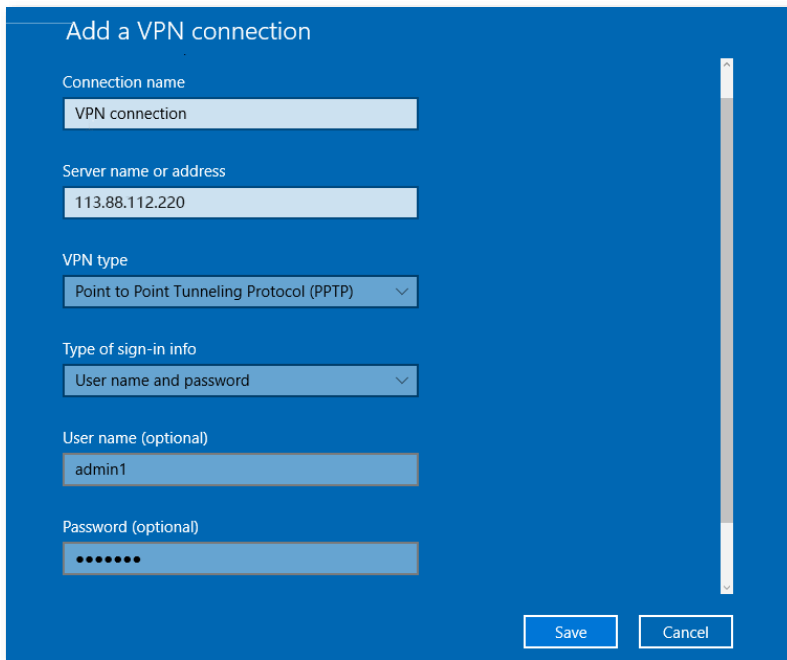


2. Choose **VPN** on the left side, and click **Add a VPN connection**.

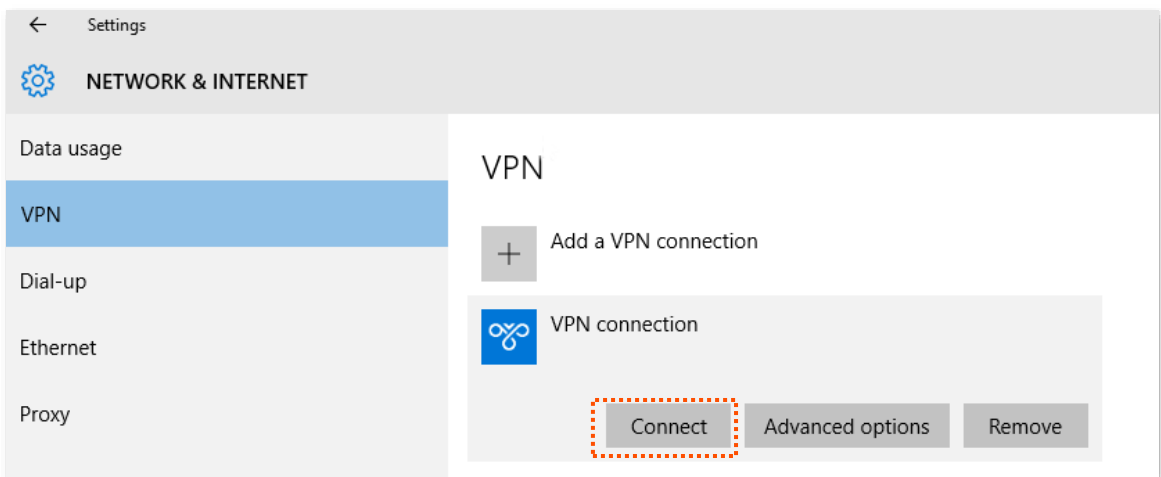


3. Configure the VPN parameters.

- Enter a connection name, such as **VPN connection**.
- 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**.




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



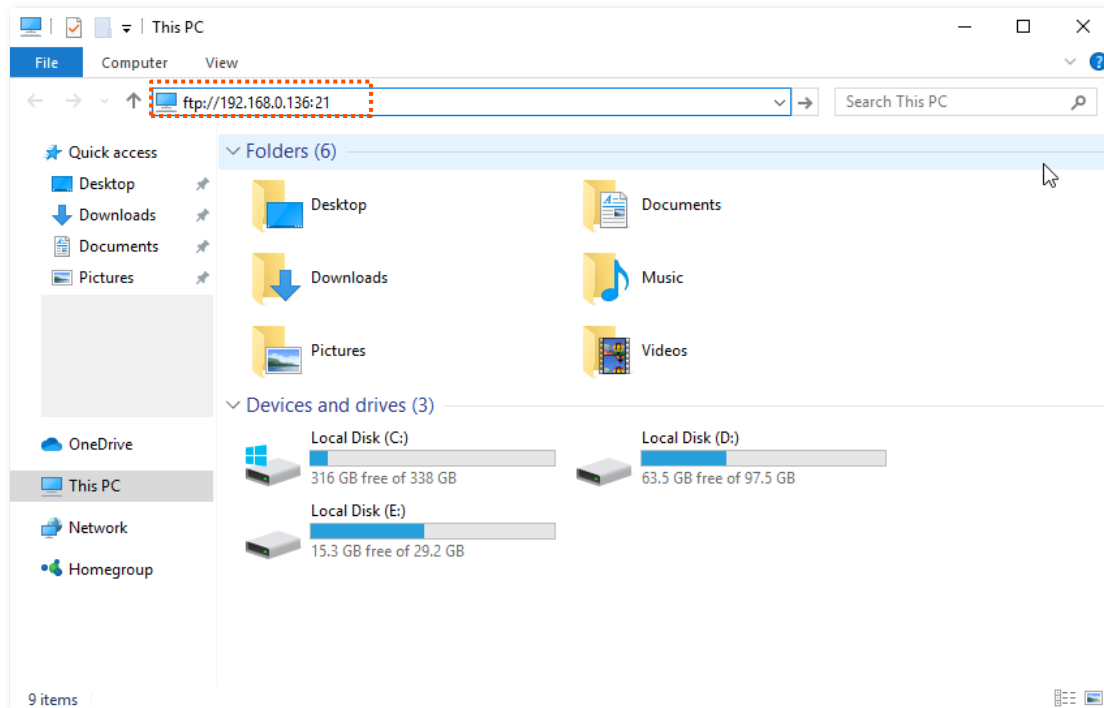
Wait a moment, the VPN connection is successful.

Step 2 Access the FTP server.

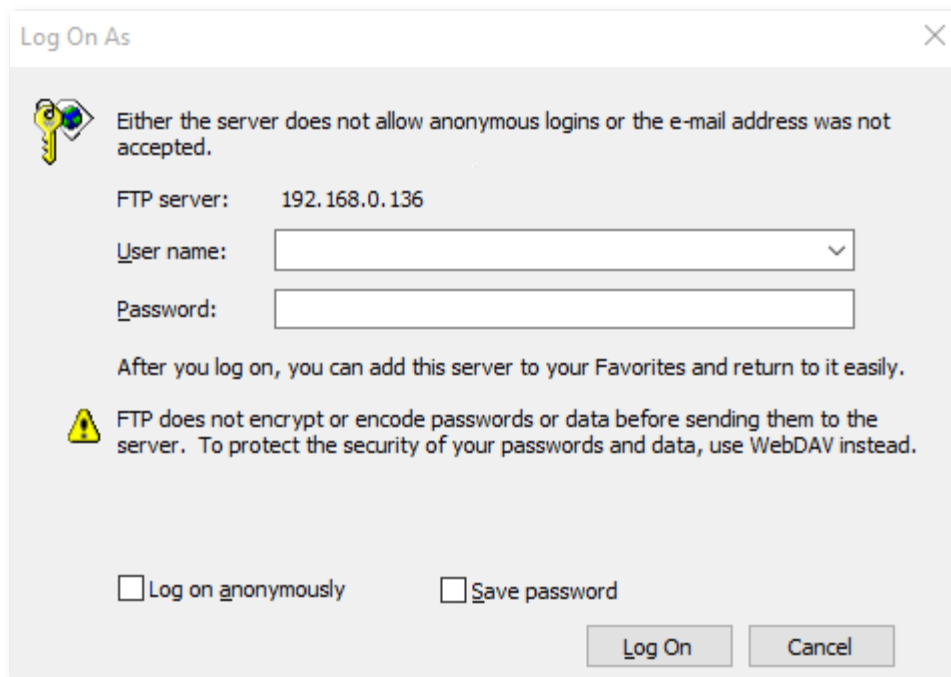
1. Click the  icon on the desktop, and enter the address in the address bar to access the FTP server, which is **ftp://192.168.0.136:21** in this example.



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.

9.5.3 PPTP/L2TP client

The routers can function as PPTP/L2TP clients 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 > Network Settings > VPN**. Enable the **PPTP/L2TP Client**, 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**

PPTP/L2TP Client

Client Type

Server IP/Domain Name

User Name

Password

Status Disconnected

The following table describes the parameters displayed on this page.

Parameter description

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

User access ISP's VPN resources

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

Goal: Access the VPN resources of your ISP more safely.

Solution: You can configure the PPTP/L2TP client function to reach the goal. 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 > Network Settings > VPN > PPTP/L2TP Client**.

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

Step 4 Choose **PPTP** for **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**.

The screenshot shows the configuration page for the PPTP/L2TP Client. At the top, there is a title 'VPN' and a brief description: '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.' Below this, there are two tabs: 'PPTP Server' and 'PPTP/L2TP Client', with the latter being selected. The configuration options are as follows:

- PPTP/L2TP Client:** A toggle switch is turned on.
- Client Type:** A dropdown menu is set to 'PPTP'.
- Server IP/Domain Name:** A text input field contains '113.88.112.220'.
- User Name:** A text input field contains 'admin1'.
- Password:** A text input field contains 'admin1'.
- Status:** The status is displayed as 'Disconnected'.

At the bottom of the form, there is an orange 'Save' button.

---End

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

10 Network security

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

This chapter includes the following sections:

[Hide the Wi-Fi network](#)

[Enable or disable MESH button](#)

[Change the login password](#)

[Firewall](#)

10.1 Hide the Wi-Fi network

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

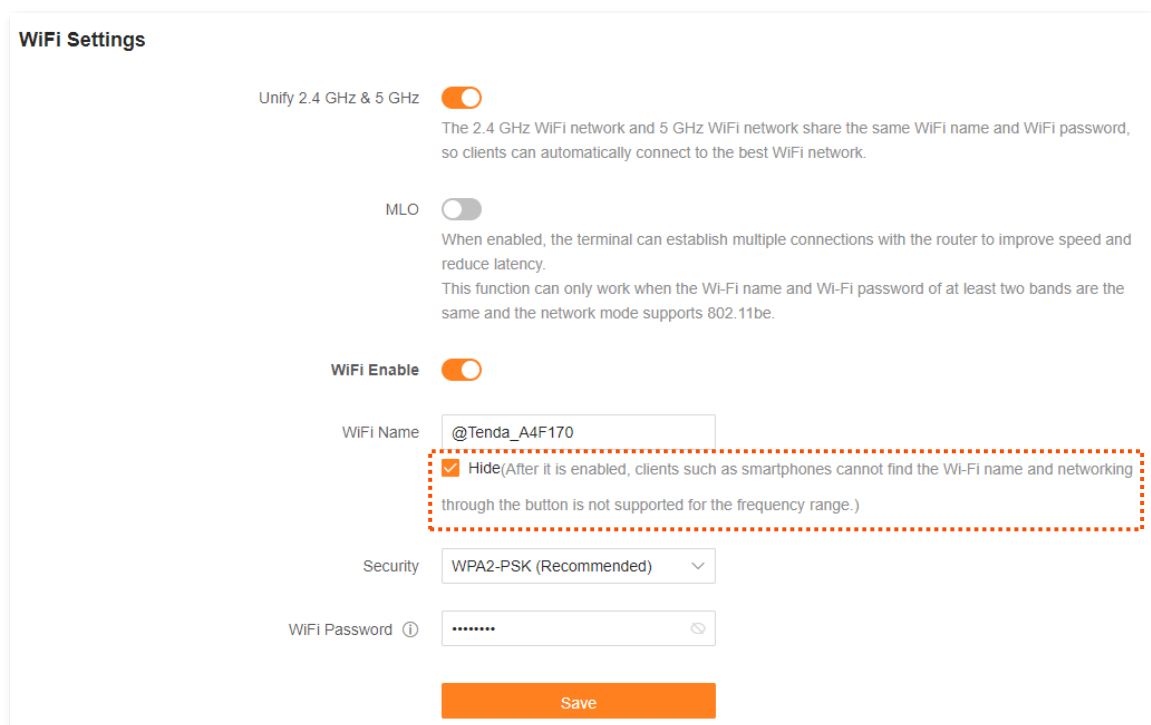
Configuration procedure:

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

Step 2 Navigate to **WiFi Settings**.

Step 3 Tick **Hide** under **WiFi Name**.

Step 4 Click **Save**.



The screenshot shows the 'WiFi Settings' page with the following configuration:

- Unify 2.4 GHz & 5 GHz:** Enabled (toggle switch).
- MLO:** Disabled (toggle switch).
- WiFi Enable:** Enabled (toggle switch).
- WiFi Name:** @Tenda_A4F170
- Hide:** Checked (checkbox). A red dashed box highlights this checkbox and its description: "Hide(After it is enabled, clients such as smartphones cannot find the Wi-Fi name and networking through the button is not supported for the frequency range.)"
- Security:** WPA2-PSK (Recommended)
- WiFi Password:** Hidden (masked with dots)
- Save:** Button at the bottom.

---End

After the settings are completed, the corresponding Wi-Fi network is invisible to Wi-Fi-enabled devices. If you want to connect to a hidden wireless network, you need to manually enter the wireless network name on a Wi-Fi-enabled device such as a smartphone. For details, see [Appendix A.3 Connect to a hidden Wi-Fi Network](#).

10.2 Enable or disable MESH/WPS button

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

You can enable or disable the MESH/WPS key networking function. This function is enabled by default.

- After enabled, the router can network with other Tenda Wi-Fi+ routers through the networking button (WPS or MESH) on the body. For details, see [Mesh button networking](#).
- After disabled, the router cannot be networked through the networking button (WPS or MESH) on the body, but can be networked through the [Scanning networking](#) and [Wired networking](#).



If you use this router in a public place, do not enable the MESH/WPS button function to ensure information security.

MESH/WPS Button

The router has a MESH/WPS button and can form a network with other Tenda routers which also have a MESH/WPS button.

MESH/WPS Button

Note:

1. For information security, do not toggle on MESH/WPS button when using the router in public areas.
2. With this function disabled, you cannot form network by using the MESH/WPS button on the device. However, you can use the Tenda WiFi app or web UI to add the device to a network.

10.3 Change the login password

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

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 Click **Save**.

Login Password

You can modify the login password of the router here.

Old Password	<input type="password" value="5 - 32 characters"/>
New Password	<input type="password" value="5 - 32 characters"/>

---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.

10.4 Firewall

The firewall function helps the router detect and defend ICMP flood attacks, TCP flood attacks and UDP flood attacks, and ignore Ping packets from the 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](#)

The following table describes the parameters displayed on this page.

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, and then suspends in a semi-connected state, thereby occupying a large number of server resources until the server denies any services.

Parameter	Description
UDP Flood Attack Defense	<p>Used to enable or disable the UDP flood attack defense.</p> <p>The UDP flood attack is implemented similarly with the 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.</p>
Block Ping from WAN	<p>Used to enable or disable the Block Ping from WAN function.</p> <p>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.</p>

11

Advanced

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

This chapter includes the following sections:

[Turn on or turn off the indicator of router](#)

[Enable or disable TWT function](#)

[IPTV](#)

[Enable or disable router's WAN/LAN auto-negotiation function](#)

[Change LAN IP address](#)

[Change DHCP server](#)

[Assign static IP address to LAN client](#)

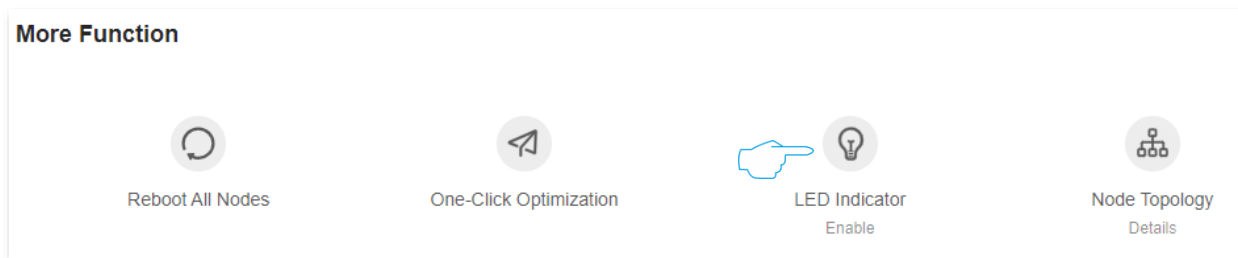
[Static routing](#)

11.1 Turn on or turn off the indicator of router

11.1.1 Turn on or turn off the indicators of all nodes

Method 1

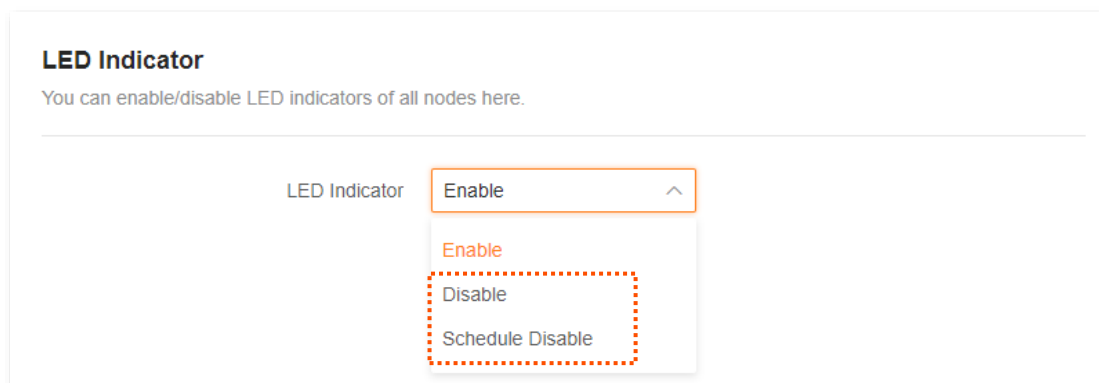
After [logging to the web UI of the router](#), click  or  in the **More Function** module of the **Network Status** page.



Method 2

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

Step 2 Navigate to **More > Smart Power Saving**, turn on or turn off the indicators of all nodes as required, and then click **Save**.



---End

11.1.2 Schedule turn off the indicators of all nodes

You can turn off the indicators of all nodes as required to save power.

Assume that you want to turn off the router's indicator from 22:00 to 7:00, and other periods are normal. For details, see the following steps.

Configuration procedure:

- Step 1** [Log in to the web UI of the router.](#)
- Step 2** Navigate to **More > Smart Power Saving > LED Indicator**.
- Step 3** Set **Schedule Disable** for LED Indicator.
- Step 4** Select **Turn Off at** to **22:00 - 7:00**.
- Step 5** Click **Save**.

LED Indicator

You can enable/disable LED indicators of all nodes here.

LED Indicator Schedule Disable ▼

Turn Off at 22:00 → 07:00 🕒

Save

---End

The following table describes the parameters displayed on this page.

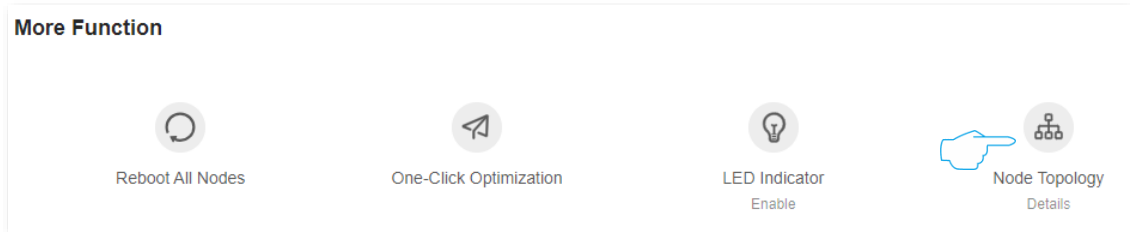
Parameter description

Parameter	Description
Enable	Specifies all indicators work normally.
Disable	Specifies all indicators are turned off.
Schedule Disable	During the set Turn Off at , all indicators of the router are turned off. Outside this period, all indicators work normally.

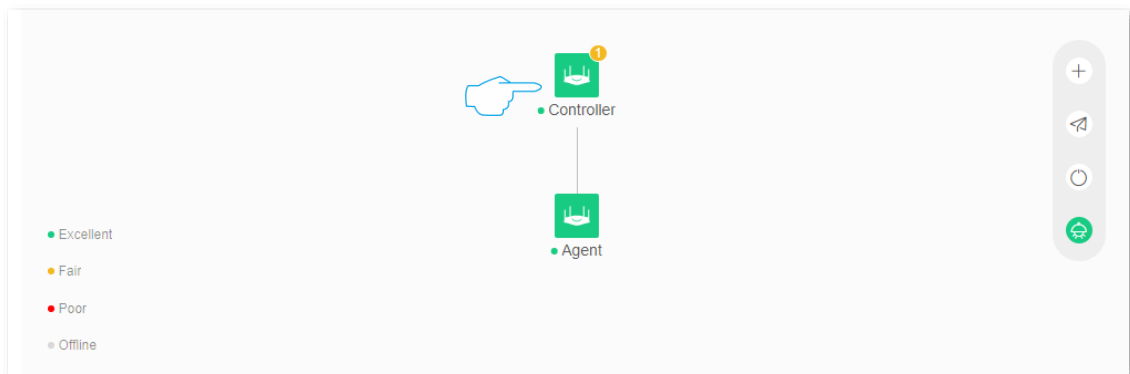
11.1.3 Turn on or turn off the indicators of single node

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

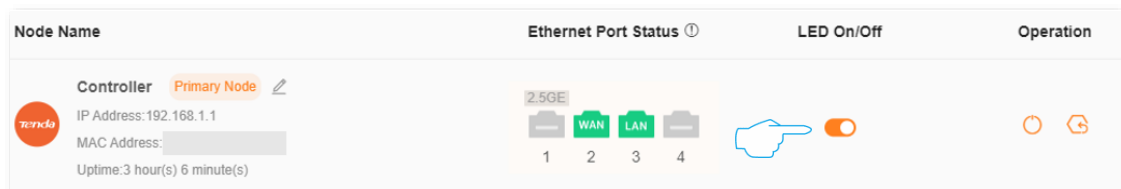
Step 2 Click  (Node Topology) in the **More Function** module of the **Network Status** page.



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.

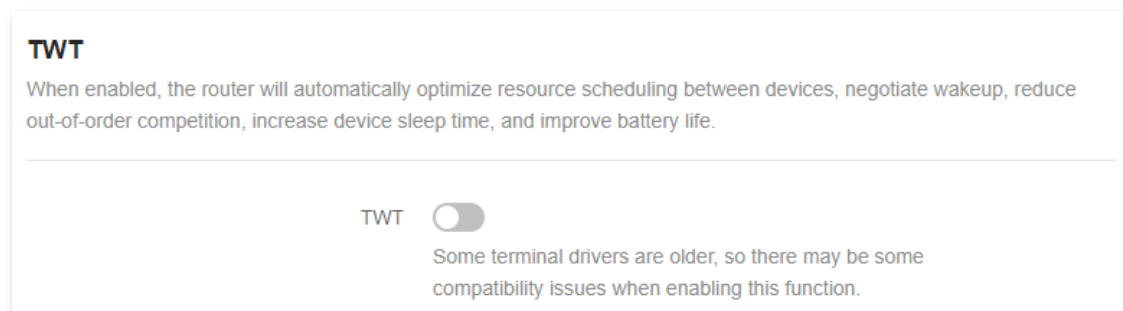


---End

11.2 Enable or disable TWT function

The Target Wakeup Time (TWT) means that after the TWT function is enabled, the router will automatically optimize the resource scheduling between devices and negotiate the wake-up time, so that clients such as a smartphone can reduce power consumption and improve device battery life when they do not need to communicate with the router.

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



11.3 IPTV

11.3.1 Overview

IPTV is the technology integrating internet, multimedia, telecommunication and many other technologies to provide interactive services, including digital TV, for family users by internet broadband lines.

If the IPTV service is included in your broadband service, you can enjoy both internet access through the router and rich IPTV contents with a set-top box when it is enabled.

If you want to watch multicast videos from the WAN side of the router on your computer, you can enable the multicast function of the router.

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

After the Multicast and STB function are enabled. See the following figure.

IPTV
You can configure multicast and IPTV function here.

Multicast
Once enabled, you can watch the multicast video source on the WAN side of the router from your client.

STB
Connect the IPTV STB to the IPTV port of the router.


VLAN
▼

Ethernet Port Selection
▼

The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
Multicast	Used to enable or disable the multicast function.

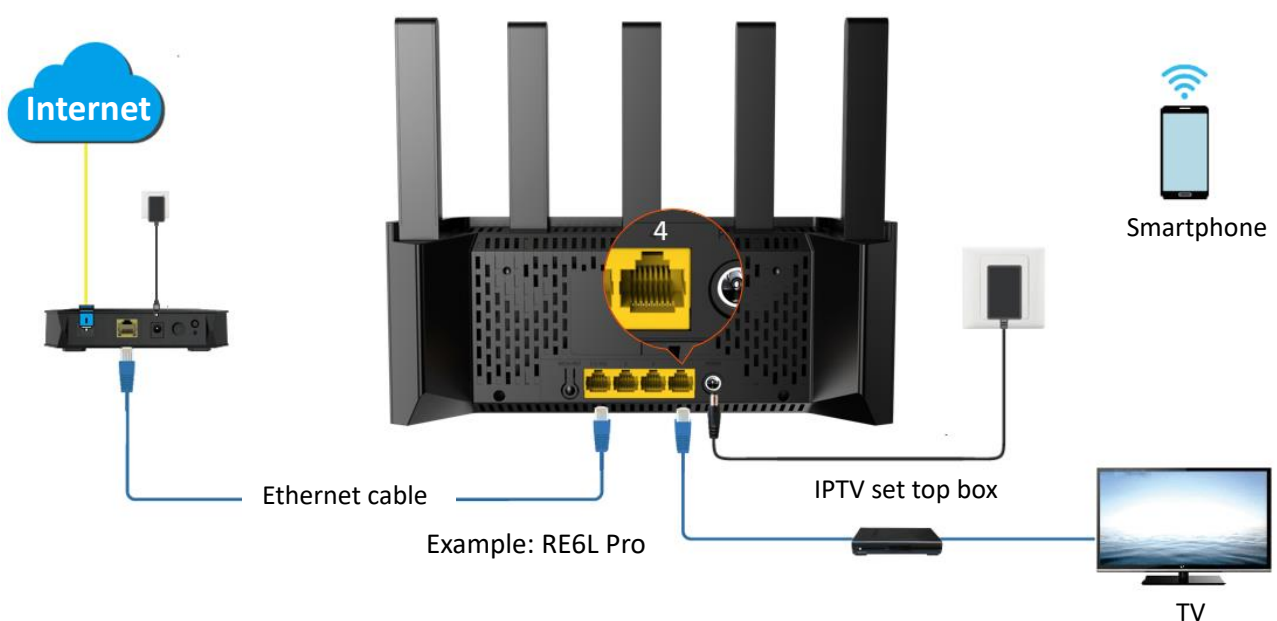
Parameter	Description
STB	Used to enable or disable the IPTV function of the router. When this function is enabled, the port IPTV/3 can be used only as an IPTV port and be connected to an IPTV set-top box.
VLAN	Specifies the VLAN ID of your IPTV service. <ul style="list-style-type: none"> • If your ISP does not provide any VLAN ID information when the IPTV service is available, keep Default. • If you have obtained the VLAN ID from your ISP when the IPTV service is available, choose Custom VLAN and enter the VLAN value. <p> TIP</p> <p>If Default is not available, you are recommended to consult your ISP to provide the VLAN ID.</p>
Ethernet Port Selection	Used to select Ethernet port for IPTV port.

11.3.2 Watch IPTV programs through the router

Scenario: The IPTV service is included in your broadband service. You have obtained the IPTV account and password from your ISP, and VLAN ID is 10.

Goal: Watch IPTV programs through the router.

Solution: You can configure the IPTV function to reach the goal.



Configuration procedure:**Step 1** Set your router.

1. [Log in to the web UI of the router.](#)
2. Navigate to **More > Network Settings > IPTV.**
3. Enable the **STB** function.
4. Select **Custom** for **VLAN**, and set VLAN ID to **10**.
5. Click **Save**.

IPTV
You can configure multicast and IPTV function here.

Multicast

Once enabled, you can watch the multicast video source on the WAN side of the router from your client.

STB

Connect the IPTV STB to the IPTV port of the router.

VLAN Custom

Custom 10

Ethernet Port Selection Ethernet Port 4

Save

Step 2 Configure the set-top box.

Use the IPTV user name and password provided by your ISP to dial up on the set-top box.

---End

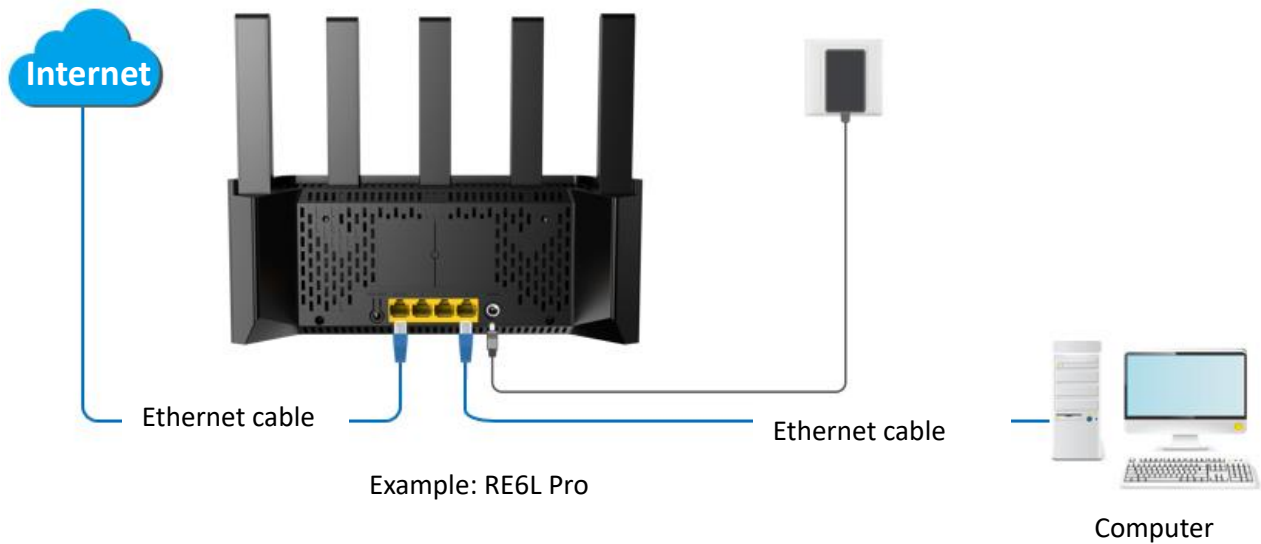
After the settings are completed, you can watch IPTV programs on your TV.

11.3.3 Watch multicast videos through the router

Scenario: You have the address of multicast videos.

Goal: You can watch multicast videos.

Solution: You can configure the multicast function to reach the goal.



TIP

By default, the [WAN/LAN auto-negotiation](#) function of the router is enabled, and the Ethernet cable connected to the internet can be connected to any Ethernet port. If the WAN/LAN auto-negotiation function is disabled, connect the Ethernet cable connected to the internet to Ethernet port 1 (WAN port).

Configuration procedure:

- Step 1** [Log in to the web UI of the router.](#)
- Step 2** Navigate to **More > Network Settings > IPTV.**
- Step 3** Enable the **Multicast.**
- Step 4** Click **Save.**

IPTV

You can configure multicast and IPTV functions here.

Multicast

Once enabled, you can watch the multicast video source on the WAN side of the router from your client.

STB

---End

After the settings are completed, you can watch multicast videos on your terminal devices.

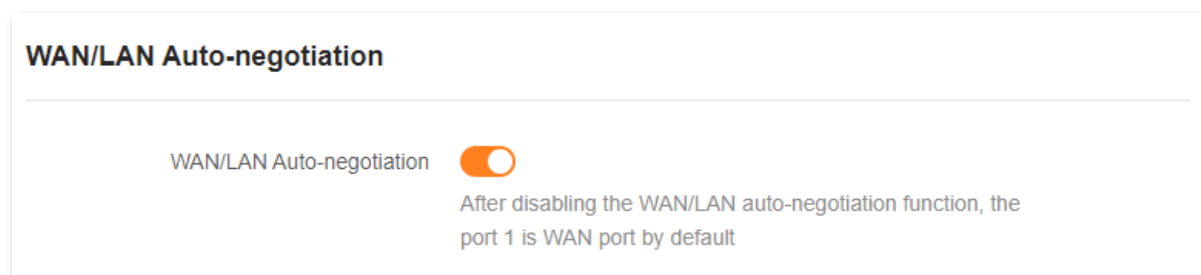
11.4 Enable or disable router's WAN/LAN auto-negotiation function

WAN/LAN auto-negotiation function, that is, the router Ethernet port does not distinguish between WAN (Internet port) and LAN (internal port), with WAN, LAN auto-adaptive characteristics. The Ethernet jack or the Ethernet cable has been connected to the computer can be connected to any Ethernet port of the router.

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

The WAN/LAN auto-negotiation function is enabled by default. When disabled, the Ethernet port 1 is WAN port, and other Ethernet ports are LAN ports.

- WAN port: Used to connect optical modem, DSL modem, cable TV modem or Ethernet jack.
- LAN port: Used to connect computers, switches, game consoles, and so on.



11.5 Change LAN IP address

The LAN IP address is the router's IP address to the LAN and also the router's management IP address. LAN users can log in to the web UI of the router using this IP address.

The default router's LAN IP address is 192.168.0.1 and the subnet mask is 255.255.255.0. Generally, you do not need to change the LAN port settings unless IP address conflicts occur. For example, the WAN IP address obtained by the router and the LAN IP address are on the same network segment. The IP address of other devices on the LAN is also 192.168.0.1.

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**.

---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.

11.6 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**.

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 -

Lease Time ⓘ

DNS

The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
DHCP Server	Used to enable or disable the DHCP server. Once enabled, the DHCP server automatically assigns internet parameters such as IP address, subnet mask, and gateway address to the terminal device. You are recommended to enable this function.
Address Pool Range	Specifies the range of IP addresses that can be assigned to clients connected to the router. The default range is 192.168.0.100 to 192.168.0.254.
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 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>It is recommended to keep the default value.</p>
DNS	<p>Specifies whether to allocate another DNS address to the client.</p> <ul style="list-style-type: none"> – 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.
Primary DNS	<p>Specifies the primary DNS address allocated to the client by the router.</p> <p> TIP</p> <p>Make sure that the primary DNS server is the IP address of the correct DNS server or DNS proxy. Otherwise, you may fail to access the internet.</p>
Secondary DNS	Specifies the secondary DNS server address of the router used to assign to the clients. It is optional.

11.7 Assign static IP address to LAN client

The DHCP Reservation function 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.



DHCP Reservation function takes effect only when **DHCP Server** is enabled.

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

Goal: 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 goal.

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 **Add** 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. (Optional) 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 rule is added successfully, it takes effect the next time the device connects to the router.

Add

Select Device: Manual

Device Name: FTP server



MAC Address: 6C:4B:90:3E:AD:AF

IP Address: 192.168.1.80

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.

Static IP Reservation List				Add
Device Name	IP Address	MAC Address	Operation	
FTP server	192.168.1.80	6c:4b:90:3e:ad:af		

11.8 Static routing

11.8.1 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 destination network, subnet mask, default gateway, and interface. The destination network and subnet mask are used to determine a destination 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
172.16.105.0	255.255.255.0	192.168.10.20	WAN1	 
0.0.0.0	0.0.0.0	172.16.200.1	WAN1	System
172.16.200.1	255.255.255.255	0.0.0.0	WAN1	System
192.168.0.0	255.255.255.0	0.0.0.0	br0	System
224.0.0.0	240.0.0.0	0.0.0.0	br0	System
239.0.0.0	255.0.0.0	0.0.0.0	br0	System

The following table describes the parameters displayed on this page.

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 no route of packets can be found under 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 router 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>

11.8.2 An example of adding a static routing 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.

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

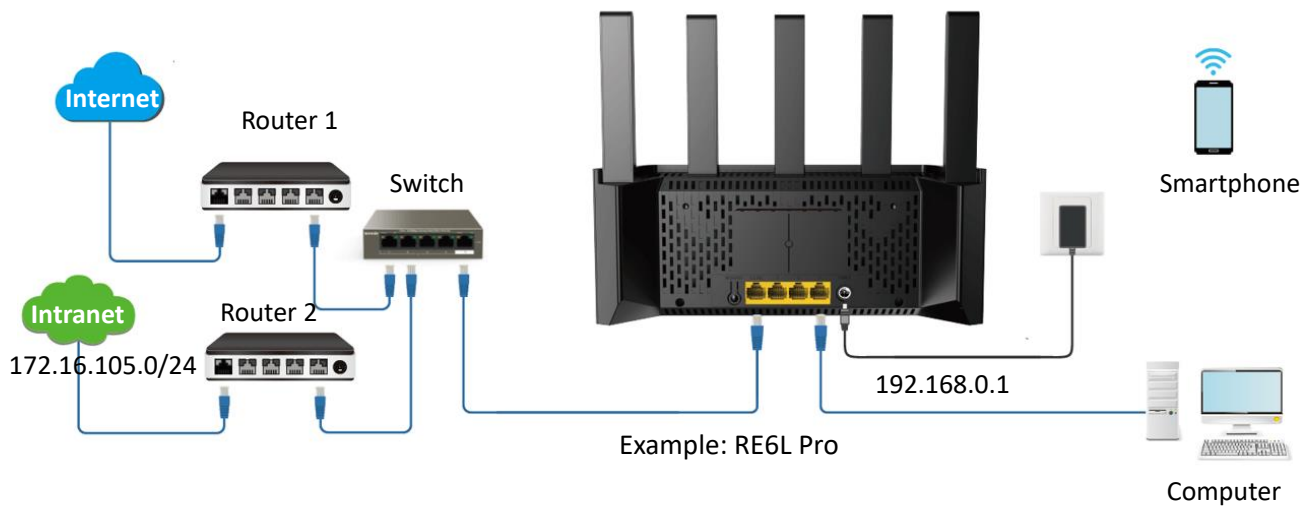
Solution: You can configure the static routing function to reach the goal.

Assume the LAN IP addresses of these devices are:

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

Information about the intranet:

- IP address: 172.16.105.0
- Subnet mask: 255.255.255.0



TIP

By default, the [WAN/LAN auto-negotiation](#) function of the router is enabled, and the Ethernet cable connected to the internet can be connected to any Ethernet port. If the WAN/LAN auto-negotiation function is disabled, connect the Ethernet cable connected to the internet to Ethernet port 1 (WAN port).

Log in to the web UI

Configure the internet access

Set the static routing rule

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.](#)

Internet Settings

Network Status Connected

Uptime 5hour(s) 7minute(s)

ISP Type

Internet Connection Type

Select this type if you can access the internet simply by plugging in an Ethernet cable for internet connection.

Advanced v

Connect

Step 3 Add a static routing rule.

1. Navigate to **More > Advanced > Static Routing**.

2. Click **Add**.

- Enter the IP address of the destination network, which is **172.16.105.0** in this example.
- Enter the subnet mask of the destination network, which is **255.255.255.0** in this example.
- Enter the ingress IP address of the next hop router, which is **192.168.10.20** in this example.

3. Click **OK**.

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

After the settings are completed, you can access both the internet and intranet through the router at the same time.

12

System maintenance

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

This chapter includes the following sections:

[Reboot device](#)

[Auto system maintenance](#)

[Firmware upgrade](#)

[Backup & restore](#)


[System time](#)

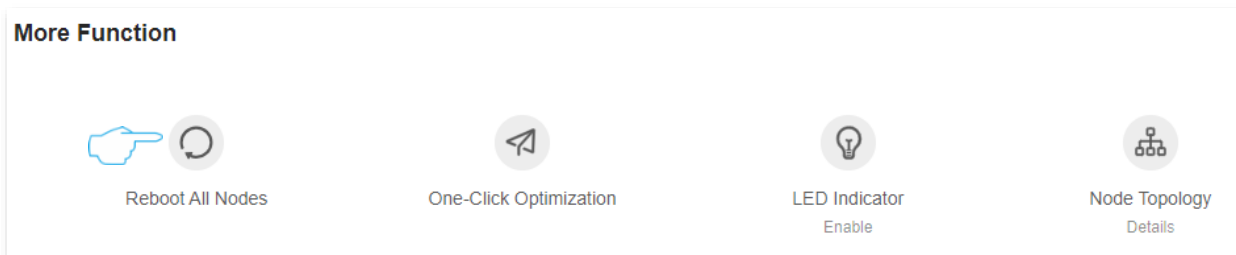
[View or export the system log](#)

12.1 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.

12.1.1 Reboot all nodes

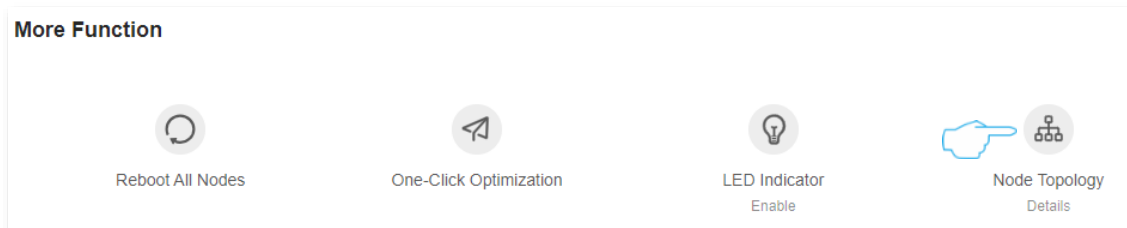
After [logging in to the web UI of the router](#), click  (**Reboot All Nodes**) in the **More Function** module of the **Network Status** page. Confirm the prompt message, and click **Reboot**. Wait until the ongoing process finishes.



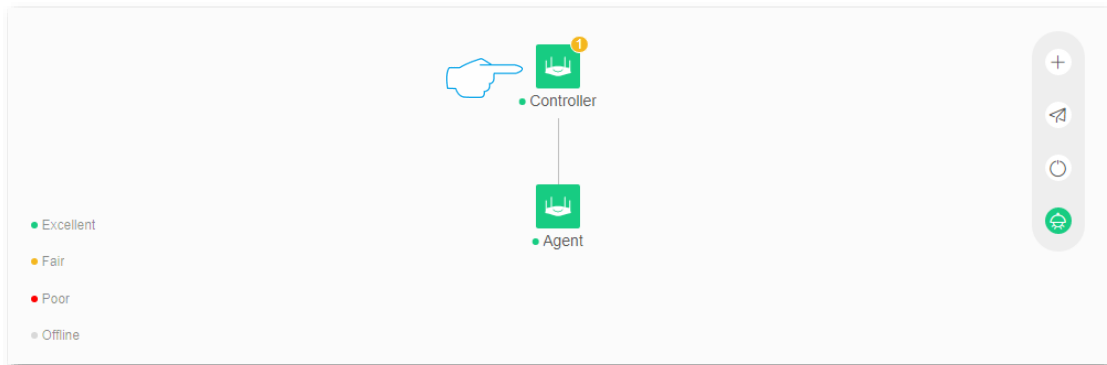
12.1.2 Reboot single node

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










Step 2 Click  (**Node Topology**) in the **More Function** module of the **Network Status** page.



Step 3 Click the node you want to reboot in **Network Status**. The following figure is for reference only.




Step 4 Click  in **Node Info**.

Node Name	Ethernet Port Status	LED On/Off	Operation
Controller Primary Node   IP Address: 192.168.1.1 MAC Address: <input type="text"/> Uptime: 3 hour(s) 6 minute(s)	2.5GE  WAN  LAN  1 2 3 4		  

Step 5 Confirm the prompt message, and click **Reboot**.

Reboot ✕

 **Do you want to reboot the device?**

-During the reboot, all connections are cut off.
 -The reboot takes about 90 seconds. Please reboot the device in relatively idle periods.

---End

Wait until the ongoing process finishes.

12.2 Auto system maintenance


Auto system maintenance enables you to restart the router 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**. This function is enabled by default.

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  ⓘ The auto system maintenance time takes effect based on the system time

Delay Reboot

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

The following table describes the parameters displayed on this page.

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>

12.3 Firmware upgrade

With this function, you can upgrade the firmware of the router to obtain the latest functions and more stable performance. The router supports online upgrade and local upgrade.

12.3.1 Online upgrade



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**.

---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**.

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, or perform other operations; otherwise, the upgrade may fail or the router may be damaged.

Device Name	Current Firmware Version	Operation
Controller Primary Node <small>New Version Available: V16.03.53.04(4086)_circle</small> Details <small>e</small>	V16.03.53.04_multi	<div style="display: flex; flex-direction: column; gap: 5px;"> <div style="border: 1px solid #ccc; padding: 2px 10px; display: inline-block;">Online Upgrade</div> <div style="border: 1px solid #ccc; padding: 2px 10px; display: inline-block;">Local Upgrade</div> </div>

---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**.

12.3.2 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 applicable firmware of the router to your local computer and unzip it.

Step 2 [Log in to the web UI of the router](#). Navigate to **More > System Settings > Firmware Upgrade**.

Step 3 Click **Local Upgrade** in the line of the node to be upgraded.

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, or perform other operations; otherwise, the upgrade may fail or the router may be damaged.

Device Name	Current Firmware Version	Operation
Controller Primary Node <small>New Version Available: V16.03.53.04(4086)_circl e</small> Details	V16.03.53.04_multi	<input type="button" value="Online Upgrade"/> <input type="button" value="Local Upgrade"/>

Step 4 Click **Select File**. Target 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

⬆️ Select File

No file chosen

Step 5 Click **Upgrade**.

---End

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

12.4 Backup & restore

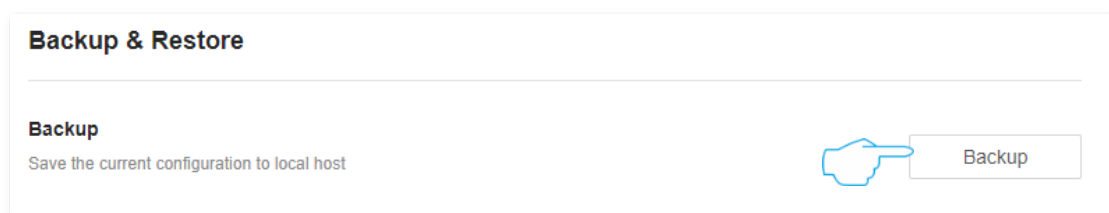
- In this module, you can back up the current configuration of the router to your computer. You are recommended to back up the configuration after the settings of the router are significantly changed, or the router works in a good condition.
- If you forget your Wi-Fi password or fail to fix network connection problems with other solutions, you can reset the router to factory settings on this page.
- After you restored the router to factory settings or upgraded it, you can use this function to restore the configuration that has been backed up.

12.4.1 Back up the configuration 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

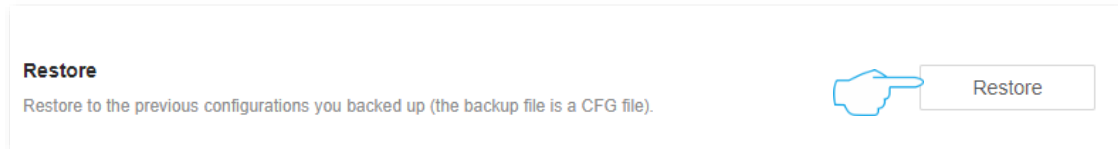
A file named **RouterCfm.cfg** will be downloaded to your local host.

12.4.2 Restore the previous configuration of the router

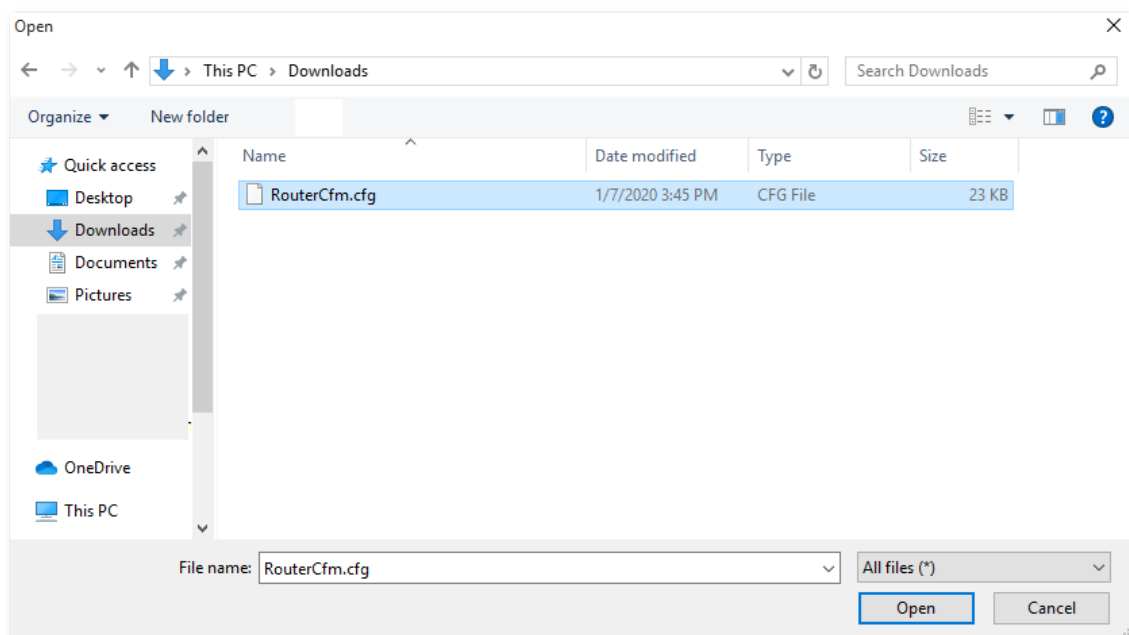
Step 1 [Log in to the web UI of the router.](#)

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.**



Step 5 Click **Restore.**

---End

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

12.4.3 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.

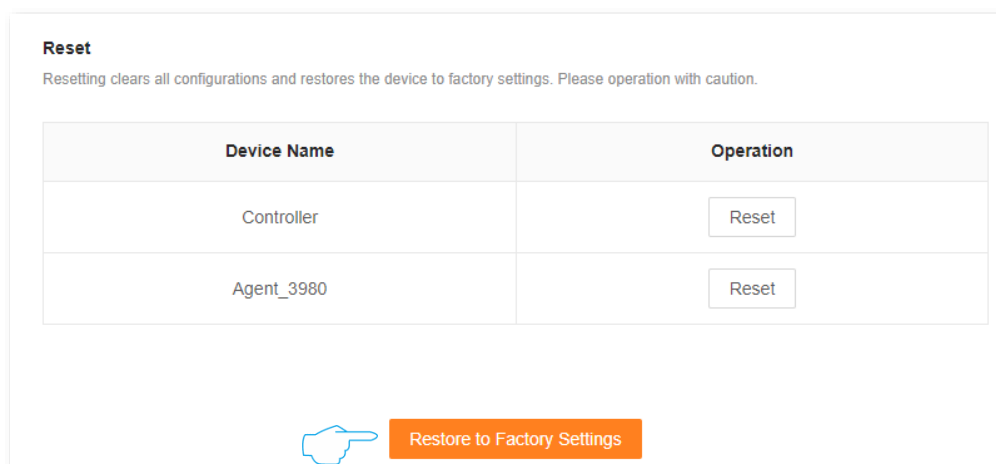
Reset all modes

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

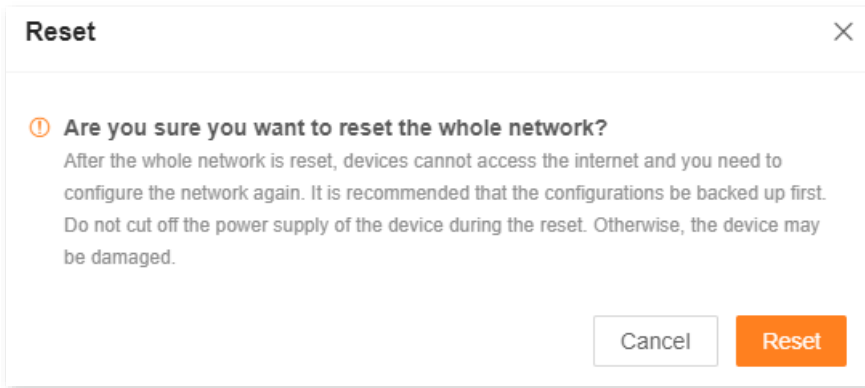
Step 1 [Log in to the web UI of the router.](#)

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

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



Step 4 Click **Reset**. Wait for the router to automatically restore factory settings.



---End

Reset a node

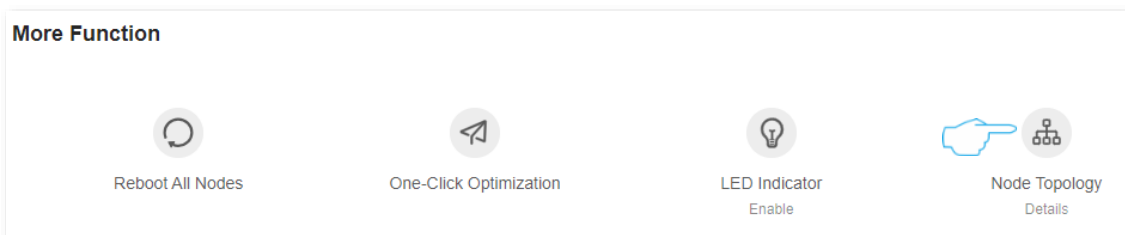


Resetting clears all configurations and restores the router to factory settings. Please operate with caution. You are recommended to [back up the configurations](#) first.

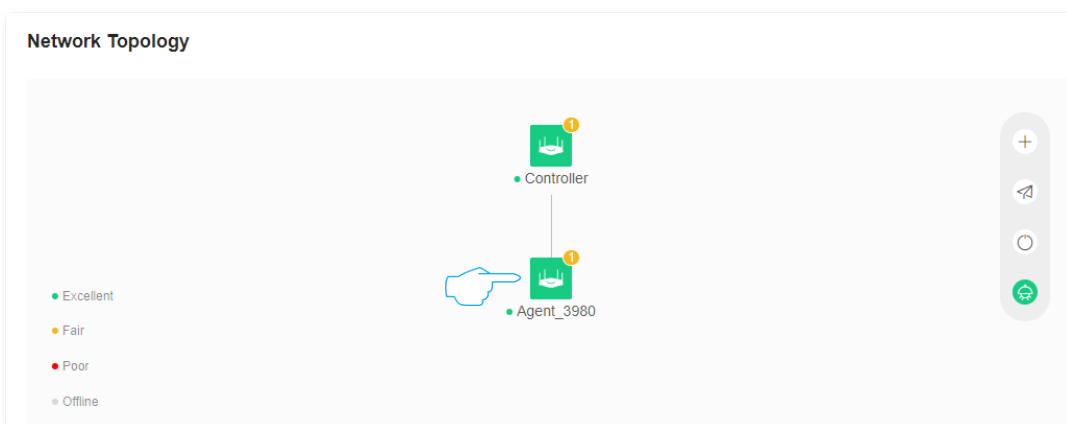
Method 1



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

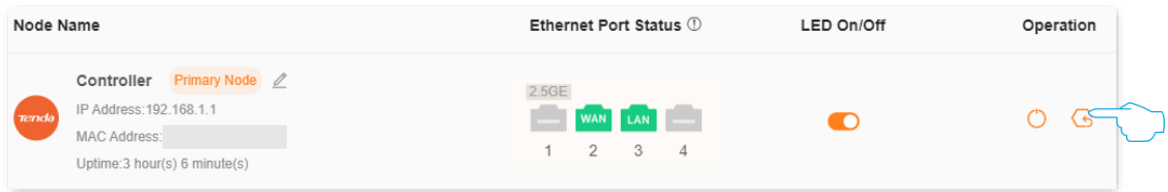
Step 2 Click  (**Node Topology**) in the **More Function** module of the **Network Status** page.



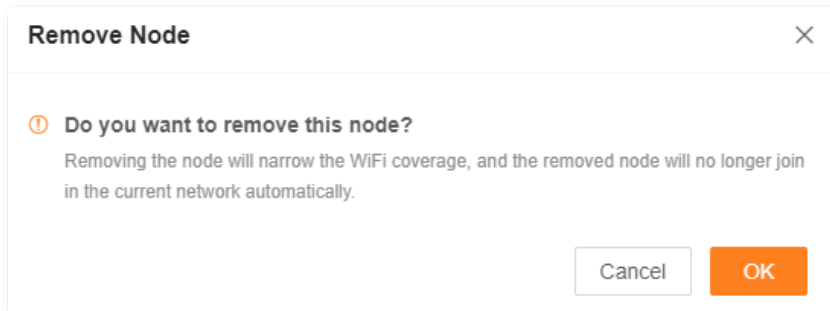
Step 3 Locate and click the icon of the node you want to restore to factory settings. The following figure is for reference only.



Step 4 Click  or  in **Node Info**. The following figure is for reference only.



Step 5 Click **OK**. Wait until the reset completes. The following figure is for reference only.



---End

Method 2

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

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

Step 3 Click **Reset** in the line of the node to be reset.

Reset	
Resetting clears all configurations and restores the device to factory settings. Please operation with caution.	
Device Name	Operation
Controller	<input type="button" value="Reset"/>
Agent	 <input type="button" value="Reset"/>

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

Reset ×

ⓘ Do you want to reset the secondary node?

After the secondary node is reset, if it is a secondary node in a package, it can automatically join in the network. Otherwise, you need to manually add it to the network. Do not cut off the power supply of the device during the reset. Otherwise, the device may be damaged.

---End

Method 3

Use the reset button (such as RESET, RST) on the device body to restore the router to factory settings.

Method: Hold the button down with a needle-like object for about 8 seconds, and then release it when the indicator blinks red fast. The device is reset.



12.5 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 system time 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 local time. By default, it is synchronized with the internet.

Synchronize with the internet

In this mode, the system time automatically synchronizes with the internet time. Once the router is successfully connected to the internet, it automatically synchronizes its system time without configuring.

After the settings are 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 2024-09-13 14:55:57

Sync Status Synced

Sync Mode

Time Zone

DST

Start 2024

End 2024

Status DST not use

The following table describes the parameters displayed on this page.

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>Required when Sync with internet time is selected for Sync Mode.</p> <p>It specifies the time zone used for the system time. Select one option as required.</p>
Local Time	<p>Displayed when Sync with Local Time is selected for Sync Mode.</p> <p>It specifies the local time set on your host.</p>
DST	Used to enable or disable the Daylight Saving Time (DST) function. It is disabled by default.
Start 2024	<p>Required when DST is enabled.</p> <p>It specifies the start time of DST.</p>
End 2024	<p>Required when DST is enabled.</p> <p>It specifies the end time of DST.</p>
Status	<p>Displayed when DST is enabled.</p> <p>It specifies whether the DST is used.</p>

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 settings are 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 2024-09-13 14:56:57

Sync Status Synced

Sync Mode

Local Time 2024-9-13 14:56:57

DST

Start 2024

End 2024

Status DST not use

12.6 View or export the 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.



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.

You can view and export the router's log as required.

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	2024-09-13 14:33:39	wan	Sending DHCP_REQUEST for 192.168.0.153 to 1
2	2024-09-13 14:19:32	system	Sync time success!
3	2024-09-13 14:18:40	wan	Get Client IP Address (192.168.0.153)
4	2024-09-13 14:18:40	wan	DHCP_ACK received from (192.168.0.252)
5	2024-09-13 14:18:40	wan	Broadcasting DHCP_REQUEST for (192.168.0.15
6	2024-09-13 14:18:40	wan	DHCP_OFFER received from (192.168.0.252)
7	2024-09-13 14:18:40	wan	Broadcasting DHCP_DISCOVER
8	2024-09-13 14:18:39	system	Port 2 is WAN
9	2024-09-13 14:18:33	system	Port 2; LAN up
10	2024-09-13 14:18:26	system	Port 2; WAN down

99 items in total

<
1
2
3
4
5
6
7
...
10
>

Appendixes

A.1 FAQ

Q1: I cannot log in to the web UI by visiting tendawifi.com. What should I do?

A1: First, try to visit <http://tendawifi.com> or <http://192.168.0.1> in the address bar (not the search bar).

If you are using a Wi-Fi-enabled device, such as a smartphone:

- Ensure that your smartphone is connected to the Wi-Fi network of the router.
 - For the first login, connect the Wi-Fi name (**@Tenda_XXXXXX**) on the label of the device's body. XXXXXX is the last six digits of the MAC address on the label.
 - When logging in again after settings, use the changed Wi-Fi name and password to connect to the Wi-Fi network.
- Ensure that the cellular network (mobile data) of the smartphone is disabled.

If you are using a wired device, such as a computer:

- Ensure that the computer is connected to an Ethernet port (If the [WAN/LAN auto-negotiation function](#) is disabled, connect the computer to any Ethernet port 2/3/4 of the router.) properly.
- Ensure that the computer is set to **Obtain an IP address automatically** and **Obtain DNS server address automatically**.

If the problem persists, reset the router by referring to [Q4](#) and try again.

Q2: I cannot access the internet after the configuration. What should I do?

A2: Try the following solutions:

- Ensure that the Ethernet port of the router is connected to a modem or Ethernet jack properly. If the [WAN/LAN auto-negotiation function](#) is disabled, connect the modem or Ethernet jack to the Ethernet port 1 (WAN port).
- Log in to the web UI of the router and navigate to the [Internet settings](#) page. Follow the instructions on the page to solve the problem.
- If the problem persists, contact your ISP.

- For Wi-Fi-enabled devices:
 - Ensure that your devices are connected to the Wi-Fi network of the router.
 - Visit **tendawifi.com** to log in to the web UI and change your Wi-Fi name and Wi-Fi password on the **WiFi Settings** page. Then try again.
- For wired devices:
 - Ensure that your wired devices are connected to an Ethernet port (If the [WAN/LAN auto-negotiation function](#) is disabled, connect the computer to any Ethernet port 2/3/4 of the router.) properly.
 - Ensure that your wired devices are set to **Obtain an IP address automatically** and **Obtain DNS server address automatically**.

Q3: The device failed to be detected by the Tenda WiFi App upon my first time using the device. What should I do?

A3: Try the following solutions:

Scenario 1: The Tenda WiFi App has never managed the router

- Ensure that your smartphone is connected to the Wi-Fi network of the device.
- Ensure that the network permission of the **Tenda WiFi** App is enabled:
 - For iOS: Search for **Tenda WiFi** in the **Settings** page of the phone, and ensure that the App has the permission to find and connect to devices on the local network.
 - For Android: Search **Location Services** in the **Settings** page of the phone, enable location services, and allow the **Tenda WiFi** App to obtain location information permissions.

Scenario 2: Tenda WiFi App has managed the router

- Ensure that the cellular network (mobile data) of the client is enabled and has logged in to the **Tenda WiFi** App account.
- If the problem persists, there may be no login account for binding in the previous management, connect to the router's Wi-Fi again for binding.

Q4: How to restore my device to factory settings?

A4: Hold down the reset button (Marked as RST, RESET) of your device for about 8 seconds, and the router is reset successfully. For more details, see [Reset](#).

Q5: Why cannot I find the Wi-Fi signal of the router?

A5: Connect your computer to Ethernet port(If the [WAN/LAN auto-negotiation function](#) is disabled, connect the computer to any Ethernet port 2/3/4 of the router.) of the router, and log in to the web UI. Navigate to **WiFi Settings** and ensure that:

- The wireless function is enabled.
- The Hide function is not ticked.
- Your Wi-Fi name does not contain any Chinese characters.

Q6: I cannot find the 5 GHz Wi-Fi network of the router on my Wi-Fi-enabled device. What should I do?

A6: Try the following solutions:

- Only devices supporting 5 GHz network can find and connect to the 5 GHz Wi-Fi network.
- Check whether you have enabled **Unify 2.4 GHz & 5 GHz** on the **WiFi Settings** page. If it is enabled, disable it and try again. After it is enabled, the 5 GHz Wi-Fi name is the same as the 2.4 GHz Wi-Fi name.
- If the Unify 2.4 GHz & 5 GHz function is disabled on the router but the smartphone can search for another 5 GHz Wi-Fi network, reset the router by referring to [Q4](#) and try again.

Q7: The router's Wi-Fi signal is poor. What should I do?

A7: Try the following solutions:

- Place the router in a high position with few obstacles.
- Keep your router away from electronics with strong interference, such as microwave ovens, induction cookers, and refrigerators.
- Keep your router away from metal barriers, such as weak current boxes, and metal frames.

Q8: If the network speed is slow after I connect my device to the router. What should I do?

A8: Try the following solutions:

- For Wi-Fi-enabled devices, such as a smartphone:
 - Use the Wi-Fi analyzer to scan the surrounding wireless signal information, set the router's channel to the less occupy channel, and then reduce the bandwidth, refer to [Change channel and bandwidth](#).
 - Try to get close to your router to test the network speed when the wireless signal strength is full. If the network speed is fast when the signal is strong, it indicates that the signal coverage is weak, resulting in a slow network speed, and the wireless network can be extended by adding new secondary nodes or wireless adapters.
- For wired device, such as a computer:
 - Ensure that the Ethernet cable is connected properly.
 - Ensure that the [Bandwidth control](#) are not configured on the router. If yes, delete

related configurations and check whether the network speed is restored.

- Loading too many applications in the background will lead to insufficient computer system resources. Please load software properly or delete unnecessary programs and files to free up resources to improve network speed.

Q9: If the device is disconnected from the router. What should I do?

A9: Try the following solutions:

- If the Wi-Fi-enabled device goes offline, the wired device can access the internet normally:
 - Refer to [Q7](#) to place the router in an appropriate position.
 - Check whether the wireless adapter driver of the Wi-Fi-enabled device is faulty. Replace the wireless adapter driver with another device or update the wireless adapter driver.
 - If the problem persists, reset the router by referring to [Q4](#) and try again.
- If the wired device goes offline, the Wi-Fi-enabled device can access the internet normally:
 - If the Ethernet cable between the computer and the router is too long or poor quality, it will cause the cable drop. Please replace the short Ethernet cable.
 - Try to replace the Ethernet port (If the [WAN/LAN auto-negotiation function](#) is disabled, connect the computer to any Ethernet port 2/3/4 of the router.) connection or use another computer connection.
- If both wired and Wi-Fi-enabled devices go offline:
 - Log in to the web UI of the router and ensure that the router is properly connected to the internet. If not, refer to [Router disconnected from the internet](#) to solve.
 - Refer to [Q7](#) to place the router in an appropriate position.
 - Ensure that the Ethernet port is connected properly, and replace a short Ethernet cable to connect to the Ethernet port. If the [WAN/LAN auto-negotiation function](#) is disabled, connect the modem or Ethernet jack to the Ethernet port 1 (WAN port)
 - When not connected to the router, directly connect the Ethernet cable to the computer to check whether the internet is disconnected. If the internet is disconnected from the internet, contact your ISP for help.
 - If the problem persists, reset the router by referring to [Q4](#) and try again.

Q10: The networking fails. What should I do?**A10:** Try the following solutions:

- Ensure that the new router is reset. If not, restore the router to factory settings first.
- Ensure that the existing router (primary node) is connected to the internet, and then refer to MESH networking and try again.

Q11: Some computers cannot search router's Wi-Fi. What should I do?**A11:** Try the following solutions:

- Change the network mode of the router's 2.4G Wi-Fi and 5G Wi-Fi to not include 802.11ax and 802.11be, and search again.
- If the router's Wi-Fi can be searched after changing the network mode, the wireless network adapter version is older and needs to be updated. You can go to the corresponding official website of the wireless network adapter to download and install, or you can use software such as driver wizard to detect and update online.
- If only 2.4G Wi-Fi is searched, first check whether the computer supports 5G band. If other 5G Wi-Fi can be searched, change the 5G Wi-Fi channel of the router to channel 36 or channel 149 in turn, and then search. If it can be searched after changing the channel, it means that the 5G wireless network adapter only supports high-channel or low-channel Wi-Fi.

A.2 Connect to a hidden Wi-Fi network

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

Assume that the **Unify 2.4 GHz & 5 GHz** function is enabled and the Wi-Fi parameters are:

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



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

Connect to the Wi-Fi network on your Wi-Fi-enabled device (Example: iPhone):

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

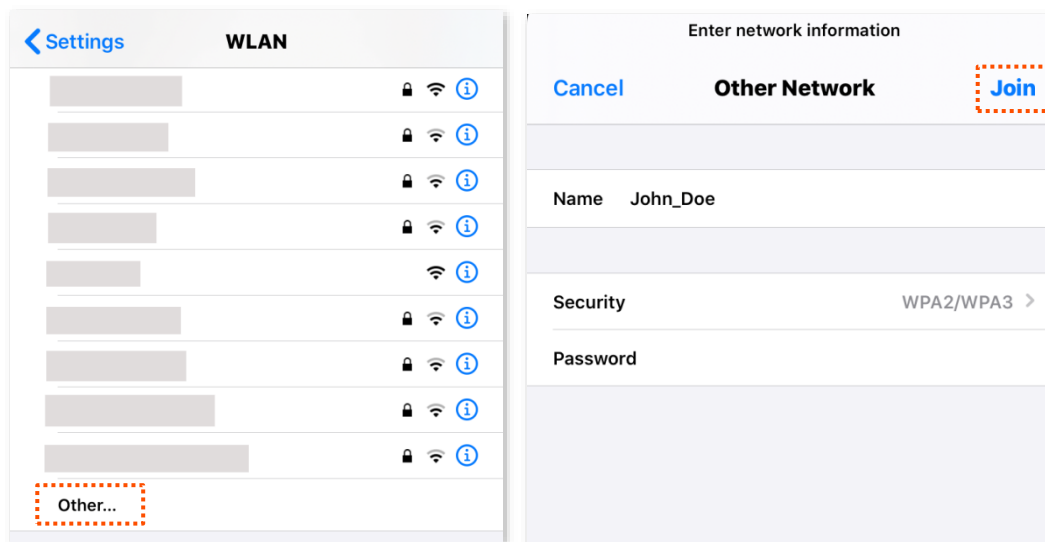
Step 2 Enable **WLAN**.

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

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

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

Step 6 Tap **Join**.



---End

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

A.3 Acronyms and Abbreviations

Acronym or Abbreviation	Full Spelling
AES	Advanced Encryption Standard
AP	Access point
DDNS	Dynamic Domain Name System
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DMZ	Demilitarized zone
DNS	Domain Name System
DSL	Digital subscriber line
DST	Daylight Saving Time
FTP	File Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPTV	Internet Protocol television
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet service provider
L2TP	Layer 2 Tunneling Protocol
LAN	Local area network
LED	Light-emitting diode
MAC	Medium access control
MLO	Multi-Link Operation
MPPE	Microsoft Point-to-Point Encryption
MTU	Maximum Transmission Unit
OFDM	Orthogonal Frequency Division Multiplexing

Acronym or Abbreviation	Full Spelling
OFDMA	Orthogonal Frequency Division Multiple Access
POP	Point of Presence
PPP	Point to Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point to Point Tunneling Protocol
RA	Router Advertisement
RUs	Resource Units
SLAAC	Stateless Address Autoconfiguration
SN	Serial Number
SSID	Service Set Identifier
STB	Set-top box
TCP	Transmission Control Protocol
TWT	Target Wakeup Time
UDP	User Datagram Protocol
UI	User interface
UPnP	Universal Plug and Play
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual local area network
VPN	Virtual private network
WAN	Wide area network
WISP	Wireless Internet Service Provider
WLAN	Wireless local area network
WPA	Wi-Fi Protected Access

Acronym or Abbreviation	Full Spelling
WPA-PSK	WPA Pre-shared Key
WPA3-SAE	WPA3-Simultaneous Authentication of Equals
WPS	Wi-Fi Protected Setup