AX5700 Tri-Band Gigabit Wi-Fi 6E Router

User Guide

V1.0

Copyright Statement

© 2022 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 user guide walks you through all functions on the AX5700 Tri-Band Gigabit Wi-Fi 6E Router. All the screenshots and product figures herein, unless otherwise specified, are taken from RX27 Pro.

TIP

The web UI of different models may differ. The web UI actually displayed shall prevail.

Conventions

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

Item	Presentation	Example
Cascading menus	>	**System** > **Live Users**
Parameter and value	Bold	Set **User Name** to **Tom**.
Variable	Italic	Format: *XX*:*XX*:*XX*:*XX*:*XX*:*XX*
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
NOTE	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.
TIP	This format is used to highlight a procedure that will save time or resources.

For more documents

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

The related documents are listed as below.

Document	Description
Data Sheet	It introduces the basic information of the device, including product overview, selling points, and specifications.
Quick Installation Guide	It introduces how to set up the device quickly for internet access, the descriptions of LED indicators, ports, and buttons, FAQ, statement information, and so on.

Technical Support

If you need more help, contact us by any of the following means. We will be glad to assist you as soon as possible.

 Hotline	Global: (86) 755-27657180 (China Time Zone) United States: 1-800-570-5892 (Toll Free: 7 x 24 hours) Canada: 1-888-998-8966 (Toll Free: Mon - Fri 9 am - 6 pm PST) Hong Kong: 00852-81931998	 Email	support@tenda.com.cn
 Website	https://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 RX27 Pro/TX27 Pro was introduced.

Version	Date	Description
V1.0	2022-06-10	Original publication.

Contents

1 Get to know your device

This chapter introduces the product in the following sections:

1.1 Product overview

The tri-band gigabit Wi-Fi 6E router adopts the next generation Wi-Fi 6E standard, reaching a tri-concurrent rate of up to 5665 Mbps (2.4 GHz: 861 Mbps, 5 GHz: 2402 Mbps, 6 GHz: 2402 Mbps). It is equipped with 7 high-power FEMs and Broadcom 1.7 GHz quad-core CPU, improving network performance and capacity. The WPA3 security protocol, guest network and parental control function ensure the safety and stability of your Wi-Fi networks.

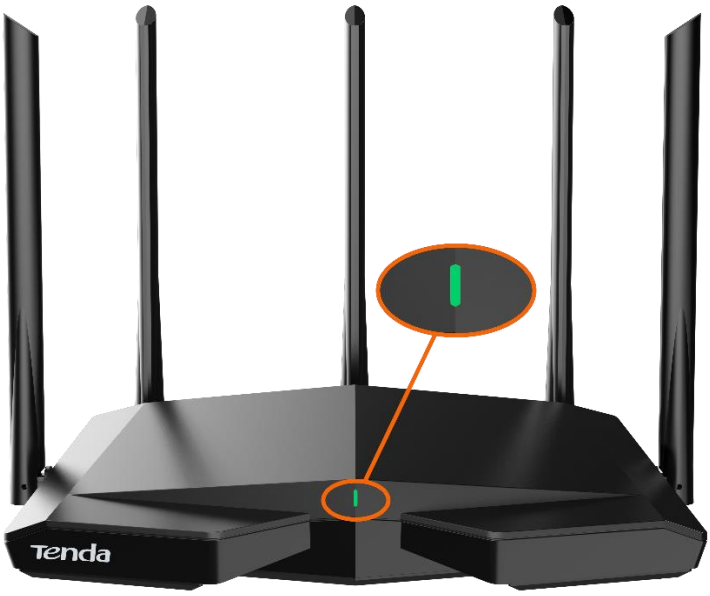
With the Mesh function, this router can also network with other devices that have the Mesh function to extend the Wi-Fi network in your house.

TIP

Currently, RX27 Pro/TX27 Pro can be networked with the same model, Mesh6X, Mesh12X, RX12 Pro, or TX12 Pro.

1.2 Appearance

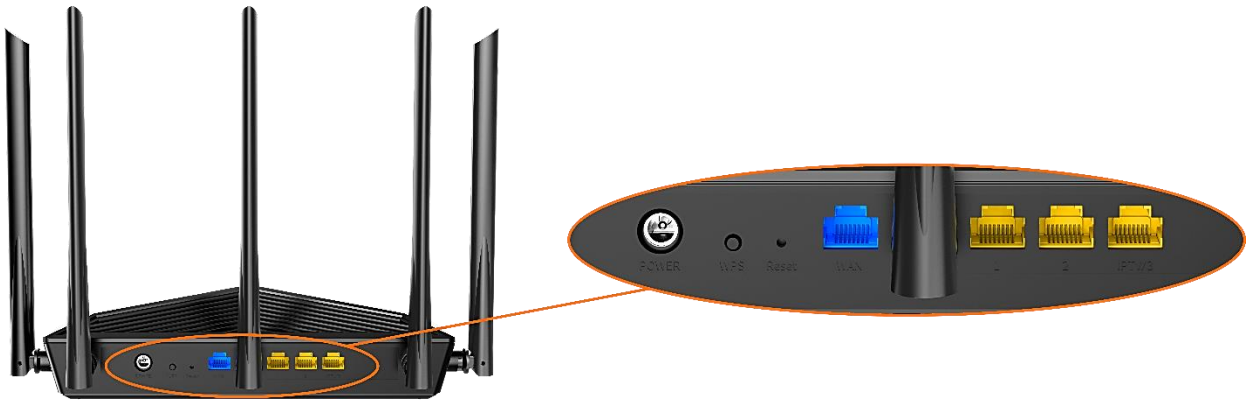
1.2.1 LED indicator



This product has only one indicator. Its behavior varies in different stages, as described in the following table.

LED indicator	Stage	Status	Description
LED indicator	Before networking	Solid green	System starting
		Blinking green slowly	Waiting for configuration or networking
	During networking	Blinking green slowly	Waiting to connect to other nodes
		Blinking green quickly	Networking by the **WPS** button or performing WPS negotiation
		Solid on	Networking completed and internet connection succeeded • Solid green: The signal is good. • Solid orange: The signal is fair.
		Blinking red slowly	Networking succeeded while internet connection failed
	Internet connection (primary node)	Solid green	Internet connection succeeded
		Blinking red slowly	Internet connection failed
	WPS	Blinking green quickly	WPS started Device connecting…
		Recovered to the original light state	Device connected
		Blinking green quickly for 2 minutes	WPS connection failed
	Reset	Blinking red quickly	Resetting
	Batch upgrade	Blinking orange quickly	Batch upgrade succeeded
		Solid orange	Batch upgrade failed

1.2.2 Buttons and Ports



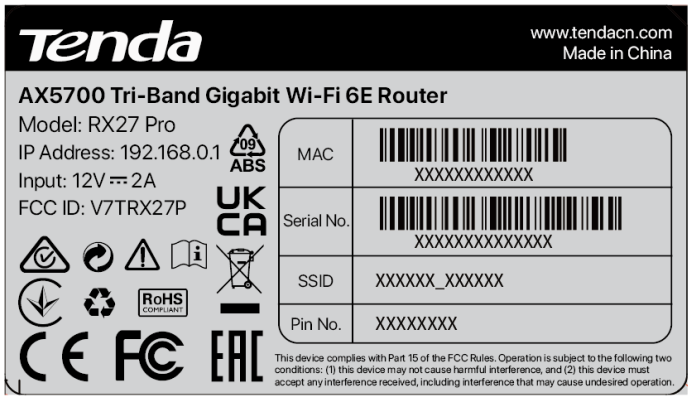
The following table describes the functions of the buttons and ports on the back of product.

Jack/Port/Button	Description
POWER	Power jack. Please use the included power adapter to connect this jack to a power source for power supply.
WPS	WPS/Mesh button. • WPS: When it is used as a WPS negotiation button, you can connect to the Wi-Fi network of the router without entering the Wi-Fi password. **Method**: Short press the button (for about 1 second), and the LED indicator blinks fast. Within 2 minutes, enable the WPS function of the other WPS-supported device to establish a WPS connection. • Mesh: When it is used as a Mesh networking button, you can extend your network with another device that supports the Mesh function. **Method:** Press this button for about 3 seconds. The LED indicator blinks green fast, which indicates the device is searching for another device to form a network. Within 2 minutes, press the **MESH/WPS** button of another device for 1 to 3 seconds to negotiate with this device.
Reset	Reset button. When the router is working normally, hold the button down using a needle-like item (such as a pin) for about 8 seconds, and then release it when the LED indicator blinks orange fast. The router is reset.

Jack/Port/Button	Description
WAN	10/100/1000 Mbps auto-negotiation WAN port. Used to connect to a modem or the Ethernet jack using an Ethernet cable for internet access. TIP After the router is connected to an existing network as a secondary node, this **WAN** port is used as a LAN port.
1, 2	10/100/1000 Mbps auto-negotiation LAN port. Used to connect to such devices as computers, switches or game machines.
IPTV/3	10/100/1000 Mbps auto-negotiation LAN/IPTV port. It is a LAN port by default. When the IPTV function is enabled, it can only serve as an IPTV port to connect to a set-top box.

1.2.3 Label

The bottom label shows the login IP address, MAC address, serial number, SSID, and password of the device. The following is an example of what the label might look like:



Model: Specifies the device model.

IP Address: Specifies the default address used to log in to the web UI of the device.

Input: Specifies the power of the device.

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

MAC: Specifies the MAC address of the LAN port of the device.

Serial No.: Specifies the serial number required if you need technical assistance to repair your device.

SSID: Specifies the default Wi-Fi name of the device.

Pin No.: Specifies the PIN code of the device.

2 Quick setup

With the Mesh function, the router can function as a single router or a Mesh device. You can configure it as a single router or an add-on node. This chapter describes how to connect the devices and enable internet access through the quick setup wizard. It contains the following sections:

2.1 Set up as a router

2.1.1 Connect the router

The "new router" and "router" in this guide refer to the router in the package.

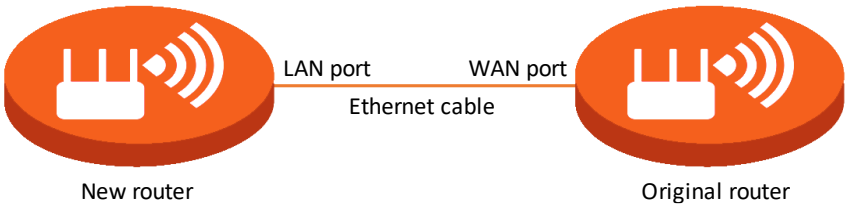
Step 1 (Optional) Import your PPPoE user name and password into the new router.

TIP

This function is only applicable when the connection type of the original router is PPPoE, except for PPPoE of some special ISPs or PPPoE connection set up manually with VLAN information.

1. Power on your original and new routers.
2. Connect the WAN port of the original router to a LAN port (1, 2 or IPTV/3) of the new router using an Ethernet cable.

   After the LED indicator of the new router blinks fast for 8 seconds, the PPPoE user name and password are imported to your new router.
3. Remove the original router.

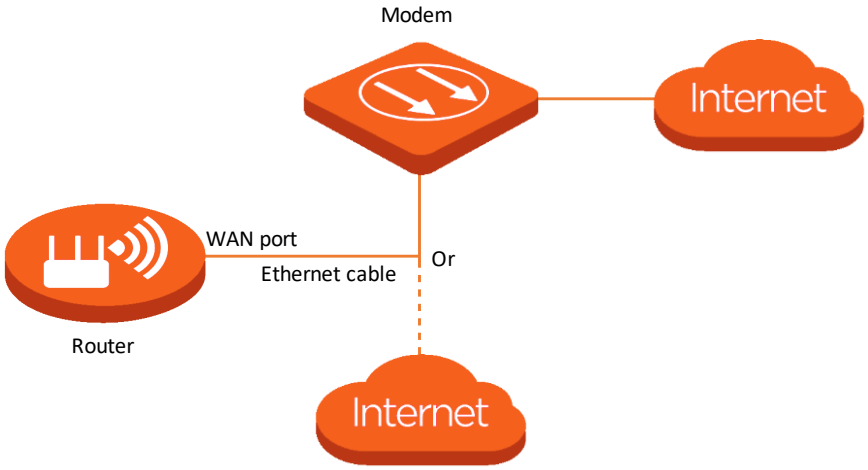


Step 2 Connect the WAN port of the router.

NOTE

If you use the modem for internet access, please power off the modem first before connecting the WAN port of the router to the LAN port of your modem.

- Ensure that the router is powered on.
- Connect the WAN port of the router to the LAN port of your modem or the Ethernet jack using an Ethernet cable.



---End

2.1.2 Connect the router to the internet

After connecting your router, you can complete quick setup for internet access by following the instructions on the web UI wizard. This wizard only occurs upon your first setup.

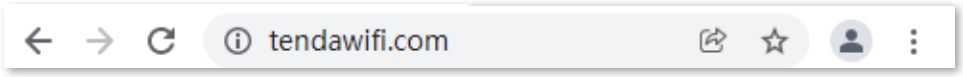
To connect your router to the internet through the quick setup wizard:

Step 1 Use an Ethernet cable to connect your computer to the **1**, **2** or **IPTV/3** port of the router.

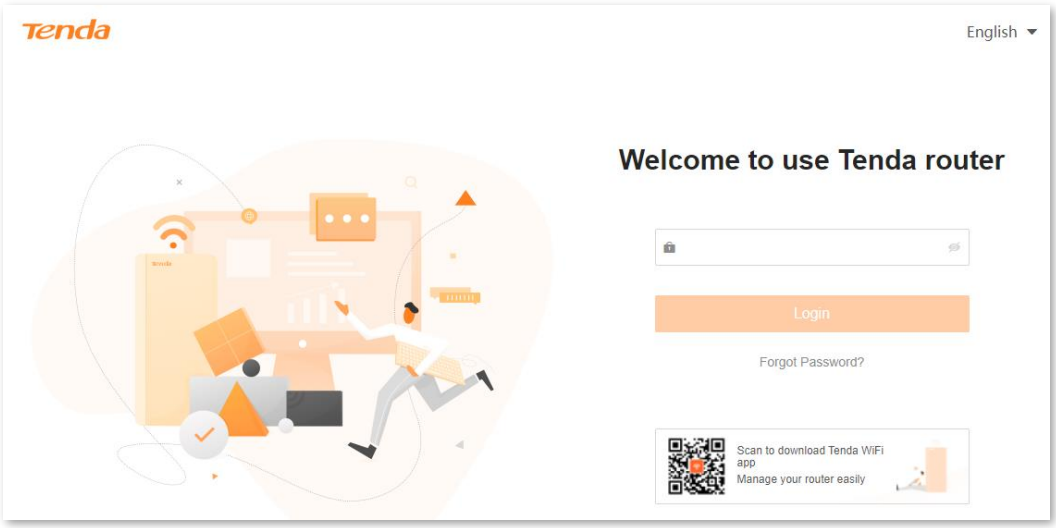
TIP

The default Wi-Fi name can be found on the bottom label of the device.

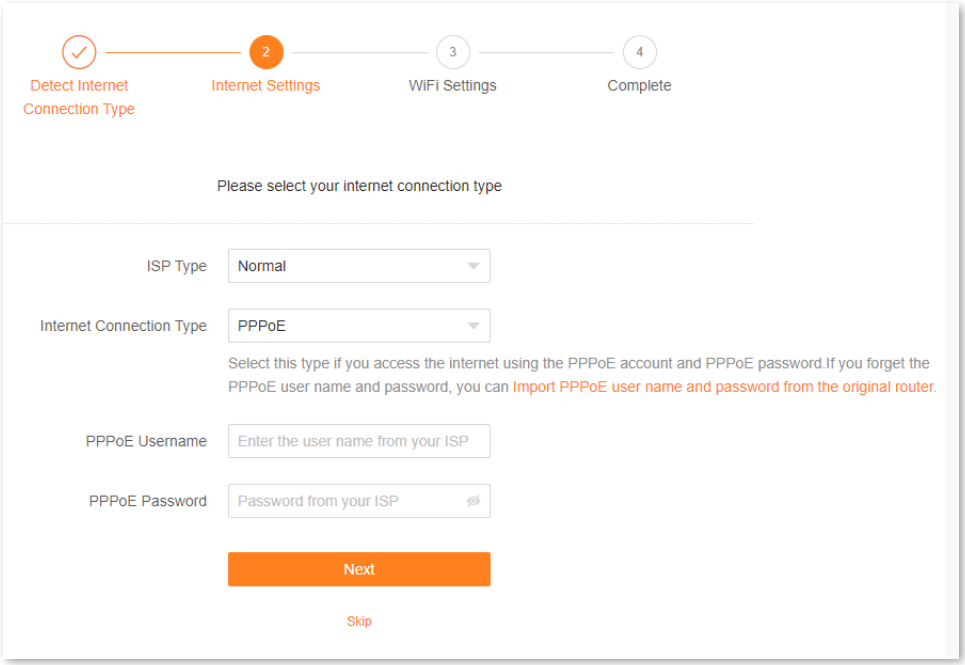
Step 2 Start a browser on the computer and enter **tendawifi.com** in the address bar to access the web UI.



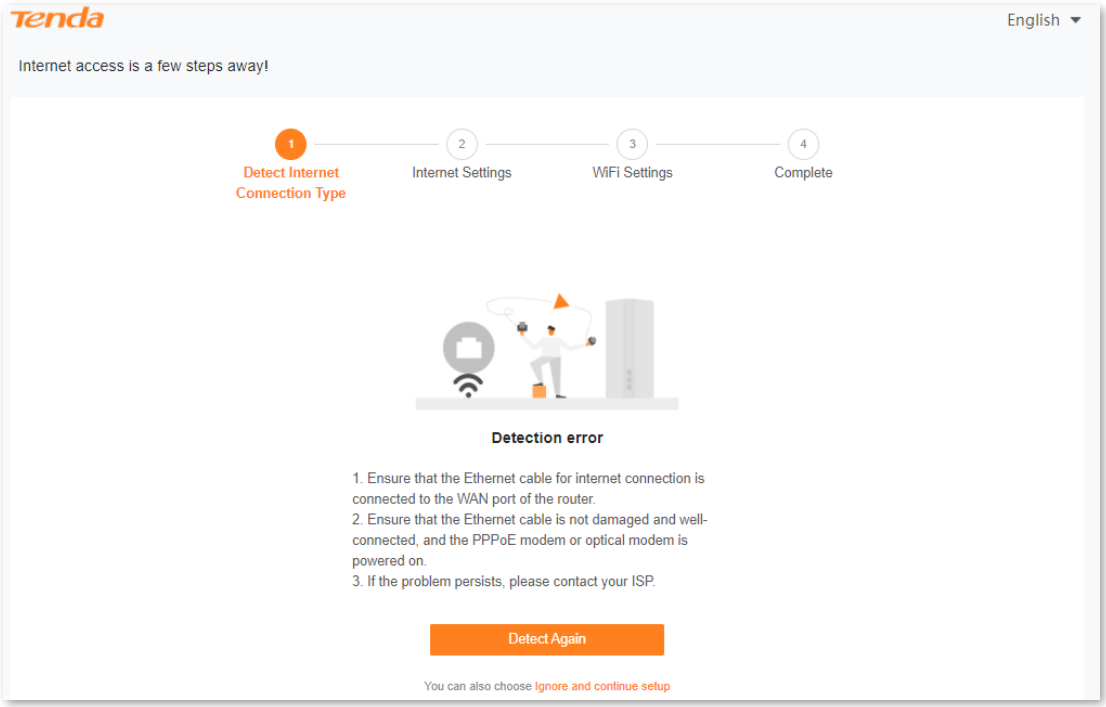
Step 3 Click **Start Now**.



- If your internet connection is normal, the following page is displayed and you can continue the setup in **Step 4**.



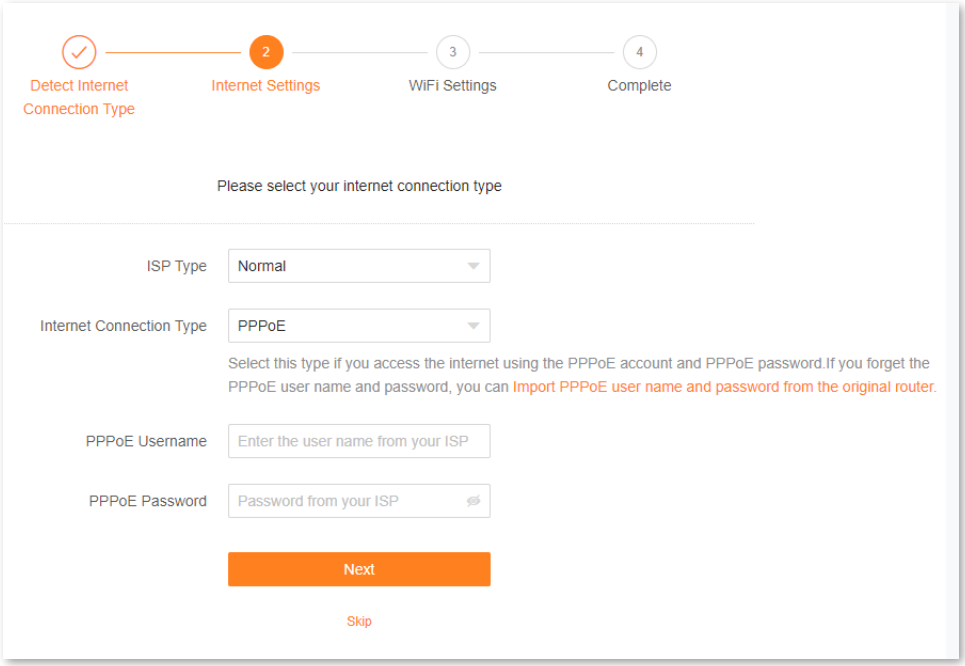
- If your internet connection is abnormal, the following page is displayed. Rectify the fault as instructed on the page, and click **Detect Again**.



Step 4 Set **ISP Type**, **Internet Connection Type** and other parameters as required. Then, click **Next**.

TIP

You can click **Import PPPoE user name and password from your original router** to see how to import PPPoE user name and password. If you have imported your PPPoE user name and password into the router, **ISP Type**, **Internet Connection Type**, **PPPoE Username** and **PPPoE Password** will be set automatically.



The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
ISP Type	Specifies the type of your ISP, such as **Normal**, **Russia**, **Unifi**, **Maxis**, **Celcom**, **Digi** and **Manual**. Parameters required for each option may differ. Refer to the following to choose your connection type: • **Normal**, **Unifi**, **Maxis**, **Celcom** and **Digi**: Select these options when your ISP provides no setup information, except for the PPPoE user name and password, or static IP address information. • **Russia:** Select this option when your ISP provides dual access information, such as PPTP, L2TP connection information. • **Manual**: Select this option when your ISP provides VLAN ID information, besides the PPPoE user name and account, or static IP address. If you are still not sure, contact your ISP for reference.

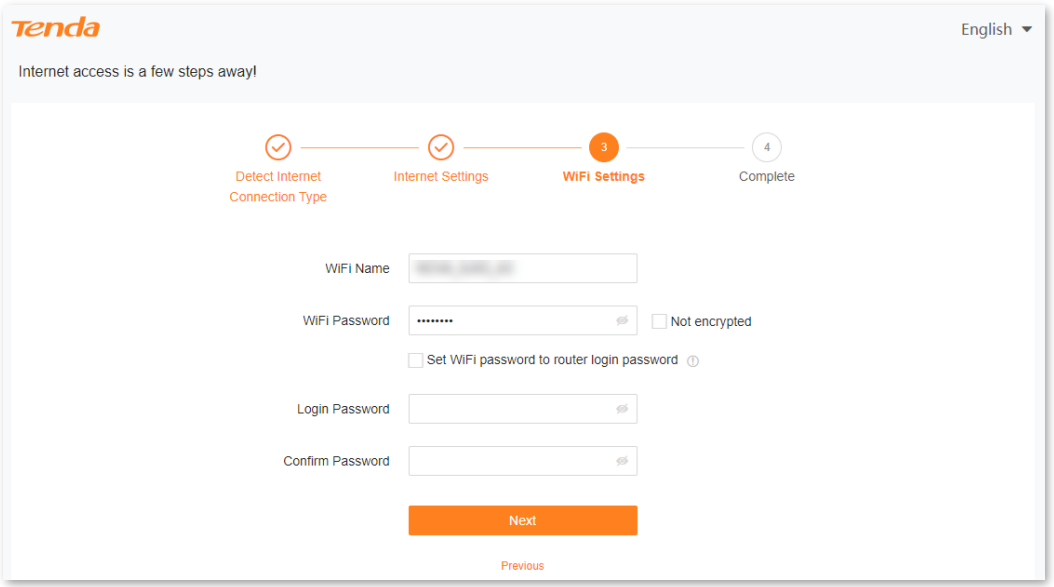
Parameter	Description
Internet Connection Type	Specifies how your router connects to the internet, including: • **PPPoE**, **Russia PPPoE**: Select this type if you access the internet using the PPPoE account and PPPoE password. **Russia PPPoE** is available only when you set **ISP Type** to **Russia**. • **Dynamic IP**: Select this type if you can access the internet by simply plugging in an Ethernet cable. • **Static IP**: Select this type if you want to access the internet using fixed IP information. • **Russia PPTP**, **Russia L2TP**, **Russia PPPoE**: These types are available when **ISP Type** is set to **Russia**. If you select **Russia PPTP** or **Russia L2TP**, the VPN function will be disabled.
PPPoE Username PPPoE Password	When the internet connection type is PPPoE, you need to enter the user name and password provided by your ISP to access the internet.
IP Address Subnet Mask Default gateway Primary DNS Secondary DNS	When the internet connection type is static IP, you need to enter the fixed IP address information provided by your ISP. TIP If your ISP provides only one DNS server, you can leave **Secondary DNS** blank.
Address Type	When you set **ISP Type** to **Russia**, this parameter is required. It specifies the method for obtaining IP address information to access the “local” network, where the internal resources of the ISP are located.
DNS Settings	This parameter is required only when **ISP Type** is set to **Russia**. It specifies how the WAN port DNS address is obtained, which is **Auto** by default. • **Auto**: The router obtains a DNS server address from the DHCP server of the upstream network automatically. • **Manual**: The DNS server address is configured manually.
Server IP Address/Domain Name User Name Password	These parameters are used for setting up internet access in the dual access network environment. When you set **ISP Type** to **Russia** and **Internet Connection Type** to **Russia PPTP** or **Russia L2TP**, these parameters are required.

Parameter	Description
Area	When you set **ISP Type** to **Maxis**, **Celcom** or **Digi**, this parameter is required. It specifies the ISP area, including: • **Maxis**: **Maxis** and **Maxis-Special** • **Celecom**: **Celcom West(BIZ)**, **Celcom West(HOME)**, **Celcom East(BIZ)** and **Celcom East(HOME)** • **Digi**: **Digi-TM**, **Digi**, **Digi-CT Sabah** and **Digi-TNB**
Internet VLAN ID IPTV VLAN ID	When you select **Manual** for **ISP Type**, you can configure these parameters. TIP **Internet VLAN ID** is required, while **IPTV VLAN ID** is optional. Blank VLAN ID indicates that the IPTV function is disabled.

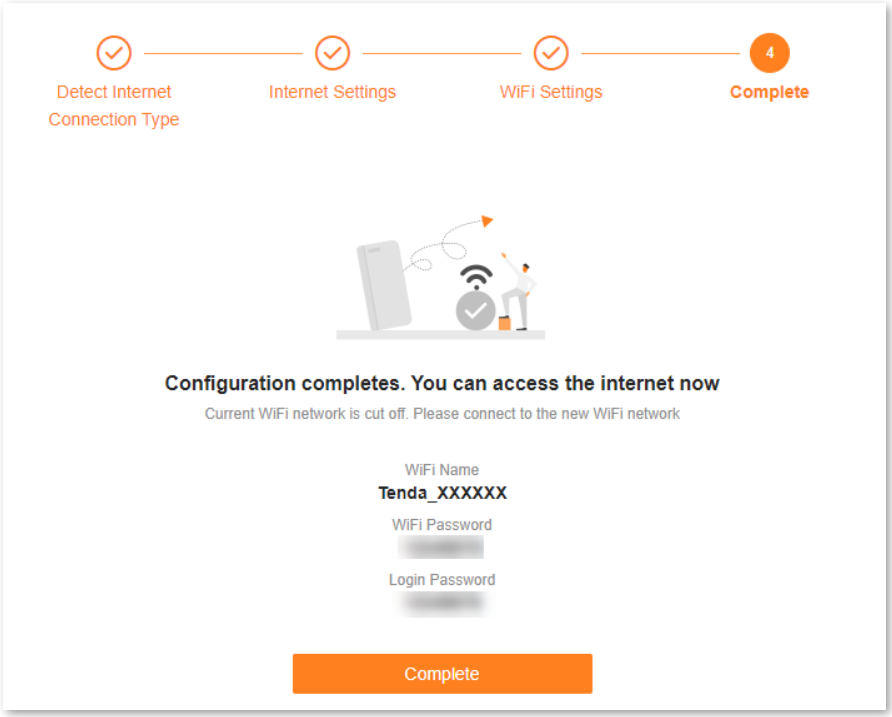
Step 5 Set parameters as required, and click **Next**.

TIP

- If you do not want to use a password, select **Not encrypted**. In this case, any client can access the network without a password. This option is not recommended as it leads to low network security.
- To use the same password for Wi-Fi access and web UI login, keep **Set WiFi password to router login password** selected, which is the default setting.
- To use different passwords for Wi-Fi access and web UI login, deselect **Set WiFi password to router login password**, and set **Wi-Fi Name** and **WiFi Password** for Wi-Fi login and **Login Password** and **Confirm Password** for web UI login.



Step 6 If the following information is displayed, the quick setup for internet access is finished. Click **Complete**.



---End

Now you can access the internet with:

- Wired devices: Connect to the LAN ports of your router
- Wireless devices: Connect to your Wi-Fi network using the Wi-Fi name and password you set

2.2 Set up as an add-on node

This section introduces how to add the router to an existing networking using the **WPS** button. For more methods, see Add a node.

TIP

- Please ensure that the router has never been used. If not, reset it first.
- Currently, RX27 Pro/TX27 Pro can be networked with the same model, Mesh6X, Mesh12X, RX12 Pro, or TX12 Pro.

Step 1 Place the router in an elevated and open position within 3 meters from your existing node.

Step 2 Use the power adapter to connect the router to a power source, and wait until its LED indicator blinks green slowly.

Step 3 Press the **WPS** button of the router for about 3 seconds. The LED indicator blinks green fast. Within 2 minutes, press the **MESH**/**WPS** button of the node of the existing network for 3 seconds to negotiate with this router.

When the LED indicator of the router lights solid green, the networking is successful and the router becomes a secondary node in the network.

Step 4 Relocate the secondary nodes to a proper position.

TIP

- Ensure that the distance between any two nodes is less than 10 meters.
- 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.

Step 5 Power on the secondary nodes again. Wait until these LED indicators blink green slowly.

TIP

If the LED indicator of any secondary node blinks green slowly for more than 3 minutes, move it closer to the primary node.

Step 6 Observe the LED indicators of the secondary nodes until the LED indicators light one of the following colors:

Solid green	Networking succeeds. Excellent connection quality.
Solid yellow	Networking succeeds. Fair connection quality.

If any secondary node's LED indicator lights solid red, relocate it by repeating **Steps 4** to **6**.

---End

Now you can access the internet with:

- Wired devices: Connect to the LAN ports of your nodes
- Wireless devices: Connect to your Wi-Fi network using the Wi-Fi name and password you set (All nodes share the same Wi-Fi name and password.)

3 Web UI

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

3.1 Log in to the web UI

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

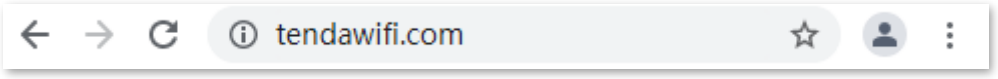
Step 1 Use an Ethernet cable to connect your computer to the **1**, **2** or **IPTV/3** port of the router, or use your smartphone to access the Wi-Fi network of the router.

In the following steps, computer connection is used for illustration.

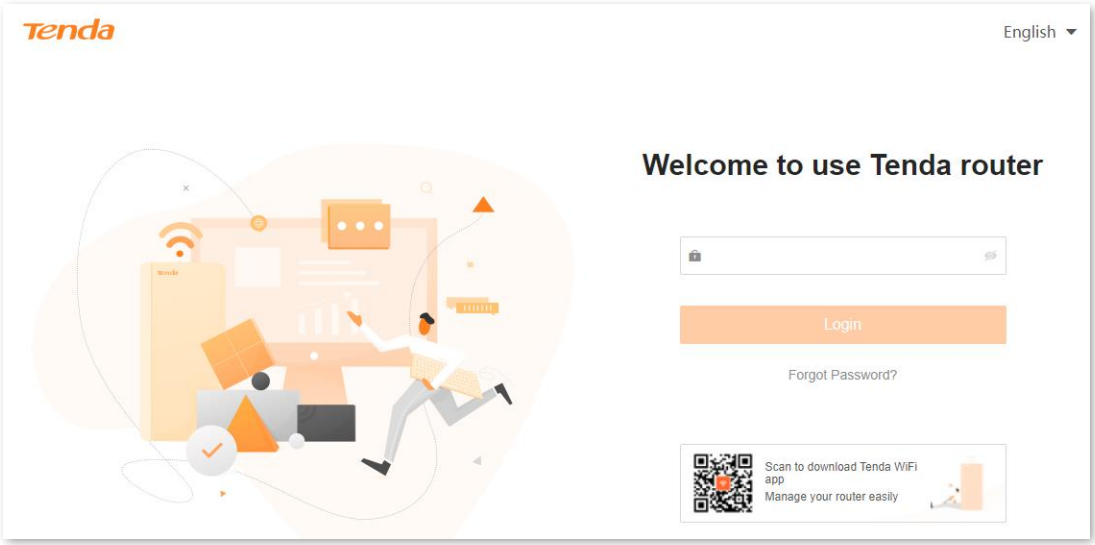
TIP

The default Wi-Fi name can be found on the bottom label of the router.

Step 2 Start a browser on the computer and enter **tendawifi.com** in the address bar to access the web UI.



Step 3 Enter your password, and click **Login**.



TIP

- If this is your first login and internet access is not configured, go to Connect the router to the internet.
- The password is the one that you specified in Connect the router to the internet. It is case-sensitive. If you forgot the password, go to Forgot my password.
- You can log in to the web UI on up to three devices concurrently.

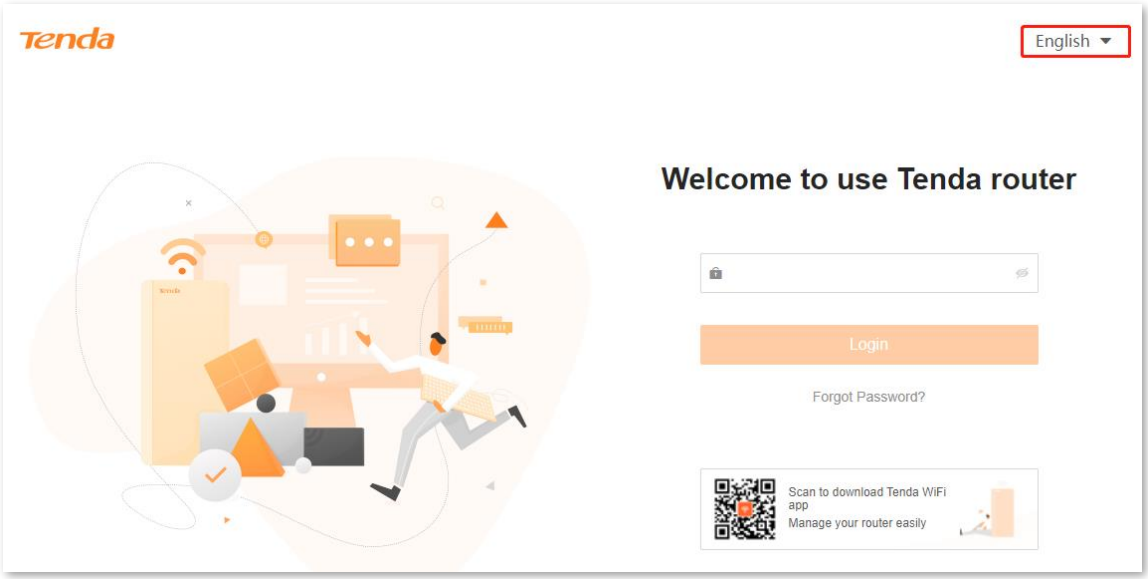
---End

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.

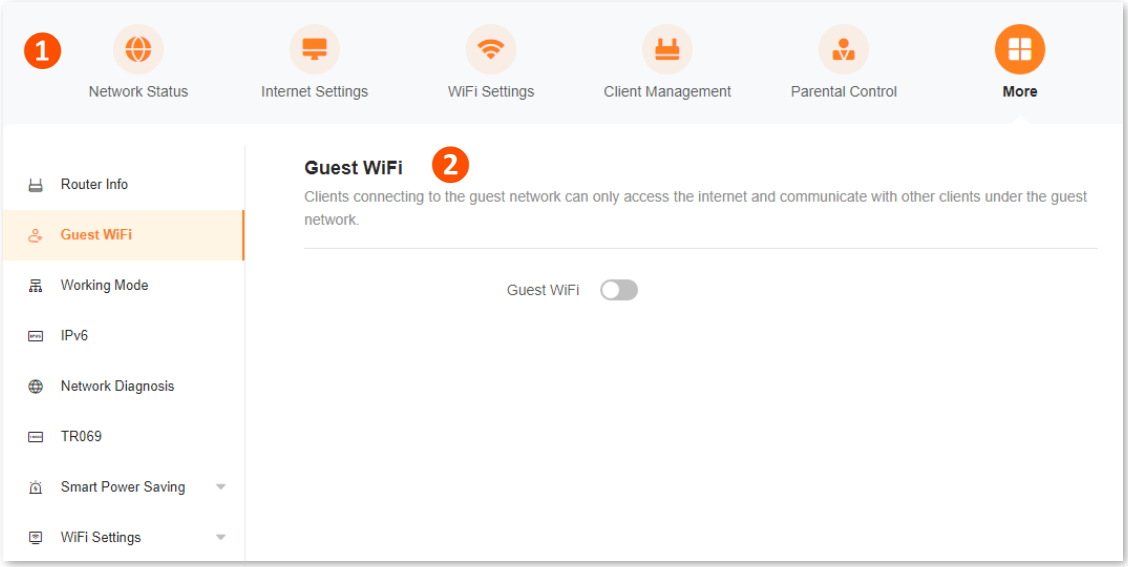
3.3 Change the language

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	Configuration area	Used to modify or view your configuration.

4 Network status

This module allows you to view basic network information, including controller and agent information, and perform quick setup on nodes, such as adding a node, one-click optimization, rebooting all nodes, and turning on/off all indicators.

This chapter includes the following sections:

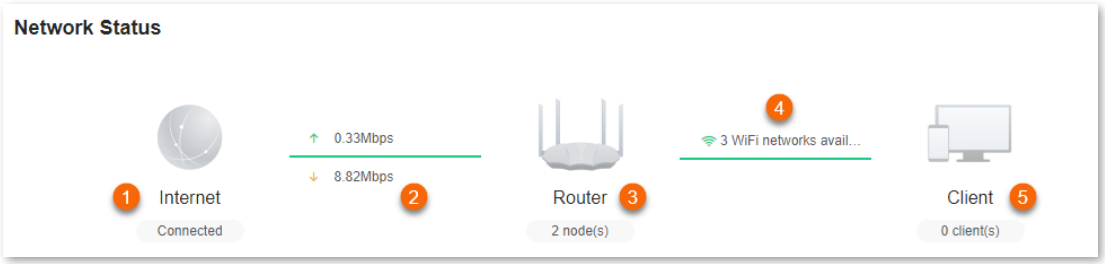
4.1 Network status

To view the network status:

Step 1 Log in to the web UI.

Step 2 Choose **Network Status**.

The following page is displayed.



---End

The following table describes the information displayed under **Network Status**.

No.	Description
1	Indicates the internet connection status. • **Connected**: The router is connected to the internet successfully. • **Disconnected**: The router is disconnected from the internet.
2	The information here varies depending on the internet connection status. • ***X.xx* Mbps**: The internet is connected successfully, and the real-time upload and download speeds are displayed, as shown in the figure above. • **Connecting**: The primary node is connecting to the internet. • Other information (for example, **No Ethernet cable is connected to the WAN port**): The internet connection failed. Click the prompt message to view tips for troubleshooting. If the problem persists, contact technical support for help.
3	Indicates the number of Mesh nodes connected in the network.
4	Indicates the number of available Wi-Fi networks. You can hover your mouse over it to see the Wi-Fi names and frequency bands.
5	Indicates the number of clients connected in the network, including secondary Mesh nodes.

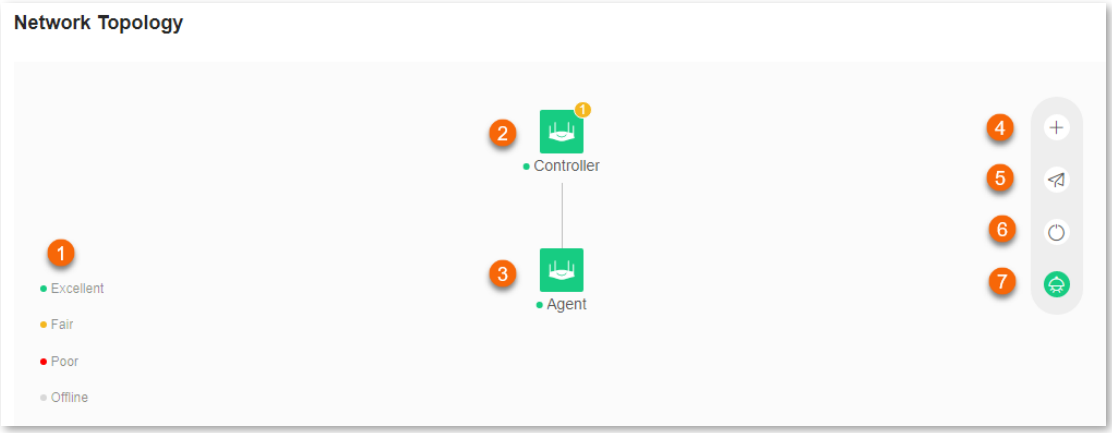
4.2 Network topology

To view the basic information of the network topology and perform quick operations:

Step 1 Log in to the web UI.

Step 2 Choose **Network Status**.

The following page is displayed.



---End

The following table describes the information displayed under **Network Topology**.

No.	Description
1	Explains the node status indicated by different colors. • **Green**: The node is connected and the networking signal is good. • **Yellow**: The node is connected and the networking signal is fair • **Red**: The node is connected and the networking signal is poor. • **Grey**: The node is offline.
2 3	Form a network topology. For details, see Controller information and Agent information.
4	Used to Add a node.
5	Used for One-click optimization.
6	Used to Reboot all nodes.
7	Used to Turn on/off all indicators.

4.2.1 Controller information

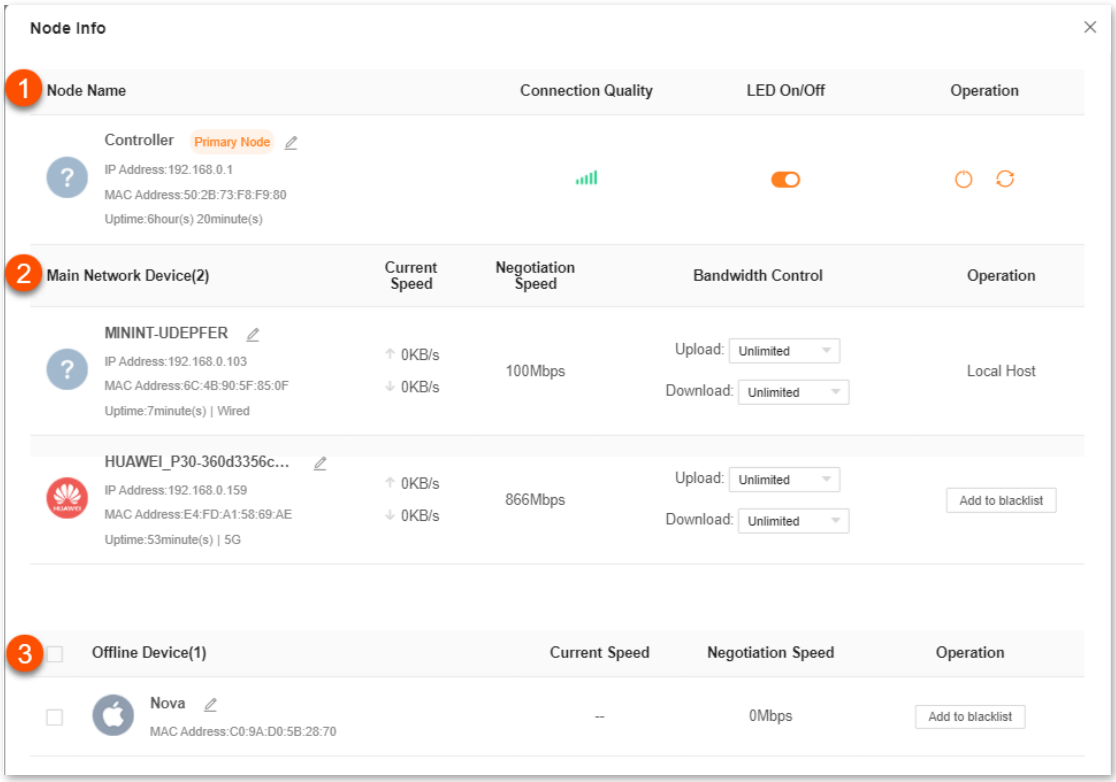
To view the information about and perform quick operations on the controller (primary node) and clients in the network:

Step 1 Log in to the web UI.

Step 2 Choose **Network Status**. Then, click 

under **Network Topology**.

The following dialog box is displayed.



---End

The following table describes the information and operation shortcuts displayed under **Node info**.

No.	Description
1	This area displays the information and operation shortcuts of the primary node, including: • **Node Name**: Indicates the name of primary node, which is **Controller** by default. You can change the name by clicking  beside **Primary Node**. • **IP address**: Indicates the IP address of the LAN port of the primary node. • **MAC address**: Indicates the MAC address of the LAN port of the primary node. • **Uptime**: Indicates the network connection time of the primary node. • **Connection Quality**: Shows the connection signal strength with the primary node. You can hover your mouse over  to see the strength value. • **LED On/Off**: Provides a  button for turning on/off the LED indicator of the primary node. You can use this function to check which device you are operating. Turn on/off all indicators prevails to this operation. • **Operation**: Provides a  button for rebooting the primary node and a  button for resetting the primary node.  Resetting clears all configurations and restores the device to factory settings. Please operate with caution.
2	This area displays the information and operation shortcuts of main network clients, including: • Client name: You can change the client name by clicking  . • **IP address**: Indicates the IP address of the client. • **MAC address**: Indicates the MAC address of the client. • **Uptime**: Indicates the network connection time of the client and the networking mode, such as **Wired**, **2.4G**, **5G** and **6G**. • **Current Speed**: Indicates the real-time upload and download speeds. • **Negotiation Speed**: Indicates the speed of negotiation. • **Bandwidth Control**: Used to set the maximum upload and download speeds, including: – **Unlimited**: The speed is not limited. – **128 KB/s**, **256 KB/s**: The maximum speed is limited to 128 KB/s or 256 KB/s. – **Custom (KB/s)**: You can set any speed in the range of 1 KB/s to 256000 KB/s. • **Operation**: – **Local Host**: Indicates that this client is the local host, which is the computer connected to the primary node in this example. For the local host, no operation is available here. – **Add to blacklist**: Used to blacklist a client. Once blacklisted, the client cannot access the internet through the Mesh system.

No.	Description
3	This area displays the information and operation shortcuts of offline clients, including: • Client name: You can change the client name by clicking . • **MAC address**: Indicates the MAC address of the client. • **Current Speed**: Unavailable. • **Negotiation Speed**: Displays the speed of negotiation. • **Operation**: Provides an **Add to blacklist** button for blacklisting clients. Once blacklisted, the client cannot access the internet through the Mesh system. TIP A maximum of 30 offline clients can be displayed here. A client will be automatically deleted from the list if it is offline for 3 days. A client is displayed under **Offline Device** after it is disconnected from the network for 90 seconds (wired client)/60 seconds (wireless client).

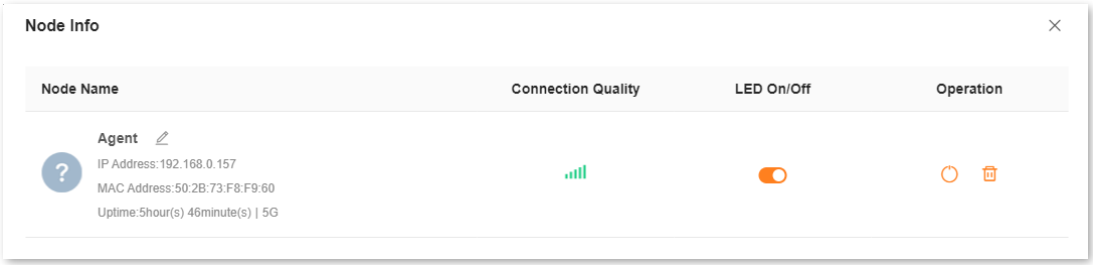
4.2.2 Agent information

To view the information about and perform quick operations on the agents (secondary nodes) in the network:

Step 1 Log in to the web UI.

Step 2 Choose **Network Status**. Then, click Agent under **Network Topology**.

The following dialog box is displayed.



---End

The following table describes the information and operation shortcuts displayed under **Node info**.

Parameter	Description
Node Name	Indicates the name of a secondary node, which is **Agent** by default. You can change the name by clicking .
IP address	Indicates the IP address of a secondary node.
MAC address	Indicates the MAC address of a secondary node.

Parameter	Description
Uptime	Indicates the network connection time of the secondary node and the networking mode, such as **Wired**, **2.4G** and **5G**.
Connection Quality	Shows the connection signal strength with the primary node. You can hover your mouse over to see the strength value.
LED On/Off	Provides a button for turning on/off the LED indicator of the secondary node. You can use this function to check which device you are operating. Turn on/off all indicators prevails to this operation.
Operation	The available options include: : Used to reboot the node. : Used to remove the node. Removing a node will narrow the Wi-Fi coverage, and the removed node will no longer join the current network automatically. To add a removed node again, go to Add a node.

4.2.3 Add a node

NOTE

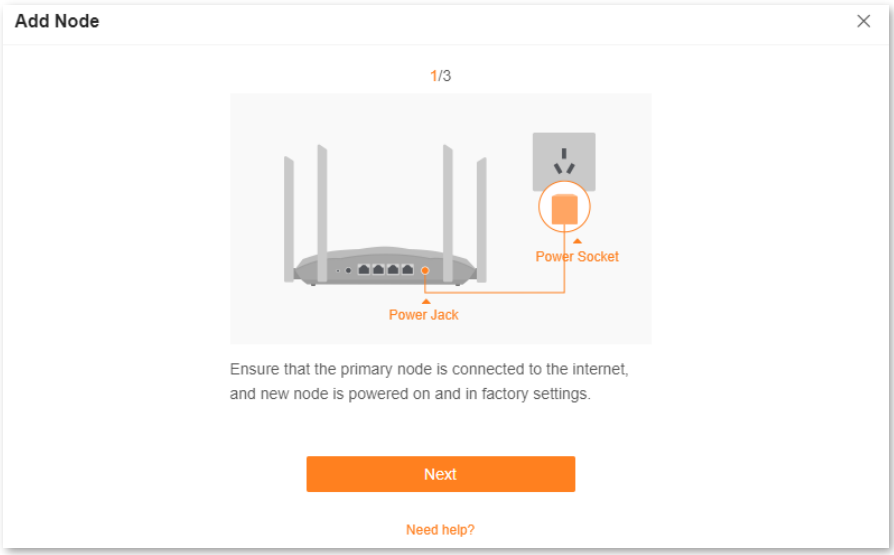
- The node to be added must support the EasyMesh or Xmesh protocol.
- The node to be added must be located within the signal coverage of the primary node.
- A maximum of nine nodes can be added.

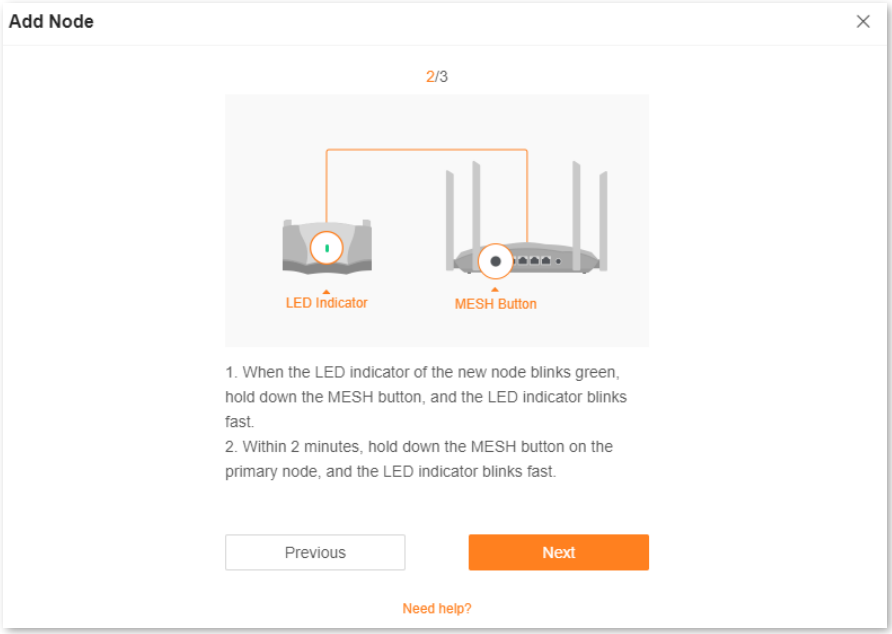
To add a node:

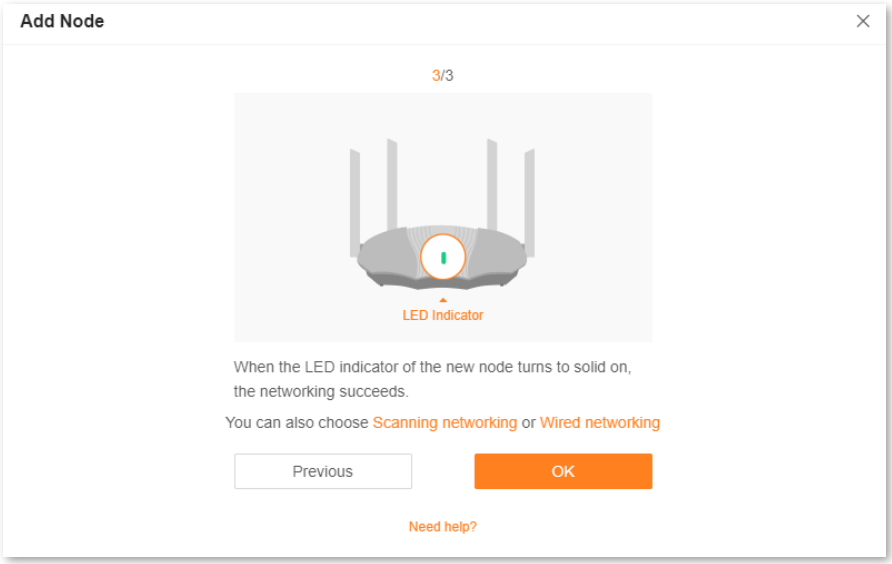
Step 1 Log in to the web UI.

Step 2 Choose **Network Status**. Then, click + under **Network Topology**.

Step 3 Follow the instructions displayed.







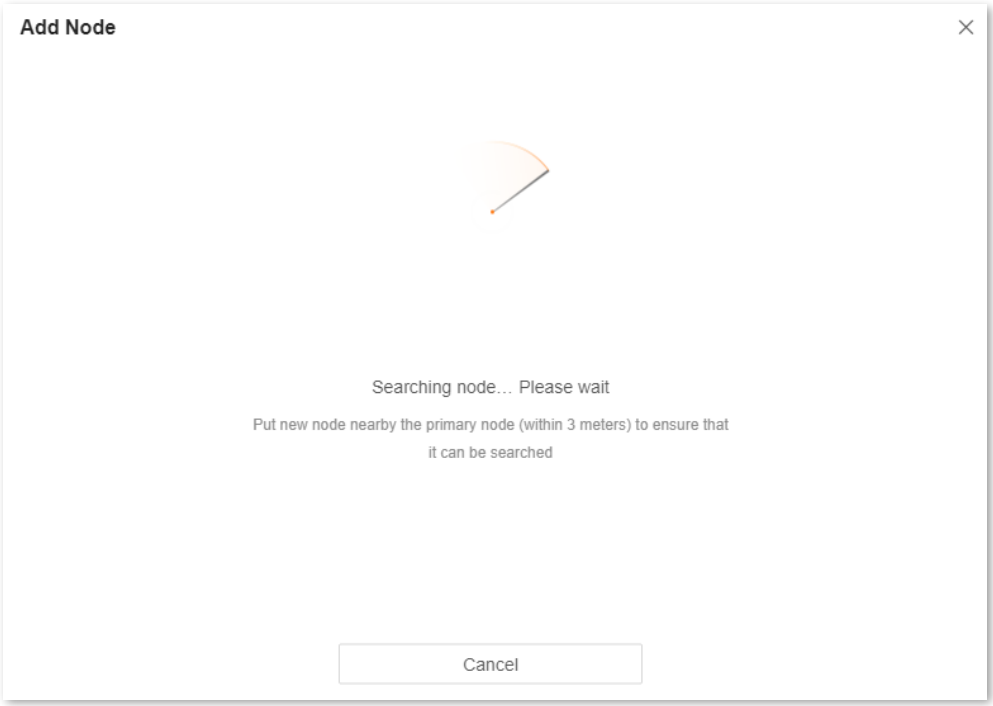
If the LED indicator of new node lights solid on and the new node is displayed in **Network Topology**, the node is added successfully.

---End

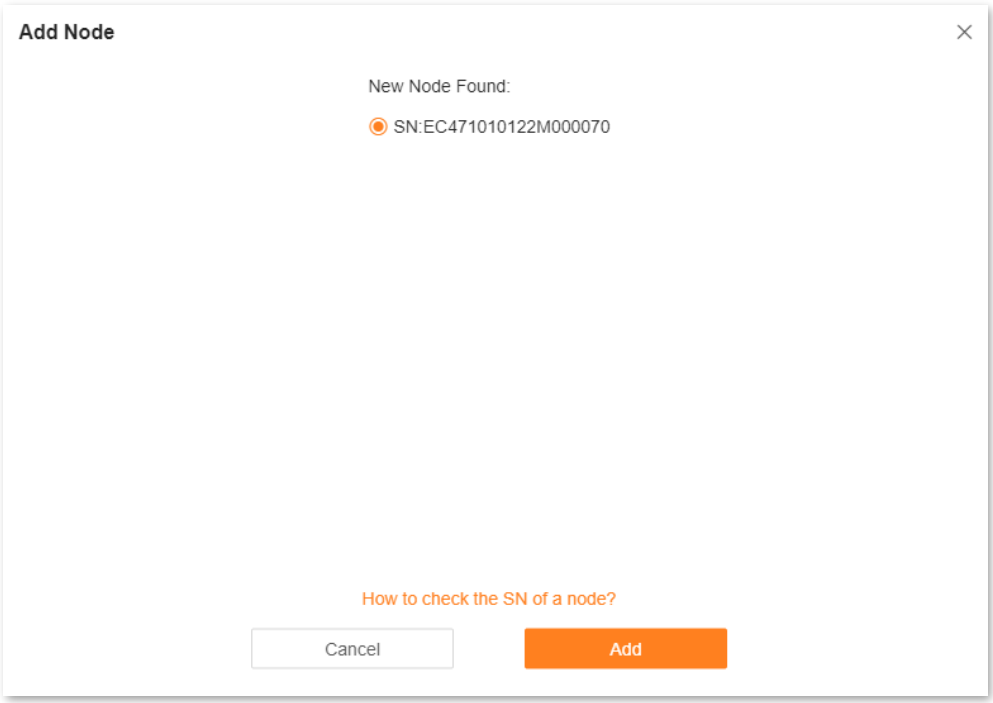
If you cannot add a node by following the preceding instructions, try the following two methods by clicking **Scanning networking** or **Wired networking** shown in the preceding figure:

- To scan a new node:

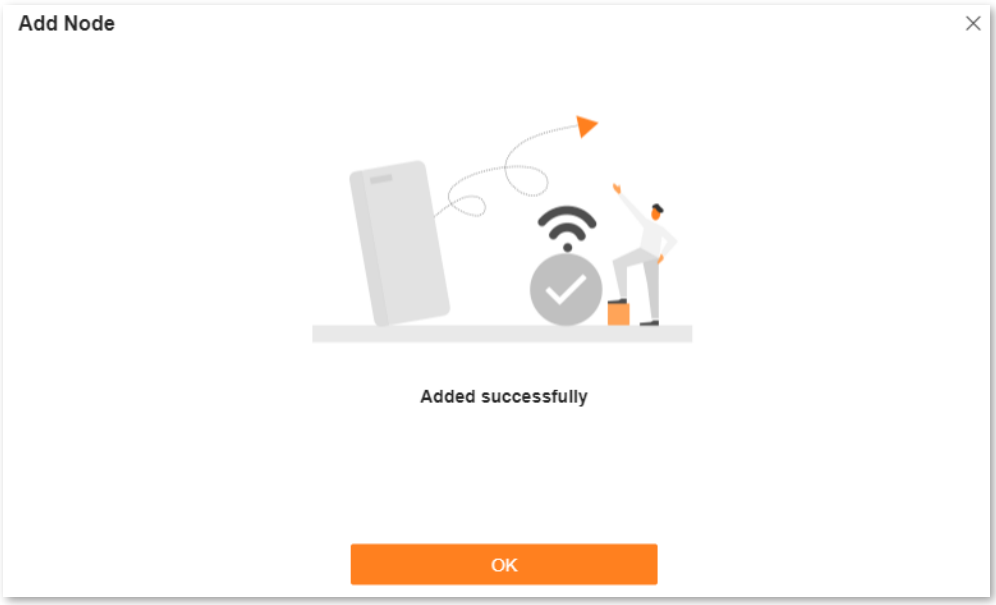
Step 1 Click **Scanning networking**.



Step 2 Select a node, and click **Add**.



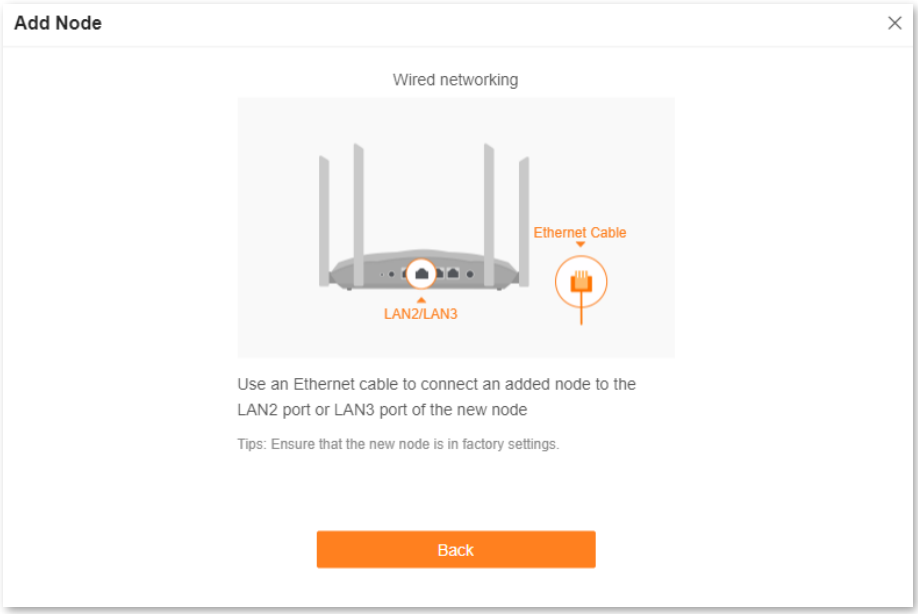
Step 3 Wait until the ongoing process is complete.



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

---End

- To perform wired networking, click **Wired networking** and follow the instructions displayed.



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

---End

4.2.4 Remove a node

NOTE

- After a node is removed, it will be restored to factory settings and all presettings will be cleared.
- Removing a node will narrow the Wi-Fi coverage, and the removed node will no longer join the current network automatically.

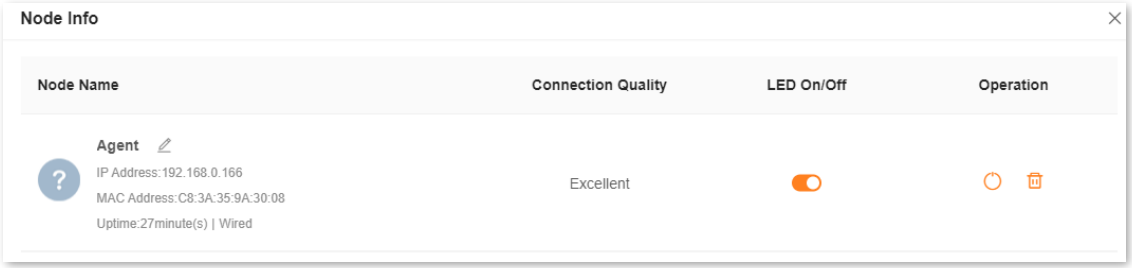
To remove a node:

Step 1 Log in to the web UI.

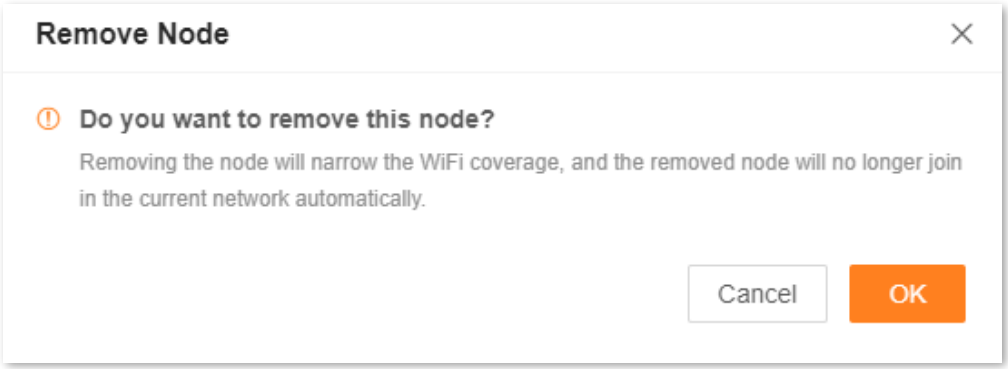
Step 2 Choose **Network Status**. Then, click 

under **Network Topology**.

Step 3 Click  under operation.



Step 4 Click **OK**.



The node is removed from the **Network Topology**.

---End

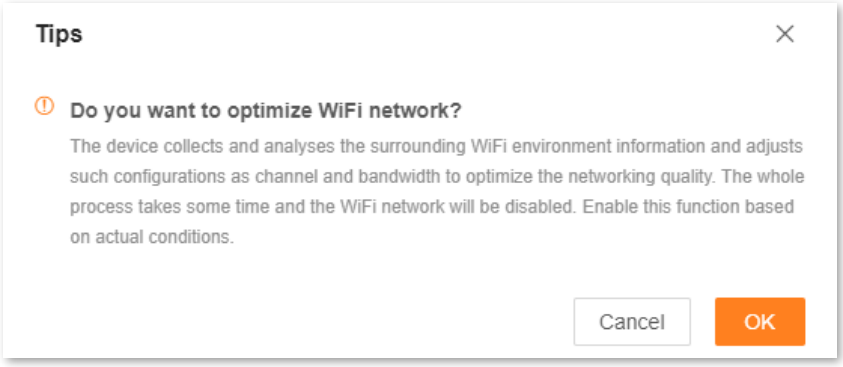
4.2.5 One-click optimization

To optimize the Wi-Fi network with one click:

Step 1 Log in to the web UI.

Step 2 Choose **Network Status**. Then, click  under **Network Topology**.

Step 3 Click **OK**.



After you click **OK**, the Wi-Fi network is disabled and it takes some time for the optimization process. Wait until the network is enabled again.

---End

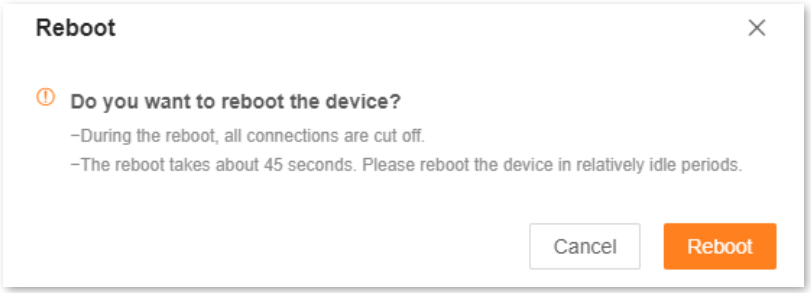
4.2.6 Reboot all nodes

To reboot all nodes by one click:

Step 1 Log in to the web UI.

Step 2 Choose **Network Status**. Then, click under **Network Topology**.

Step 3 Click **Reboot**. Wait until all nodes are restarted.



---End

4.2.7 Turn on/off all indicators

TIP

This operation prevails to LED indicator operations for each node and Smart power saving.

To turn on/off indicators of all nodes by one click:

Step 1 Log in to the web UI.

Step 2 Choose **Network Status**. Then, click or under **Network Topology**.

The indicators turn on/off immediately.

---End

5 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 Connect the router to the internet to configure the internet access. After that, you can change the internet settings by following the instructions in this chapter.

This chapter includes the following sections:

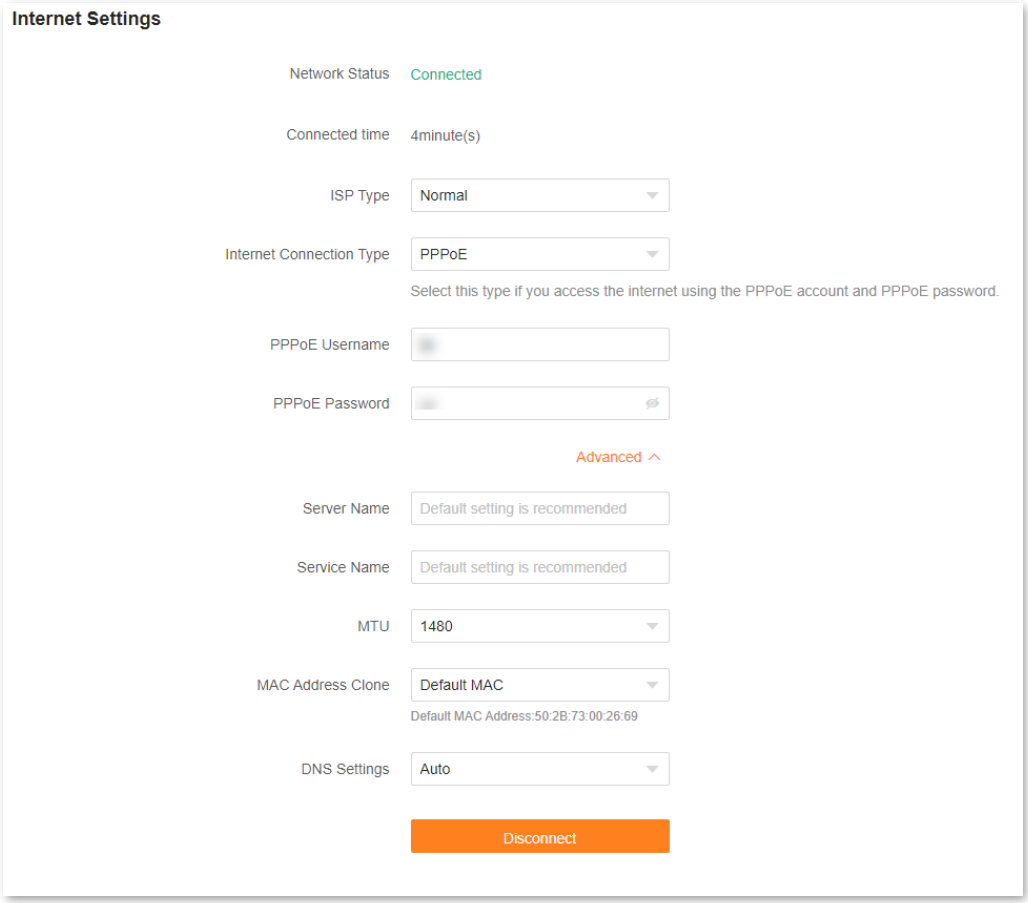
5.1 Overview

TIP

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

To access the internet settings page, log in to the web UI, and choose **Internet Settings**.

The following page is displayed.



The following table describes the parameters displayed on this page.

Parameter description

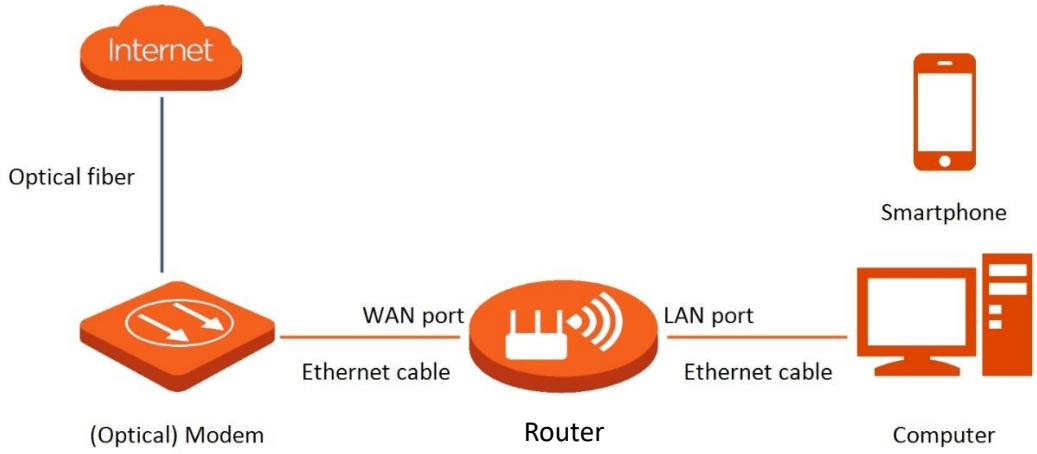
Parameter	Description
Network Status	Indicates the internet connection status. • **Connected**: The internet connection is successful. • Other information (for example, **No Ethernet cable is connected to the WAN port**): The internet connection failed. Perform troubleshooting according to the tips displayed.
Connected time	Indicates the network connection time of the router.

Parameter	Description
ISP Type	See Parameter description in Connect the router to the internet.
Internet Connection Type	
PPPoE Username	
PPPoE Password	
IP Address	
Subnet Mask	
Default gateway	
Primary DNS	
Secondary DNS	
Address Type	
DNS Settings	
Server IP Address/Domain Name	
User Name	
Password	
Area	
Internet VLAN ID	
IPTV VLAN ID	
Server Name	Displayed after you click **Advanced** if the connection type is PPPoE.
Service Name	They specify the PPPoE server name and PPPoE service name of the broadband service that you purchased. If you obtain the service name and server name from your ISP when purchasing the broadband service, you can change them on this page after completing the internet settings. Otherwise, keep the default settings.

Parameter	Description
MTU	Displayed after you click **Advanced**. It specifies the largest data packet transmitted by a network device. Do not change the value unless: • Your ISP or our technical support suggests you change it when you have problems connecting to your ISP or other internet services. • You use VPN and encounter serious performance problems. • You used a program to optimize MTU for performance reasons, and now you have connectivity or performance problems. TIP A wrong/improper MTU value may cause Internet communication problems. For example, you may be unable to access certain Websites, frames within Websites, secure login pages, FTP or POP servers. The MTU value range is as follows: • When the internet connection type is PPPoE, the default value is **1480**. Its allowed range is 1280 to 1492. • When the internet connection type is dynamic IP or static IP, the default value is **1500**. Its allowed range is 1280 to 1500. • When the internet connection type is PPTP/L2TP, the default value is **1400**. Its allowed range is 1280 to 1460.
MAC Address Clone	Used to clone and change the MAC address of the WAN port of primary node. If the primary node cannot be connected to the Internet after internet settings, the reason may be that the ISP binds internet access information to a MAC address. At this point, perform MAC address clone and try to surf the internet. • **Default MAC**: Keep the factory setting of MAC address. • **Clone Local Host MAC**: Set the MAC address of the router to the same as that of the device which is configuring the router. • **Custom**: Manually set a MAC address.
Custom MAC Address	Required when you select **Custom** for **MAC Address Clone** under **Advanced**. You can enter the customized MAC address here.

5.2 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.



To access the internet with a PPPoE account:

Step 1 Log in to the web UI, and choose **Internet Settings**.

Step 2 Set **ISP Type**.

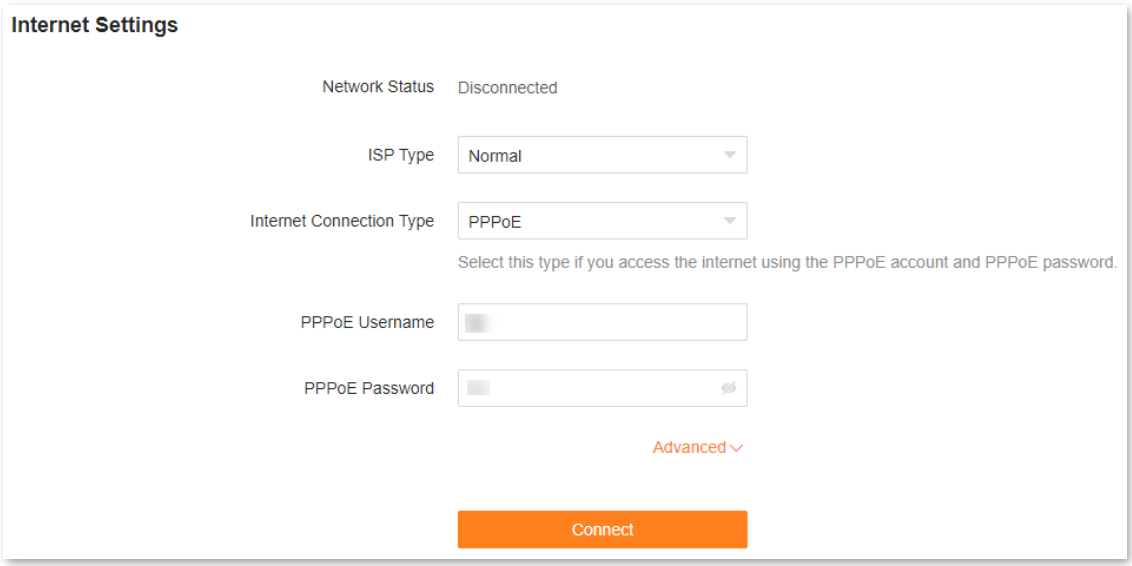
TIP

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.

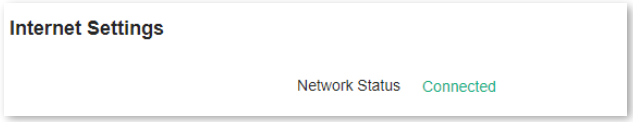
Step 3 Set **Internet Connection Type** to **PPPoE**.

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

Step 5 Click **Connect**.



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



---End

TIP

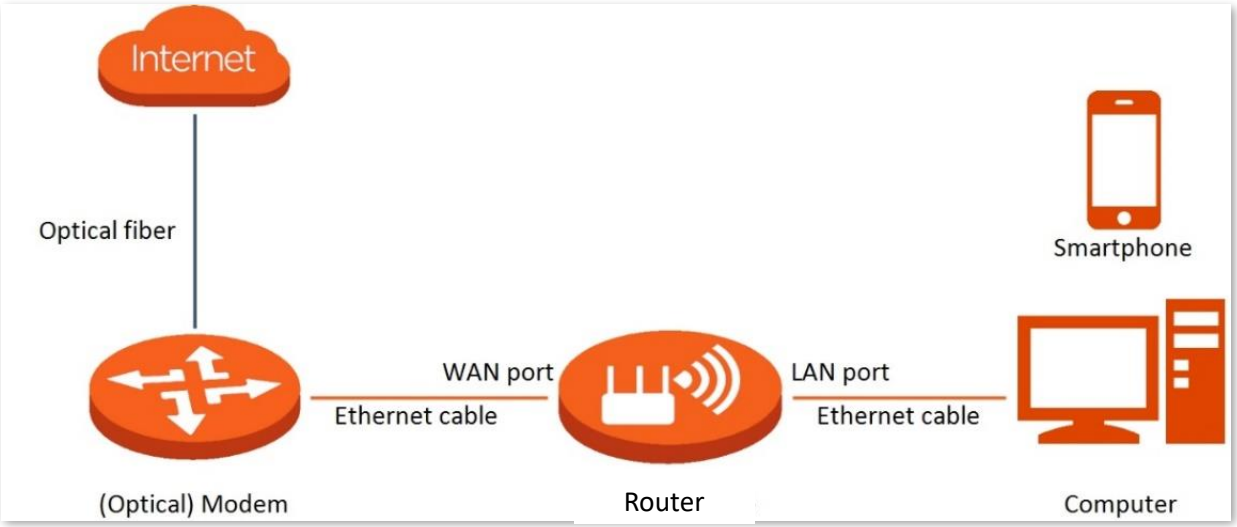
If there is no response from the remote server, troubleshoot as prompted under **Network Status** on the **Internet Settings** page.

5.3 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.



To access the internet through dynamic IP address:

Step 1 Log in to the web UI, and choose **Internet Settings**.

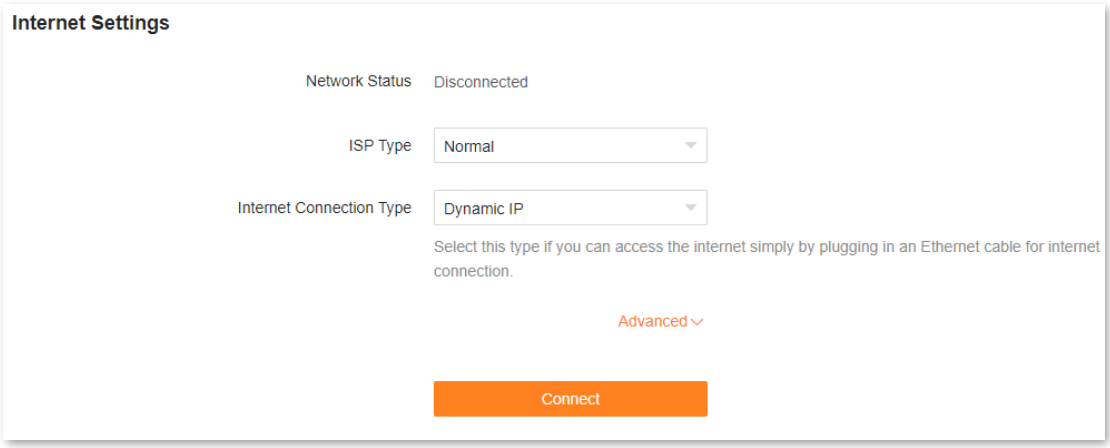
Step 2 Set **ISP Type**.

TIP

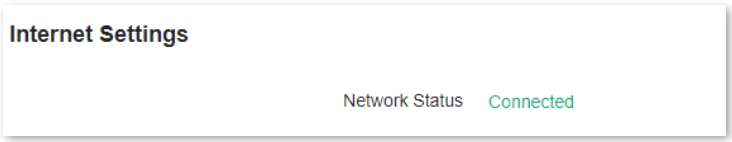
If you select **Manual** for **ISP Type**, enter **Internet VLAN ID** and **IPTV VLAN ID** (if any) provided by your ISP. Blank VLAN ID indicates that the IPTV function is disabled.

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

Step 4 Click **Connect.**



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



---End

5.4 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, and choose **Internet Settings**.

Step 2 Set **ISP Type**.

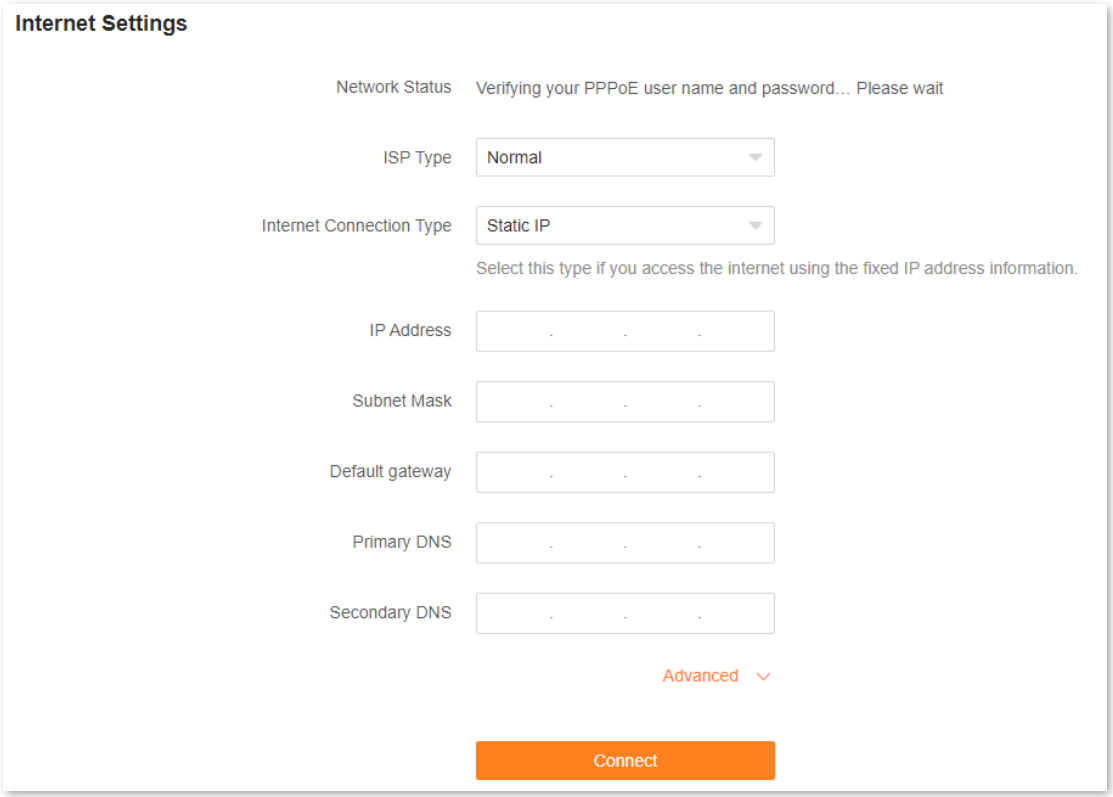
TIP

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.

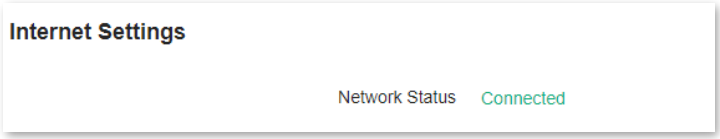
Step 3 Set **Internet Connection Type** to **Static IP**.

Step 4 Set **IP Address**, **Subnet Mask**, **Default gateway** and **Primary DNS**, and **Secondary DNS** with the information provided by your ISP.

Step 5 Click **Connect.**



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



---End

5.5 Set up dual access connection

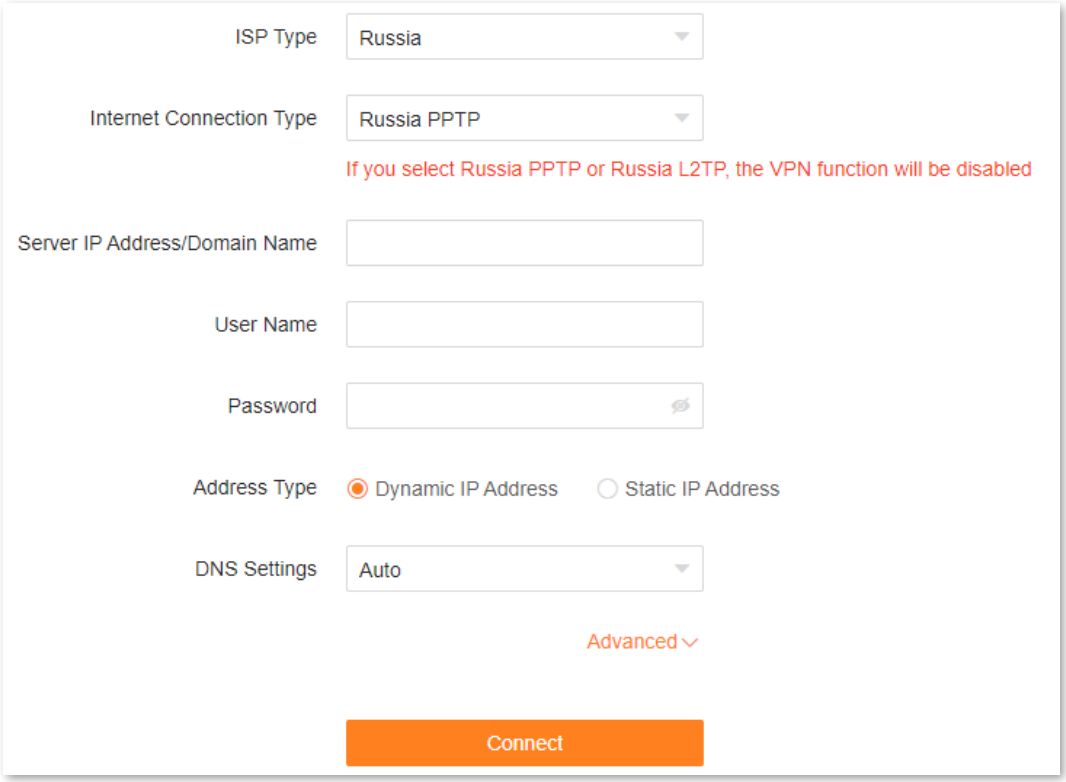
In countries like Russia, the ISP may require you to set up dual access. One is for access to the internet through PPPoE, PPTP or L2TP, and the other is for access to the “local” resources where the ISP is located through DHCP or static IP address. If your ISP provides such connection information, you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

To set up dual access connection:

Step 1 Log in to the web UI, and choose **Internet Settings**.

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

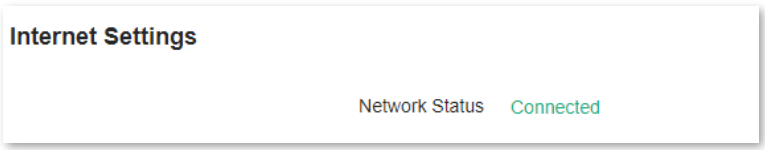
Step 3 Set **Internet Connection Type**, which is **Russia PPTP** in this example, and fill in required parameters.



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

Step 5 Click **Connect**.

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



---End

6 Wi-Fi Settings

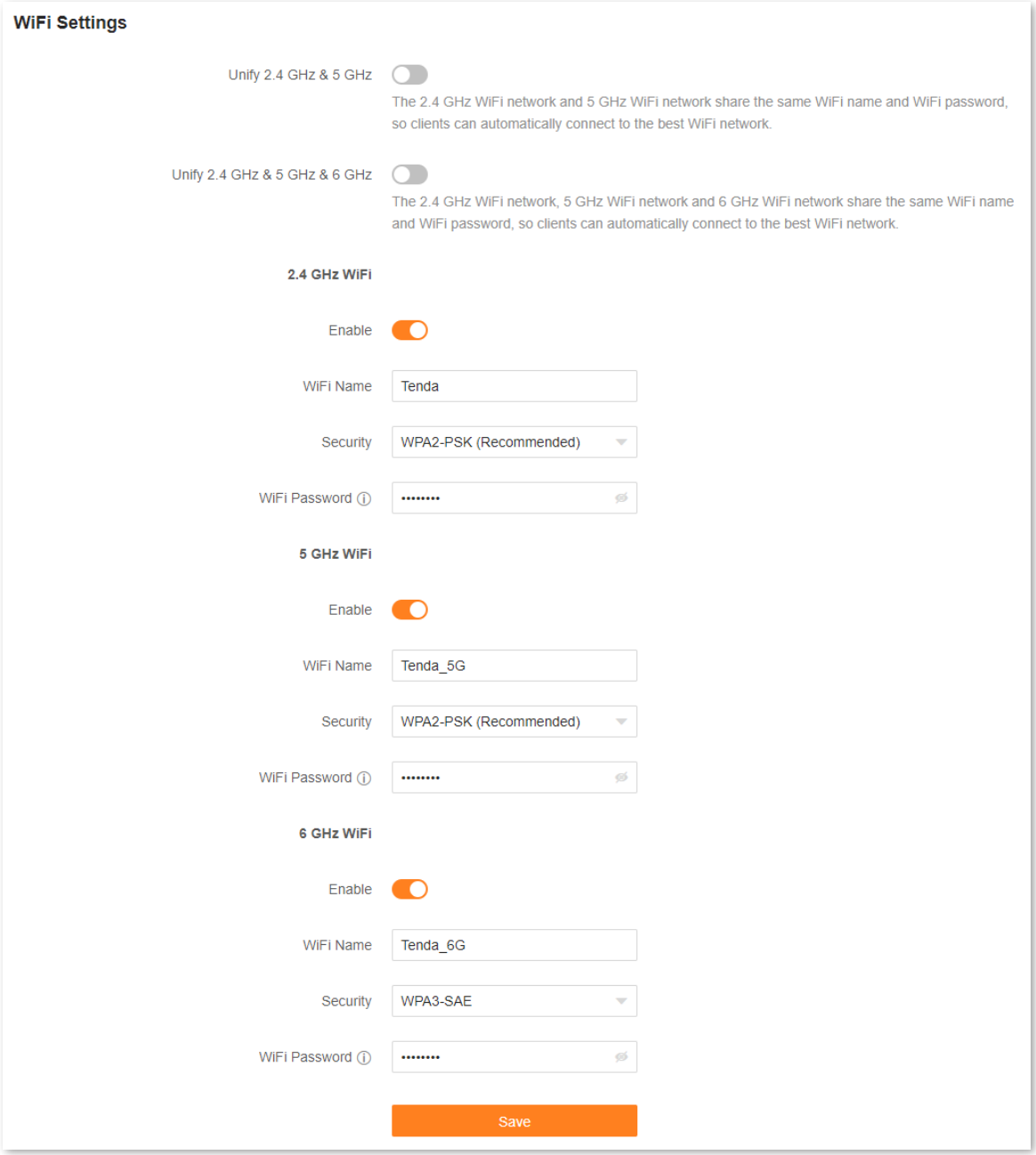
This chapter introduces basic Wi-Fi settings, including changing the Wi-Fi name, password and encryption mode, and separating the 2.4 GHz, 5 GHz and 6 GHz networking.

This chapter includes the following sections:

6.1 Basic settings

To access the Wi-Fi settings page, log in to the web UI, and choose **WiFi Settings**.

On this page, you can configure basic WiFi parameters, such as the WiFi name and password.



The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
Unify 2.4 GHz & 5 GHz	Used to enable or disable the Unify 2.4 GHz & 5 GHz function. When this function is enabled, the 2.4 GHz and 5 GHz Wi-Fi networks share the same SSID and password. WiFi-enabled clients connected to it will use the frequency with better connection quality. For details, see Separate the 2.4 GHz, 5 GHz and 6 GHz Wi-Fi networks.
Unify 2.4 GHz & 5 GHz & 6 GHz	Used to enable or disable the Unify 2.4 GHz & 5 GHz & 6 GHz function. When this function is enabled, the 2.4 GHz, 5 GHz and 6 GHz Wi-Fi networks share the same SSID and password. WiFi-enabled clients connected to it will use the frequency with better connection quality. For details, see Separate the 2.4 GHz, 5 GHz and 6 GHz Wi-Fi networks.
Enable	Used to enable or disable the Wi-Fi networks of the router.
WiFi Name	Specifies the Wi-Fi network name (SSID) of the corresponding Wi-Fi network.
Security	Specifies the encryption mode supported by the router, including: • **Not encrypted**: Indicates that the Wi-Fi network is not encrypted and any clients can access the network without a password. This option is not recommended as it leads to low network security. • **WPA2-PSK (Recommended)**: The network is encrypted with WPA2-PSK/AES. • **WPA3-SAE/WPA2-PSK**: The network is encrypted with both WPA3-SAE and WPA2-PSK, improving both security and compatibility. TIP WPA3-SAE is the upgraded version of WPA2-PSK. If your WiFi-enabled client does not support WPA3-SAE, or you get poor Wi-Fi experience, it is recommended to use **WPA2-PSK (Recommended)**.
WiFi Password	Specifies the password for connecting to the Wi-Fi network. You are strongly recommended to set a Wi-Fi password for security. TIP It is recommended to use the combination of numbers, uppercase letters, lowercase letters and special symbols in the password to enhance the security of the Wi-Fi network.

6.2 Unify the 2.4 GHz, 5 GHz and 6 GHz Wi-Fi networks

The router supports 2.4 GHz, 5 GHz and 6 GHz Wi-Fi networks, which are separated by default. You can unify their Wi-Fi names and passwords as required.

To separate the Wi-Fi names of the networks:

Step 1 Log in to the web UI, and choose **WiFi Settings**.

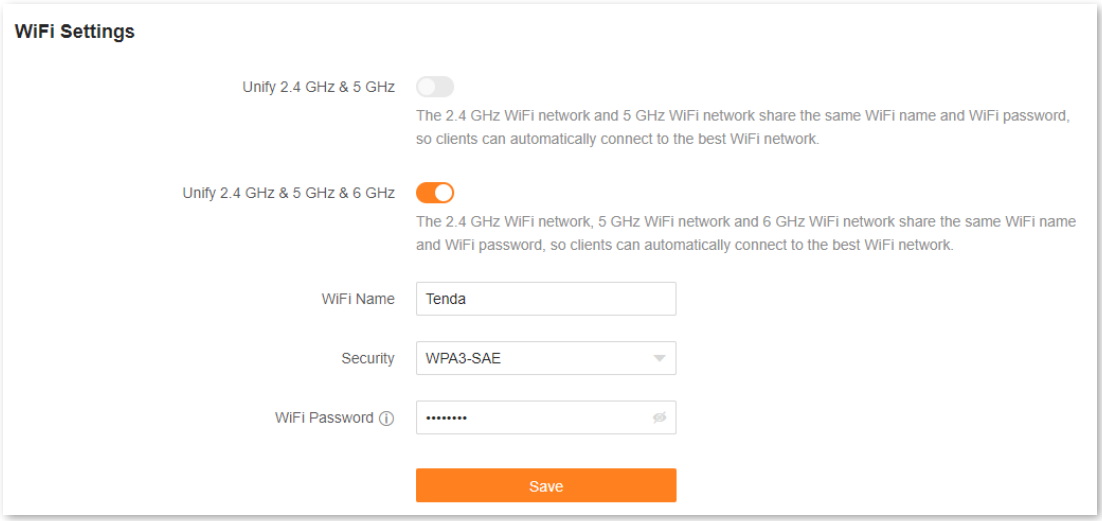
Step 2 Enable **Unify 2.4 GHz & 5 GHz** or **Unify 2.4 GHz & 5 GHz & 6 GHz** as required.

In this example, **Unify 2.4 GHz & 5 GHz & 6 GHz** is enabled.

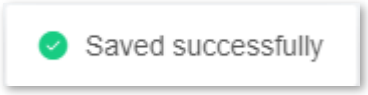
Step 3 Set **WiFi Name** and **WiFi Password**.

In this example, the Wi-Fi networks are named **Tenda**.

Step 4 Click **Save**.



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



---End

Now you can connect to the Wi-Fi networks using the same Wi-Fi name and password.

6.3 Separate the 2.4 GHz, 5 GHz and 6 GHz Wi-Fi networks

To separate the Wi-Fi names of the networks:

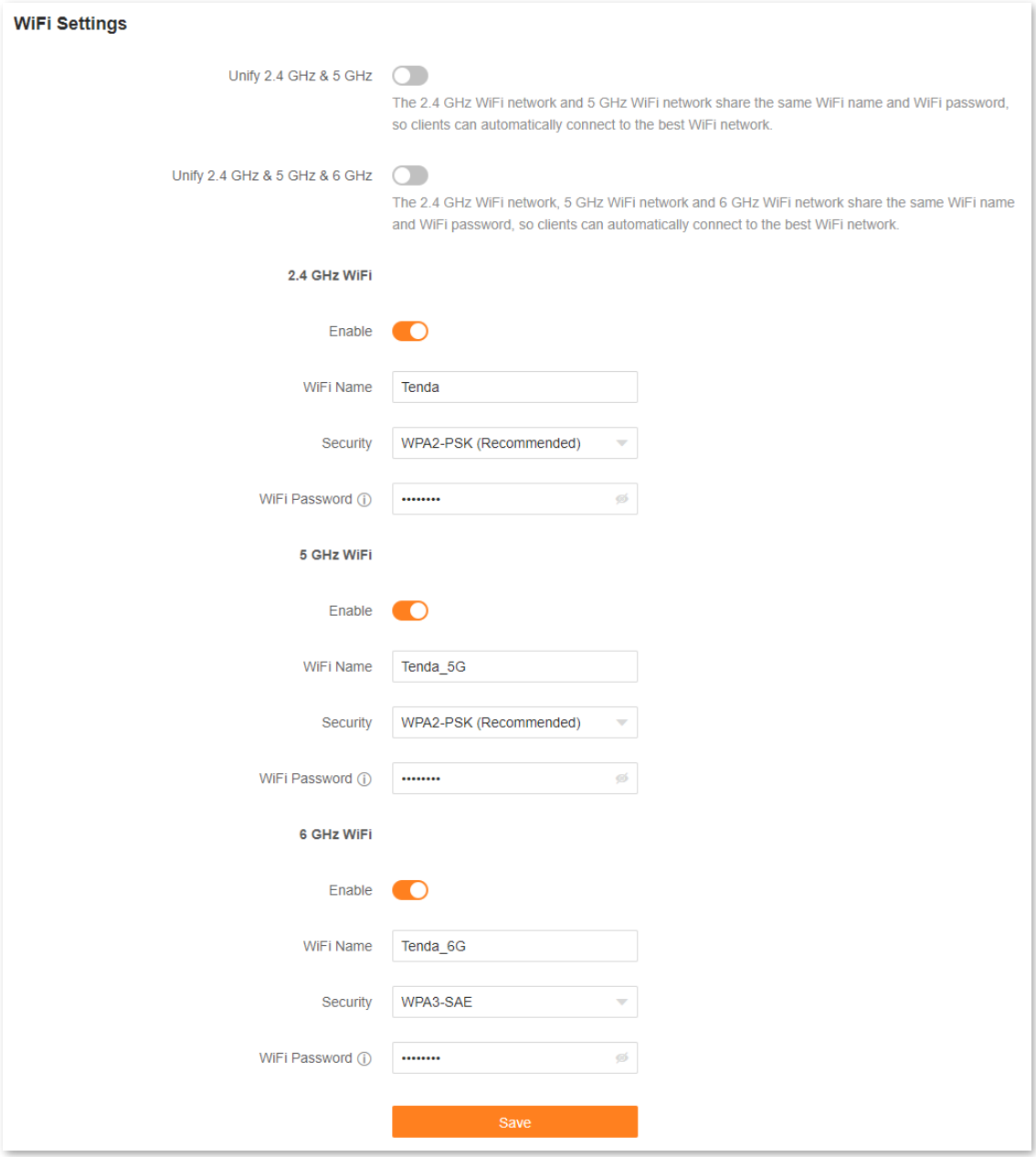
Step 1 Log in to the web UI, and choose **WiFi Settings**.

Step 2 Disable **Unify 2.4 GHz & 5 GHz** or **Unify 2.4 GHz & 5 GHz & 6 GHz** as required.

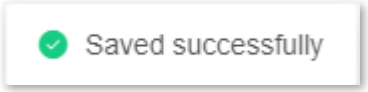
Step 3 Set **WiFi Name** and **WiFi Password** of each WiFi network.

In this example, the 2.4 GHz, 5 GHz and 6 GHz Wi-Fi networks are named **Tenda**, **Tenda_5G** and **Tenda_6G**, respectively.

Step 4 Click **Save**.



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



---End

Now you can connect to the Wi-Fi networks using different Wi-Fi names and passwords.

6.4 Hide the WiFi network

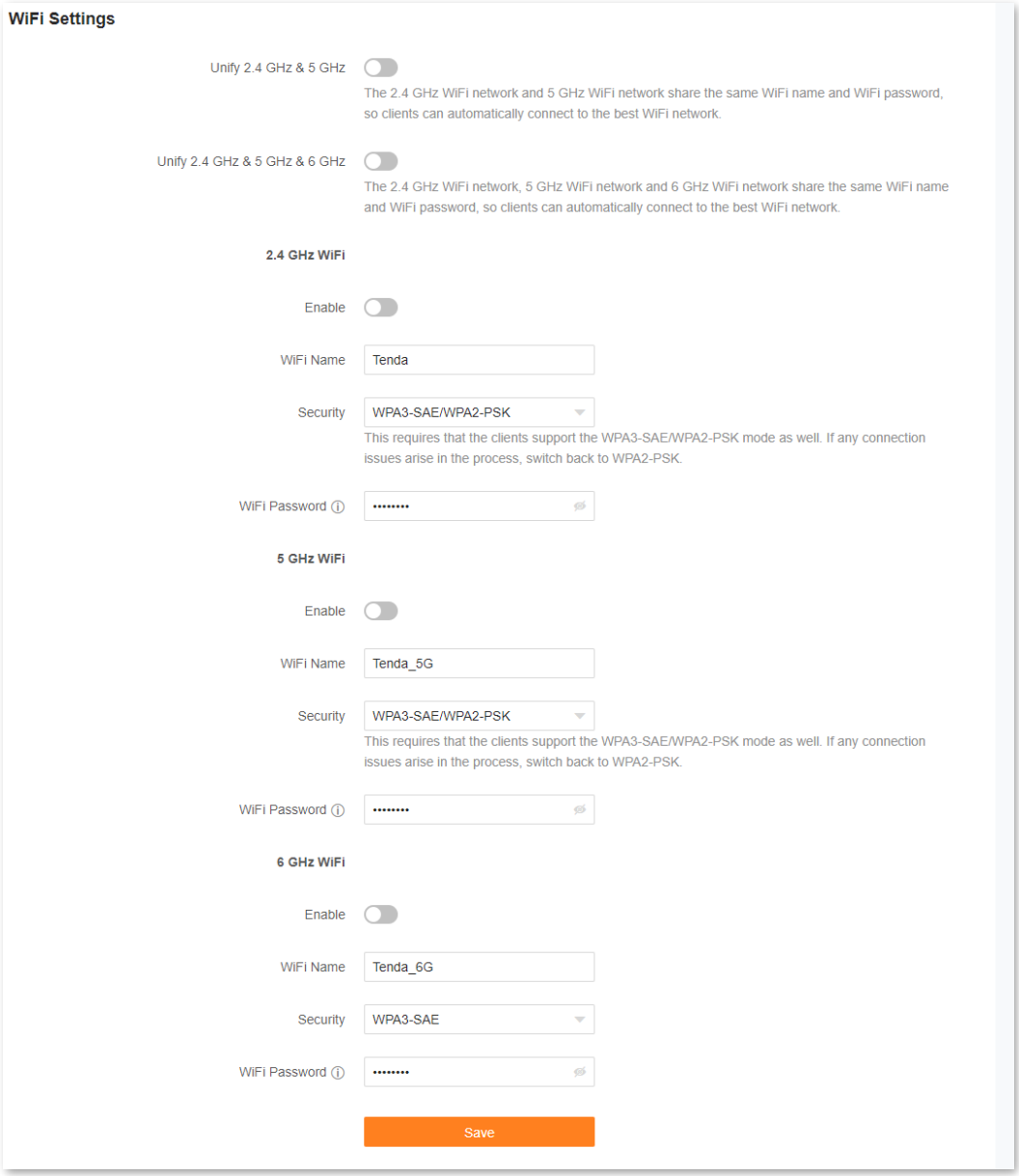
The hidden WiFi networks are invisible to WiFi-enabled devices, which improves the security of the networks.

Step 1 Log in to the web UI, and choose **WiFi Settings**.

Step 2 Toggle off **Unify 2.4 GHz & 5 GHz** or **Unify 2.4 GHz & 5 GHz & 6 GHz**.

Step 3 Toggle off **Enable** of each WiFi network.

Step 4 Click **Save**.



---End

When the configuration is completed, the corresponding WiFi networks are invisible to WiFi-enabled devices.

6.5 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 2.4 GHz Wi-Fi name is hidden and the WiFi parameters are:

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

TIP

If you do not remember the wireless parameters of the WiFi 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 WiFi-enabled device (Example: iPhone):

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

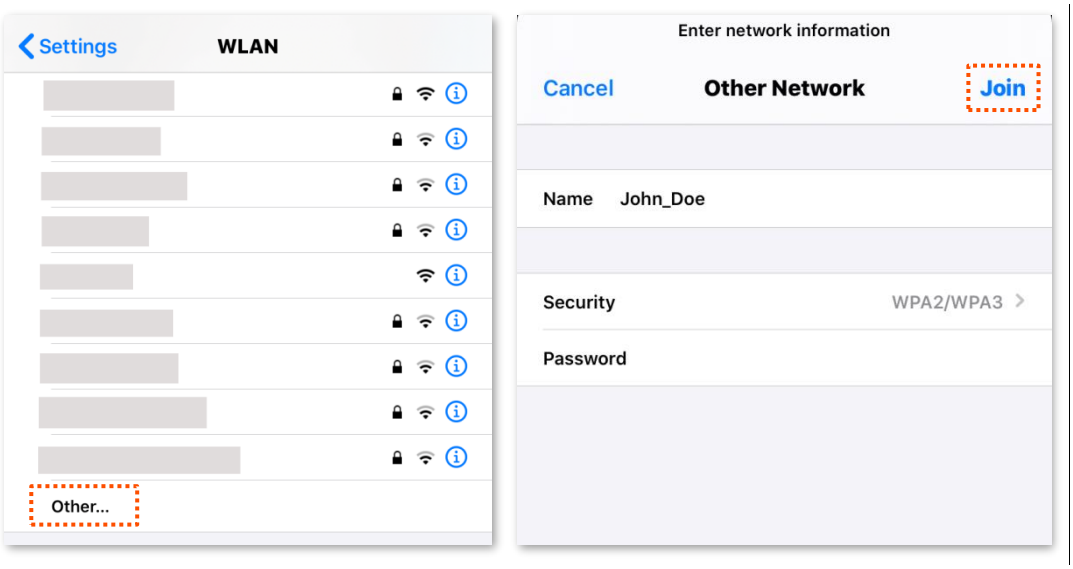
Step 2 Enable **WLAN**.

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

7 Client management

This chapter describes how to manage your clients, including:

7.1 View client information

To view information of clients:

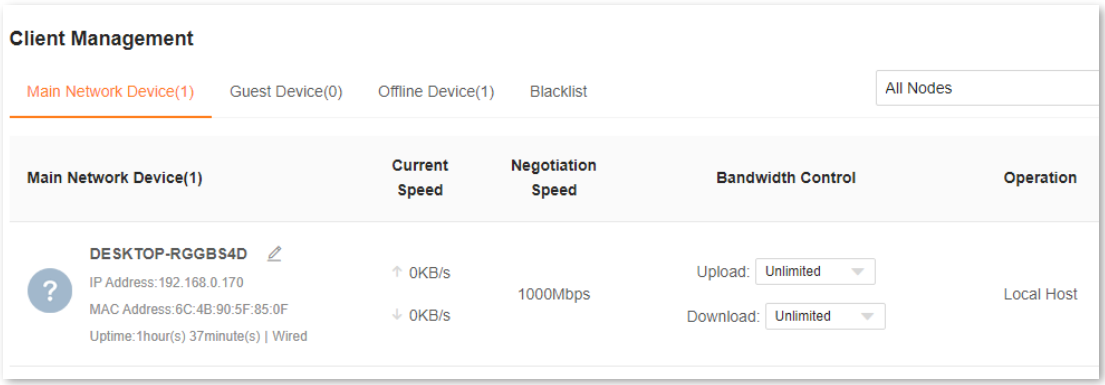
Step 1 Log in to the web UI.

Step 2 Choose **Client Management**.

TIP

- The information of all clients is displayed by default.
- To view information of only the clients connected to the controller (primary node), select the controller from the drop-down list box under **Client Management**. The controller name is **Controller** by default. You can change it in Controller information.
- To view information of only clients connected to an agent, select the agent from the drop-down list box under **Client Management**. If you have multiple agents and you keep default names for them, multiple **Agent** will be displayed in the drop-down list box under **Client Management**. You can change the agent names in Agent information.
- To view information on blacklisted clients, choose **Blacklist** on the right.

The following page is displayed.



---End

The following table describes the information and operation shortcuts displayed under **Client Management**.

Parameter	Description
Main Network Device	This tab page displays the information and operation shortcuts of main network clients, including: • Client name: You can change the client name by clicking  . • **IP address**: Indicates the IP address of the client. • **MAC address**: Indicates the MAC address of the client. • **Uptime**: Indicates the network connection time of the client and the networking mode, such as **Wired**, **2.4G**, **5G** and **6G**. • **Current Speed**: Indicates the real-time upload and download speeds. • **Negotiation Speed**: Indicates the speed of negotiation. • **Bandwidth Control**: Used to set the maximum upload and download speeds, including: – **Unlimited**: The speed is not limited. – **128 KB/s**, **256 KB/s**: The maximum speed is limited to 128 KB/s or 256 KB/s. – **Custom (KB/s)**: You can set any speed in the range of 1 KB/s to 256000 KB/s. • **Operation**: – **Local Host**: Indicates that this client is the local host, which is the computer connected to the router in this example. For the local host, no operation is available here. – **Add to blacklist**: Used to blacklist a client. Once blacklisted, the client cannot access the internet through the router.
Guest Device	This tab page displays the information and operation shortcuts of clients connected to the guest network, including: • **Current Speed**: Indicates the real-time upload and download speeds. • **Negotiation Speed**: Indicates the speed of negotiation. • **Operation**: Provides an **Add to blacklist** button for blacklisting clients. Once blacklisted, the client cannot access the internet through the router.
Offline Device	This tab page displays the information and operation shortcuts of offline clients, including: • Client name: You can change the client name by clicking  . • **MAC address**: Indicates the MAC address of the client. • **Current Speed**: Unavailable. • **Negotiation Speed**: Indicates the speed of negotiation. • **Operation**: Provides an **Add to blacklist** button for blacklisting clients. Once blacklisted, the client cannot access the internet through the router's network. A maximum of 30 offline clients can be displayed here. A client is displayed under **Offline Device** after it is disconnected from the network for 90 seconds (wired client)/60 seconds (wireless client). A client will be automatically deleted from this list if it is offline for 3 days.

Parameter	Description
Blacklist	This tab page displays the information and operation shortcuts of blacklisted clients, including: • **Device Name**: Indicates the name of the blacklisted client. • **MAC address**: Indicates the MAC address of the client. • **Operation**: Provides a **Remove from the blacklist** button for removing clients from the blacklist.

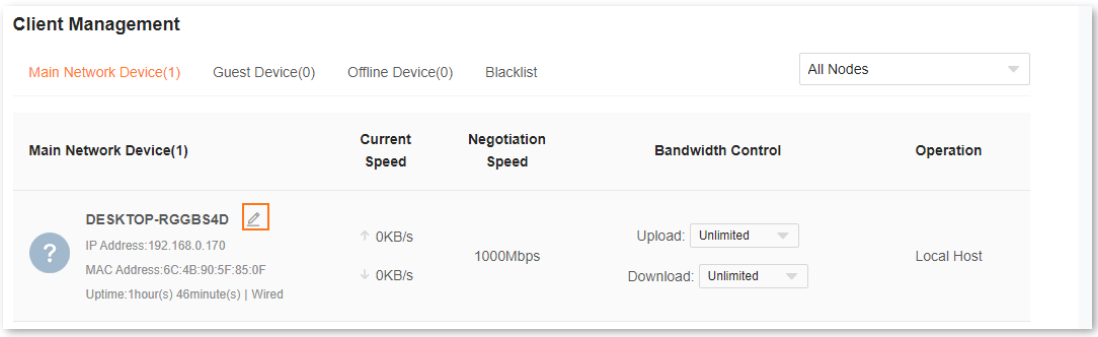
7.2 Change a client name

You can change the names of all clients connected to the network on the web UI. Here changing the name of main network client is used as an example. The operations for changing other client names are similar.

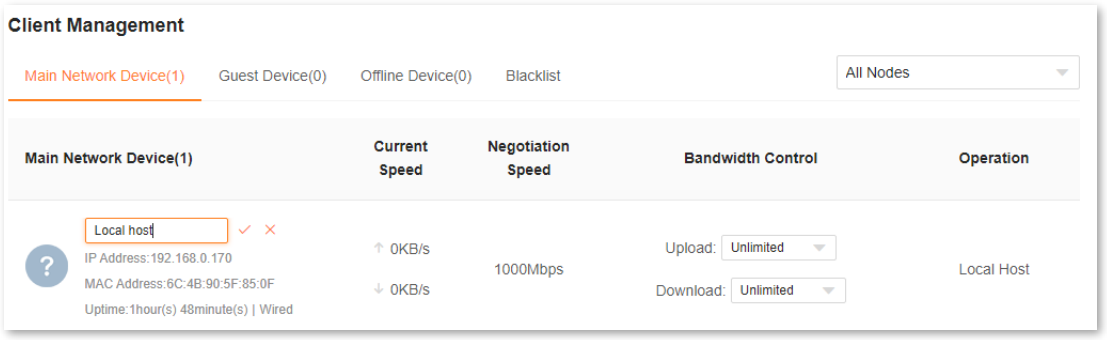
To change the name of a client:

Step 1 Log in to the web UI, and choose **Client Management**.

Step 2 Click beside the client name.



Step 3 Enter a new name and click .



The new client name is saved.

---End

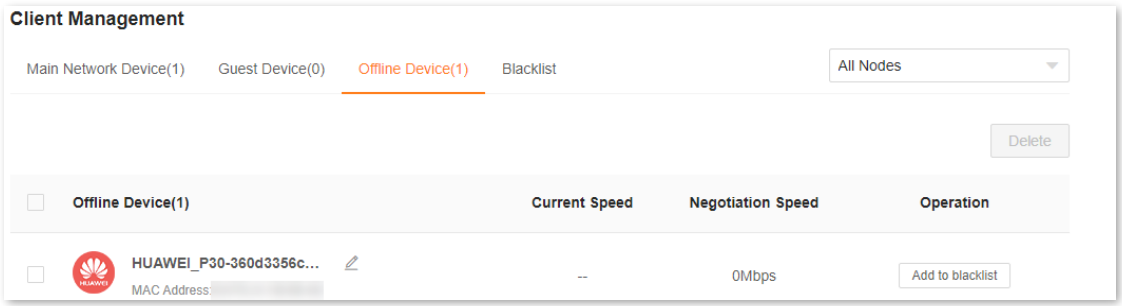
7.3 Add a client to the blacklist

If you find any unknown client connects to your network and you want to block it from accessing your network, you can blacklist it here. All clients connected to the network can be blacklisted, except the local host. Here blacklisting a main network client is used as an example. The operations for blacklisting other clients are similar.

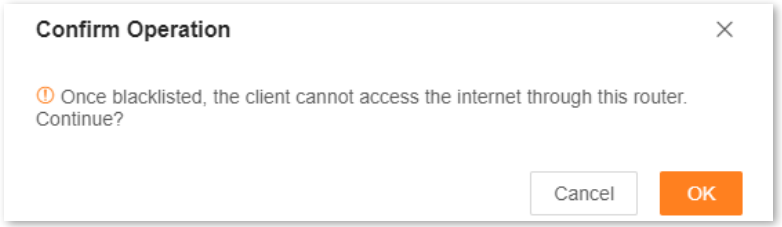
To blacklist a client:

Step 1 Log in to the web UI, and choose **Client Management**.

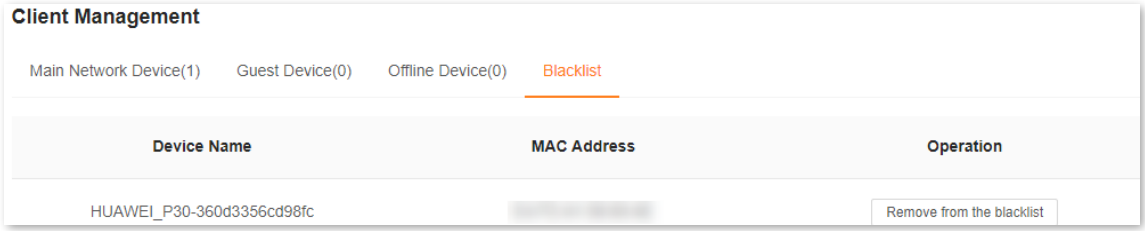
Step 2 Click **Add to blacklist** under **Operation** in the line of the client to be blacklisted.



Step 3 Click **OK**.



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



TIP

- If you blacklist a wired client, the wired client will fail to access the network.
- If you blacklist a wireless client, the wireless client will be kicked offline and cannot connect to the router again.
- A maximum of 64 clients can be blacklisted.
- The blacklist rule prevails when conflicting with the parent control rule.

---End

7.4 Remove a client from the blacklist

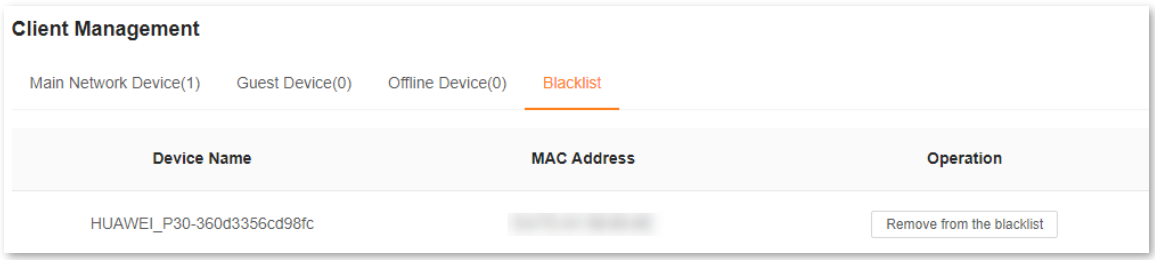
If you blacklist a client by mistake, you can remove it from the blacklist.

To remove a client from the blacklist:

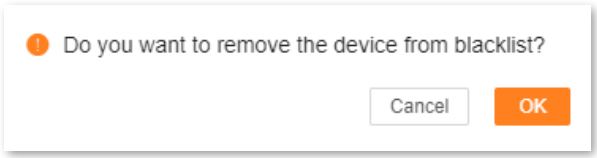
Step 1 Log in to the web UI, and choose **Client Management**.

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 Click **OK**.



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

---End

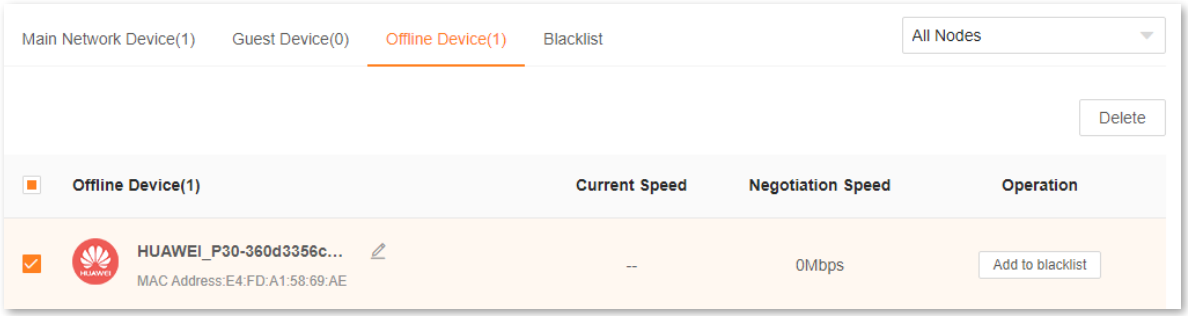
7.5 Delete an offline client

You can delete any offline client that is connected to the network before.

To delete an offline client:

Step 1 Log in to the web UI, and choose **Client Management**.

Step 2 Select the offline client to be deleted, and click **Delete** on the upper right corner of **Offline Device**.



The client you selected is removed from the device list.

TIP

The deleted client can be displayed in the device list again upon its next network access.

---End

8 Parental control

This function allows you to configure various parental control rules to control access to certain websites or block certain clients from accessing the internet.

This chapter includes the following sections:

8.1 Create a parental control rule

8.1.1 Add a parental control rule

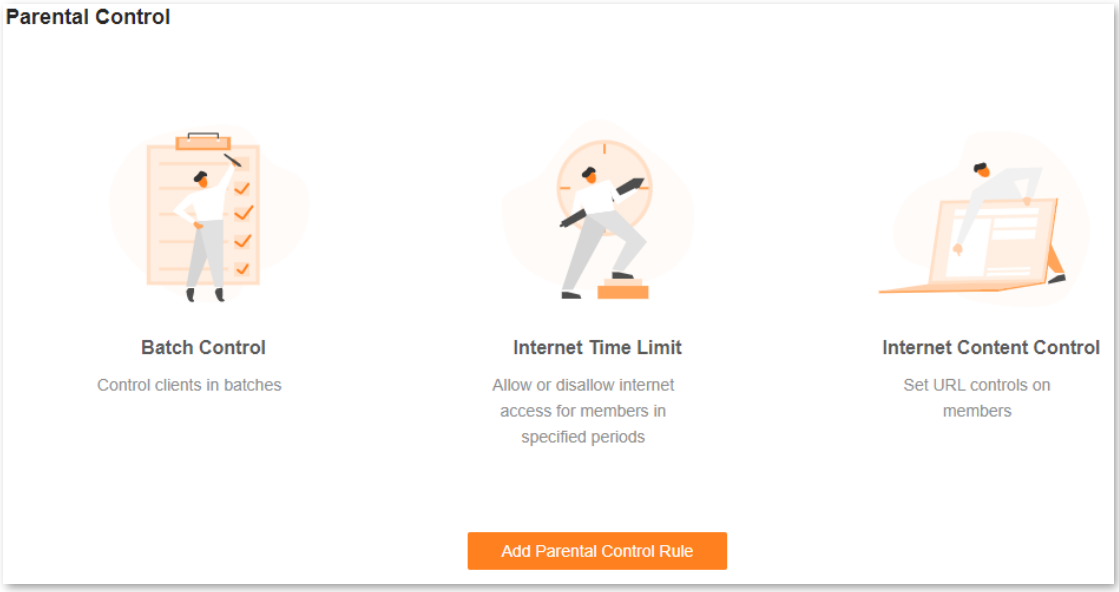
NOTE

- The blacklist rule prevails when conflicting with the parent control rule.
- A maximum of 10 rules can be added.
- A maximum of 30 clients can be controlled.

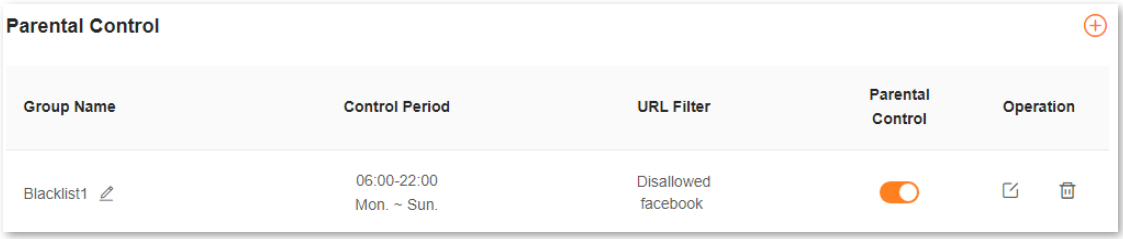
To add a parental control rule:

Step 1 Log in to the web UI, and choose **Parental Control**.

If you did not add a parental control rule before, the following page is displayed.



If you have added parental control rules before, the following page is displayed.

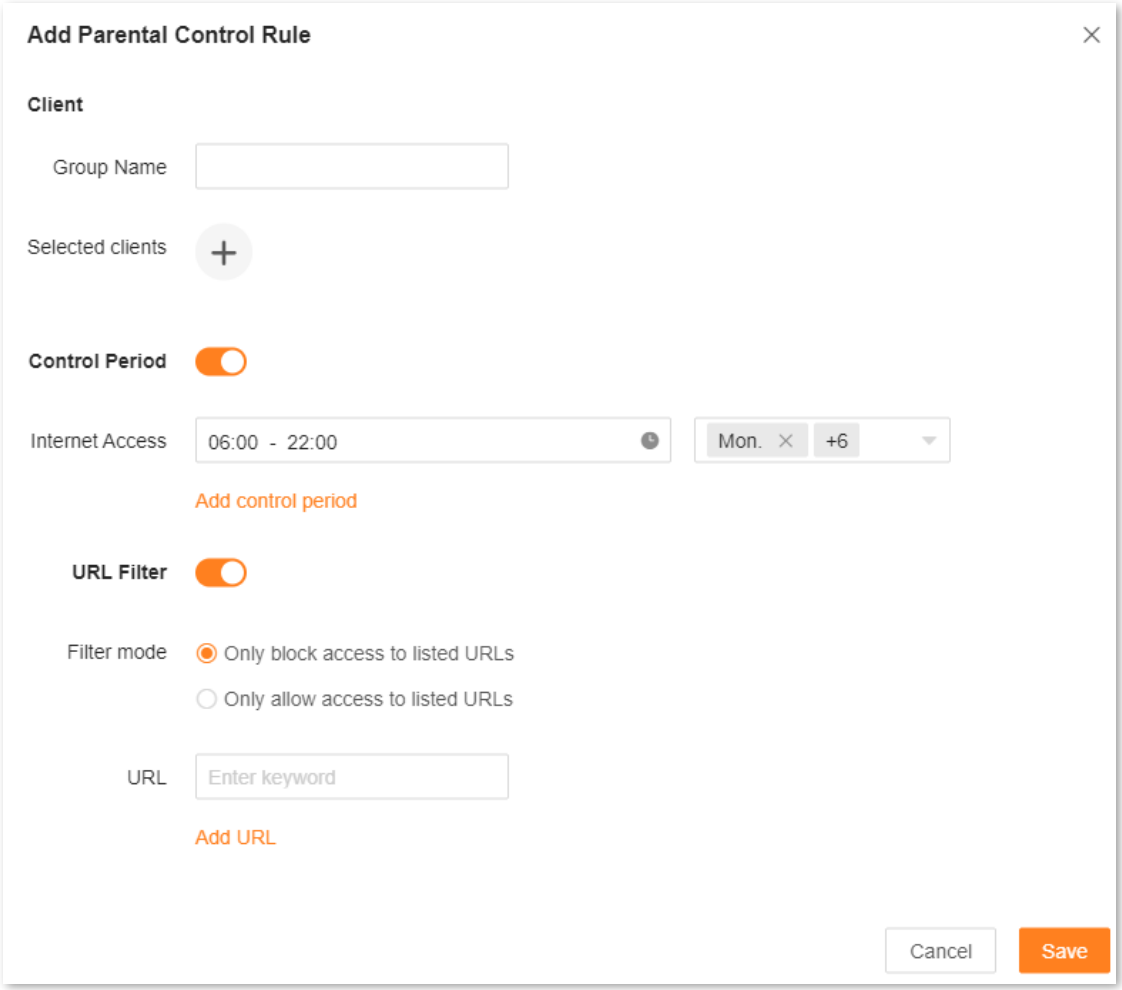


Step 2 Click **Add Parental Control Rule** or ⊕.

Step 3 Set the parameters as required.

TIP

A maximum of 10 control periods and 10 URLs can be added.



Step 4 Click **Save**.

The parental control rule that you set is displayed on the **Parental Control** page.

---End

The following table describes the parameters under **Add Parental Control Rule**.

Parameter description

Parameter	Description
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	Specifies whether the parental control rule takes effect. • When it is toggled on, internet access is allowed only in the period specified by **Internet Access**. • When it is toggled off, internet access is allowed all the time.

Parameter	Description
Internet Access	Required when **Control Period** is toggled on. It specifies the period during which the client can access the internet.
Add control period	Available when **Control Period** is toggled on. If you want to set multiple periods, click this button.
URL Filter	Specifies whether the URL filter rule is applied. • When it is toggled on, **Filter mode** and **URL** must be set. The parental control rule takes effect on specific websites. • When it is toggled off, the URL filter rule is not applied.
Filter mode	Required when **URL Filter** is toggled on. Two modes are available here. • **Only block access to listed URLs**: The **Selected clients** are only blocked from accessing the websites specified by **URL**. • **Only allow access to listed URLs**: The **Selected clients** can only access the websites specified by **URL**.
URL	Specifies the websites that the **Selected clients** are blocked from accessing or allowed to access.
Add URL	Available when **URL Filter** is toggled on. If you want to set multiple URLs, click this button.

8.1.2 An example of adding parental control rules

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

Goal: Your kid cannot access such websites as Facebook, Twitter, Youtube and Instagram from 8:00 to 22:00 on weekends and cannot access the internet at all between 22:00 to 8:00 on weekends using the computer at home.

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

To add such a rule:

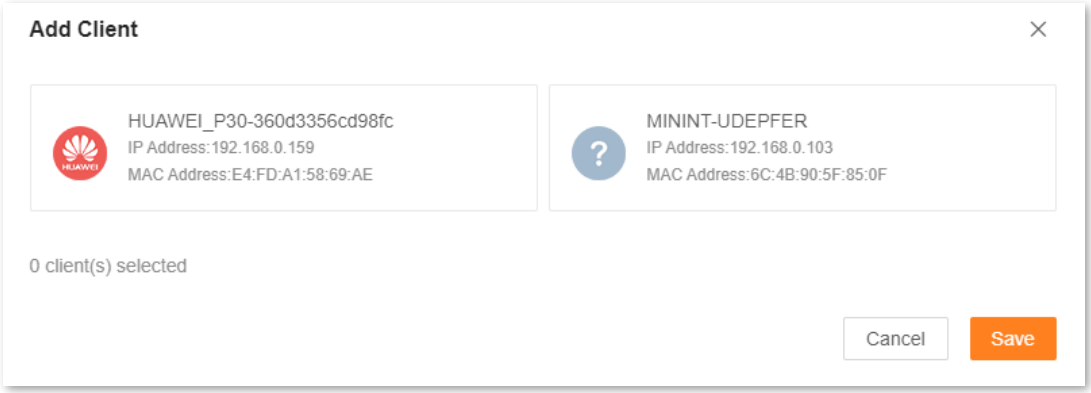
Step 1 Log in to the web UI, and choose **Parental Control**.

Step 2 Click **Add Parental Control Rule** or ⊕.

Step 3 Set **Group Name**, for example, **Parental control rule 1**.

Step 4 Click + beside **Selected clients**.

The following dialog box is displayed.

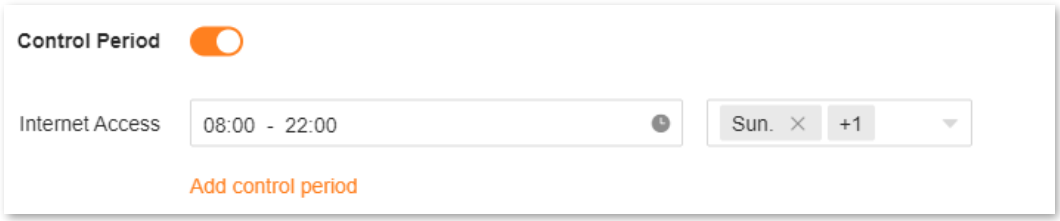


Step 5 Select the clients to which this parental control rule is applied, and click **Save**.

Step 6 Toggle on **Control Period**.

Step 7 Specify the period during which the target websites are blocked, which is 08:00 to 22:00 on weekends in this example.

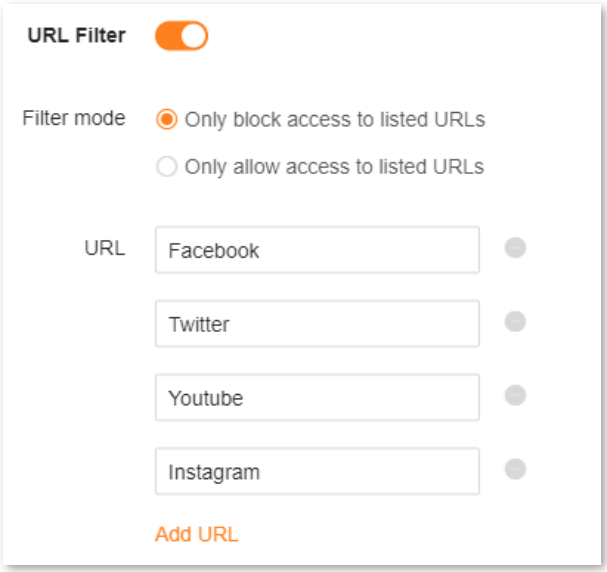
1. Click the left field to set **Start Time** to **08:00** and **End Time** to **22:00**.
2. Select **Sat.** and **Sun.** from the right drop-down list box.



Step 8 Toggle on **URL Filter**.

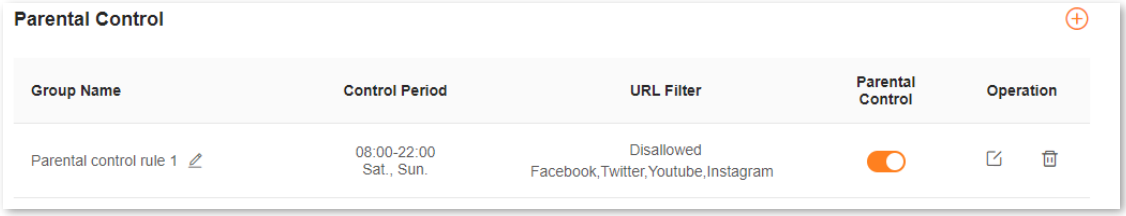
Step 9 Select **Only block access to listed URLs** for **Filter mode**.

Step 10 Enter **Facebook**, **Twitter**, **Youtube**, and **Instagram** for **URL**.



Step 11 Click **Save**.

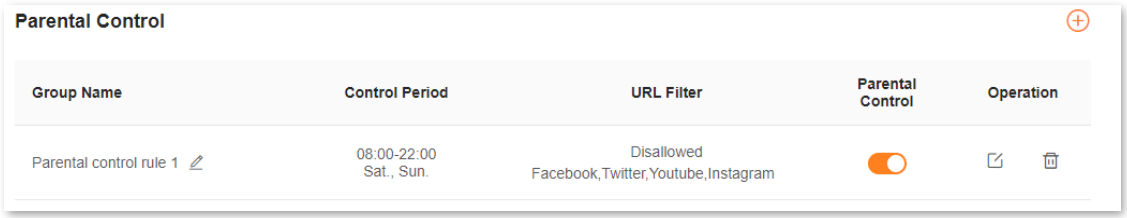
The following page is displayed, and your kid can access any websites except for Facebook, Twitter, Youtube and Instagram from 8:00 to 22:00 on weekends and cannot access the internet at all between 22:00 to 8:00 on weekends.



---End

8.2 Other operations on the parental control rules

By default, a parental control rule is enabled after you added it successfully, as shown in the following figure. You can disable, modify or delete a parental control rule after logging in to the web UI of the router and choosing **Parental Control**.



The following table describes the parameters under **Parental Control**.

Parameter description

Parameter	Description
Group Name	Specifies the name of the client group that the parental control rule applies to. You can change the group name by clicking beside it.
Control Period	Specifies the period during which the parental control rule takes effect.
URL Filter	Specifies the websites that are allowed or disallowed to be accessed by the client group. If **Unlimited** is displayed, website access is not limited.
Parental control	Used to enable or disable the parental control rule.
Operation	The available options include: : Used to edit a parental control rule. : Used to delete a parental control rule.

9 More

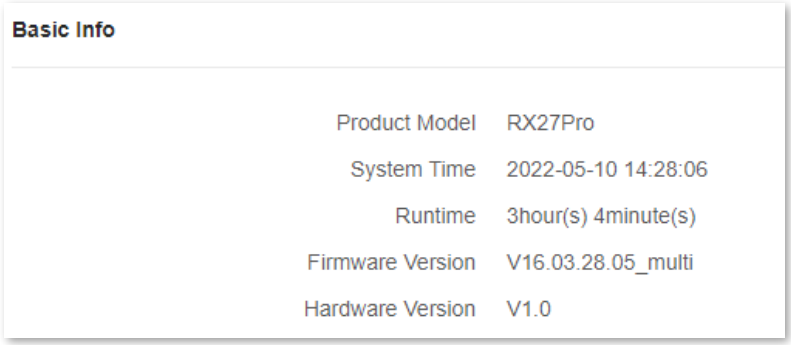
This chapter describes other settings you may need when using the router, including:

9.1 Router information

On this page, you can view the information of the router, including Basic information, WAN port information, LAN information and IPv6 status.

To access the page, log in to the web UI and navigate to **More** > **Router Info**.

9.1.1 Basic information



In this part, you can view basic information about the router, as described in the following table.

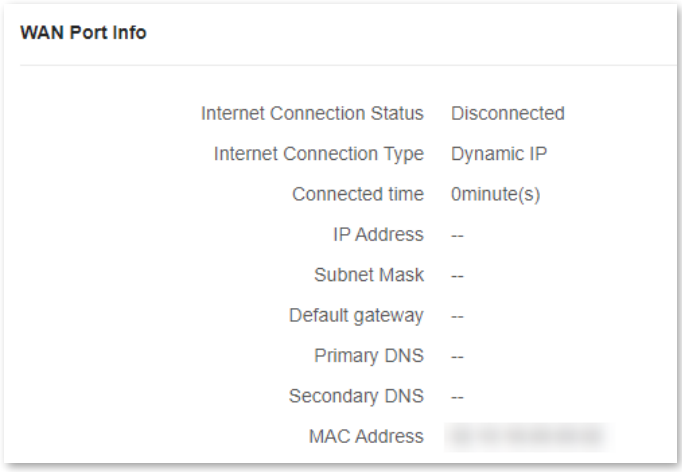
Parameter description

Parameter	Description
Product Model	Specifies the model of the router.
System Time	Specifies the current system time.
Runtime	Specifies the network connection time of the router.
Firmware Version	Specifies the firmware version of the router.
Hardware Version	Specifies the hardware version of the router.

9.1.2 WAN port information

TIP

This part is displayed only in the router mode.

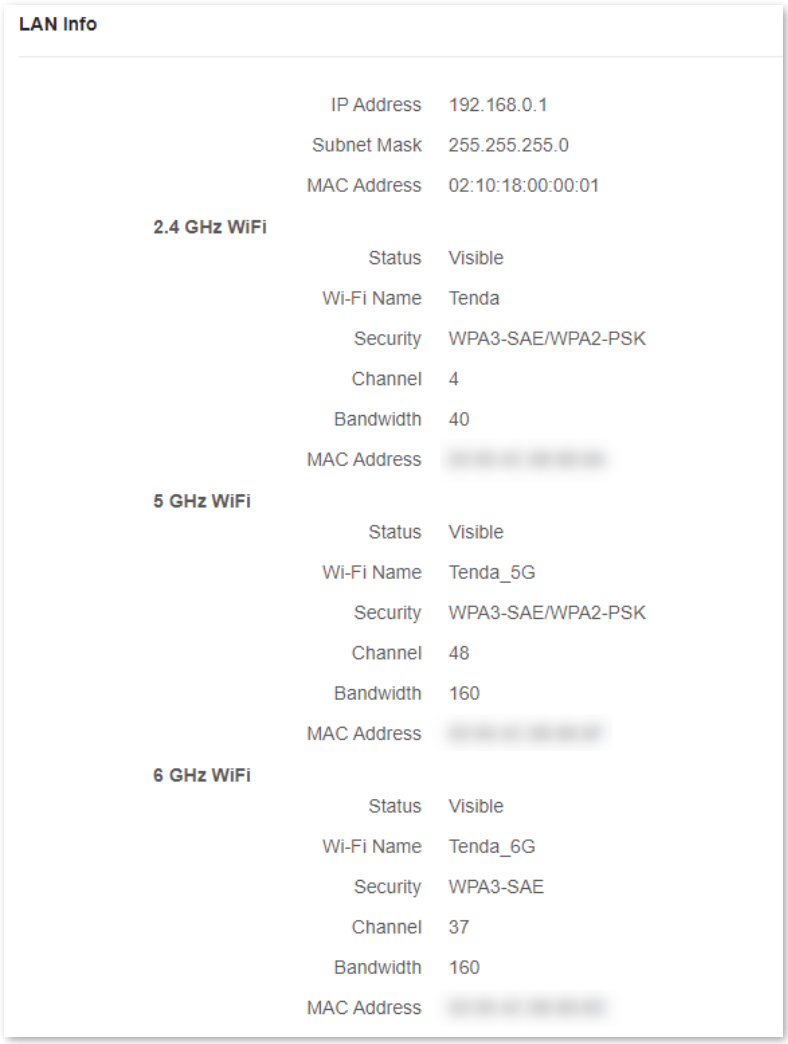


In this part, you can view WAN port information of the router, as described in the following table.

Parameter description

Parameter	Description
Internet Connection Status	Specifies the internet connection status of the WAN port.
Internet Connection Type	Specifies the internet connection type of the WAN port. **PPPoE** is used as an example here.
Connected time	Specifies the internet connection time of the router.
IP Address	Specifies the WAN IP address of the router.
Subnet Mask	Specifies the WAN subnet mask of the router.
Default gateway	Specifies the gateway IP address of the router.
Primary DNS	Specify the IP address of primary and secondary DNS servers of the router.
Secondary DNS	
MAC Address	Specifies the WAN MAC address of the router.

9.1.3 LAN information



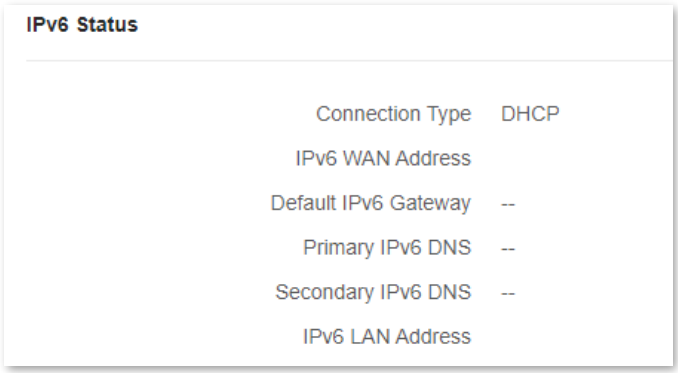
In this part, you can view LAN information of the router, as described in the following table.

Parameter description

Parameter	Description
IP Address	Specifies the LAN IP address of the router, which is also the IP address for logging in to the web UI of the router.
Subnet Mask	Specifies the LAN subnet mask of the router.
MAC Address	Specifies the LAN MAC address of the router.
Status	Specifies the visibility of the Wi-Fi network.
Wi-Fi Name	Specifies the Wi-Fi name of the respective Wi-Fi network.
Security	Specifies the security mode of the respective Wi-Fi network.

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

9.1.4 IPv6 Status



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

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

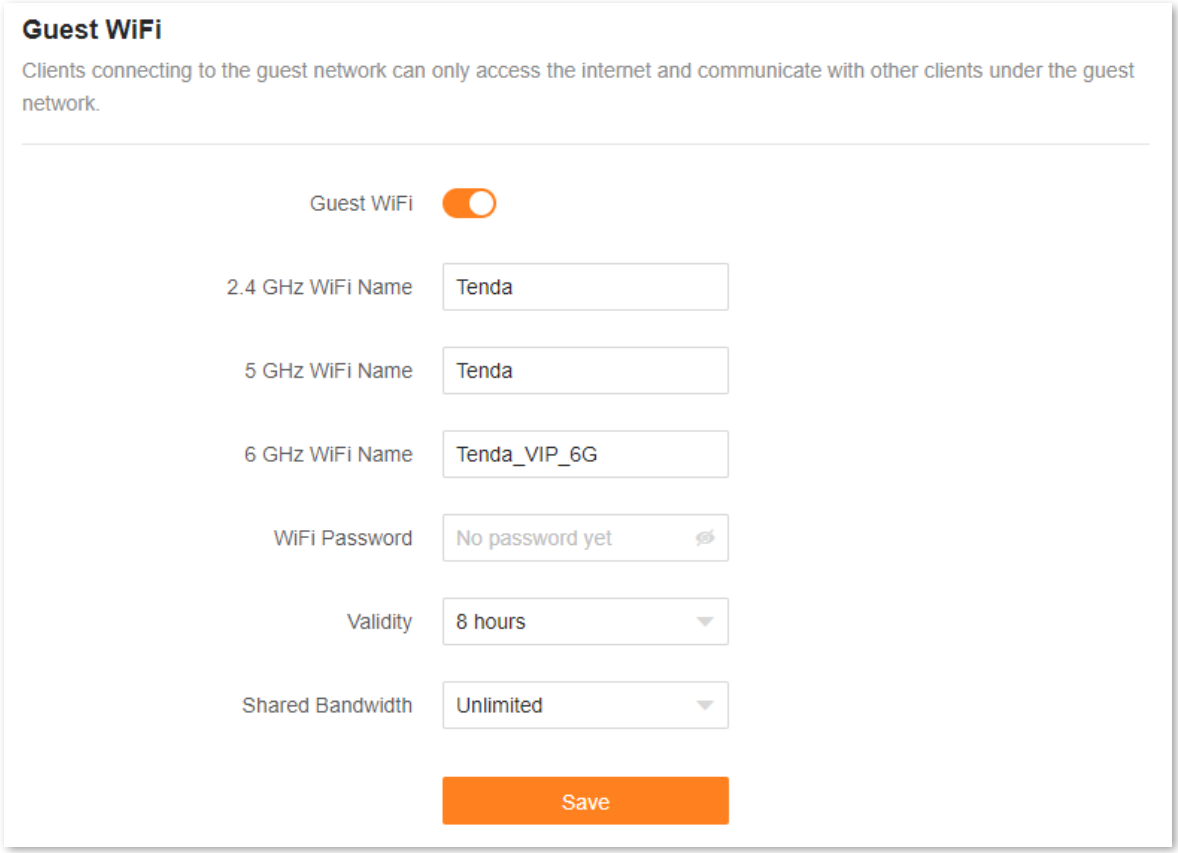
9.2 Guest Wi-Fi

9.2.1 Overview

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

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

To access the configuration page, log in to the web UI of the router and navigate to the **Guest Network**. This function is disabled by default. The following figure shows the **Guest WiFi** page with the **Guest WiFi** function enabled.



Parameter description

Parameter	Description
Guest WiFi	Used to enable or disable the guest network function.
2.4 GHz WiFi Name	Specifies the Wi-Fi name of the router's guest network.
5 GHz WiFi Name	You can change the Wi-Fi names (SSIDs) as required. To distinguish the guest network

Parameter	Description
6 GHz WiFi Name	from the main network, you are recommended to set different Wi-Fi network names.
WiFi Password	Specifies the password for the router's two guest networks. It is optional and can be left blank.
Validity	Specifies the validity period of the guest networks. The guest network function will be disabled automatically out of the validity period.
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**.

9.2.2 An example of configuring the guest network

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

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

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

Assume that:

- Wi-Fi names for 2.4 GHz, 5 GHz and 6 GHz networks: **John_Doe**, **John_Doe_5G** and **John_Doe_6G**.
- Wi-Fi password for 2.4 GHz, 5 GHz and 6 GHz networks: **Tenda+245**.
- The shared bandwidth for guests: **8 Mbps**.

To achieve such a goal:

Step 1 Log in to the web UI.

Step 2 Choose **More** > **Guest WiFi**.

Step 3 Enable **Guest WiFi**.

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

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

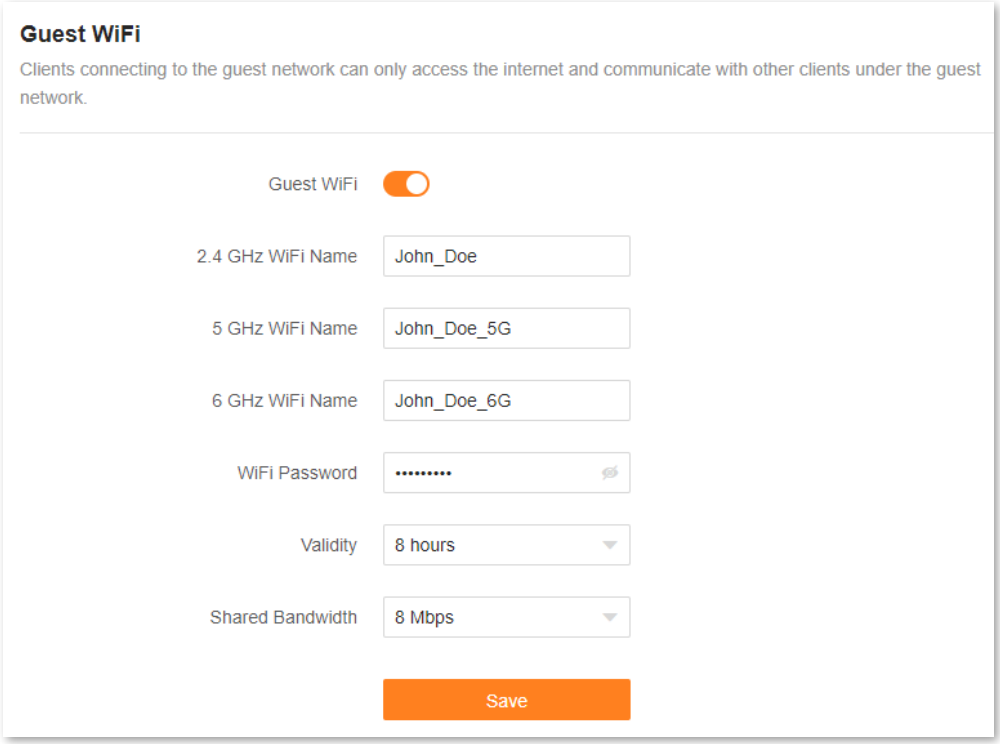
Step 6 Set **6 GHz WiFi Name**, which is **John_Doe_6G** in this example.

Step 7 Set **WiFi Password**, which is **Tenda+245** in this example.

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

Step 9 Set the bandwidth in the **Shared Bandwidth** drop-down box, which is **8 Mbps** in this example.

Step 10 Click **Save**.

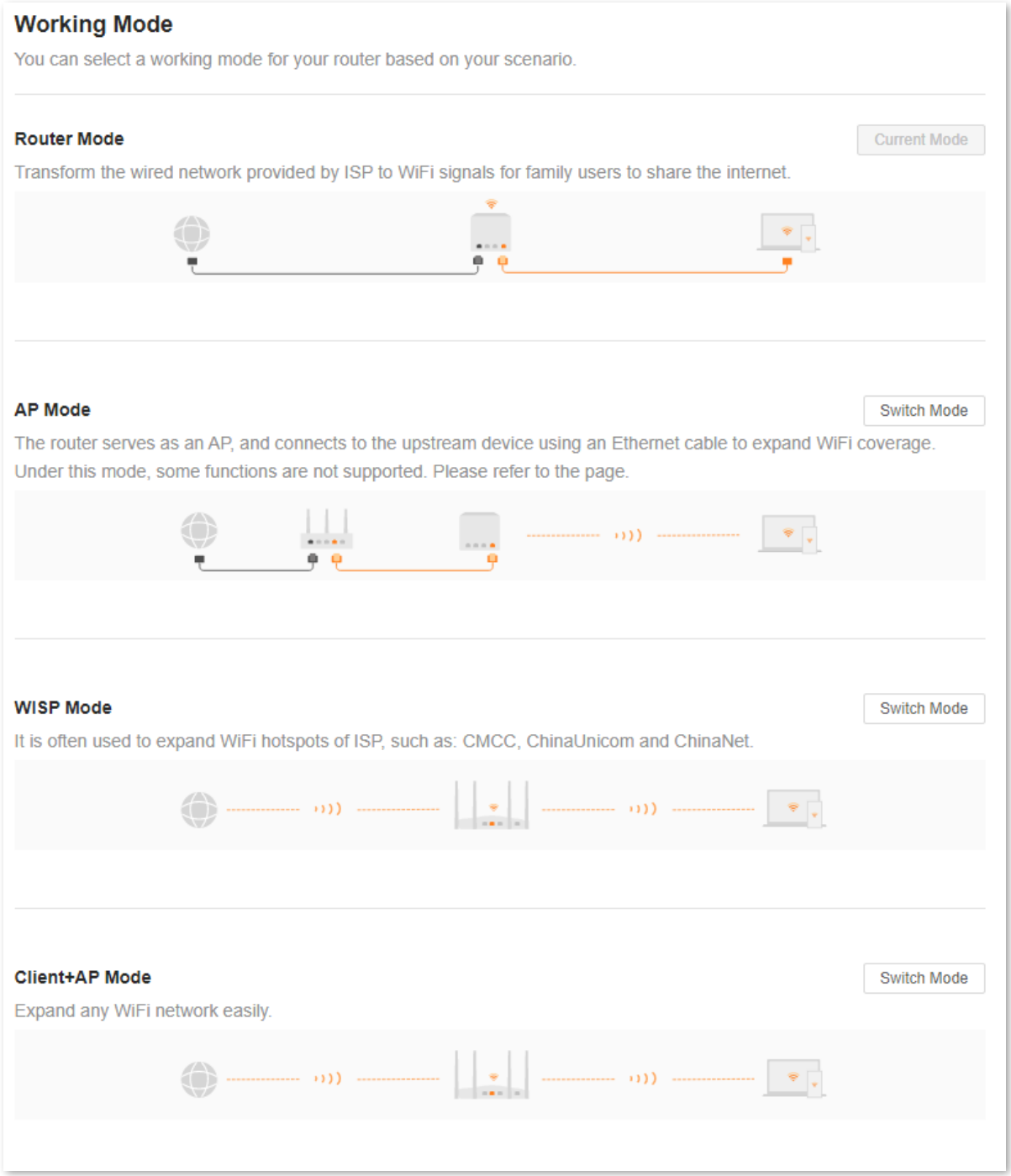


During the 8 hours after the configuration, guests can connect their WiFi-enabled devices, such as smartphones, to **John_Doe**, **John_Doe_5G** or **John_Doe_6G** to access the internet and enjoy the shared bandwidth of 8 Mbps.

---End

9.3 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.

9.3.1 Router mode

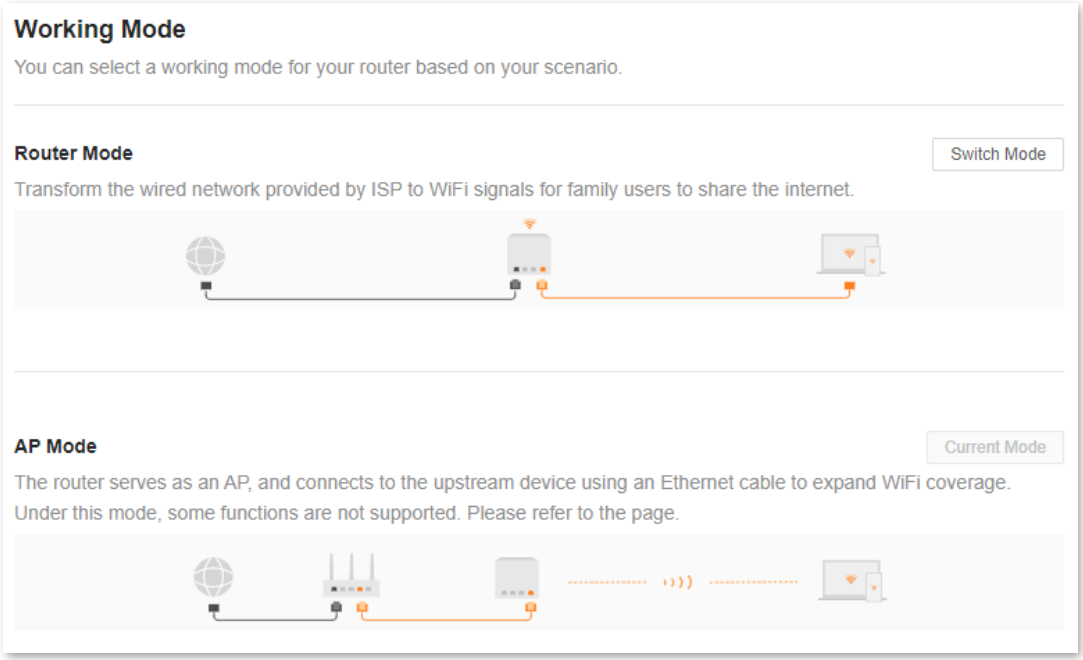
By default, the router works in the router mode. All functions are available in this mode.

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

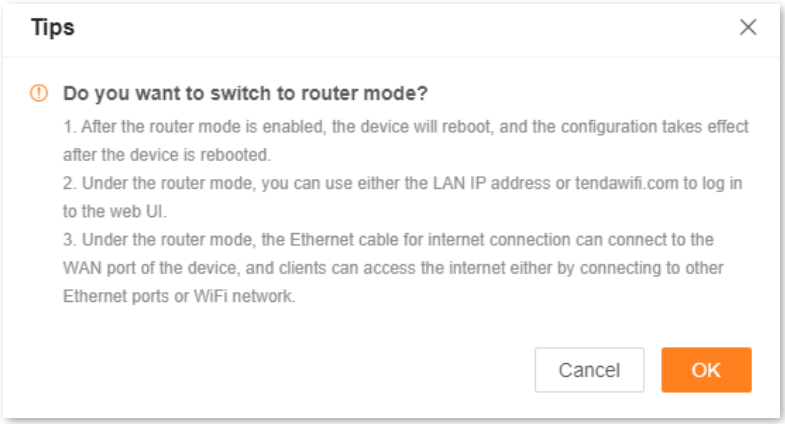
Step 1 Log in to the web UI.

Step 2 Choose **More** > **Working Mode**.

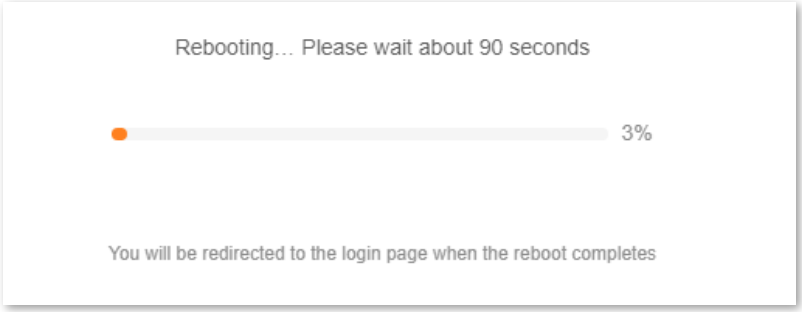
Step 3 Click **Switch mode**.



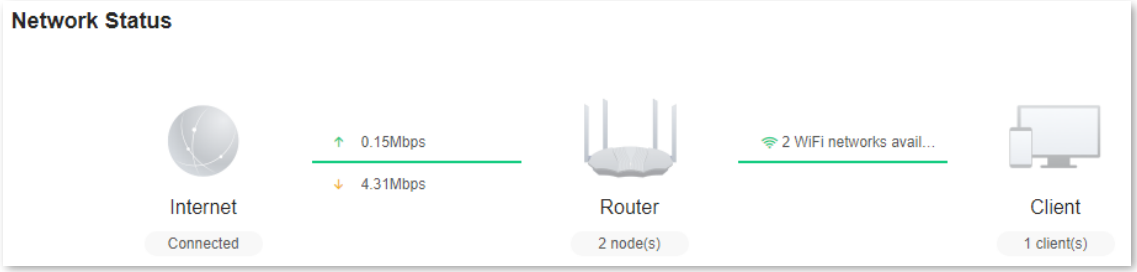
Step 4 Click **OK**.



Step 5 Wait until the device is restarted.



Step 6 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.



---End

9.3.2 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.

TIP

When the router is set to AP mode:

- Every physical port can be used as a LAN port.
- The LAN IP address of the router will be changed. Please log in to the web UI of the router by visiting **tendawifi.com**.
- 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:

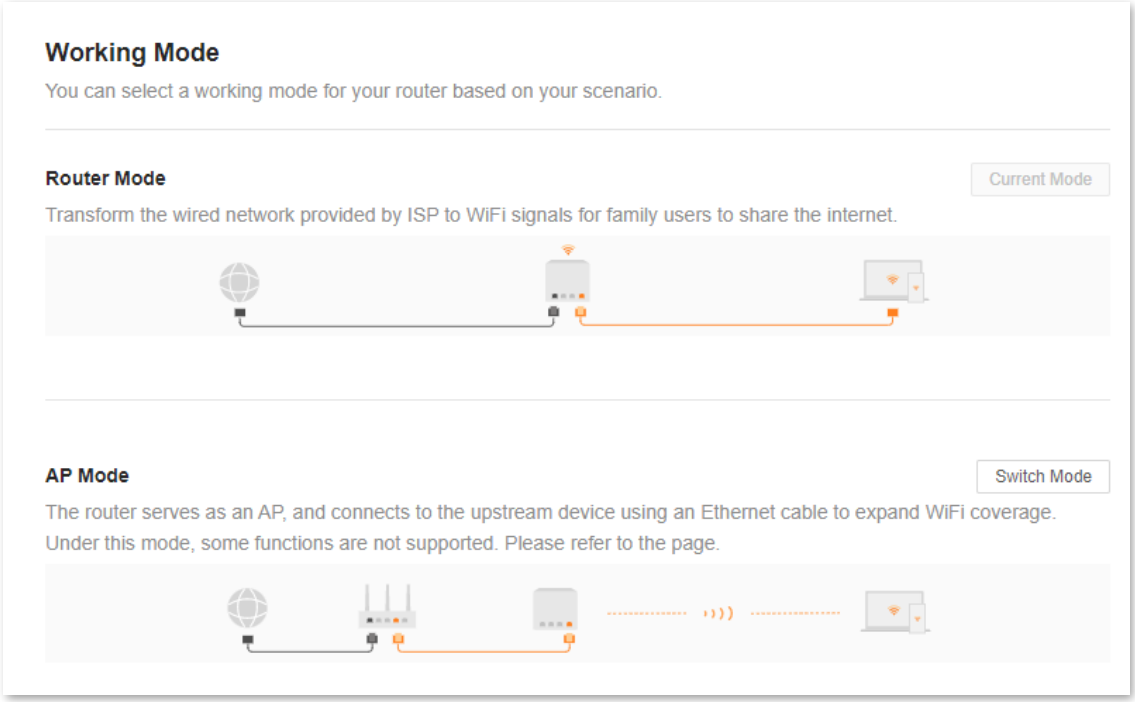
TIP

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**.

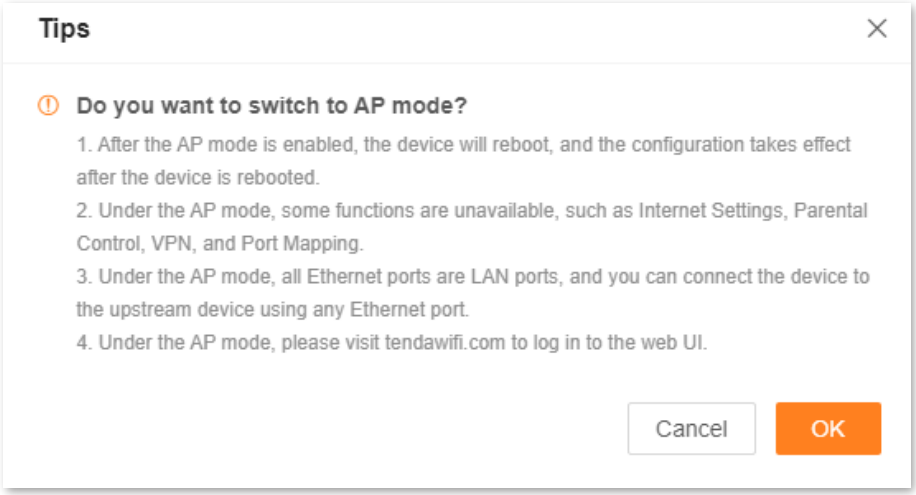
Step 1 Log in to the web UI.

Step 2 Choose **More** > **Working Mode**.

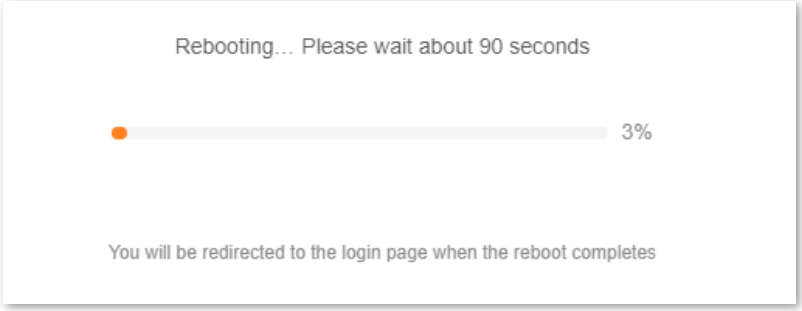
Step 3 Click **Switch mode** after **AP Mode**.



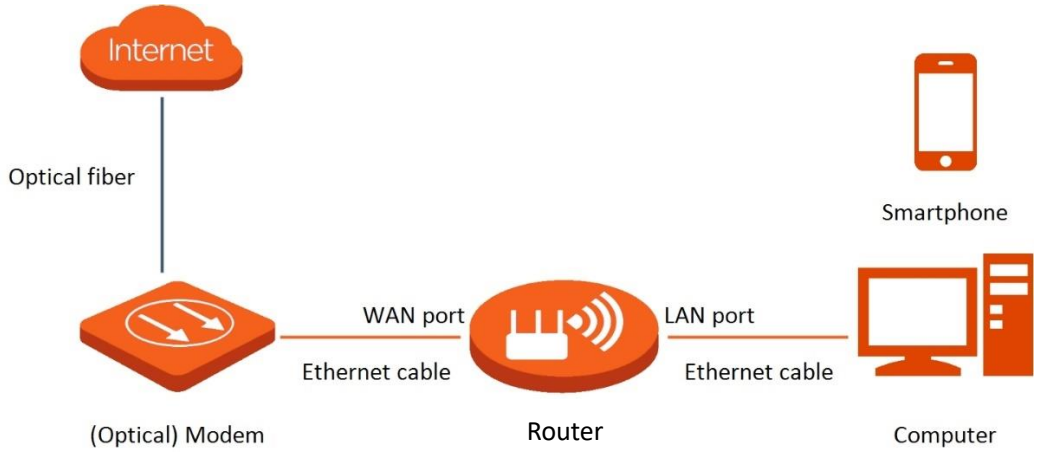
Step 4 Click **OK**.



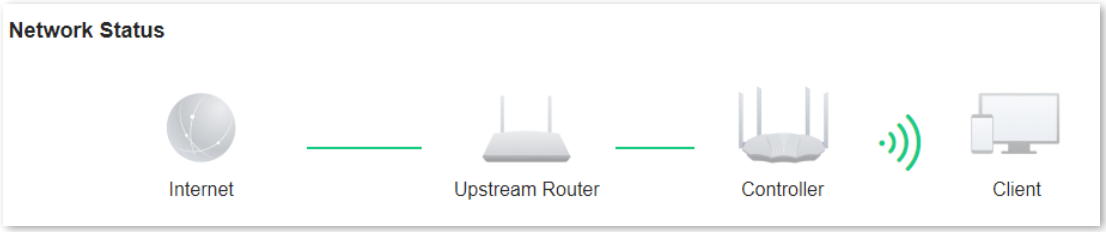
Step 5 Wait until the device is restarted.



Step 6 Connect the upstream device, such as a gateway, to any port of the router.



Step 7 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.



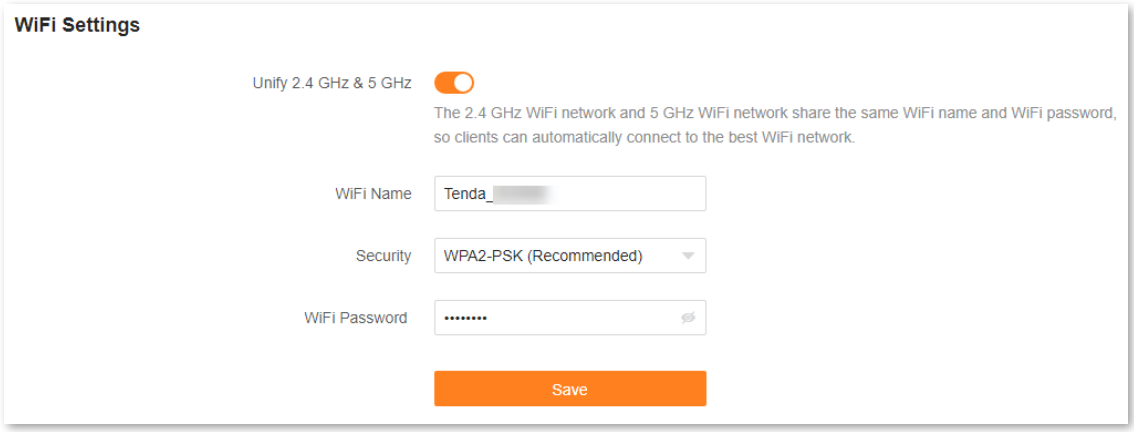
---End

NOTE

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 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 original router is connected to the internet successfully.
- Ensure that your WiFi-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 configured to obtain an IP address and DNS server automatically.

9.3.3 WISP mode

When there is already a router with internet access at your home, you can refer to the configurations in this part to extend the Wi-Fi hotspots of ISP.

To switch the working mode to WISP mode:

TIP

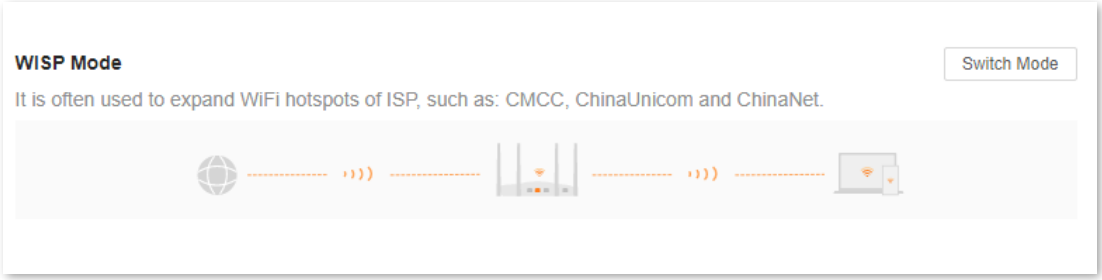
- If you have finished the quick setup wizard before, start a web browser and visit **tendawifi.com** on a connected client, then start from Step 4.
- When WISP mode is chosen and the LAN IP of the router is at the same network segment as that of the upstream device, the router will change the LAN IP address to a different network segment to avoid conflict.
- After the router is set to WISP mode, you are required to access the internet by referring to the configuring procedures in Internet Settings based on the connection type you choose.
- Some functions will be unavailable. Refer to the web UI for available functions.

Step 1 Place the new router near the original router and power it on. Connect your WiFi-enabled device to the Wi-Fi network of your new router, or connect a computer to a LAN port of the router. Do not connect any device to the WAN port of the new router.

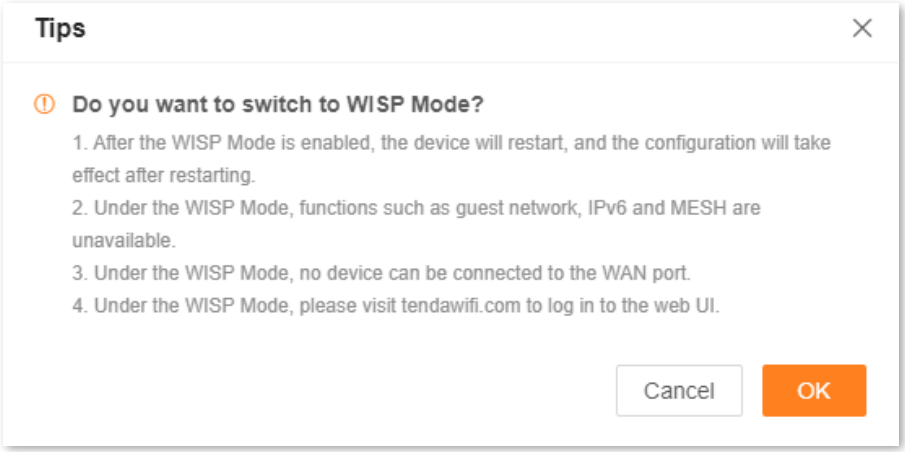
Step 2 Log in to the web UI.

Step 3 Choose **More** > **Working Mode**.

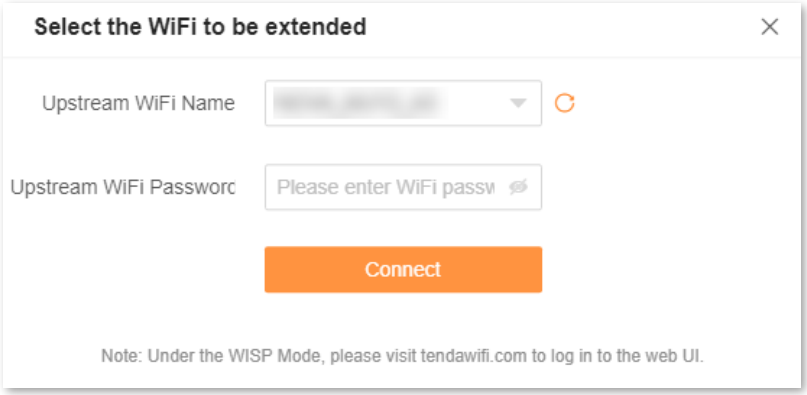
Step 4 Click **Switch mode** after **WISP Mode**.



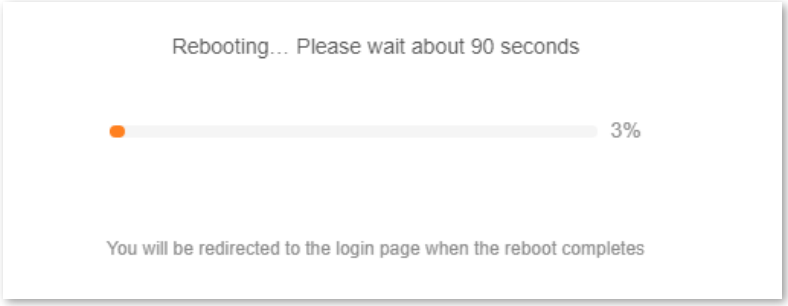
Step 5 Click **OK**.



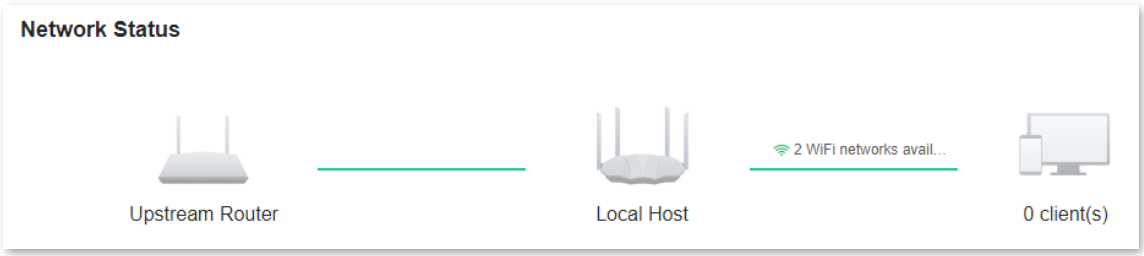
Step 6 Select the Wi-Fi to be extended from the **Upstream WiFi Name** drop-down list box, set **Upstream WiFi Password**, and click **Connect**.



Step 7 Wait until the device is restarted.



Step 8 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.



TIP

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

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

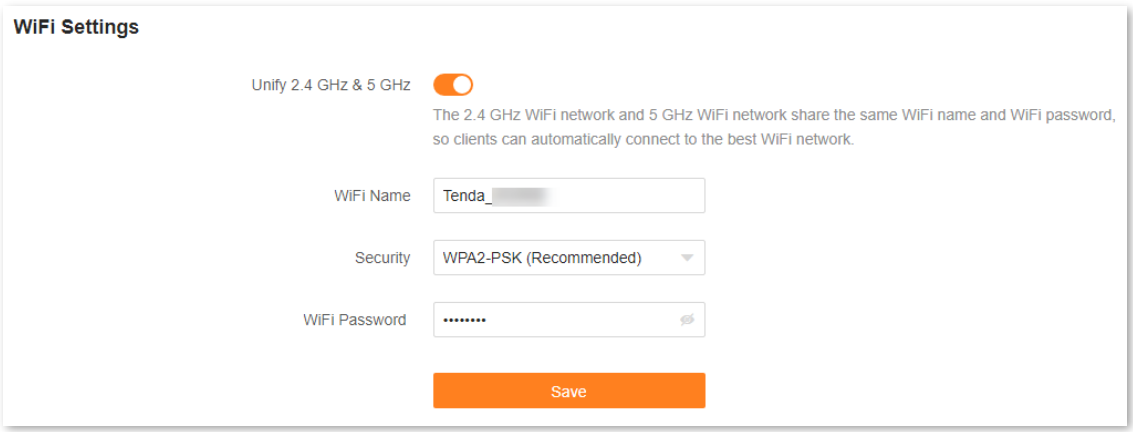
NOTE

Do not connect any device to the WAN port of the new router after setting the router to WISP mode.

---End

To access the internet, connect your computer to a LAN port of the new router, or connect your smart phone 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 original router is connected to the internet successfully.
- Ensure that your WiFi-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 configured to obtain an IP address and DNS sever automatically.

9.3.4 Client+AP mode

When there is already a router with internet access at your home, you can refer to the configurations in this part to extend any type of Wi-Fi network.

To switch the working mode to WISP mode:

TIP

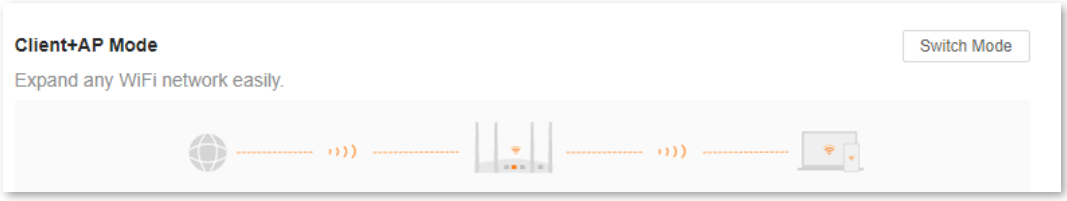
- Some functions will be unavailable. Refer to the web UI for available functions.
- If you have finished the quick setup wizard before, start a web browser and visit **tendawifi.com** on a connected client, then start from Step 4.

Step 1 Place the new router near the original router and power it on. Connect your WiFi-enabled device to the Wi-Fi network of your new router, or connect a computer to a LAN port of the router. Do not connect any device to the WAN port of the new router.

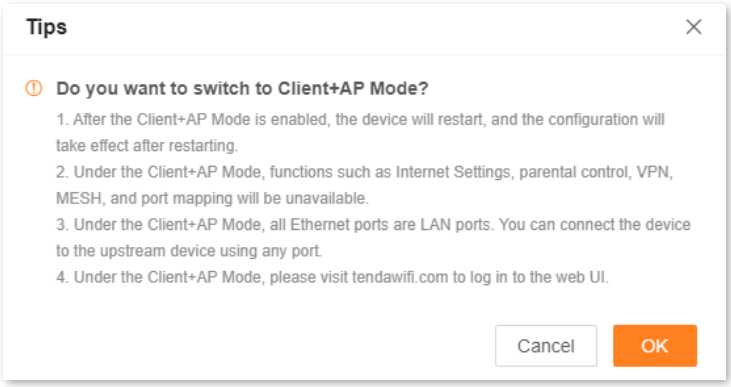
Step 2 Log in to the web UI.

Step 3 Choose **More** > **Working Mode**.

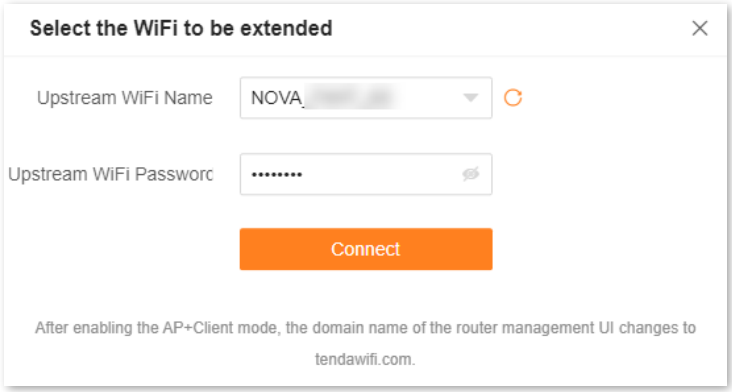
Step 4 Click **Switch mode** after **Client+AP Mode**.



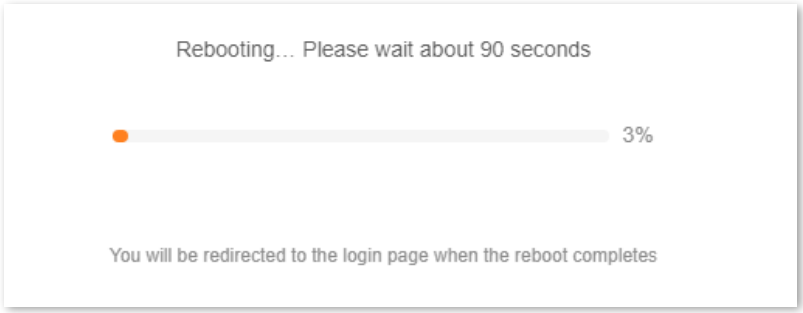
Step 5 Click **OK**.



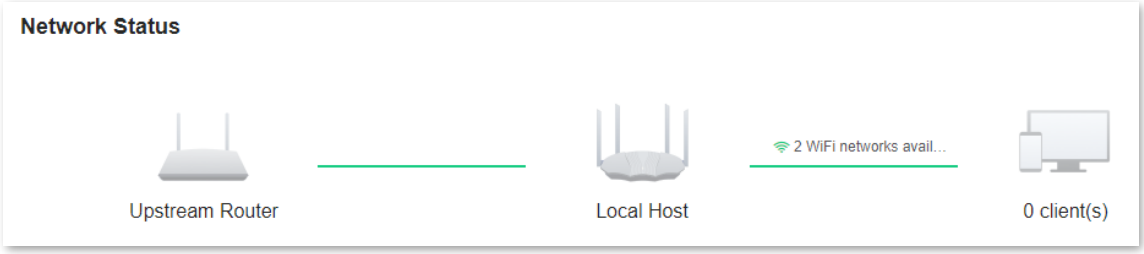
Step 6 Select the Wi-Fi to be extended from the **Upstream WiFi Name** drop-down list box, set **Upstream WiFi Password**, and click **Connect**.



Step 7 Wait until the device is restarted.



Step 8 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.



TIP

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

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

NOTE

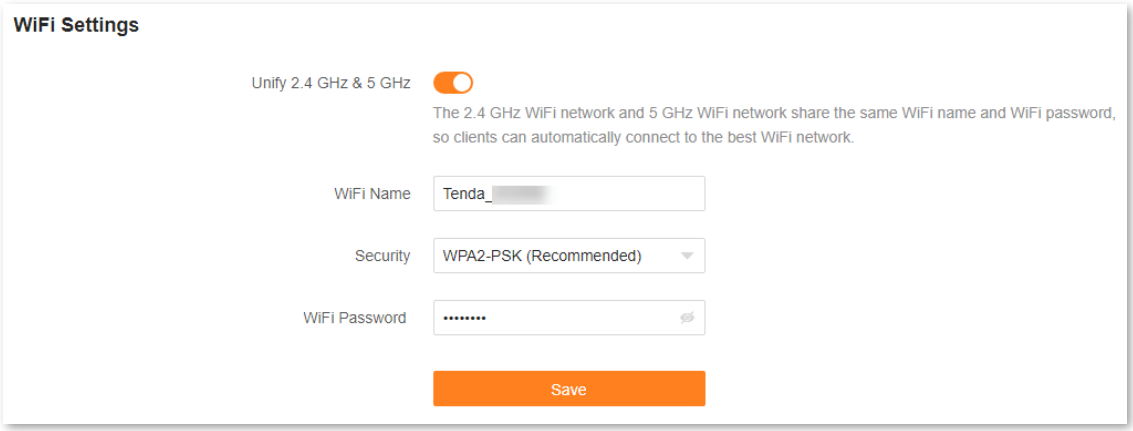
After the new router is set to Client+AP mode:

- Do not connect any device to the WAN port of the new router.
- The LAN IP address of the router will change. Please log in to the web UI of the router by visiting **tendawifi.com**. 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.

---End

To access the internet, connect your computer to a LAN port of the new router, or connect your smart phone to the WiFi network of the new router.

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



TIP

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

- Ensure that the original router is connected to the internet successfully.
- Ensure that your WiFi-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 configured to obtain an IP address and DNS sever automatically.

9.4 IPv6

TIP

This function is only available in the router mode.

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

Scenario	Connection Type
• 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

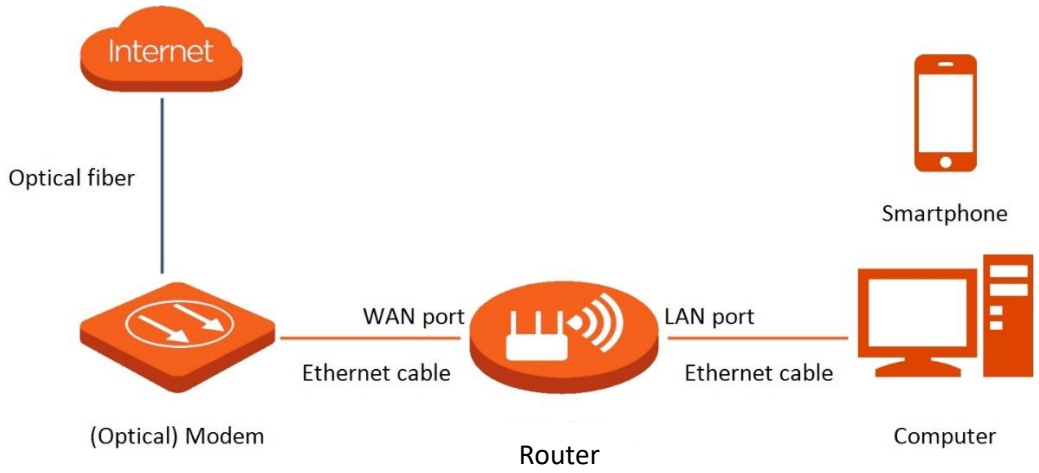
TIP

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.

9.4.1 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.



Configuration procedure:

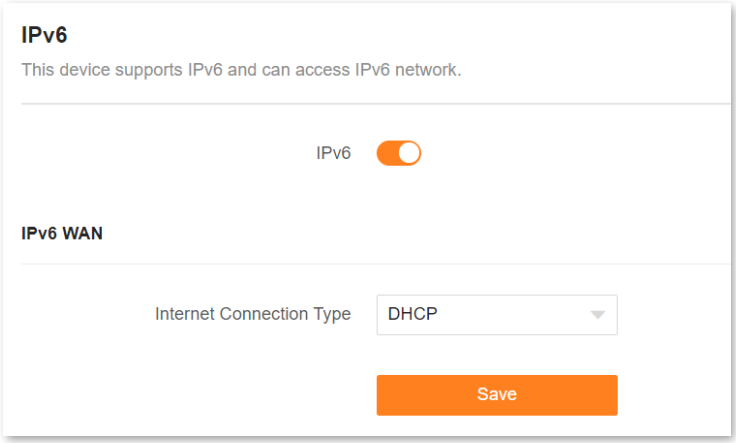
Step 1 Log in to the web UI.

Step 2 Choose **More** > **IPv6**.

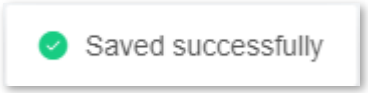
Step 3 Enable the **IPv6** function.

Step 4 Set **Internet Connection Type** to **DHCP**.

Step 5 Click **Save**.



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

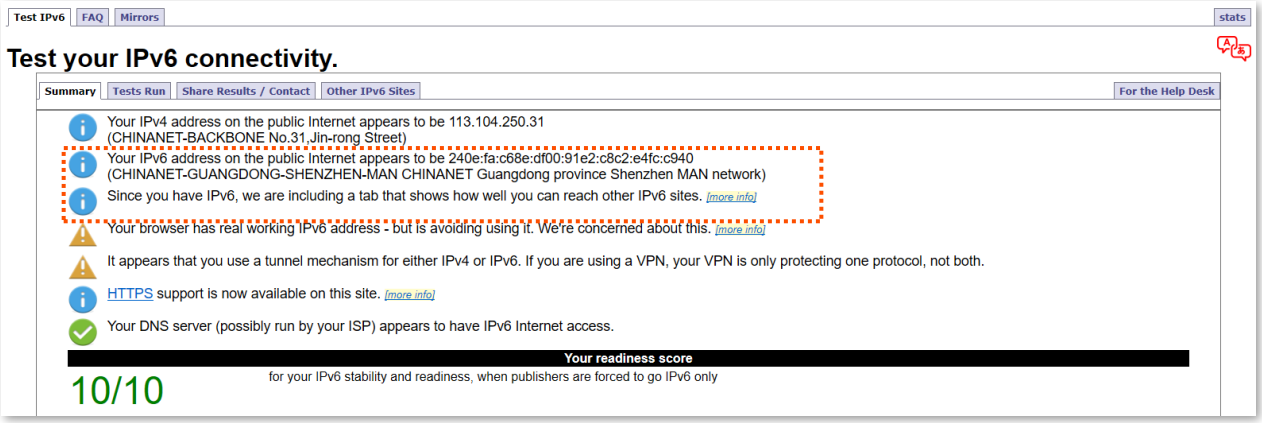


---End

IPv6 network test:

Start a web browser on a phone or a computer that is connected to the router, and visit **test-ipv6.com**. The website will test your IPv6 connection status.

When “You have IPv6” is shown on the page, it indicates that the configuration succeeded and you can access IPv6 services.

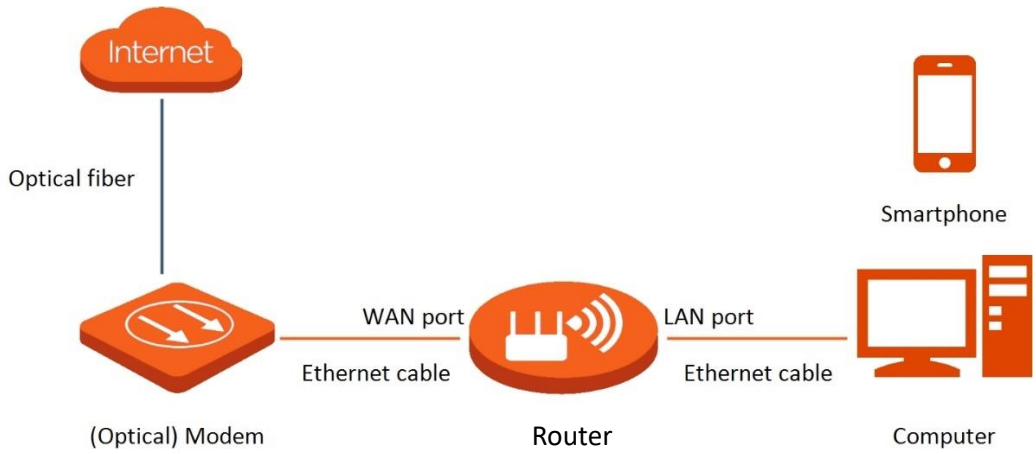


If the IPv6 network test fails, try the following solutions:

- Ensure that clients connected to the router obtain their IPv6 address through DHCPv6.
- Consult your ISP for help.

9.4.2 PPPoEv6

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



Configuration procedure:

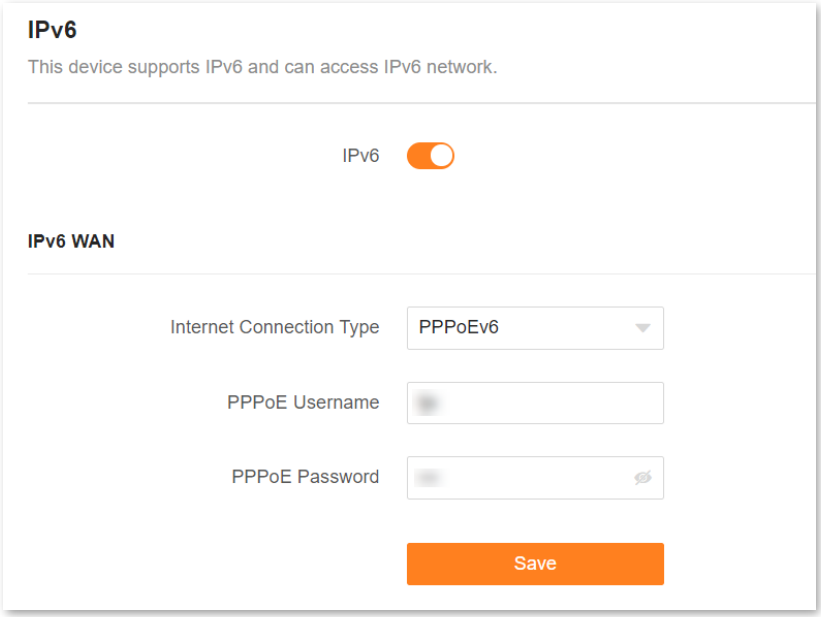
Step 1 Log in to the web UI.

Step 2 Choose **More** > **IPv6**.

Step 3 Enable the **IPv6** function.

Step 4 Set **Internet Connection Type** to **PPPoEv6**.

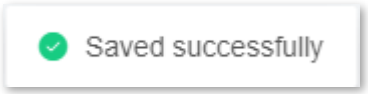
Step 5 Set **PPPoE Username** and **PPPoE Password**, and click **Save**.



Parameter description

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

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

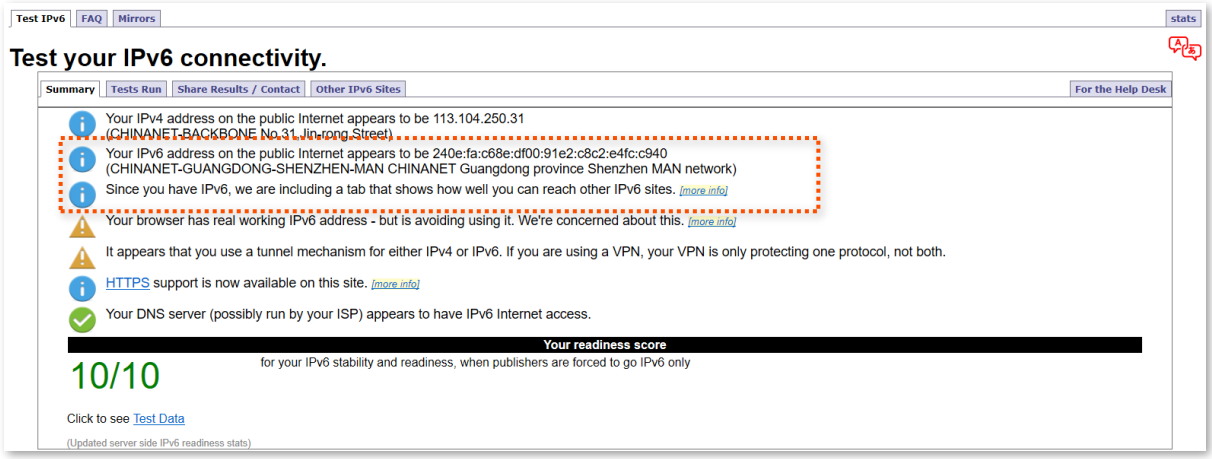


---End

IPv6 network test:

Start a web browser on a phone or a computer that is connected to the router, and visit **test-ipv6.com**. The website will test your IPv6 connection status.

When “You have IPv6” is shown on the page, it indicates that the configuration succeeded and you can access IPv6 services.



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

- Ensure that clients connected to the router obtain their IPv6 address through PPPoEv6.
- Consult your ISP for help.

9.4.3 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.

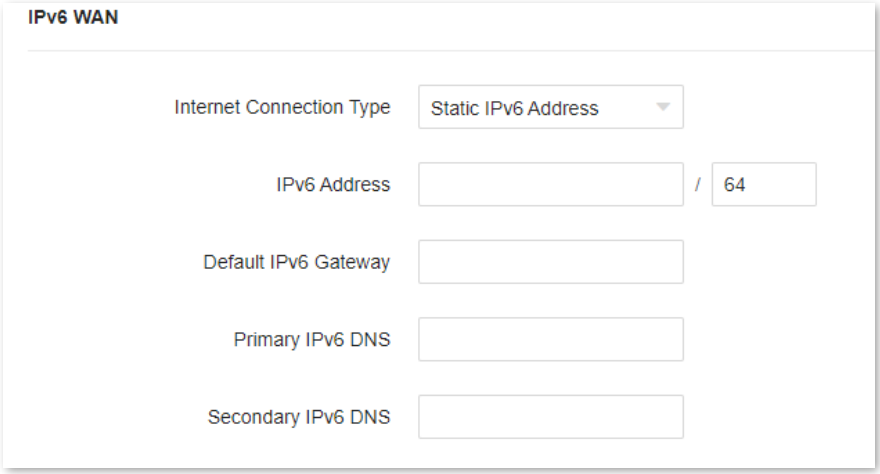
Step 2 Choose **More** > **IPv6**.

Step 3 Enable the **IPv6** function.

Step 4 Set the **Connection Type** to **Static IPv6 Address**.

Step 5 Enter the required parameters under **IPv6 WAN**.

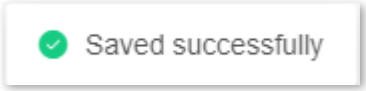
Step 6 Click **Save**.



Parameter description

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

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

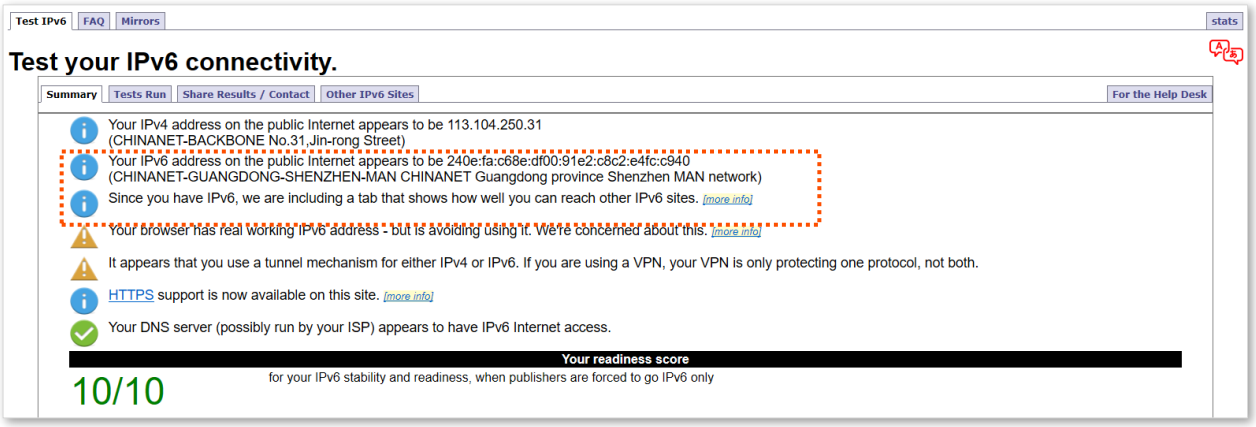


---End

IPv6 network test:

Start a web browser on a phone or a computer that is connected to the router, and visit **test-ipv6.com**. The website will test your IPv6 connection status.

When “You have IPv6” is shown on the page, it indicates that the configuration succeeded and you can access IPv6 services.



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

- Ensure that you have entered the correct WAN IPv6 address.
- Ensure that clients connected to the router obtain their IPv6 address through DHCPv6.
- Consult your ISP for help.

9.5 Network diagnosis

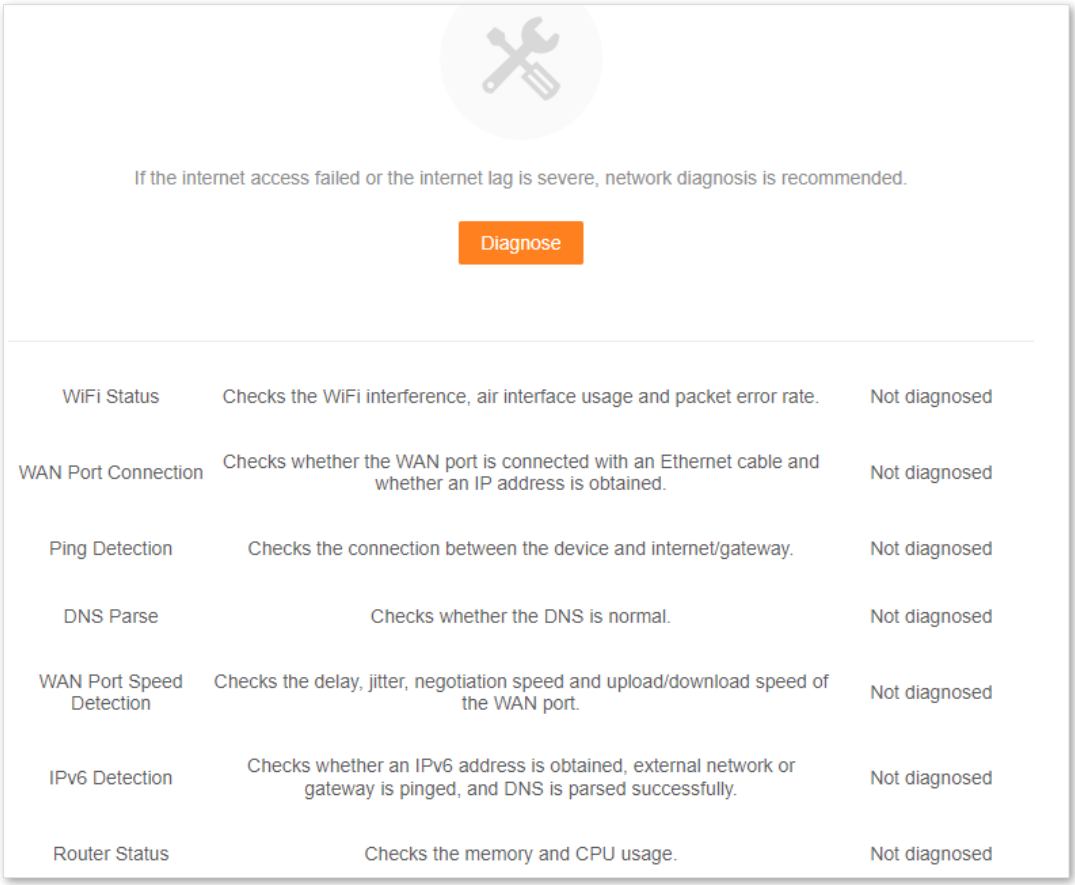
If the network fails or the internet lag is severe, you can choose **More** > **Network Diagnosis** to troubleshoot the fault.

To perform troubleshooting:

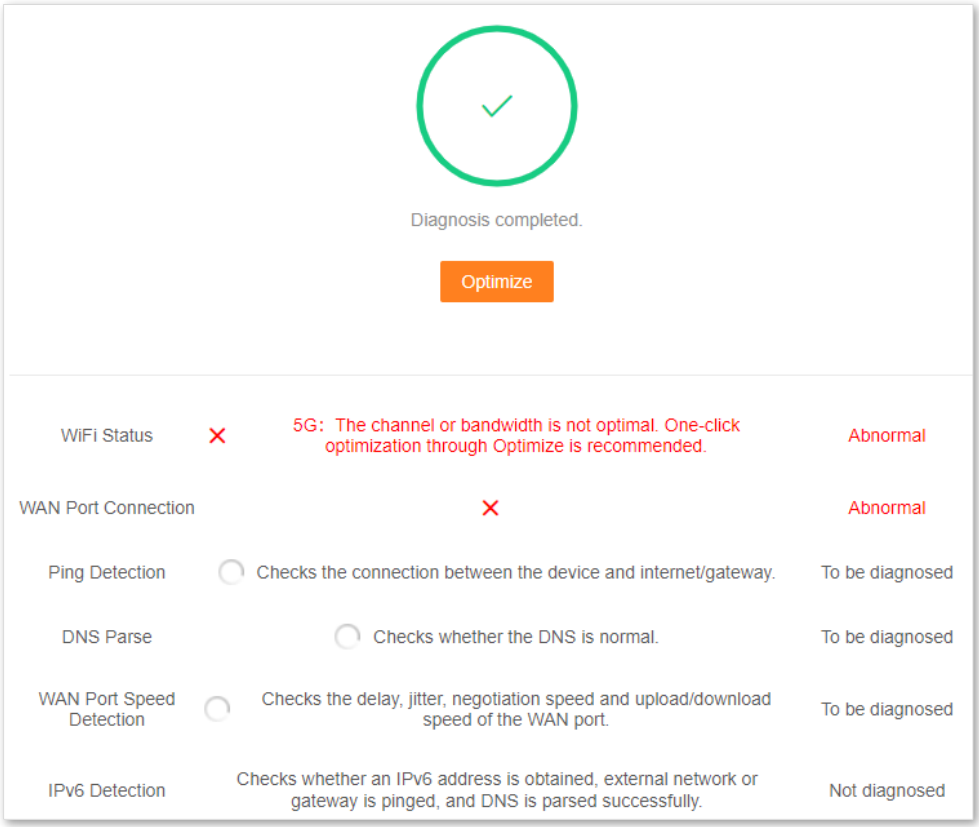
Step 1 Log in to the web UI.

Step 2 Choose **More** > **Network Diagnosis**.

Step 3 Click **Diagnose**.



Step 4 Check the diagnosis result and click **Optimize** to rectify the faults.

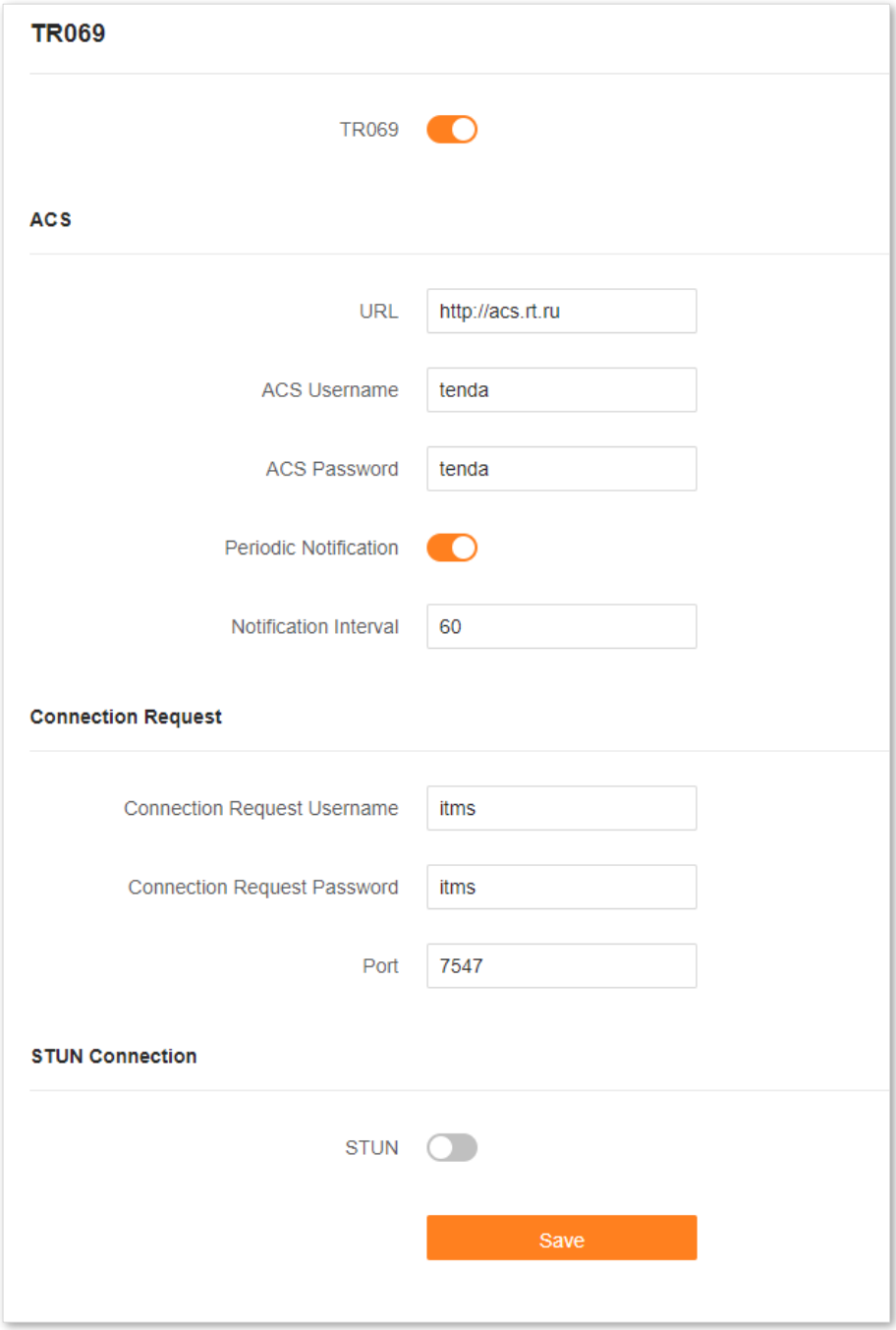


---End

9.6 TR069

The CPE WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) from the internet to perform auto-configuration, provision, collection, and diagnostics to the router. This function is disabled by default, and you can enable it as required.

To access the configuration page, log in to the web UI of the router and choose **More** > **TR069**.



The following table describes the parameters displayed on this page.

Parameter description

Parameter		Description
TR069		Used to enable or disable the TR069 function.
ACS	URL	Specifies the domain name of the ACS.
	ACS Username	Specifies the user name used to authenticate the router when the router connects to the ACS using the CPE WAN management protocol.
	ACS Password	Specifies the password used to authenticate the router when the router connects to the ACS using the CPE WAN management protocol.
	Periodic Notification	Used to enable/disable the router to periodically inform the ACS.
	Notification Interval	Specifies the interval at which the router sends messages to inform the ACS.
Connection Request	Connection Request Username	Specifies the user name used to authenticate the ACS when it sends the connection request to the router.
	Connection Request Password	Specifies the password used to authenticate the ACS when it sends the connection request to the router.
	Port	Specifies the port used to receive the connection request sent by the ACS.
STUN Connection	STUN	Used to enable or disable the STUN function, which facilitates the communication between the router and the public network when the router is under a LAN.
	STUN Server Address	Specifies the IP address of the STUN server.
	STUN Server Port	Specifies the port of the STUN server.

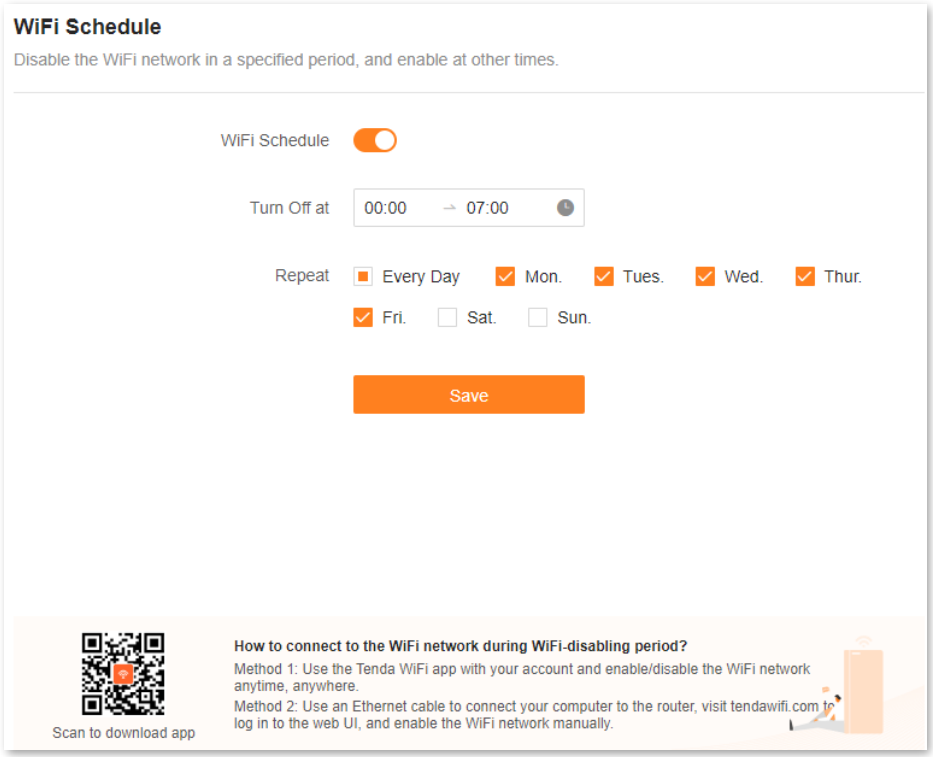
9.7 Smart power saving

9.7.1 WiFi schedule

Overview

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

To access the configuration page, log in to the web UI of the router, and choose **More** > **Smart Power Saving** > **WiFi Schedule**. The following figure displays the page when the WiFi Schedule function is enabled.



TIP

To make the WiFi schedule work properly, please ensure the system time is synchronized with the internet time. Refer to System time for configuration.

The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
WiFi Schedule	Specifies whether to enable or disable the WiFi Schedule function.
Turn Off at	Specifies the period during which the Wi-Fi networks are disabled.

Parameter	Description
Repeat	Specifies the days on which the Wi-Fi networks are disabled during the specified period.

Set a WiFi schedule

Assume that you want to disable the Wi-Fi networks from 22:00 to 7:00 every day.

Configuration procedure:

Step 5 Log in to the web UI.

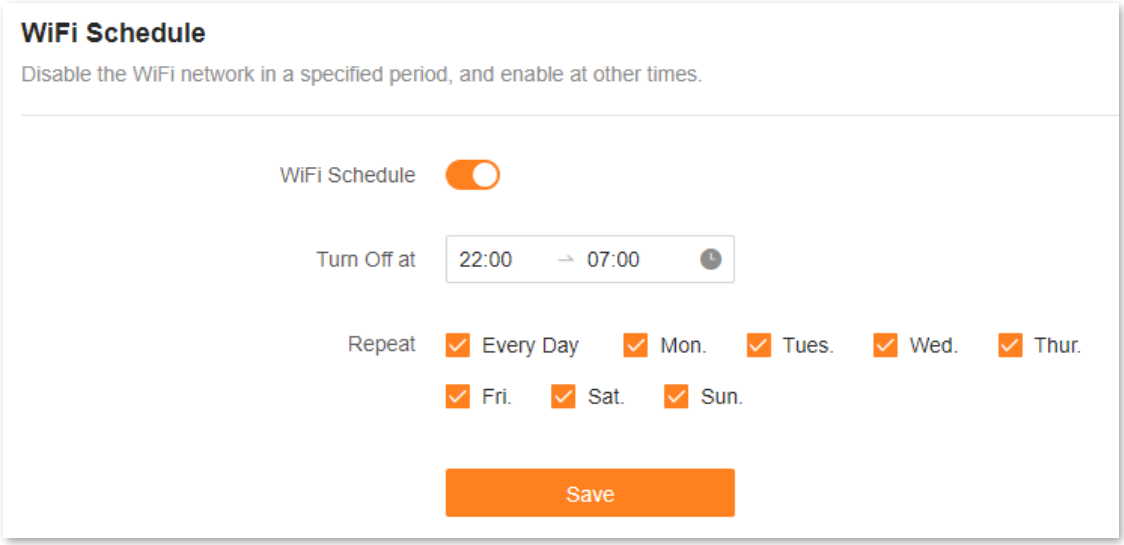
Step 6 Choose **More** > **Smart Power Saving** > **WiFi Schedule**.

Step 7 Enable **WiFi Schedule.**

Step 8 Set a period for the Wi-Fi networks to be disabled, which is **22:00 – 07:00** in this example.

Step 9 Set the days when the function works, which is **Every Day** in this example.

Step 10 Click **Save**.



---End

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

9.7.2 LED Indicator

You can turn off the LED indicators of all nodes as required to save power. By default, all the indicators are turned on.

TIP

Turn on/off all indicators prevails to this operation.

To configure the power saving mode:

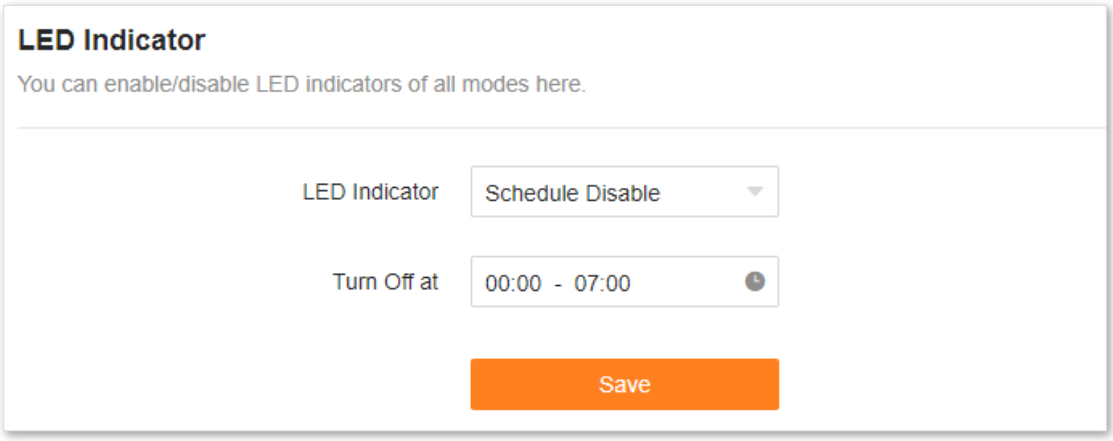
Step 1 Log in to the web UI.

Step 2 Choose **More** > **Smart Power Saving** > **LED Indicator**.

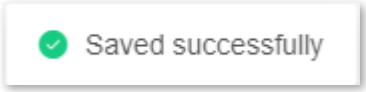
Step 3 Set **LED Indicator** as required.

- To turn on all indicators, select **Enable**.
- To turn off all indicators all the time, select **Disable**.
- To turn off all indicators in a specific period, select **Schedule Disable** and set **Turn Off at** to the required period.

Step 4 Click **Save**.



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



---End

9.8 Advanced Wi-Fi settings

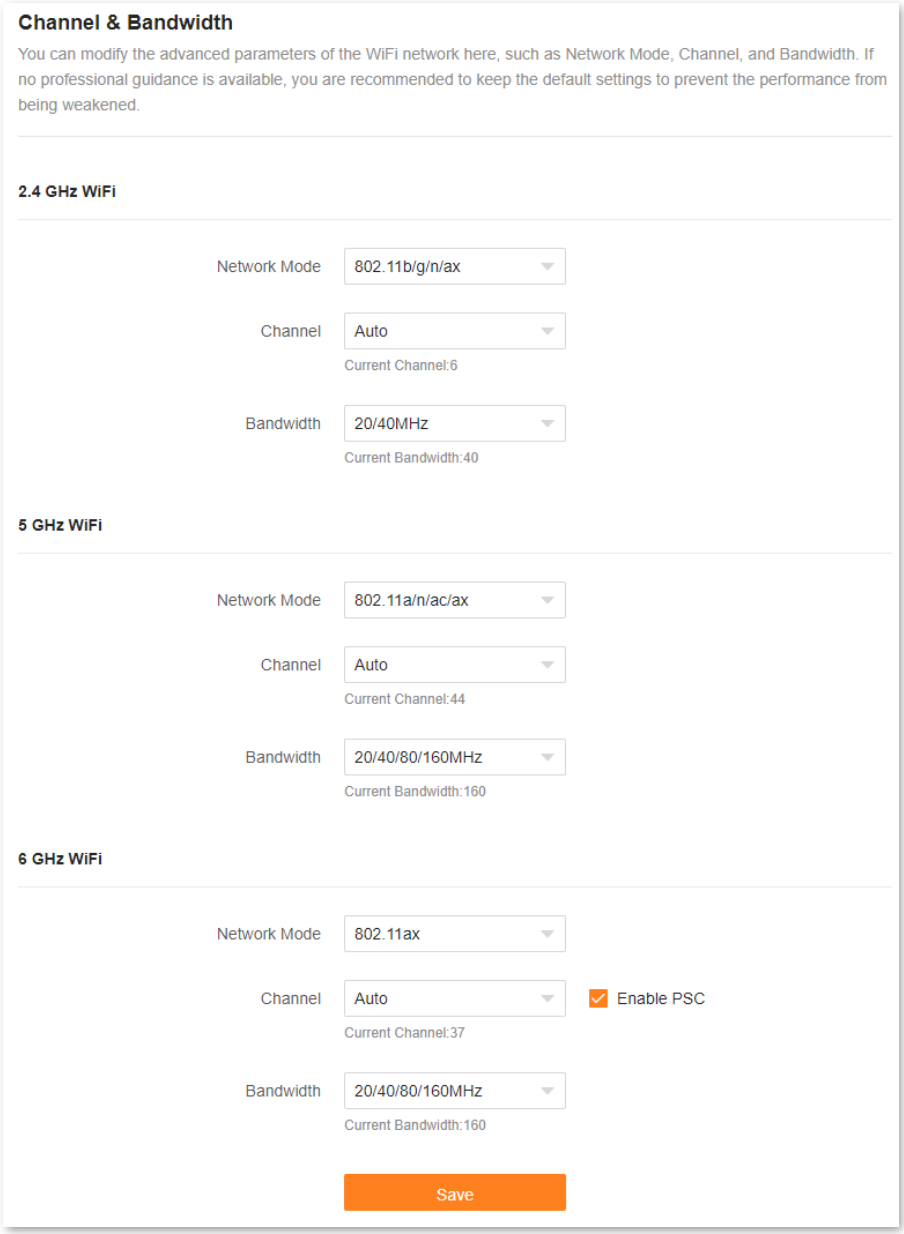
9.8.1 Channel & bandwidth

In this section, you are allowed to change the network mode, Wi-Fi channel, and Wi-Fi bandwidth of 2.4 GHz, 5 GHz and 6 GHz Wi-Fi networks.

To access the configuration page, log in to the web UI of the router, and choose **More** > **WiFi Settings** > **Channel & Bandwidth**.

TIP

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



The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
Network Mode	Specifies various protocols used for wireless transmission. 2.4 GHz Wi-Fi network supports the 802.11b/g/n Mixed and 802.11b/g/n/ax Mixed modes. • **802.11b/g/n**: Indicates that devices compliant with the IEEE 802.11b or IEEE 802.11g protocol, and devices working at 2.4 GHz and compliant with the IEEE 802.11n can connect to the 2.4 GHz Wi-Fi network of the router. • **802.11b/g/n/ax**: Indicates that devices compliant with the IEEE 802.11b or IEEE 802.11g protocol, and devices working at 2.4 GHz and compliant with the IEEE 802.11n or IEEE 802.11ax protocol can connect to the 2.4 GHz Wi-Fi network of the router. 5 GHz Wi-Fi network supports the 802.11a/n Mixed, 802.11a/n/ac Mixed and 802.11a/n/ac/ax Mixed modes. • **802.11a/n**: Indicates that devices compliant with the IEEE 802.11a protocol, and devices working at 5 GHz and compliant with the IEEE 802.11n can connect to the router. • **802.11a/n/ac**: Indicates that devices compliant with the IEEE 802.11a or IEEE 802.11ac protocol, and devices working at 5 GHz and compliant with the IEEE 802.11n can connect to the router. • **802.11a/n/ac/ax**: Indicates that devices compliant with the IEEE 802.11a or IEEE 802.11ac protocol, and devices working at 5 GHz and compliant with the IEEE 802.11n or IEEE 802.11ax protocol can connect to the router. 6 GHz Wi-Fi network supports the 802.11ax mode. • **802.11ax**: Indicates that devices working at 6 GHz and compliant with the IEEE 802.11ax can connect to the router.
Channel	Specifies the channel in which the Wi-Fi network works. By default, the wireless channel is **Auto**, which indicates that the router selects a channel for the Wi-Fi network automatically. You are recommended to choose a channel with less interference for better wireless transmission efficiency. You can use a third-party tool to scan the Wi-Fi signals nearby to understand the channel usage situations.

Parameter	Description
Bandwidth	Specifies the bandwidth of the wireless channel of a Wi-Fi network. Please change the default settings only when necessary. • **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.
Enable PSC	Specifies whether the Preferred Scanning Channel (PSC) function is enabled. When it is enabled, the success rate and stability of Wi-Fi 6E wireless terminals connecting to the router's 6 GHz network will be improved. It is enabled by default.

9.8.2 WPS

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

To access the configuration page, log in to the web UI of the router, and choose **WiFi Settings** > **WPS**.

TIP

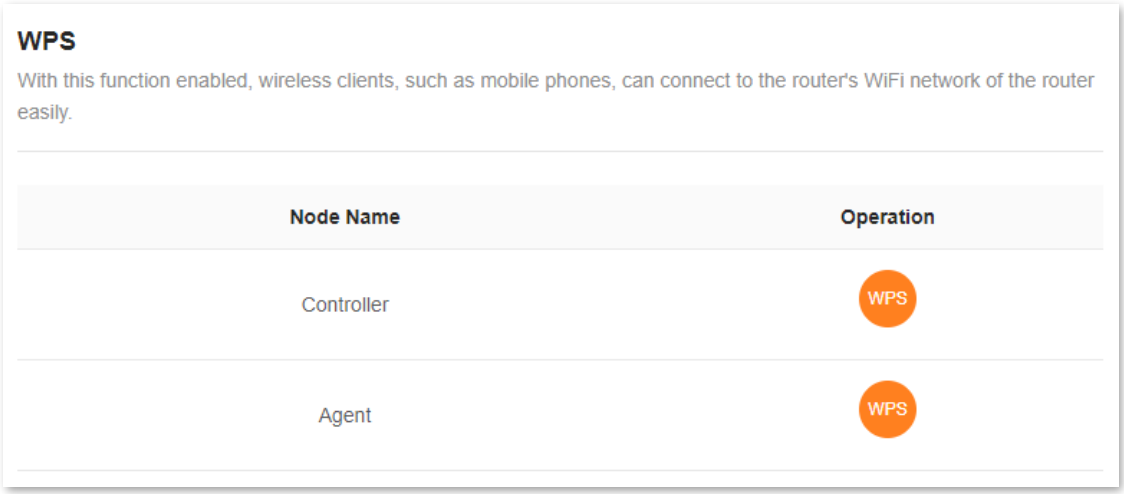
- This function only applies to WPS-enabled Wi-Fi devices. It is enabled by default and cannot be disabled.
- Wi-Fi networks encrypted with WPA3 cannot be connected through WPS.
- The WPS negotiation times out in 120 seconds. The **WPS** button is disabled during WPS negotiation.

To connect devices to the Wi-Fi network using the WPS function:

Step 1 Log in to the web UI.

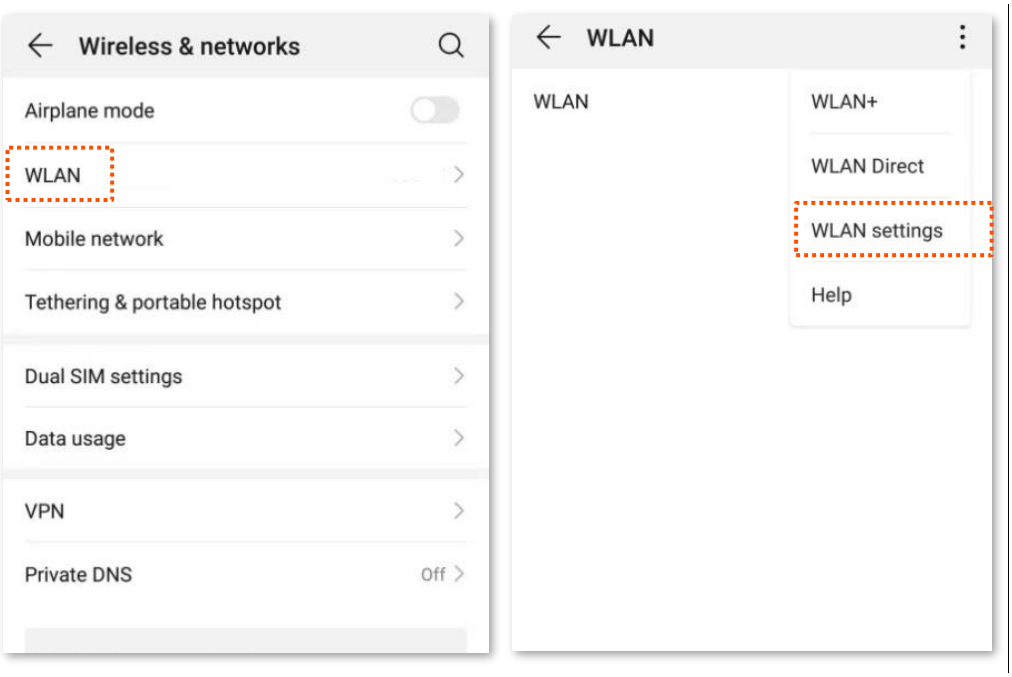
Step 2 Choose **More** > **WiFi Settings** > **WPS.**

Step 3 Click the **WPS** button in the line of the node to which the device is to be connected.

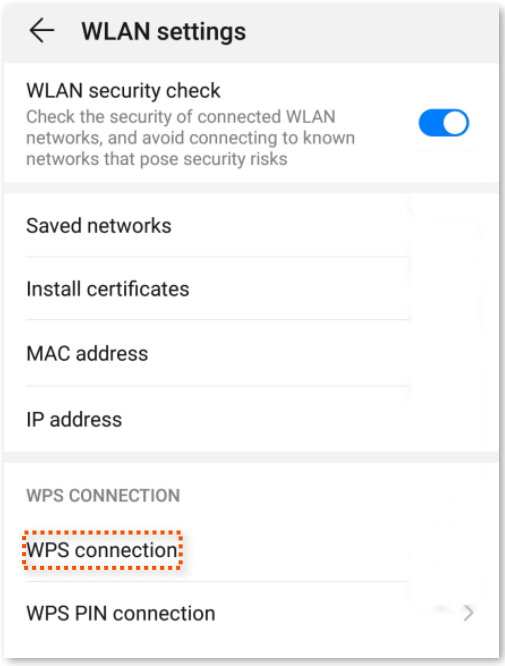


Step 4 Configure the WPS function on your WiFi-enabled devices **within 2 minutes**. Configuration on various devices may differ (Example: HUAWEI P10).

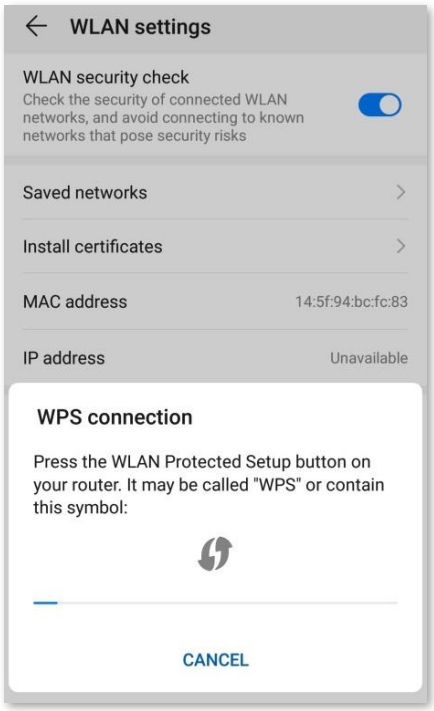
1. Find **WLAN** settings on your phone.
2. Tap ⋮, and choose **WLAN settings**.



3. Choose WPS connection.



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



---End

9.8.3 MESH button function

You can use the **WPS** button to network your Tenda devices that support the Mesh function. On this page, you can enable or disable the Mesh function of the **WPS** button as required.

TIP

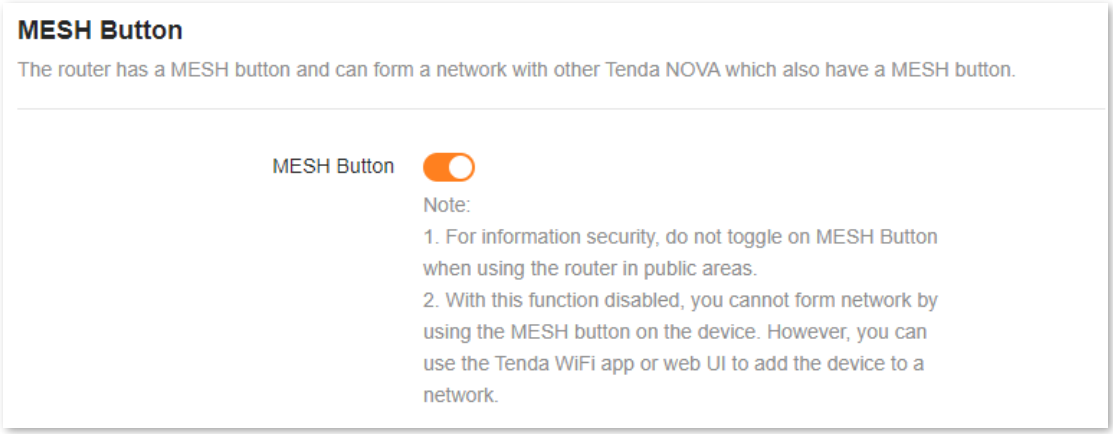
- For information security, do not toggle on **MESH Button** when using the router in public areas.
- With this function disabled, you cannot form a network by using the **WPS** button on the device. However, you can use the Tenda WiFi app or web UI to add the device to a network.

To enable or disable the Mesh function of the **WPS** button:

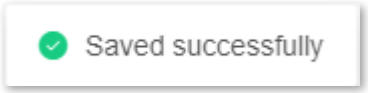
Step 1 Log in to the web UI of the router.

Step 2 Choose **More** > **WiFi Settings** > **MESH Button.**

Step 3 Toggle on or off **MESH Button**.



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



---End

9.9 Network settings

9.9.1 LAN Settings

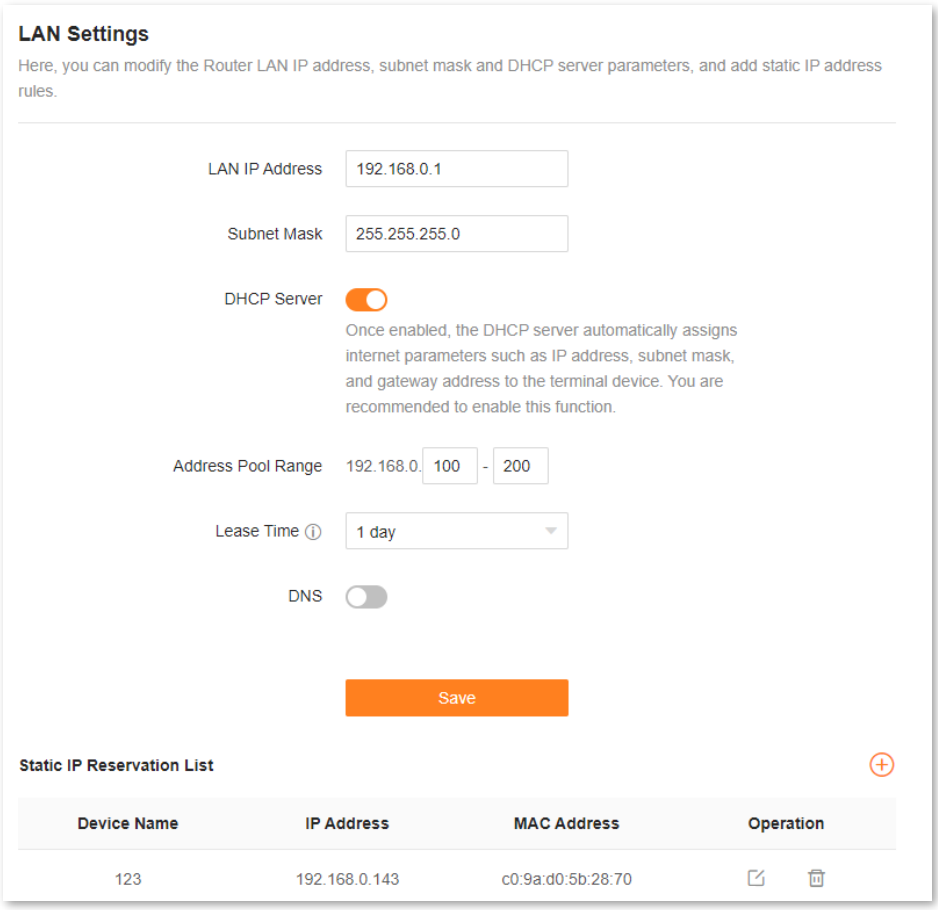
To access the configuration page, log in to the web UI of the router, and choose **More** > **Network Settings** > **LAN Settings**.

Overview

On this page, you can:

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

  The DHCP server can automatically assign IP addresses, subnet masks, gateways and other information to clients within the LAN. If you disable this function, you need to manually configure the IP address information on the client to access the Internet. Do not disable the DHCP server function unless necessary.
- **Configure the DNS information assigned to clients.**
- **Assign static IP addresses to LAN clients.**



The following table describes the parameters displayed on this page.

Parameter description

Parameter		Description
LAN IP Address		Specifies the LAN IP address of the router, which is also the management IP address for logging in to the web UI of the router.
Subnet Mask		Specifies the subnet mask of the LAN port, used to identify the IP address range of the local area network.
DHCP Server		Used to enable or disable the DHCP server. Once enabled, the DHCP server automatically assigns internet parameters such as IP address, subnet mask, and gateway address to the terminal device. 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		Specifies the valid duration of the IP address that is assigned to a client. When the lease time reaches half, the client will send a DHCP Request to the DHCP server for renewal. If the renewal succeeds, the lease is renewed based on the time of the renewal application. If the renewal fails, the renewal process is repeated 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. It is recommended to keep the default value.
DNS		Specifies whether to allocate another DNS address to the client. When it is disabled, the LAN port IP address of the router is used as the DNS address of the client. When it is enabled, **Primary DNS** must be set and **Secondary DNS** is optional. TIP This router has the DNS proxy function.
Primary DNS		Specifies the primary DNS address allocated to the client by the router. TIP Make sure that the primary DNS server is the IP address of the correct DNS server or DNS proxy. Otherwise, you may fail to access the internet.
Secondary DNS		Specifies the secondary DNS server address of the router used to assign to the clients. It is optional.
Static IP Reservation List	Device Name	Specifies the name of the client.
	IP Address	Specifies the IP address reserved for the client.
	MAC Address	Specifies the MAC address of the client.

Parameter	Description
Operation	The available options include: : Used to edit a static IP address reservation rule. : Used to delete a static IP address reservation rule.

Assign a static IP address to a LAN client:

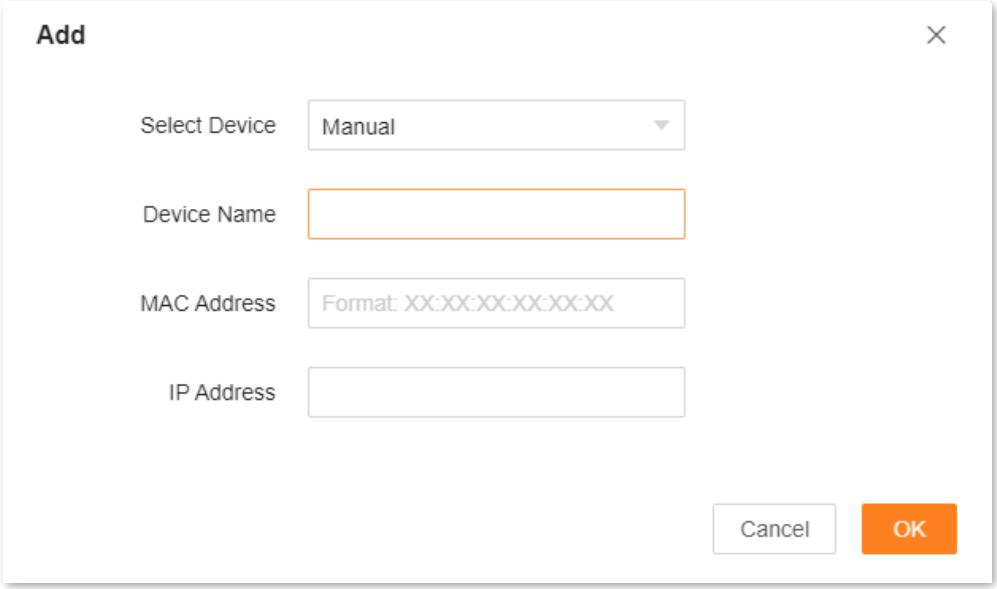
Step 1 Log in to the web UI.

Step 2 Choose **More** > **Network Settings** > **LAN Settings**.

Step 3 Click ⊕ in **Static IP Reservation List**.

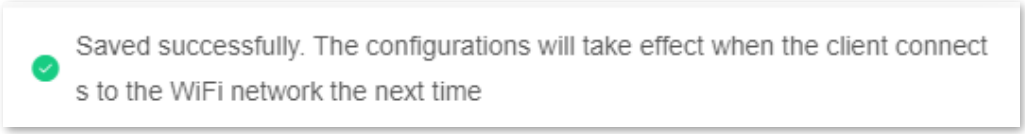
Step 4 Set **Select Device**.

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



Step 5 Click **OK**.

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

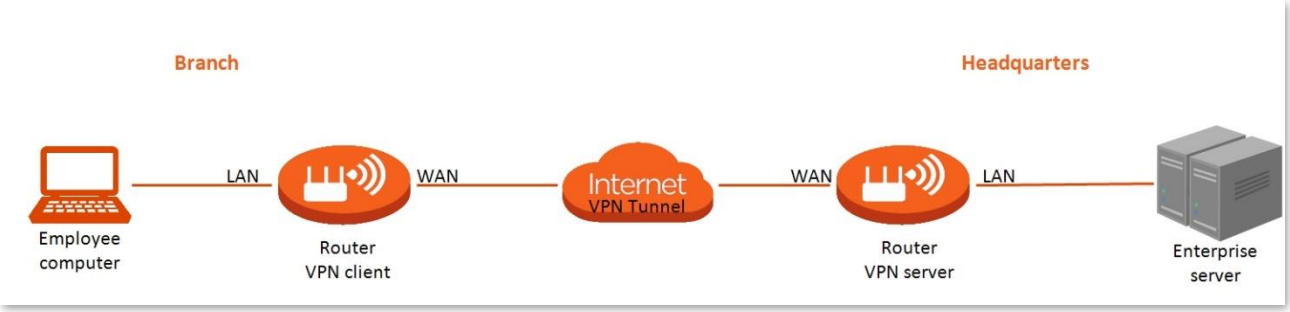


---End

9.9.2 VPN

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

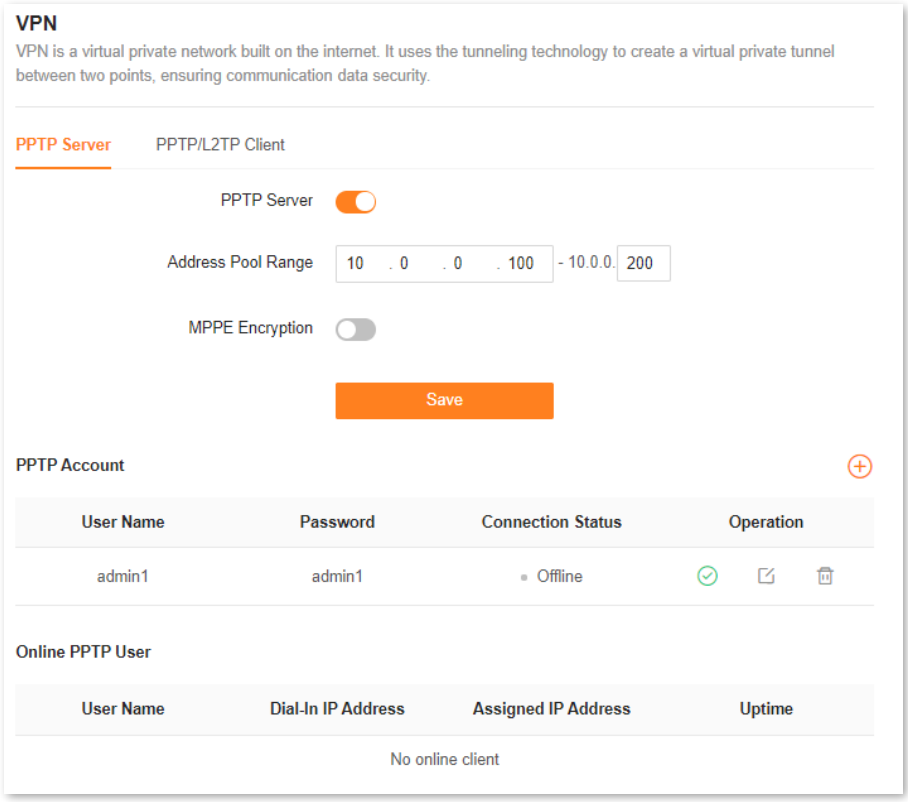
The typology of a VPN network is shown below.



PPTP server

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

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



The following table describes the parameters displayed on this page.

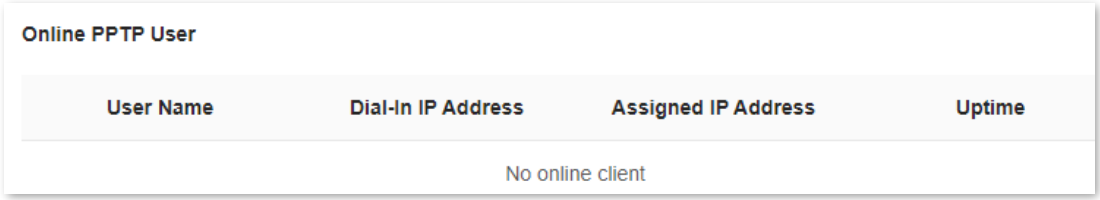
Parameter description

Parameter		Description
PPTP Server	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.
PPTP Account	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.
	Operation	The available operations include: : Indicates that the PPTP user account is available. You can click it to disable the account. : Indicates that the PPTP user account is unavailable. You can click it to enable the account. : Used to edit a PPTP user account. : Used to delete a PPTP user account.

- ## 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 choose **More** > **Network Settings** > **VPN** > **PPTP Server**.



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.

- ## Enable internet users to access resources of the FTP server

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**.

TIP

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:

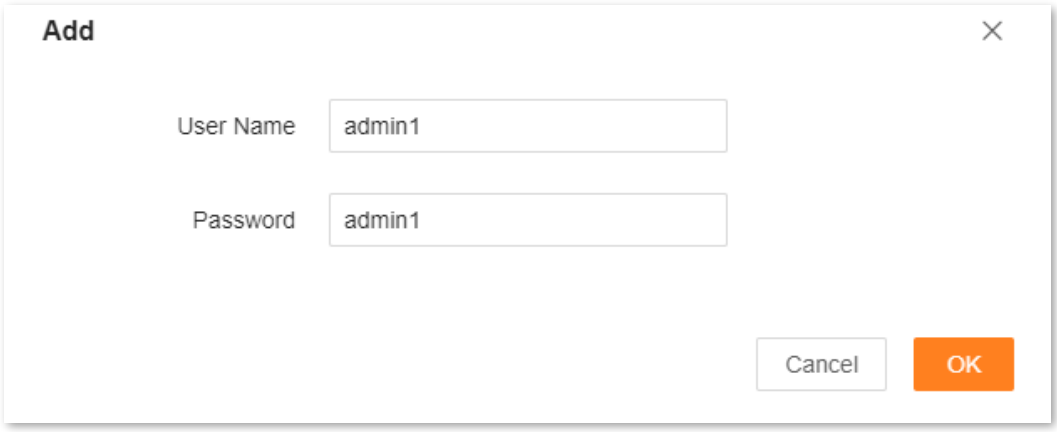
Step 1 Log in to the web UI.

Step 2 Choose **More** > **Network Settings** > **VPN** > **PPTP Server**.

Step 3 Enable **PPTP Server**.

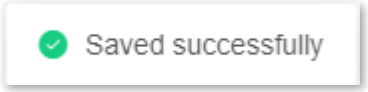
Step 4 Enable **MPPE Encryption**, which means that the encryption digit remains the default value “128”.

Step 5 Click ⊕. Set **User Name** and **Password** for the PPTP server, which are both **admin1** in this example. Then, click **OK**.



Step 6 Click **Save.**

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

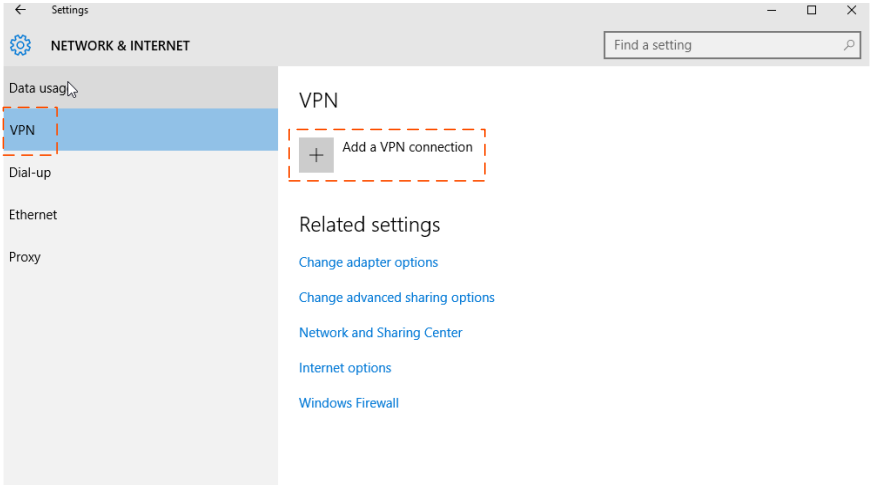


---End

After completing the configuration, internet users can access the FTP server by following these steps:

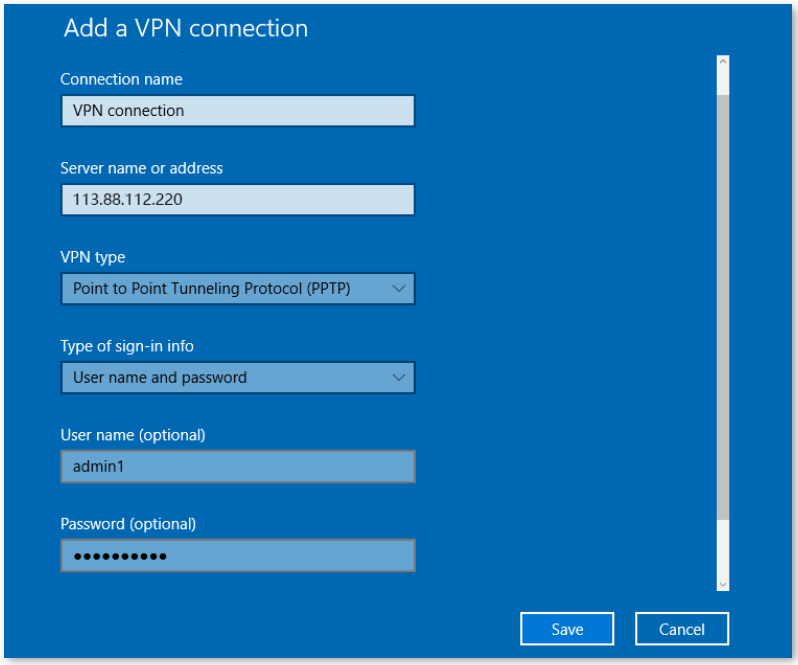
Step 1 Click the icon at the bottom right corner on the desktop of another computer with internet access, and then click **Network settings**.

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

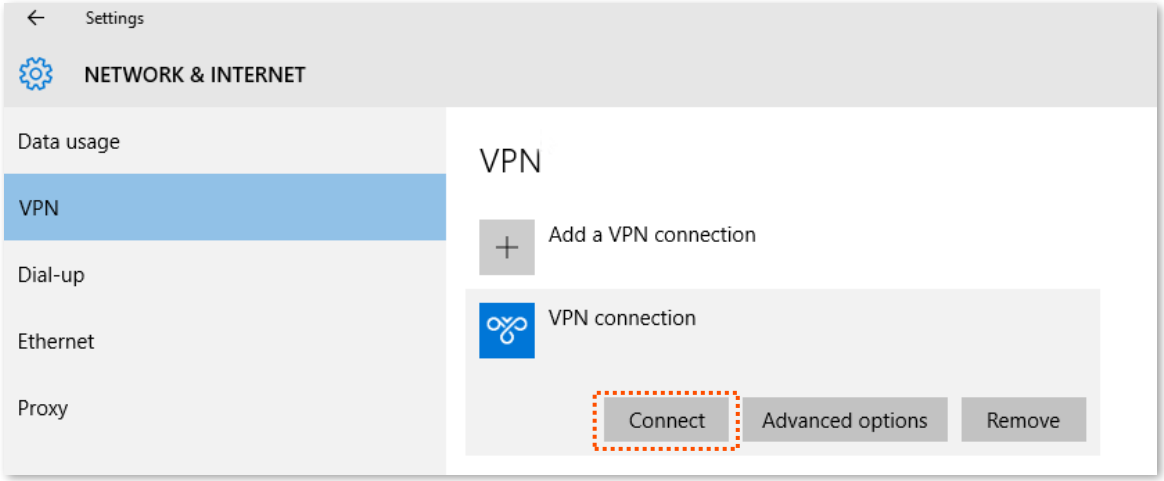


Step 3 Configure the VPN parameters.

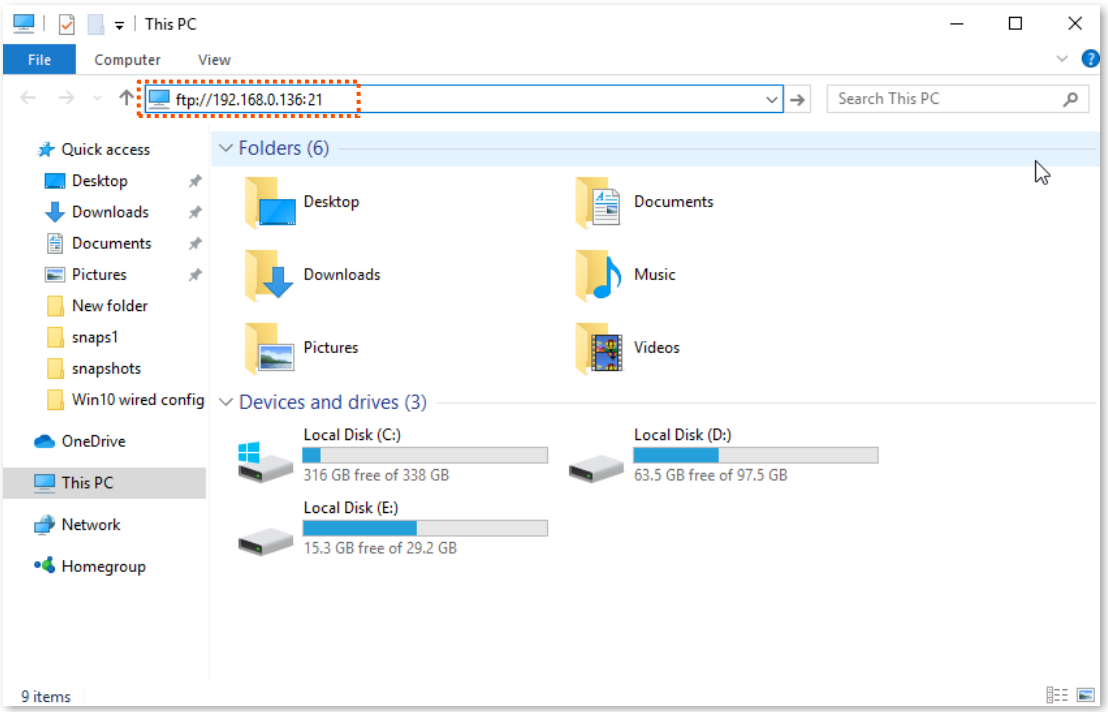
1. Enter a connection name, such as **VPN connection**.
2. Enter the server address, which is **113.88.112.220** in this example.
3. Select a VPN type, which is **Point to Point Tunneling Protocol (PPTP)** in this example.
4. Select a type of sign-in info, which is **User name and password** in this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



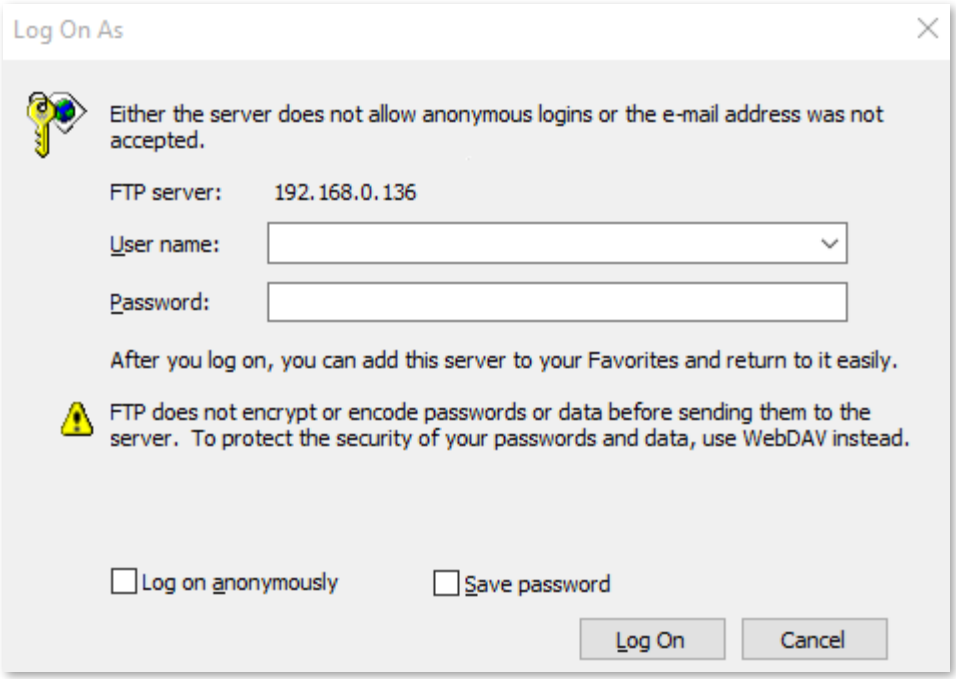
Step 4 Find the VPN connection added, and click **Connect**.



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



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



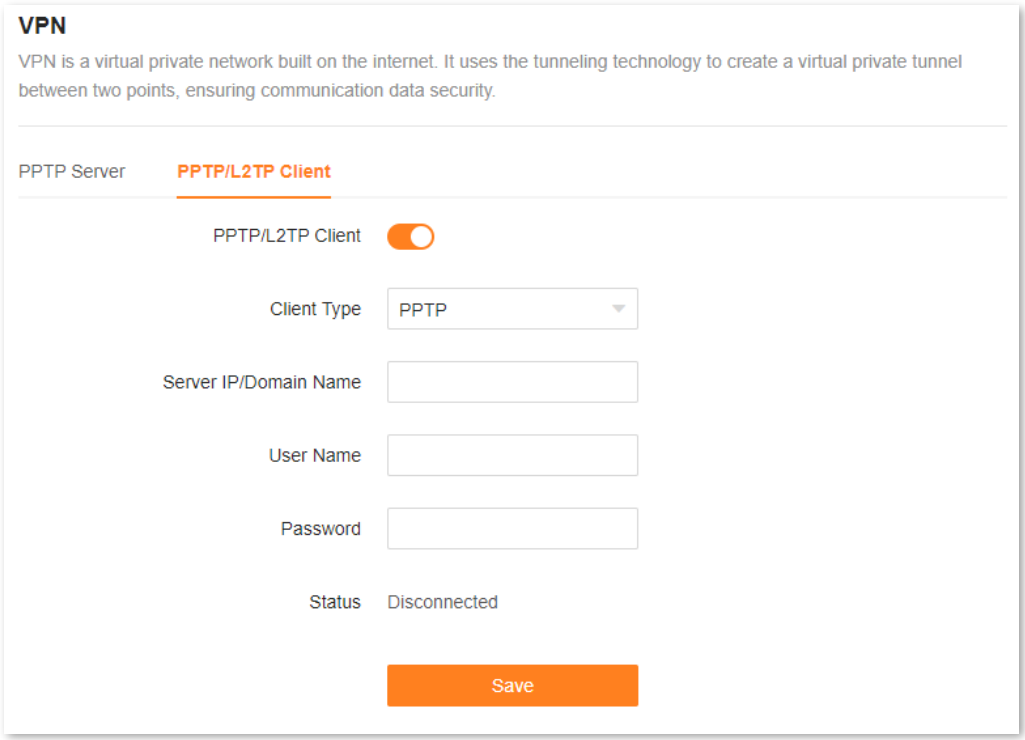
---End

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

PPTP/L2TP client

This series of routers can function as PPTP/L2TP clients and connect to PPTP/L2TP servers.

The PPTP/L2TP client function is disabled by default. When it is enabled, the page is shown below.



Parameter description

Parameter	Description
PPTP/L2TP Client	Used to enable or disable the PPTP/L2TP client function.
Client Type	Specifies the client type that the router serves as, either PPTP or L2TP. • **PPTP**: When the router is connecting to a PPTP server, 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.

- **Access VPN resources with the router**

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.

Step 2 Choose **More** > **Network Settings** > **VPN** > **PPTP/L2TP Client**.

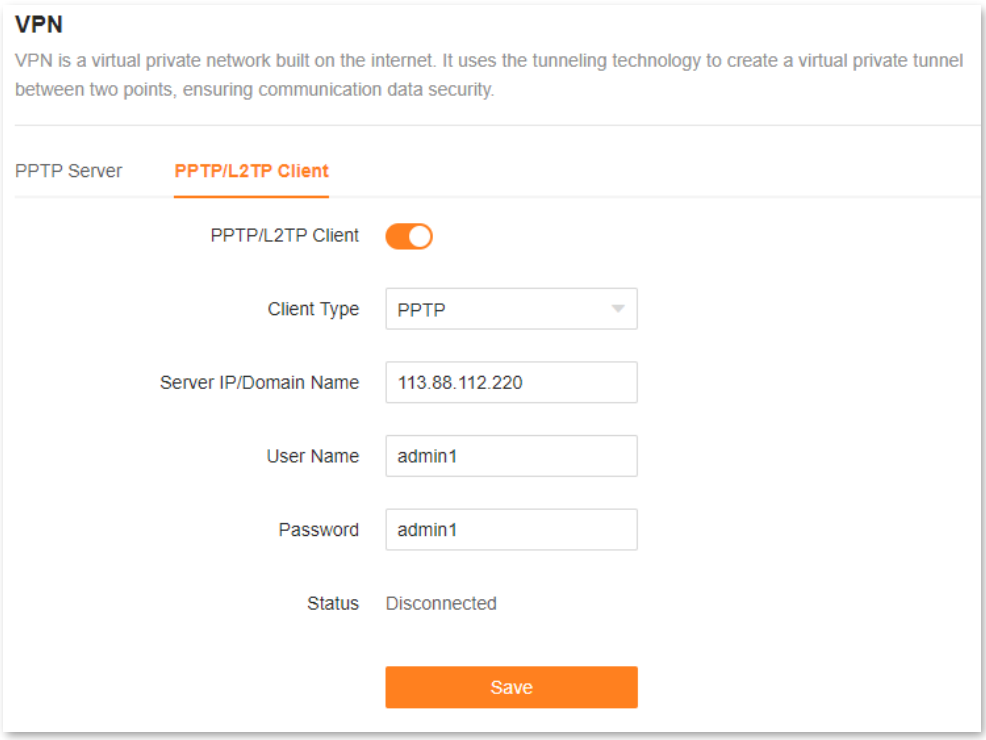
Step 3 Enable **PPTP/L2TP Client.**

Step 4 Choose **PPTP** for **Client Type**.

Step 5 Set **Server IP Address/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**.



---End

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

9.9.3 IPTV

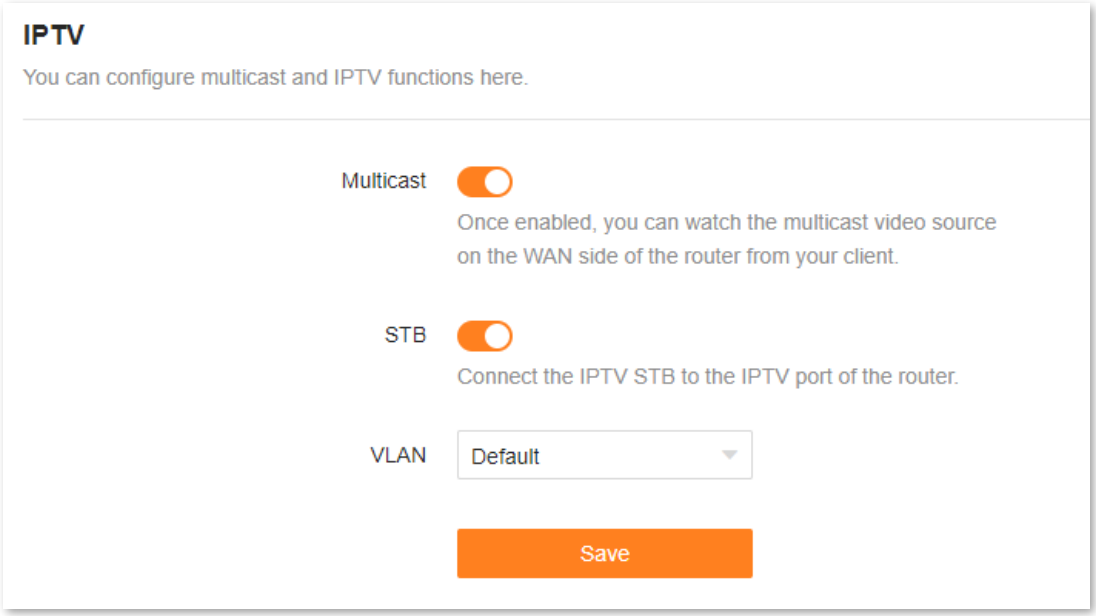
IPTV is the technology integrating internet, multimedia, telecommunication and many other technologies to provide interactive services, including digital TV, for family users by internet broadband lines.

You can set the multicast and STB functions here.

- **Multicast**: 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.
- **STB** (set-top box): 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.

To access the configuration page, log in to the web UI of the router and choose **More** > **Network Settings** > **IPTV**.

The IPTV function is disabled by default. When it is enabled, the page is shown below.



The following table describes the parameters displayed on this page.

Parameter description

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

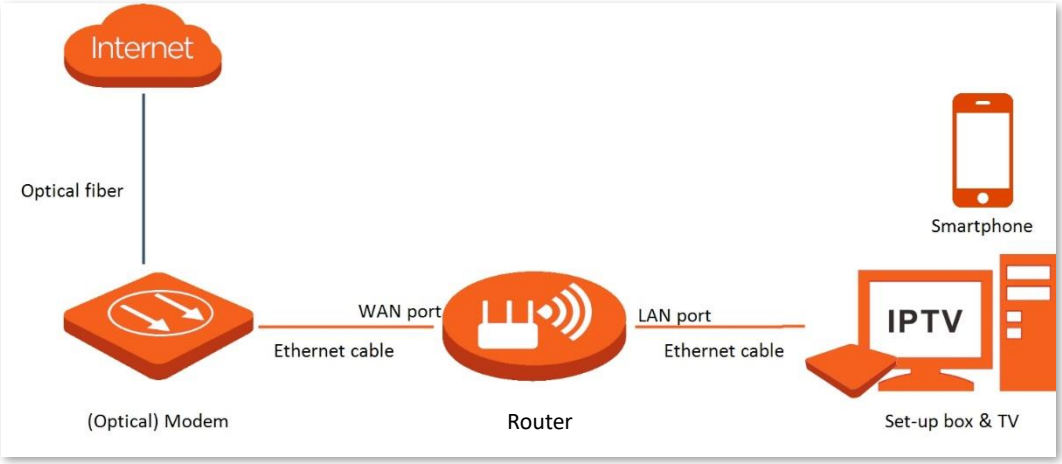
Parameter	Description
VLAN	Specifies the VLAN ID of your IPTV service. • If your ISP does not provide any VLAN ID information when the IPTV service is available, keep **Default**. • If you have obtained the VLAN ID from your ISP when the IPTV service is available, choose **Custom** VLAN and enter the VLAN value.

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, but no VLAN information.

Goal: Watch IPTV programs through the router.

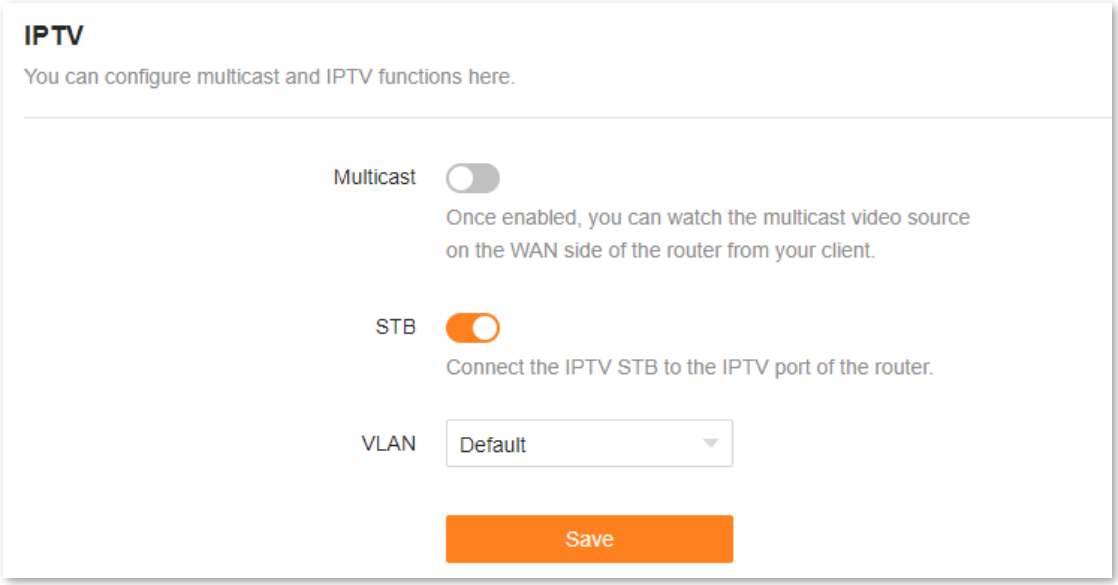
Solution: You can configure the IPTV function to reach the goal.



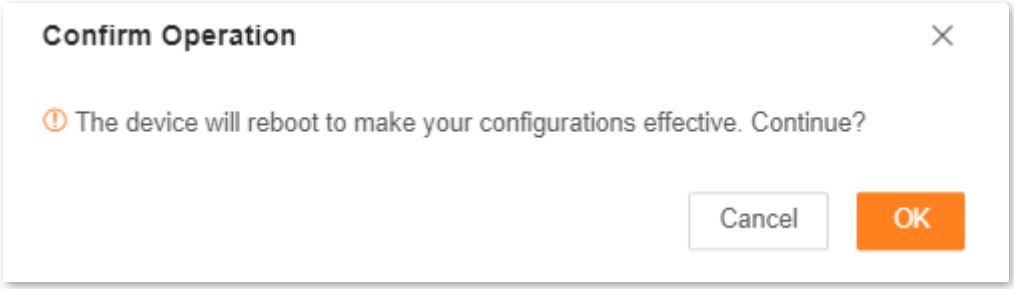
Configuration procedure:

Step 1 Set your router.

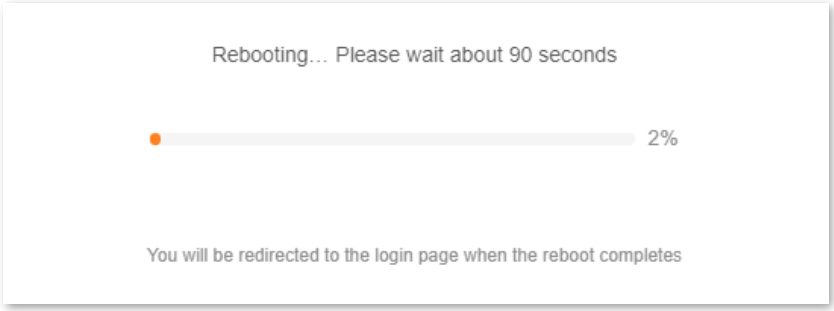
1. Log in to the web UI.
2. Choose **More** > **Network Settings** > **IPTV**.
3. Enable the **STB** function.
4. Click **Save**.



5. Click **OK**.



Wait until the router is restarted.



Step 2 Configure the set-top box.

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

---End

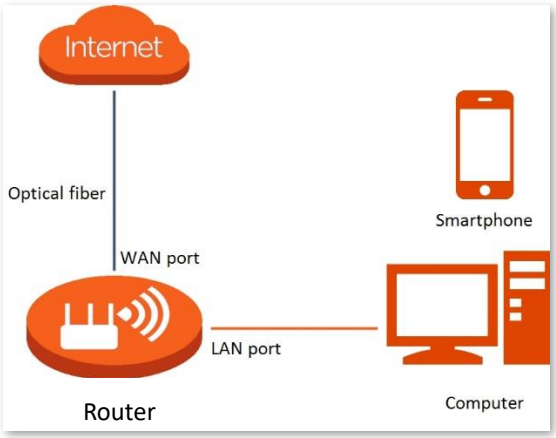
After completing the configuration, you can watch IPTV programs on your TV.

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.



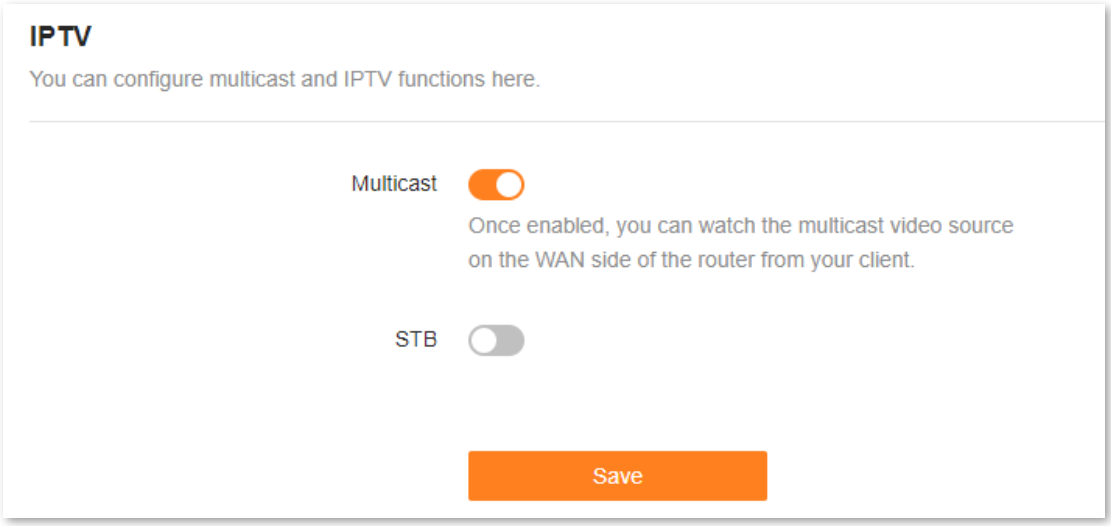
Configuration procedure:

Step 1 Log in to the web UI.

Step 2 Choose **More** > **Network Settings** > **IPTV**.

Step 3 Enable the **Multicast** function.

Step 4 Click **Save**.



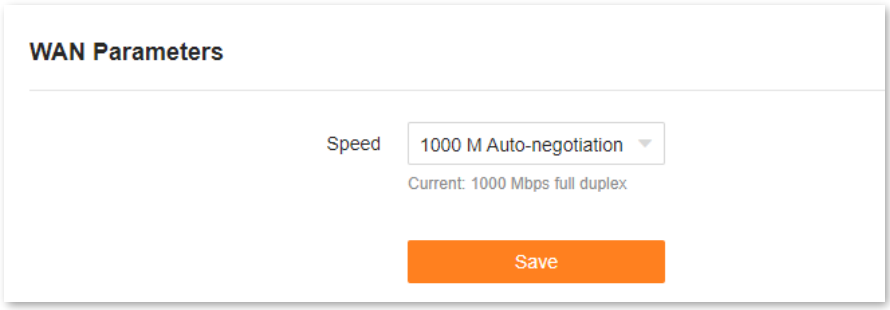
---End

After completing the configuration, you can watch multicast videos on your terminal devices.

9.9.4 WAN parameters

When the Ethernet cable is intact and connected to the WAN port properly, but **No Ethernet cable is connected to the WAN port** is still shown on the **Internet Settings** page, you can try to change the **Speed** to **10 Mbps full duplex** or **10 Mbps half duplex** to solve the problem. Otherwise, keep the default settings.

To access the configuration page, log in to the web UI of the router, and choose **More** > **Network Settings** > **WAN Parameters**.



The following table describes the parameters displayed on this page.

Parameter description

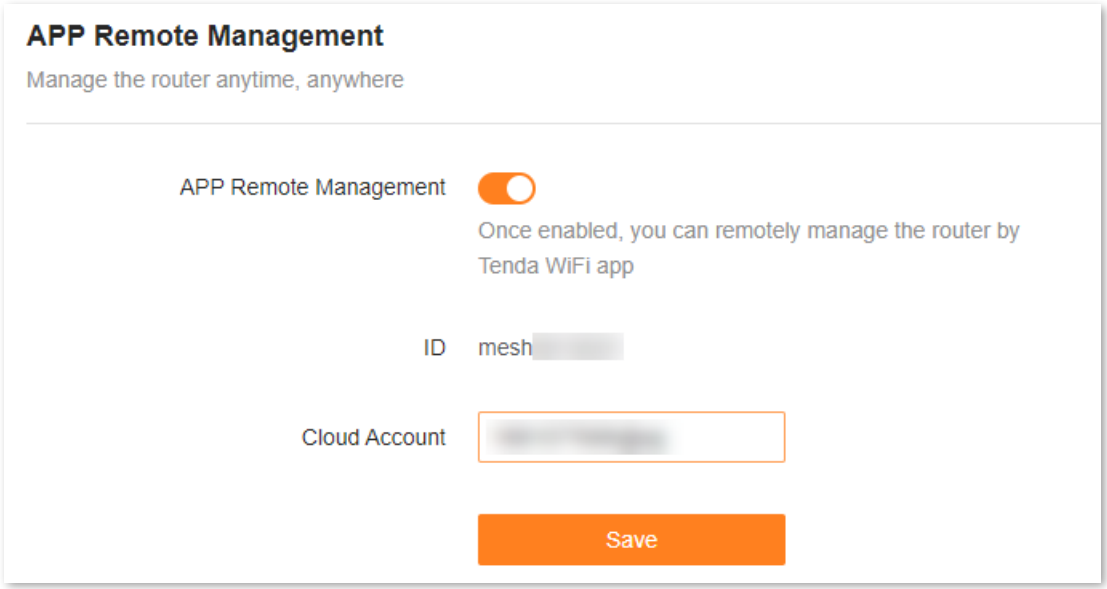
Speed	Application
1000 M Auto-negotiation	Indicates that the speed and duplex mode are determined through the negotiation with the peer port.
100 Mbps full duplex	Indicates that the WAN port is working at the speed of 100 Mbps, and the port can receive and send data packets at the same time.
100 Mbps half duplex	Indicates that the WAN port is working at the speed of 100 Mbps, but the port can only receive or send data packets alternately.
10 Mbps full duplex	Indicates that the WAN port is working at the speed of 10 Mbps, and the port can receive and send data packets at the same time.
10 Mbps half duplex	Indicates that the WAN port is working at the speed of 10 Mbps, but the port can only receive or send data packets alternately.

9.10 Other advanced settings

9.10.1 App remote management

The router can be managed remotely using the Tenda WiFi app. The app remote management function is disabled by default. You can enable this function as required.

To access the configuration page, log in to the web UI of the router, and choose **More** > **Advanced** > **APP Remote Management**.



The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
APP Remote Management	Used to enable or disable the app remote management function. It is enabled by default.
ID	Specifies the ID of the router, which is automatically allocated.
Cloud Account	Specifies the account bound on your Tenda WiFi app.

9.10.2 MAC address filter

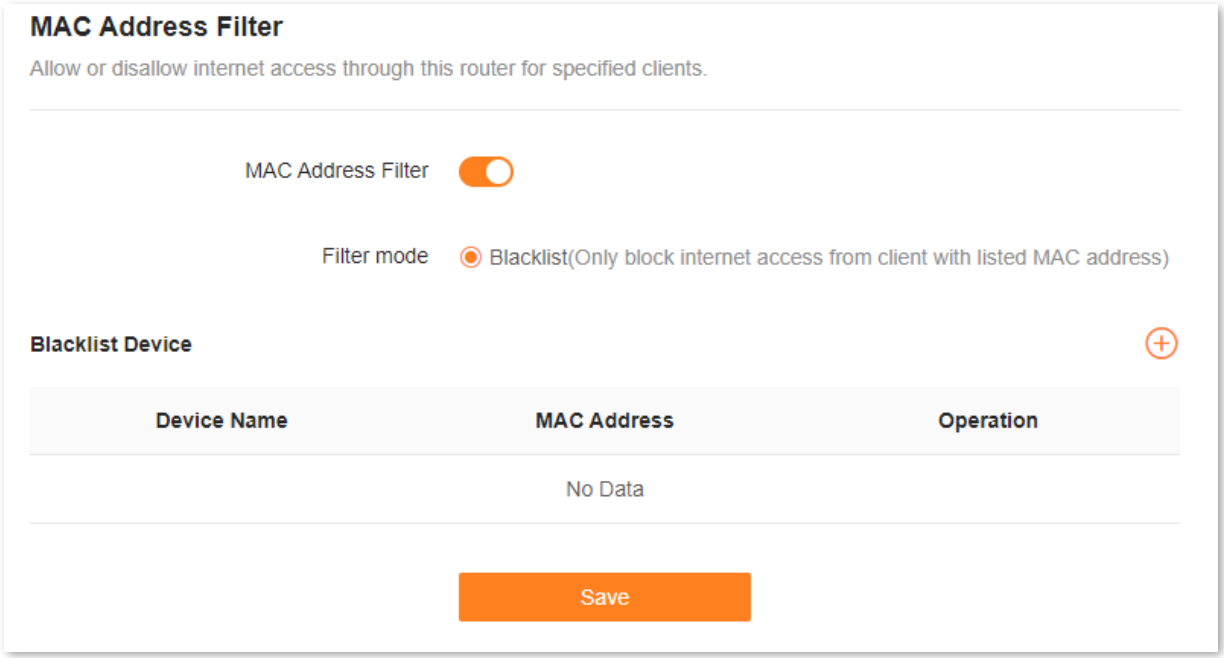
Overview

With this function, you can blacklist clients by MAC addresses to prohibit them from accessing the internet through the router.

TIP

- If you blacklist a wired client, the client will fail to access the network, but it can still connect to the router.
- If you blacklist a wireless device, the client will be kicked offline and cannot connect to the router again.
- A maximum of 64 devices can be blacklisted.

To access the configuration page, log in to the web UI of the router, and choose **More** > **Advanced** > **MAC Address Filter**.



The following table describes the parameters displayed on this page.

Parameter description

Parameter		Description
MAC Address Filter		Used to enable or disable the MAC address filter function.
Filter mode		Specifies the MAC address filter mode. **Blacklist**: WiFi-enabled clients listed are unable to connect to the Wi-Fi network of the router.
Blacklist Device	Device Name	Specifies the name of the blacklisted client.
	MAC Address	Specifies the MAC address of the blacklisted client.
	Operation	: Used to remove a client from the blacklist.

Only prohibit specified clients from accessing the internet

Scenario: As an important test is coming, you want to prohibit your kid's phone from accessing the internet.

Goal: Only prohibit your kid's phone 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	8C:EC:4B:B3:04:92	Connected

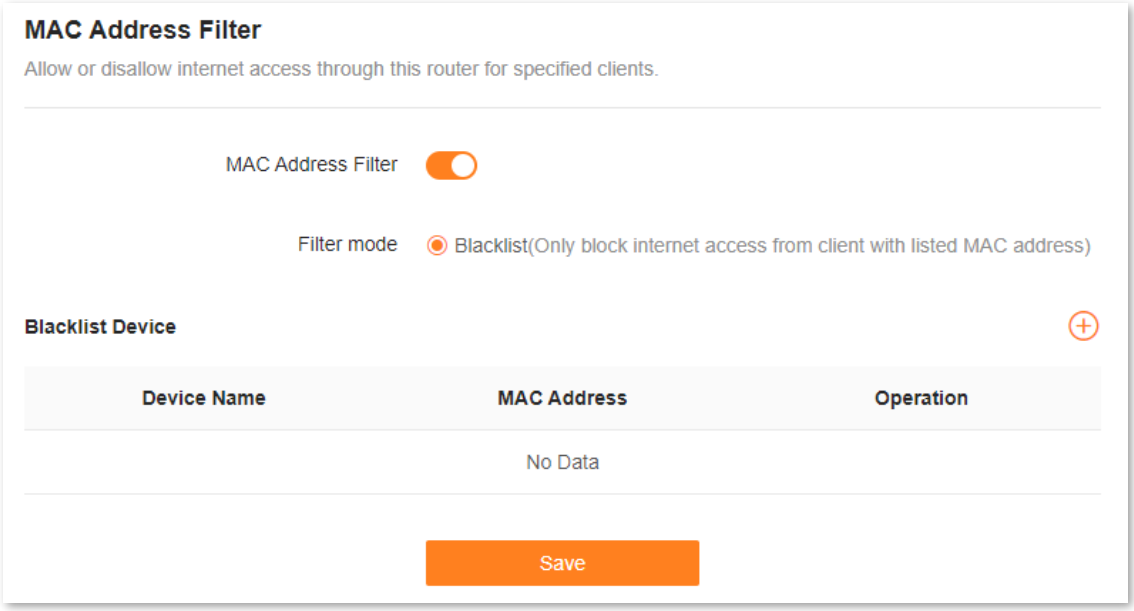
Configuration procedure:

Step 1 Log in to the web UI.

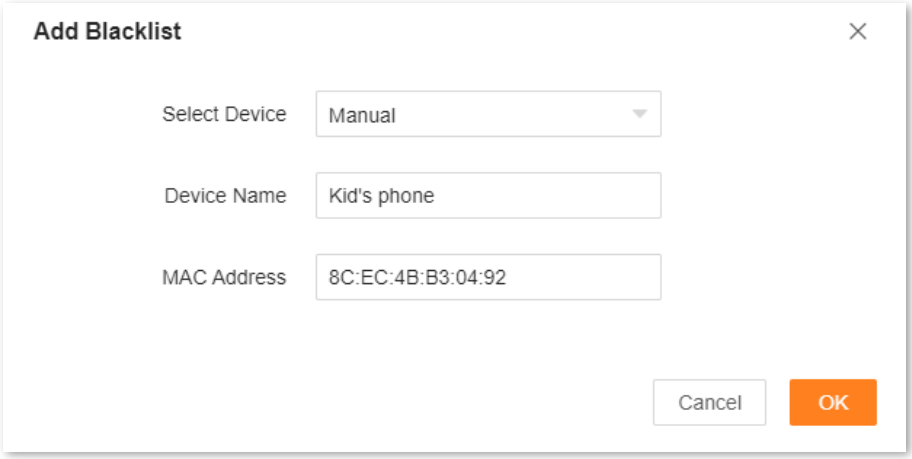
Step 2 Choose **More** > **Advanced** > **MAC Address Filter**.

Step 3 Enable **MAC Address Filter**.

Step 4 Click ⊕.

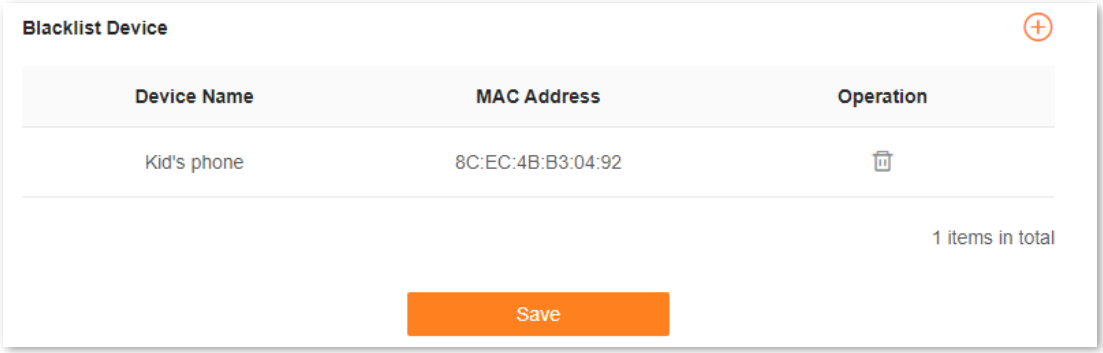


Step 5 Set **Device Name**. Enter **MAC Address** of the client, which is **8C:EC:4B:B3:04:92** in this example.



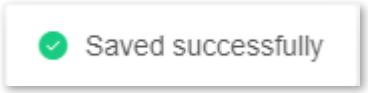
Step 6 Click **OK**.

The blacklisted client is displayed under **Blacklist Device**.



Step 7 Click **Save**.

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



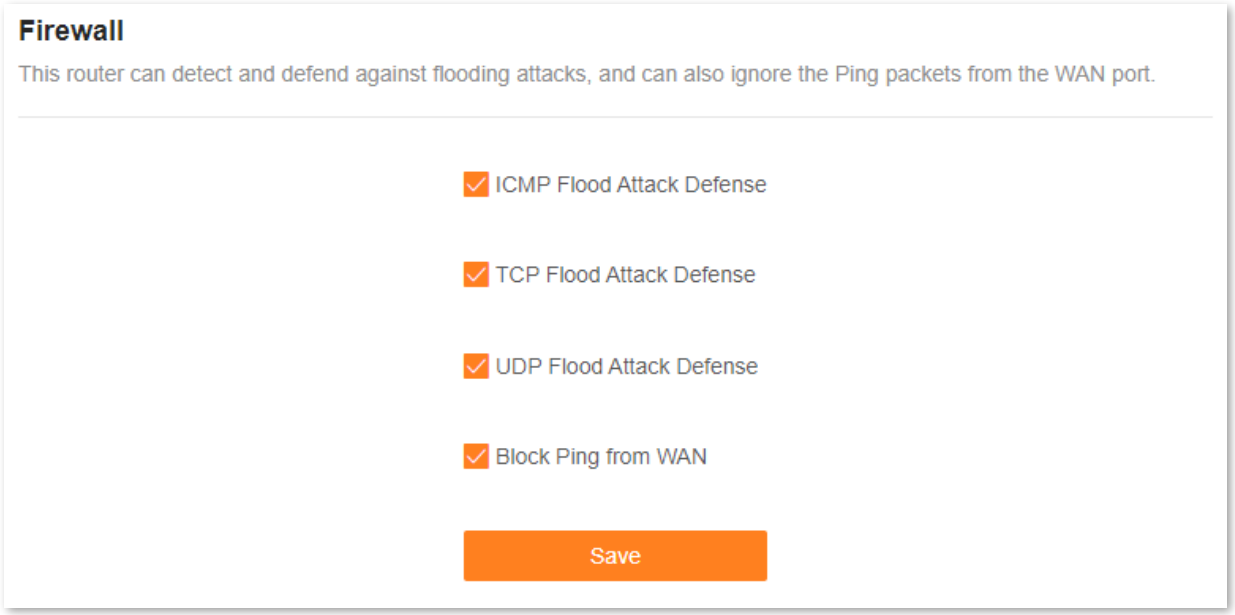
---End

After the configuration is completed, only your kid's phone is prohibited from accessing the internet through the router.

9.10.3 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 choose **More** > **Advanced** > **Firewall**.



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.
UDP Flood Attack Defense	Used to enable or disable the UDP flood attack defense. 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.
Block Ping From WAN	Used to enable or disable the Block Ping From WAN function. When it is enabled, the router automatically ignores the ping to its WAN from hosts from the internet and prevents itself from being exposed, while preventing external ping attacks.

9.10.4 DMZ host

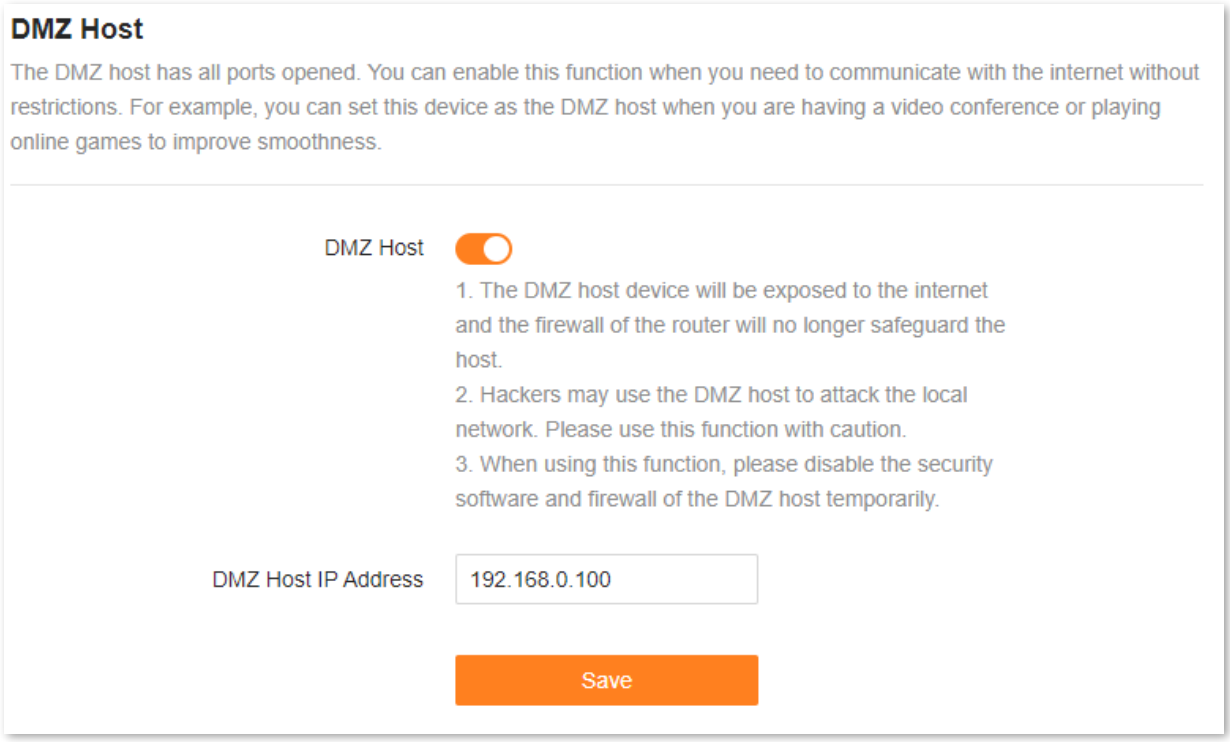
Overview

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.

NOTE

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

To access the configuration page, log in to the web UI of the router, and choose **More** > **Advanced** > **DMZ Host**.



The following table describes the parameters displayed on this page.

Parameter description

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

An example of enabling internet users to 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.

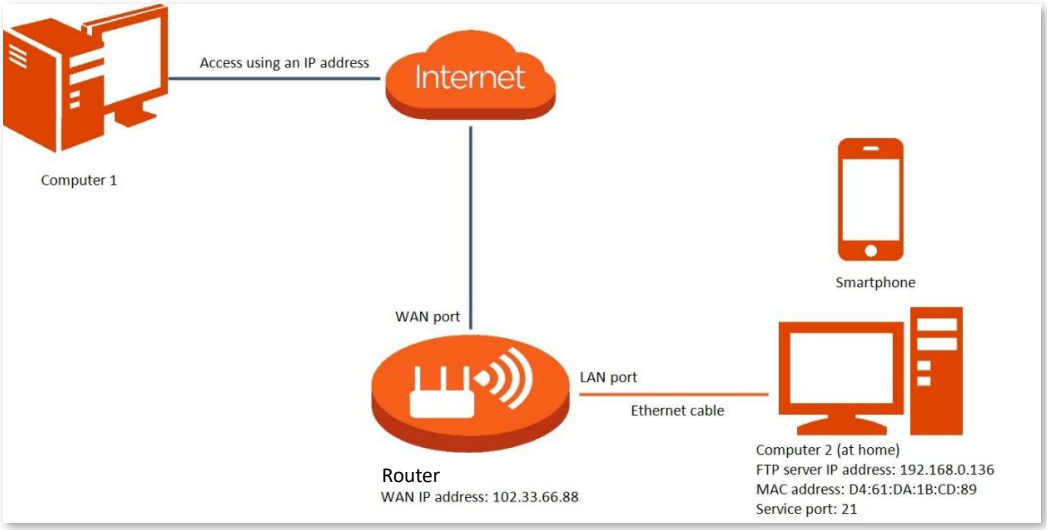
Solution: You can configure the DMZ host function to reach the goal.

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**
- WAN IP address of the router: **102.33.66.88**

TIP

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.

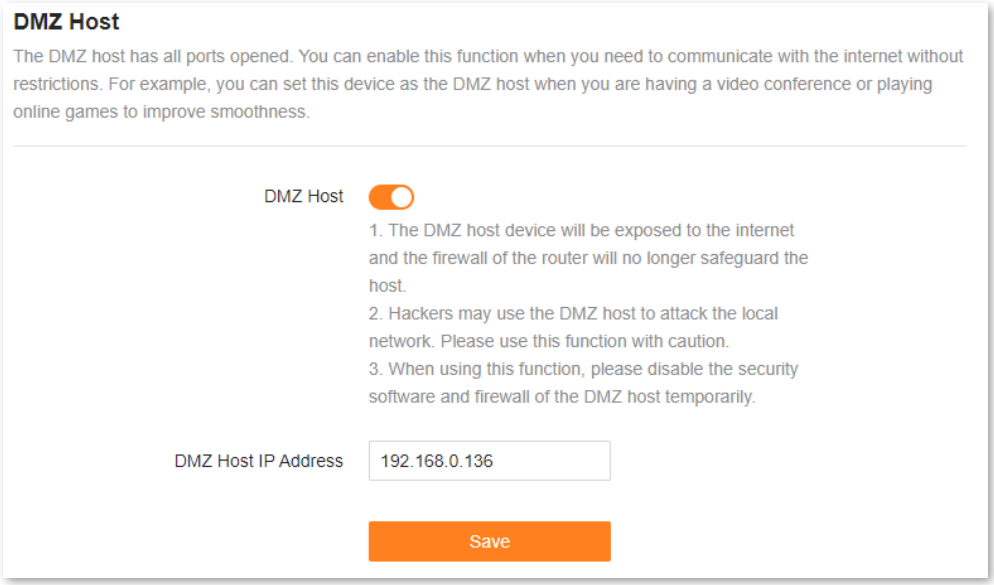


Configuration procedure:

Step 1 Log in to the web UI.

Step 2 Set the server host as the DMZ host.

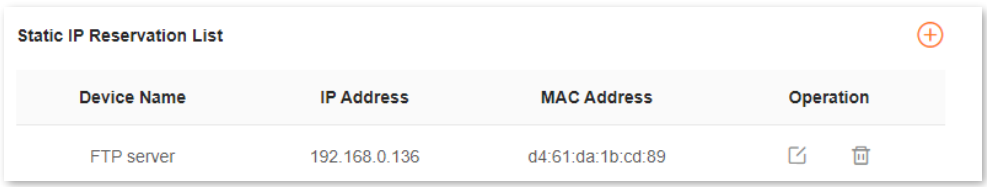
1. Choose **More** > **Advanced** > **DMZ Host**.
2. Enable **DMZ Host**.
3. Enter the IP address of the host, which is **192.168.0.136** in this example.
4. Click **Save**.



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

1. Choose **More** > **Network Settings** > **LAN Settings**.
2. Click ⊕.
3. Set **Device Name** for the server host, which is **FTP server** in this example.
4. Enter the MAC Address of the host of the server, which is **D4:61:DA:1B:CD:89** in this example.
5. Enter the reserved IP Address for the server host, which is **192.168.0.136** in this example.
6. Click **OK**.

   The client is displayed under **Static IP Reservation List**.



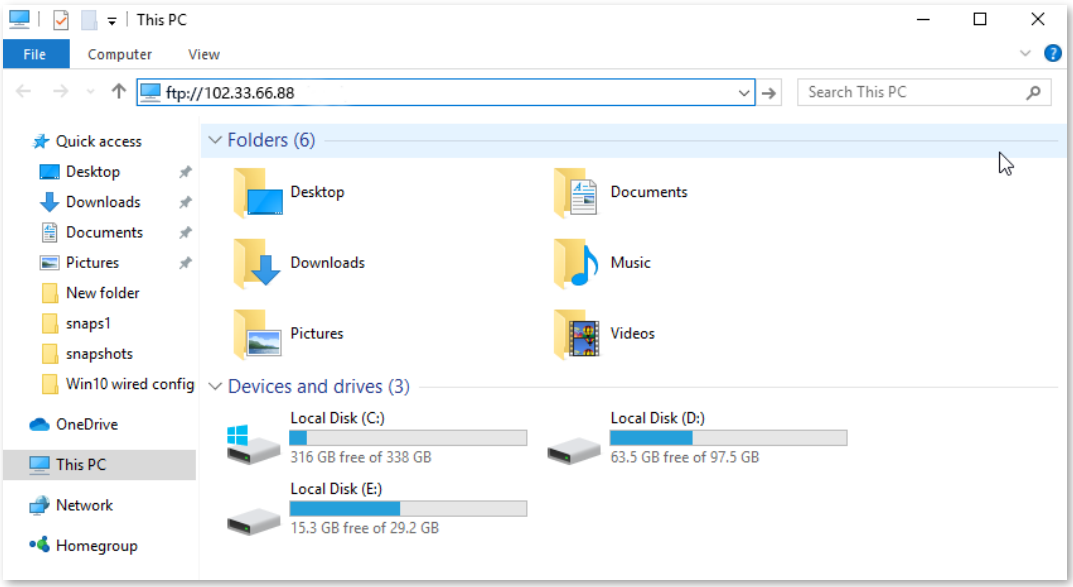
----End

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*".

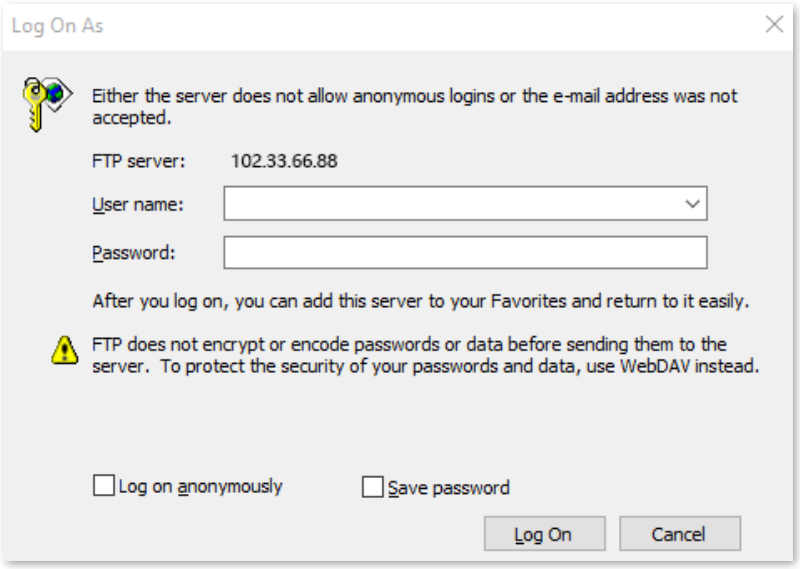
In this example, the address is "**ftp://102.33.66.88**". You can find the WAN IP address of the router in WAN port information.

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.

TIP

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.

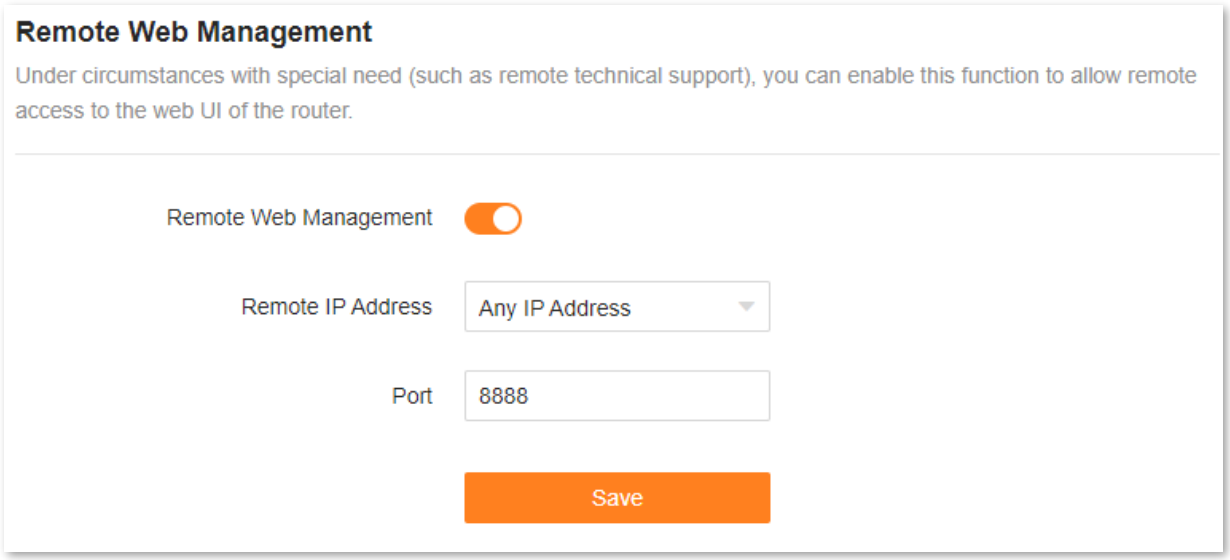
9.10.5 Remote web management

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.

To access the configuration page, log in to the web UI of the router, and choose **More** > **Advanced** > **Remote Web Management.**

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



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	Specifies the IP address of the host which can access the web UI of the router remotely. • **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	Specifies the port number of the router which is opened for remote management. You can change it as required. TIP • The port number from 1 to 1024 has been occupied by familiar services. It is strongly recommended to enter a port number from 1025 to 65535 to prevent conflict. • Remote web management can be achieved by visiting "http://*WAN IP address of the router*:*Port number*". If the DDNS host function is enabled, the web UI can also be accessed through "http://*Domain name of the router's WAN port*:*Port number*".

An example of enabling Tenda technical support to access and manage the web UI

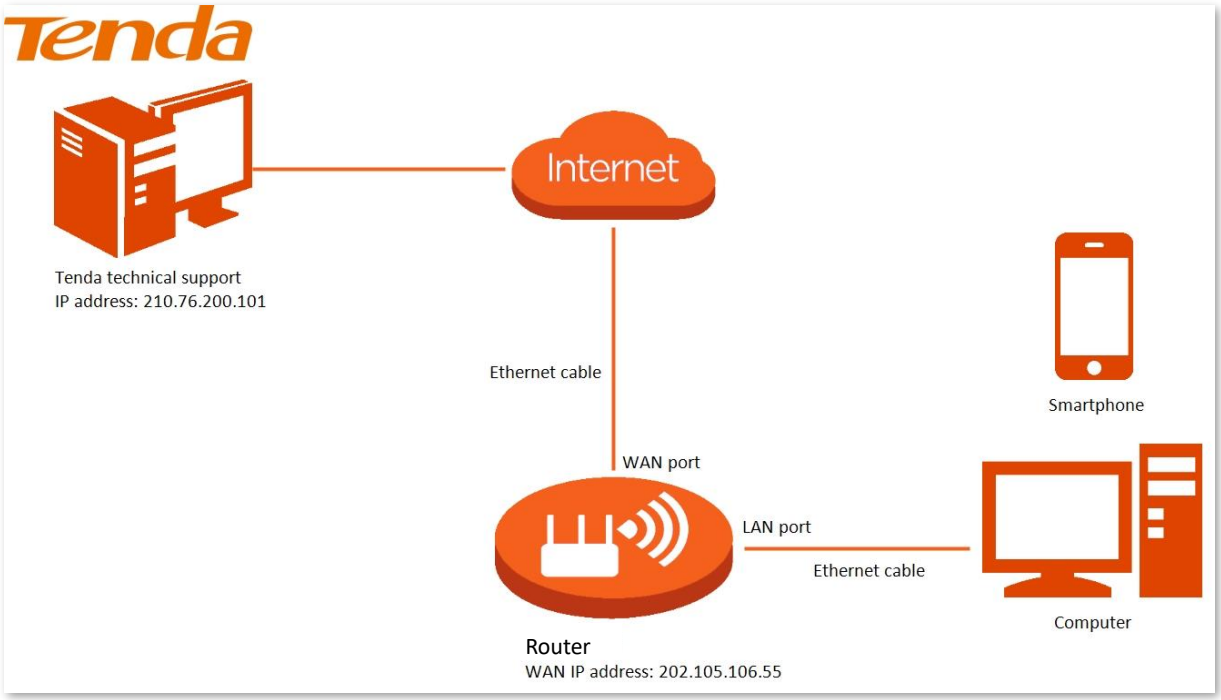
Scenario: You encounter a problem in configuring the router, and the router can access the internet.

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**



Configuration procedure:

Step 1 Log in to the web UI.

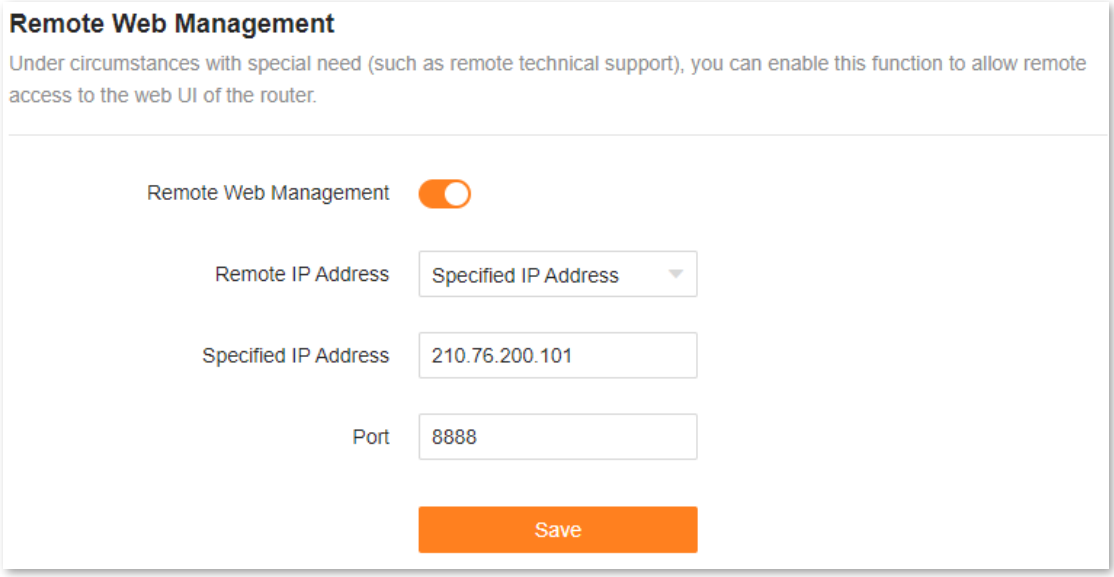
Step 2 Choose **More** > **Advanced** > **Remote Web Management**.

Step 3 Enable **Remote Web Management**.

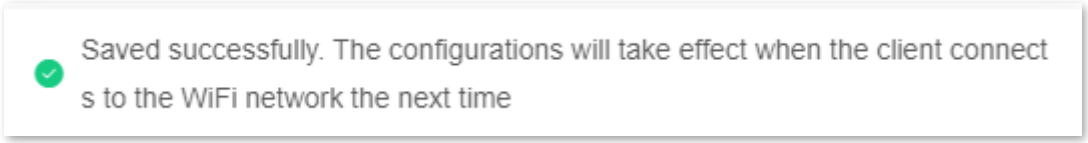
Step 4 Select **Specified IP Address** for **Remote Web Management**.

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**.



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



---End

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.

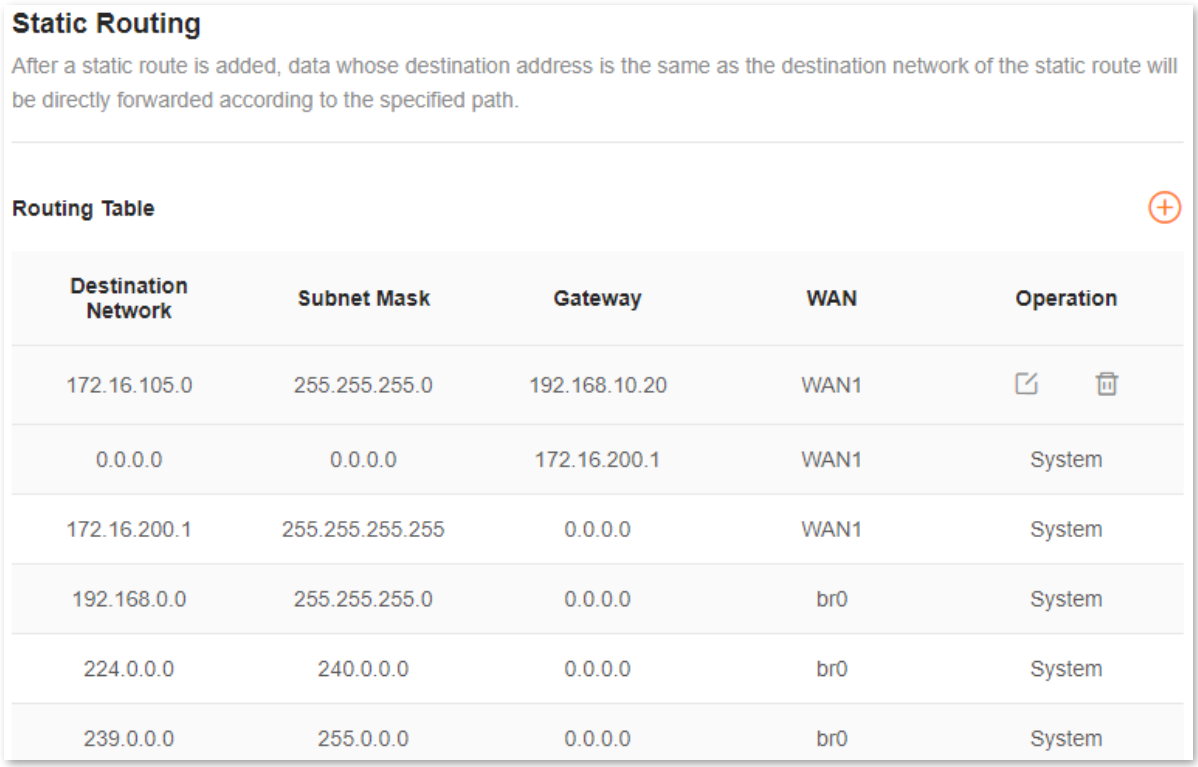
9.10.6 Static routing

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 choose **More** > **Advanced** > **Static Routing**. A maximum of 10 static routes can be added here.



The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
Destination Network	Specifies the IP address of the destination network. If **Destination Network** and **Subnet Mask** are both **0.0.0.0**, this is the default route. TIP When no route of packets can be found under **Routing Table**, the router will forward the packets using the default route.
Subnet Mask	Specifies the subnet mask of the destination network.
Gateway	Specifies the ingress IP address of the next hop router after the data packet exits from the interface of the router. **0.0.0.0** indicates that the destination network is directly connected to the router.
WAN	Specifies the interface that the packet exits from.
Operation	The available options include: : Used to modify a static routing rule. : Used to delete a static routing rule.

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.

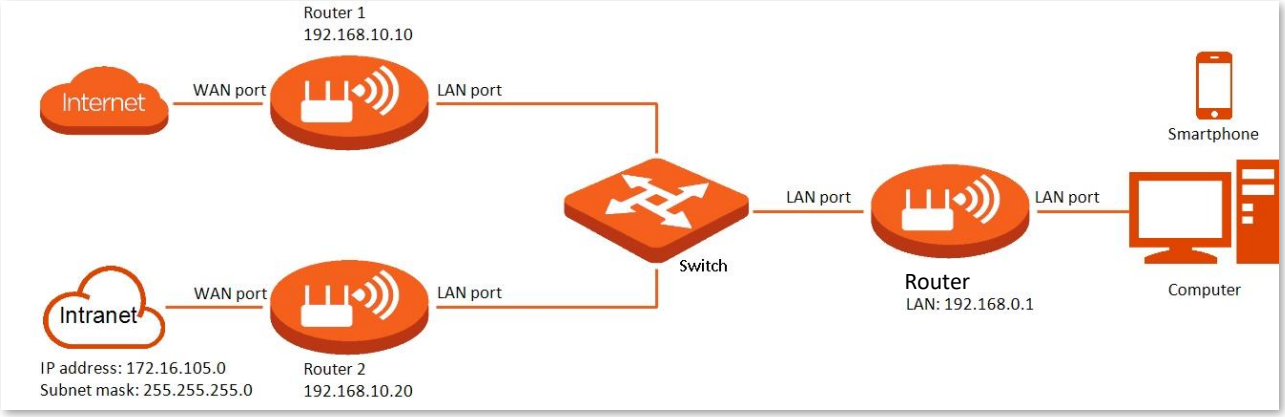
Solution: You can configure the static routing function to reach the goal.

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:

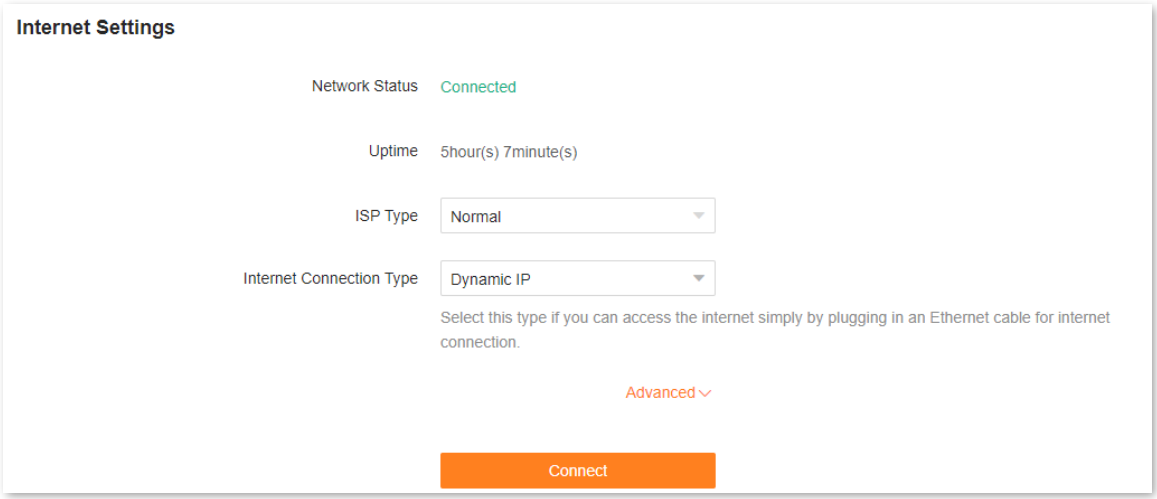
- IP address: 172.16.105.0
- Subnet mask: 255.255.255.0



Configuration procedure:

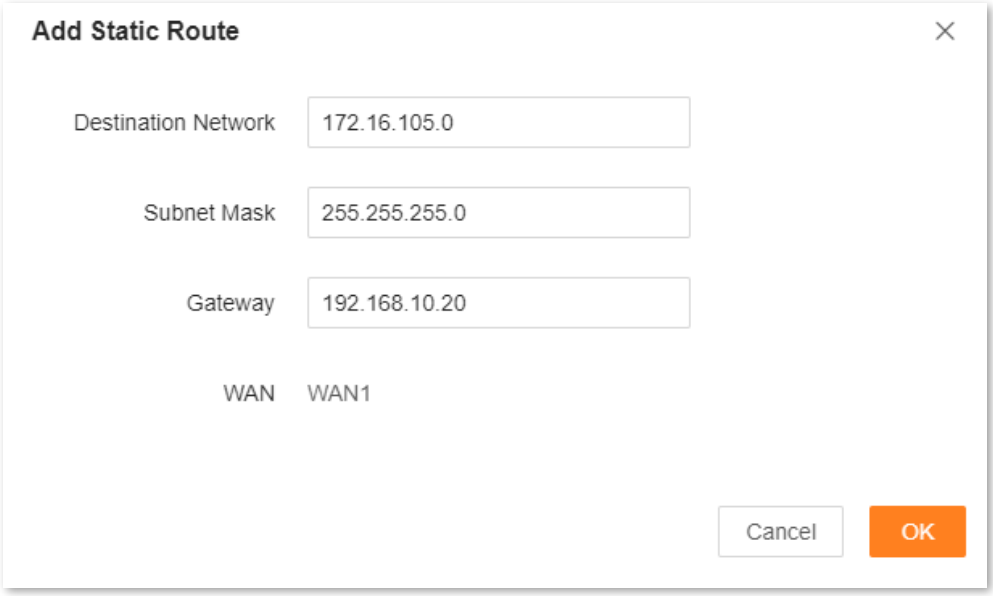
Step 1 Log in to the web UI.

Step 2 Refer to Access the internet through a dynamic IP address to configure the internet access for RX27 Pro.

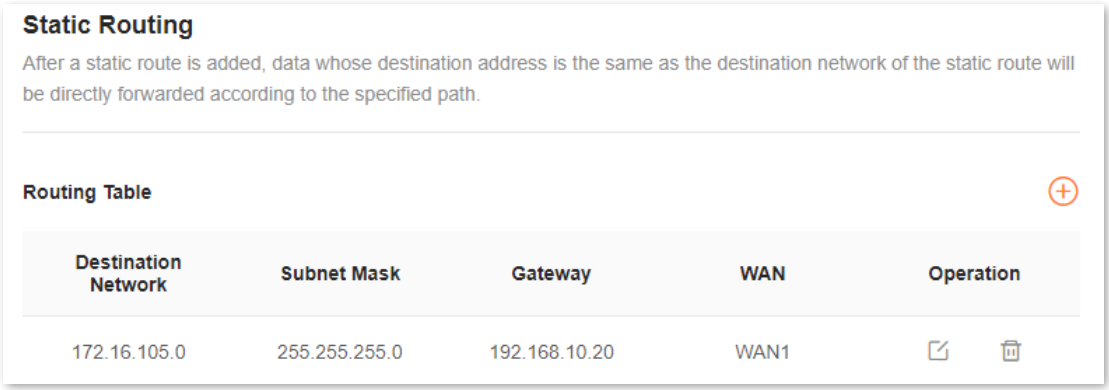


Step 3 Add a static routing rule on RX27 Pro.

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



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



---End

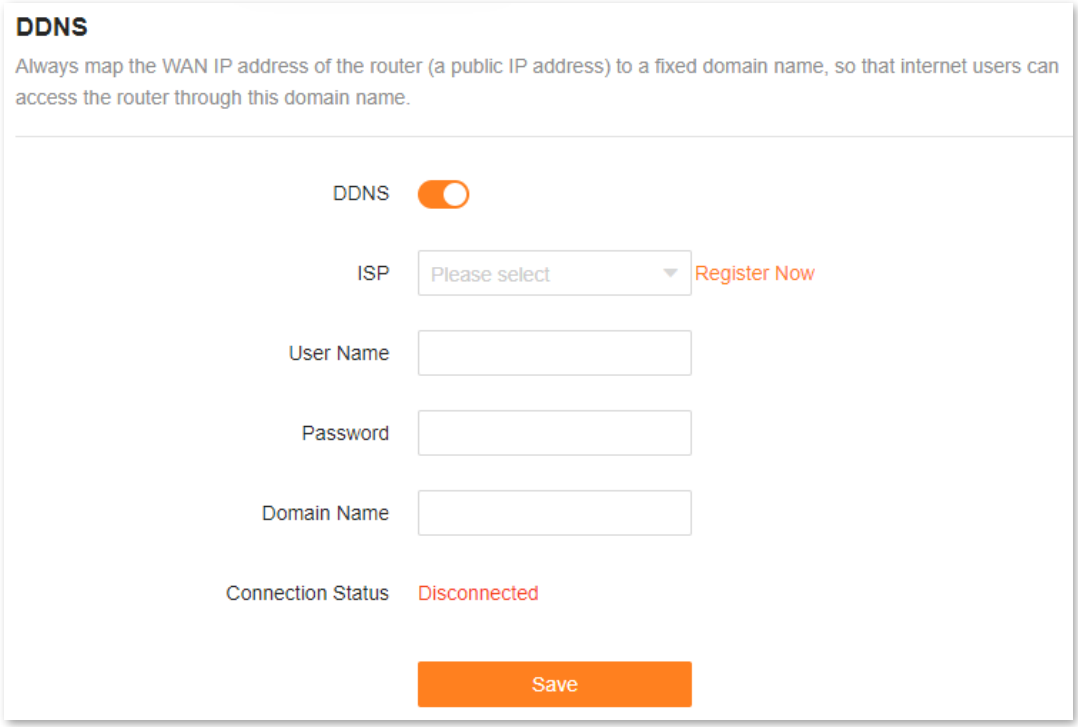
After completing the configuration, you can access both the internet and intranet through RX27 Pro at the same time.

9.10.7 DDNS

Overview

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

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



The following table describes the parameters displayed on this page.

Parameter description

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

An example of enabling 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:

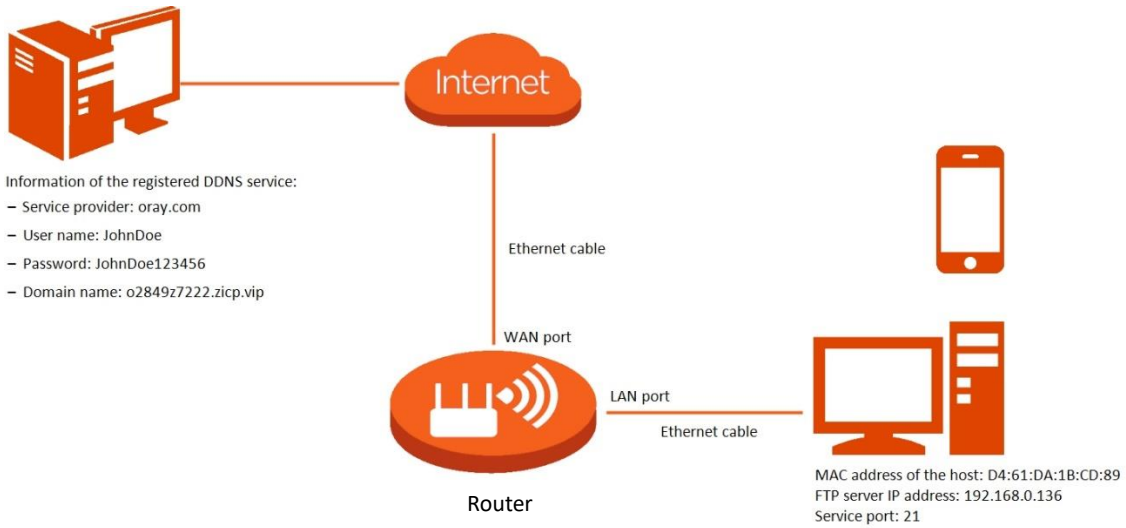
- IP address: **192.168.0.136**
- MAC address of the host: **D4:61:DA:1B:CD:89**
- Service port: **21**

Information of the registered DDNS service:

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

TIP

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.

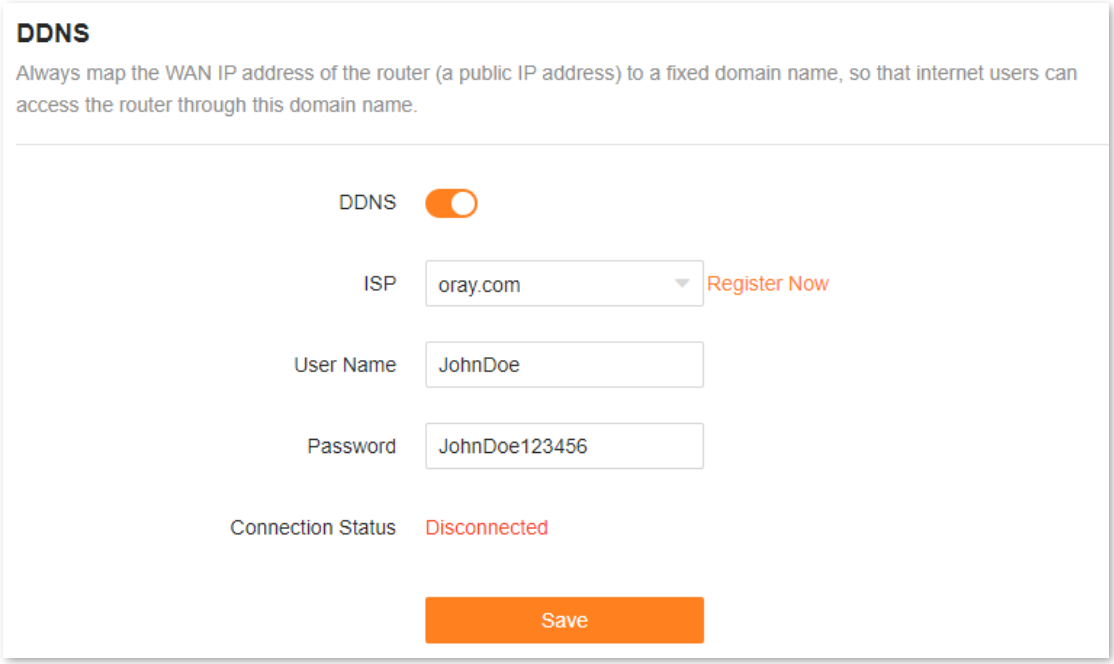


Configuration procedure:

Step 1 Log in to the web UI.

Step 2 Configure the DDNS function.

1. Choose **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**.

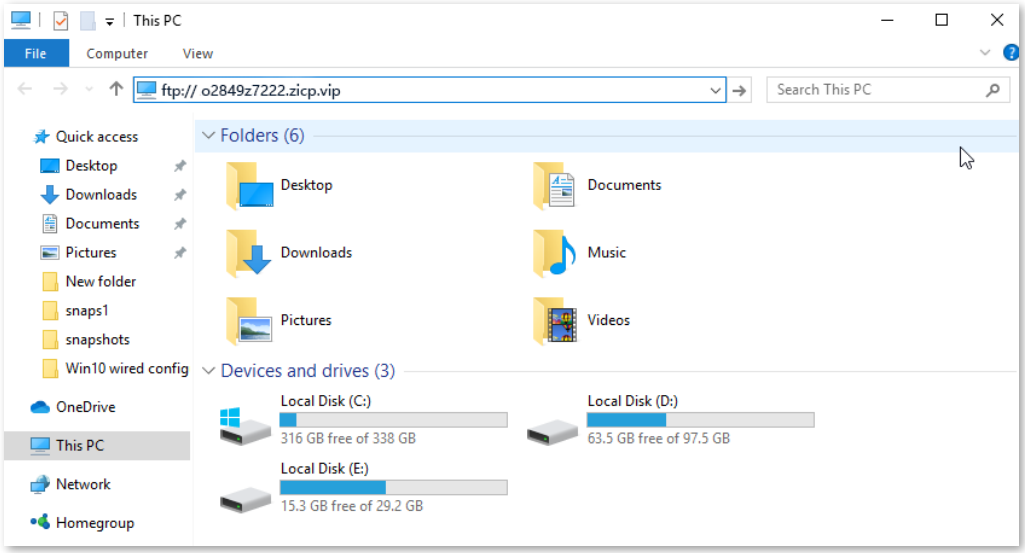


Wait until **Connected** is displayed after **Connection Status**, which indicates that the configuration is successful.

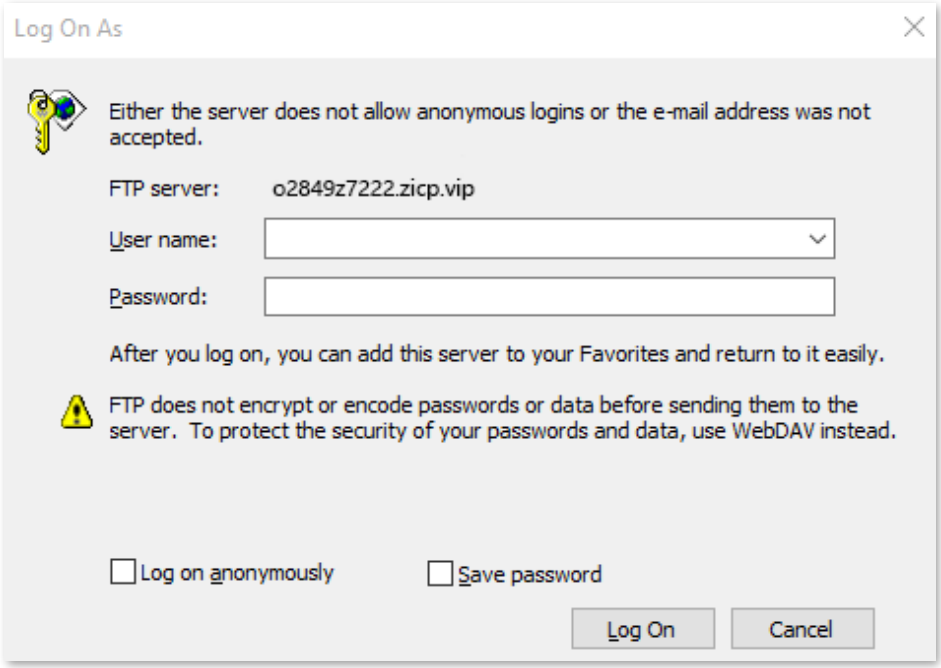
Step 3 Configure the port mapping function by following the steps in Port mapping.

---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.



TIP

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

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

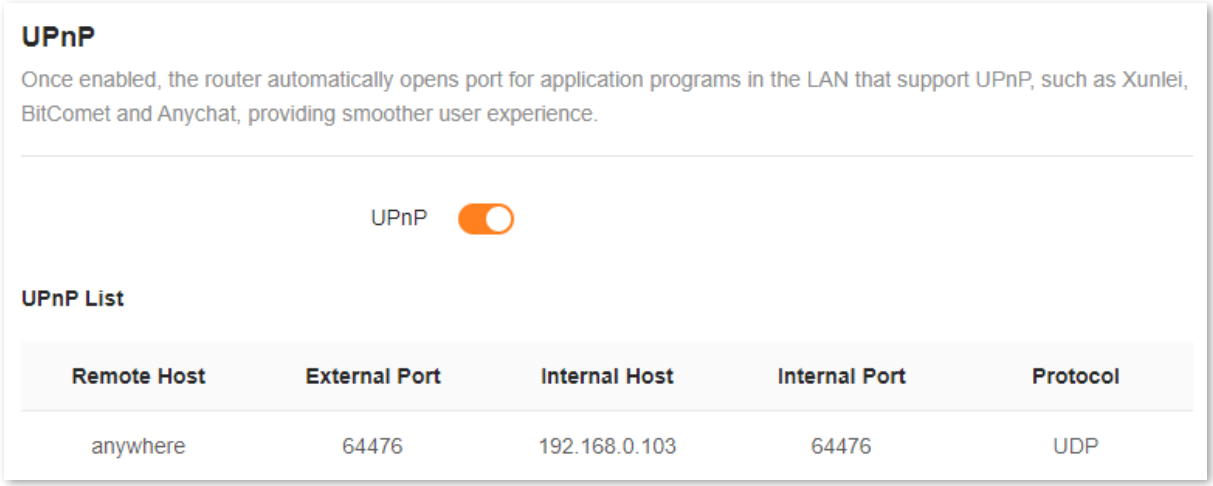
9.10.8 UPnP

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 choose **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.



The following table describes the parameters displayed on this page.

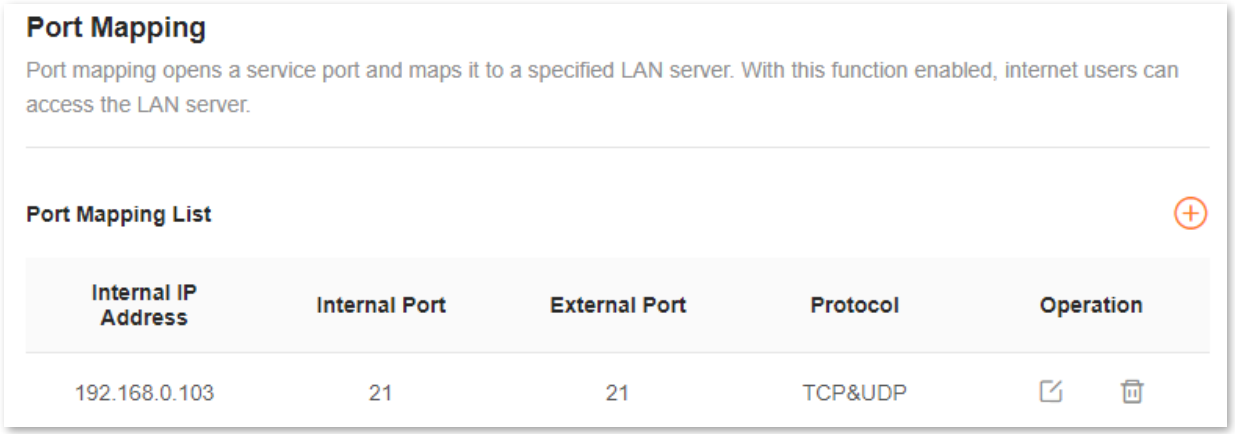
Parameter description

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

9.10.9 Port mapping

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 choose **More** > **Advanced** > **Port Mapping**.



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.
External Port	Specifies the external port for the internal port to map with.
Protocol	Specifies the mapping protocol.
Operation	The available options include: : Used to edit a port mapping rule. : Used to delete a port mapping rule.

An example of configuring port mapping

Scenario: You want to share some large files with your friends who are not on your LAN. However, it is not convenient to transfer such large files across the network.

Goal: Set up your own PC as an FTP server and let your friends access these files.

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

Assume that:

- IP address of the FTP server: 192.168.0.100
- User name and password of the FTP server: admin
- Port of the FTP server: 21
- IP address of the WAN port: 172.16.200.72

To achieve such a goal:

Step 1 Log in to the web UI.

Step 2 Choose **More** > **Advanced** > **Port Mapping**.

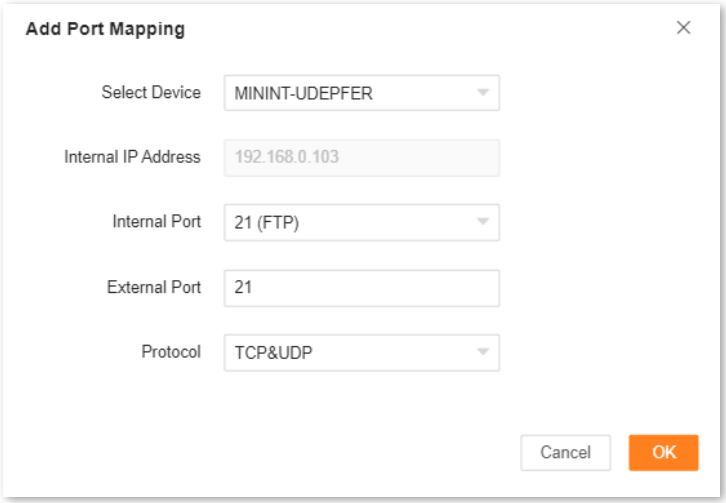
Step 3 Click ⊕.

Step 4 Select your computer for **Select Device**, **21 (FTP)** for **Internal Port**, and **TCP&UDP** for **Protocol**.

TIP

- 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.

Step 5 Click **OK**.



---End

Now your friends can access your files by visiting ftp:// 172.16.200.72 using their computers with internet access.

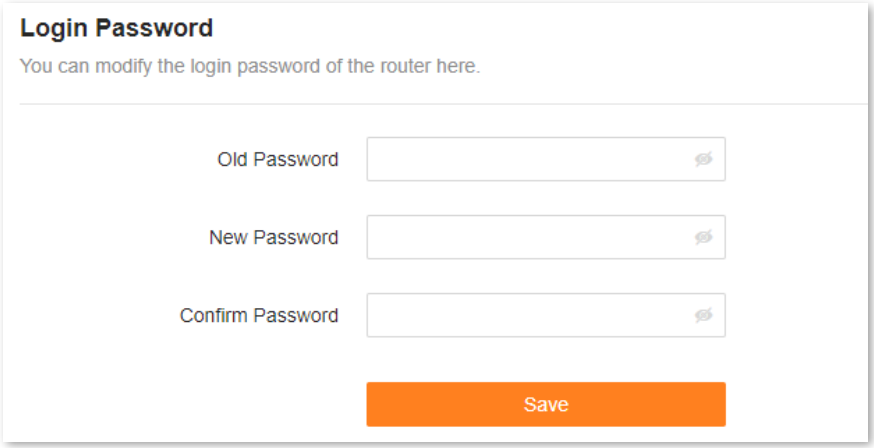
9.11 System settings

9.11.1 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.

To access the configuration page, log in to the web UI and choose **More** > **System Settings** > **Login Password**.

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



The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
Old Password	Specifies the original password that you set before.
New Password	Specify the new password that you want to set.
Confirm Password	

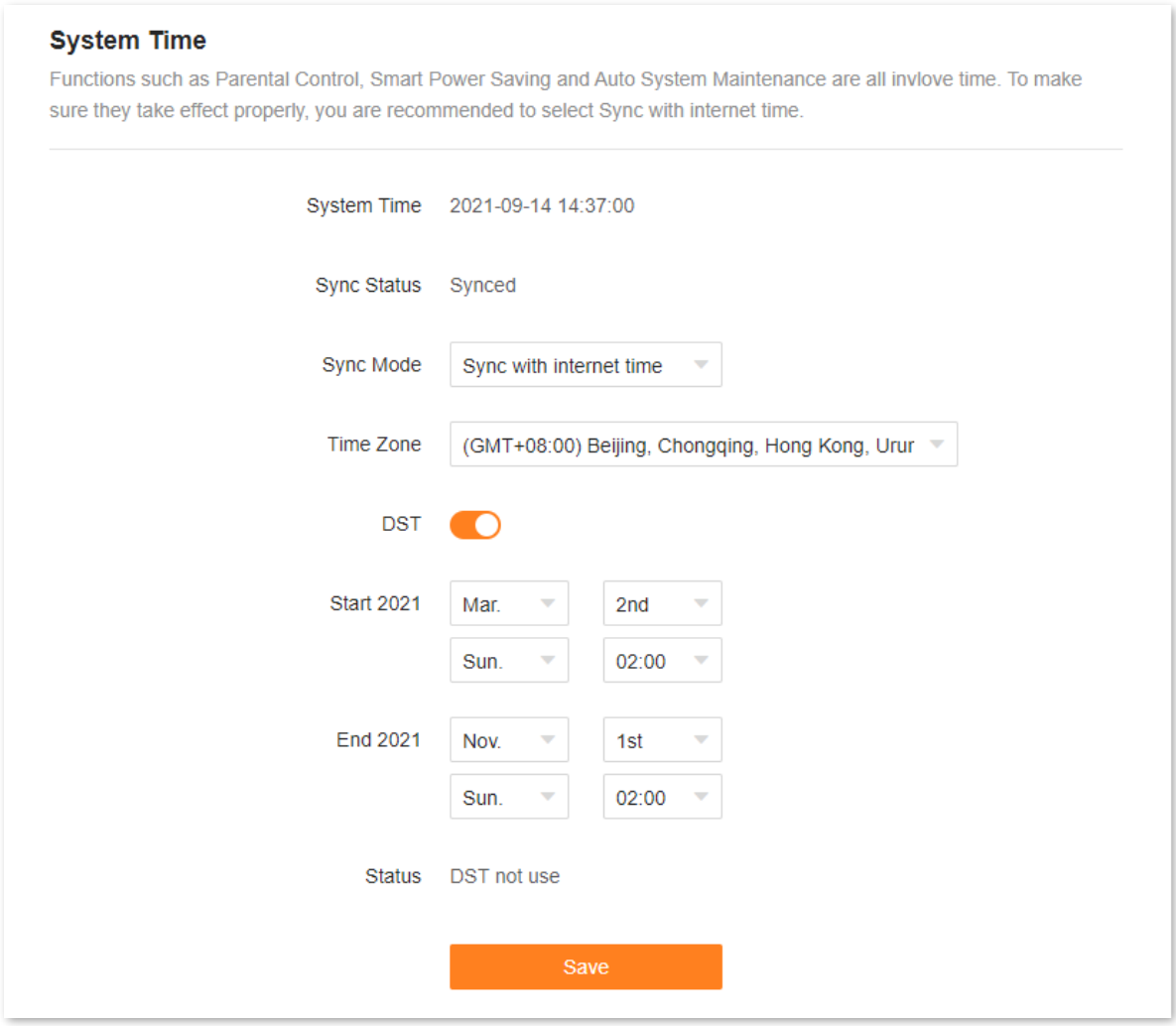
TIP

If you forgot your password, see Forgot my password.

9.11.2 System time

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

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



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	Specifies the sync mode of the system time. • **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	Required when **Sync with internet time** is selected for **Sync Mode**. It specifies the time zone used for the system time. Select one option as required.

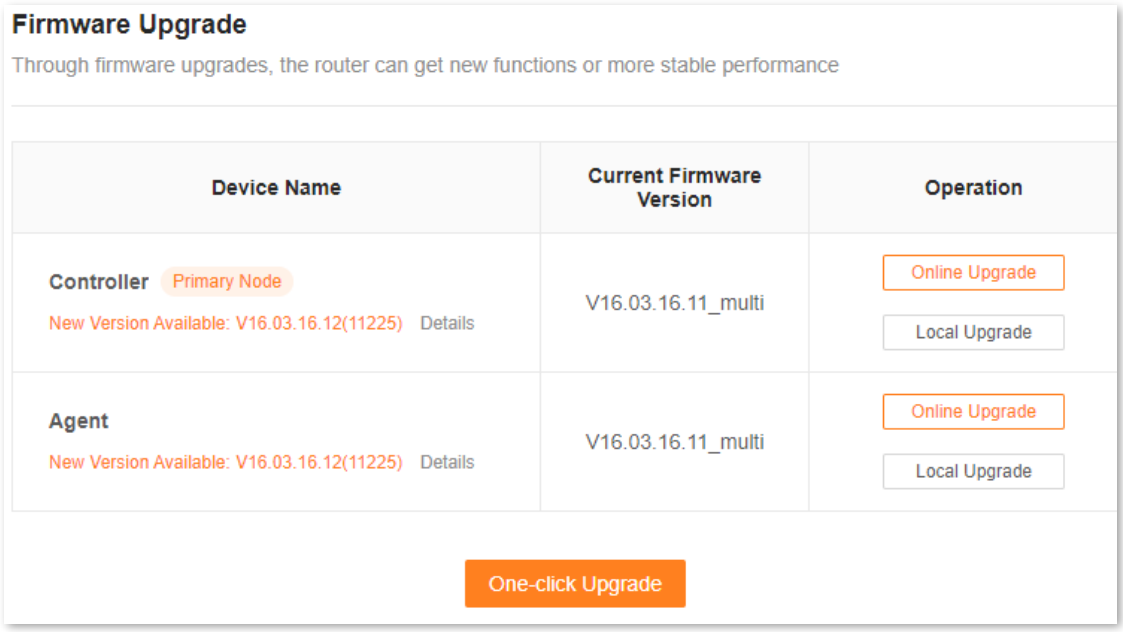
Parameter	Description
Local Time	Displayed when **Sync with Local Time** is selected for **Sync Mode**. It specifies the local time set on your host.
DST	Used to enable or disable the Daylight Saving Time (DST) function. It is disabled by default.
Start *2021*	Required when **DST** is enabled. It specifies the start time of DST.
End *2021*	Required when **DST** is enabled. It specifies the end time of DST.
Status	Displayed when **DST** is enabled. It specifies whether the DST is used.

9.11.3 Firmware upgrade

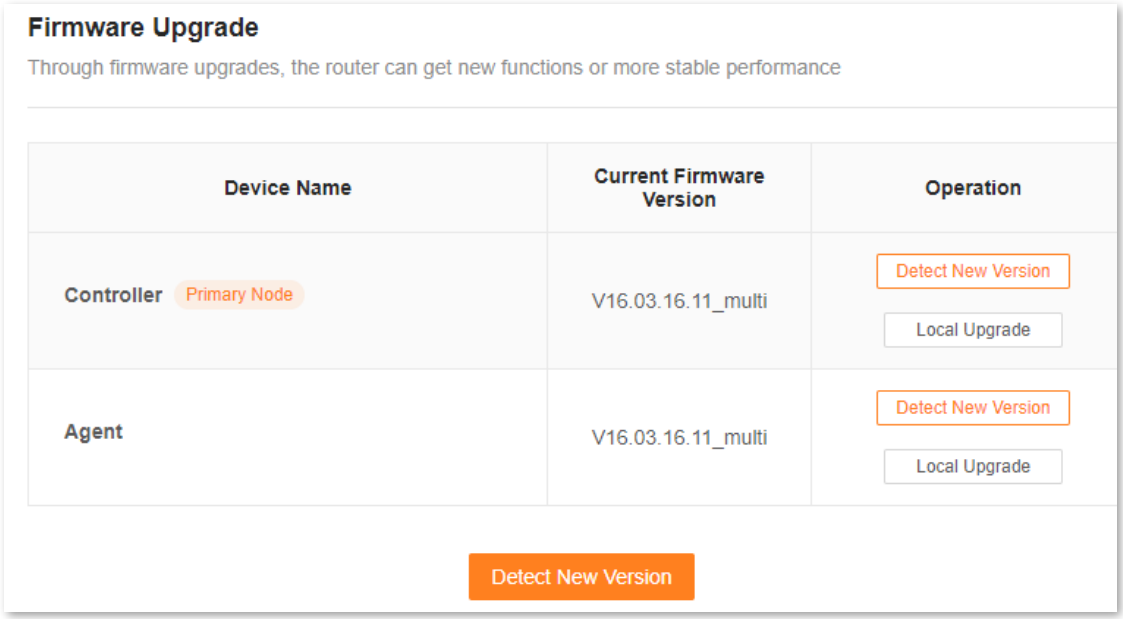
With this function, you can upgrade the firmware of the router to obtain the latest functions and more stable performance. The router supports one-click upgrade, online upgrade and local upgrade.

To access the configuration page, log in to the web UI of the router, and choose **More** > **System Settings**> **Firmware Upgrade**.

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



If auto-detection does not start, you can click **Detect New Version** to check for new versions.



One-click upgrade

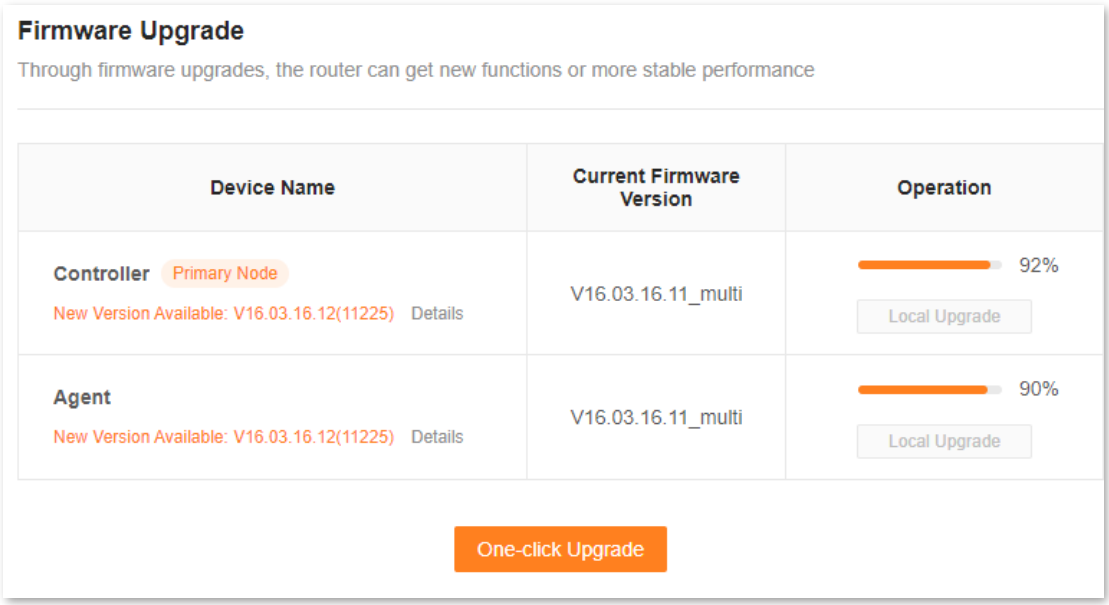
To perform one-click upgrade on all nodes:

Step 1 Log in to the web UI.

Step 2 Choose **More** > **System Settings** > **Firmware Upgrade**.

Step 3 Click **One-click Upgrade**.

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



Online upgrade

To perform online upgrade on a single node:

Step 1 Log in to the web UI.

Step 2 Choose **More** > **System Settings** > **Firmware Upgrade**.

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

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

---End

TIP

For better performance of the new firmware of the router, you are recommended to reset the router to factory settings and re-configure the router after the upgrade completes.

Local upgrade

NOTE

To prevent the router from being damaged:

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

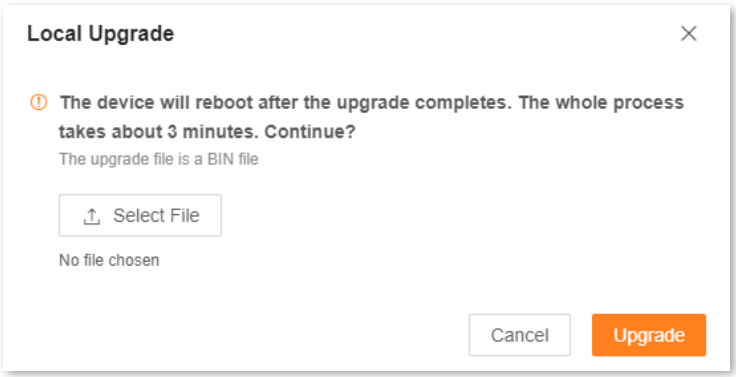
Step 1 Go to www.tendacn.com. Download applicable firmware of the router to your local computer and unzip it.

Step 2 Log in to the web UI.

Step 3 Choose **More** > **System Settings** > **Firmware Upgrade**.

Step 4 Click **Local Upgrade** in the line of the node to be upgraded.

Step 5 Click **Select File**.



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

Step 7 Click **Upgrade**.

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

---End

TIP

For better performance of the new firmware, you are recommended to reset the router to factory settings and re-configure the router after the upgrade completes.

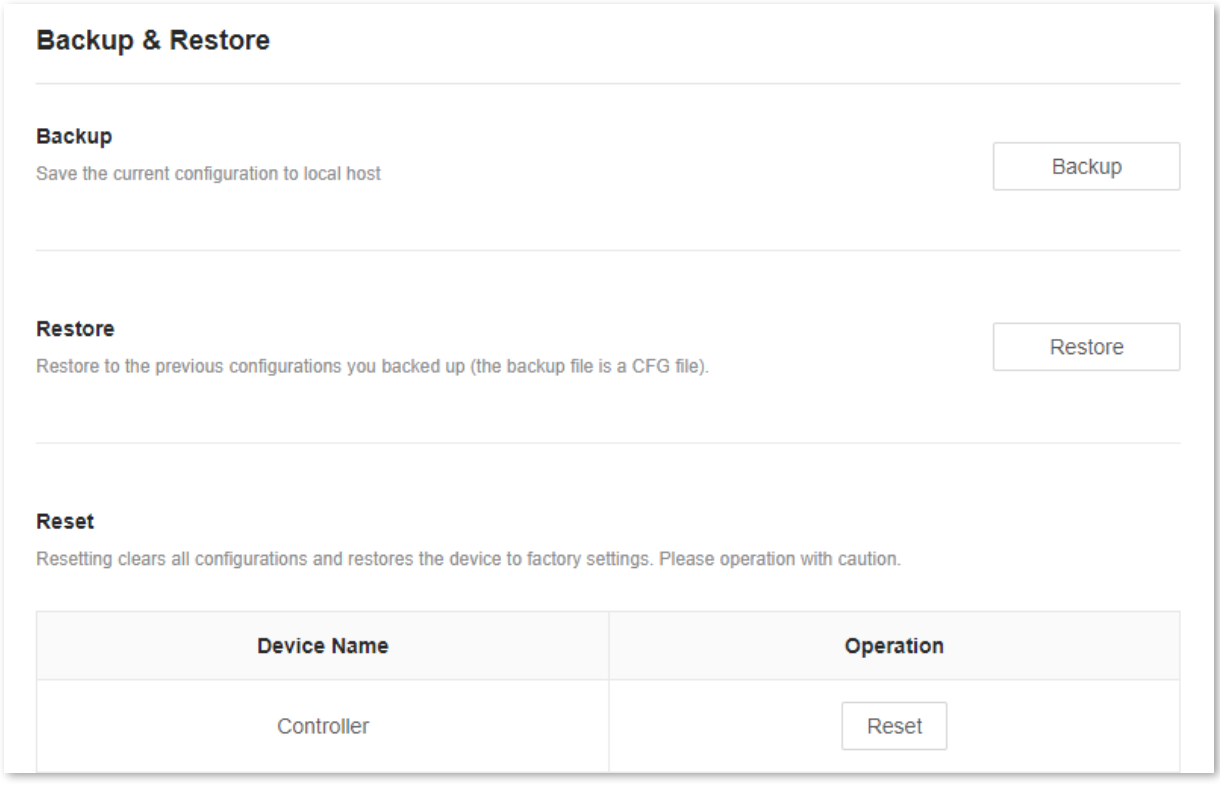
9.11.4 Backup & restore

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

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



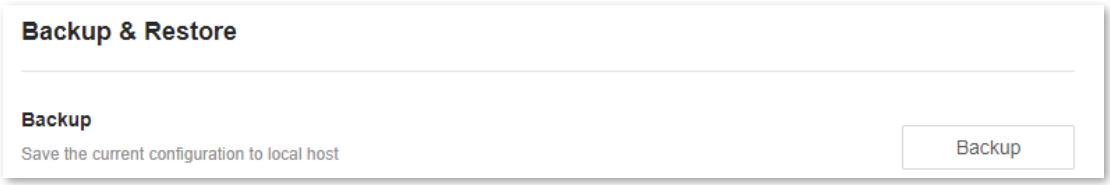
Back up the configuration of the router

To back up the configuration of the router:

Step 1 Log in to the web UI.

Step 2 Choose **More** > **System Settings** > **Backup & Restore.**

Step 3 Click **Backup**.



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

---End

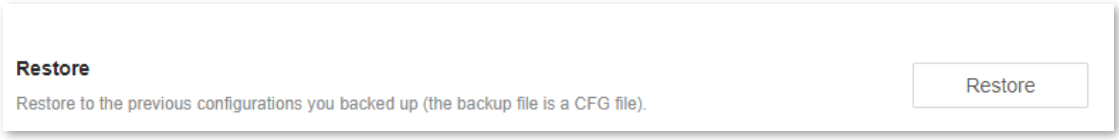
Restore the previous configuration of the router

To restore the previous configuration of the router:

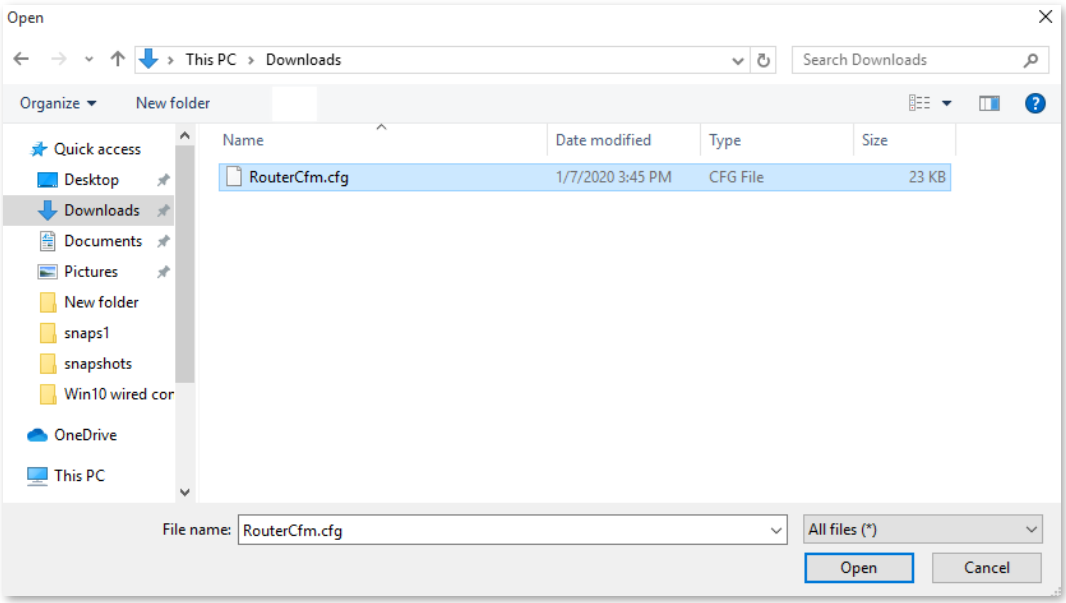
Step 1 Log in to the web UI.

Step 2 Choose **More** > **System Settings** > **Backup & Restore.**

Step 3 Click **Restore**.



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



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

---End

Reset a node

NOTE

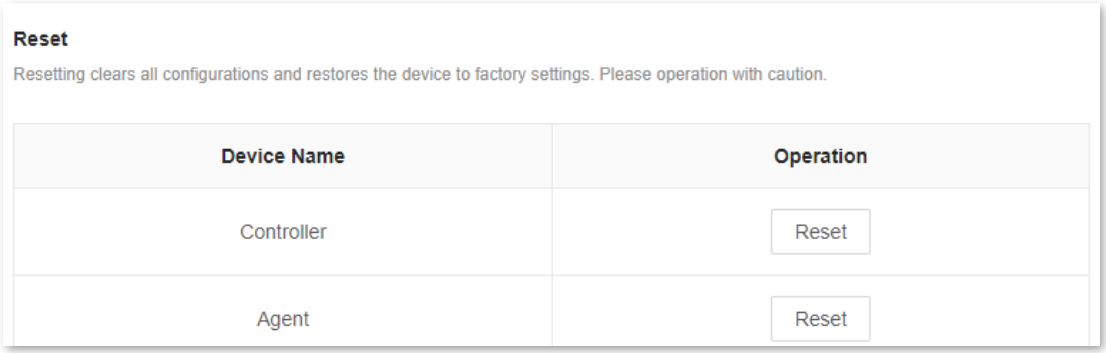
Resetting clears all configurations and restores the router to factory settings. Please operate with caution.

To reset a node:

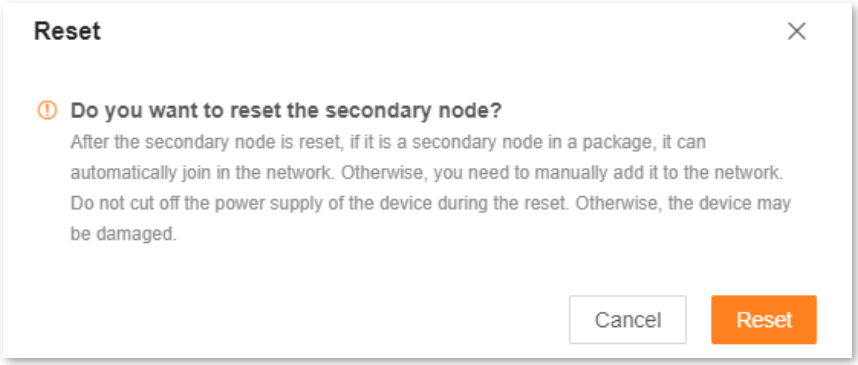
Step 1 Log in to the web UI.

Step 2 Choose **More** > **System Settings** > **Backup & Restore.**

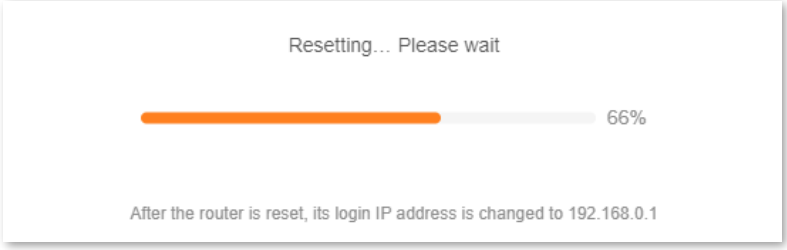
Step 3 Click **Reset** in the line of the node to be reset.



Step 4 Click **Reset** in the displayed dialog box.



Wait until the reset completes.

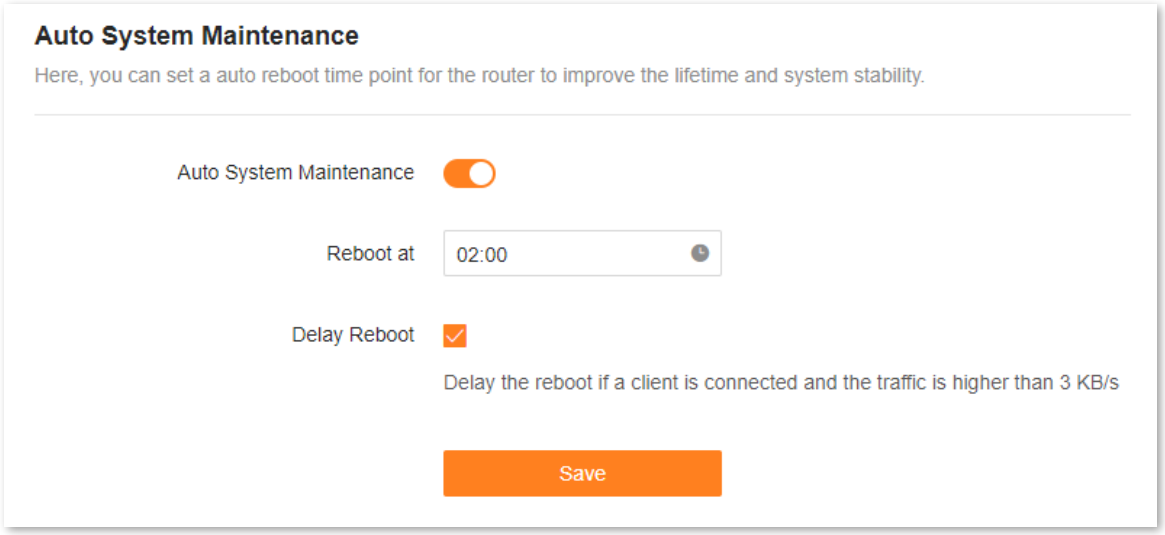


---End

9.11.5 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 choose **More** > **System Settings** > **Auto System Maintenance.**



The following table describes the parameters displayed on this page.

Parameter description

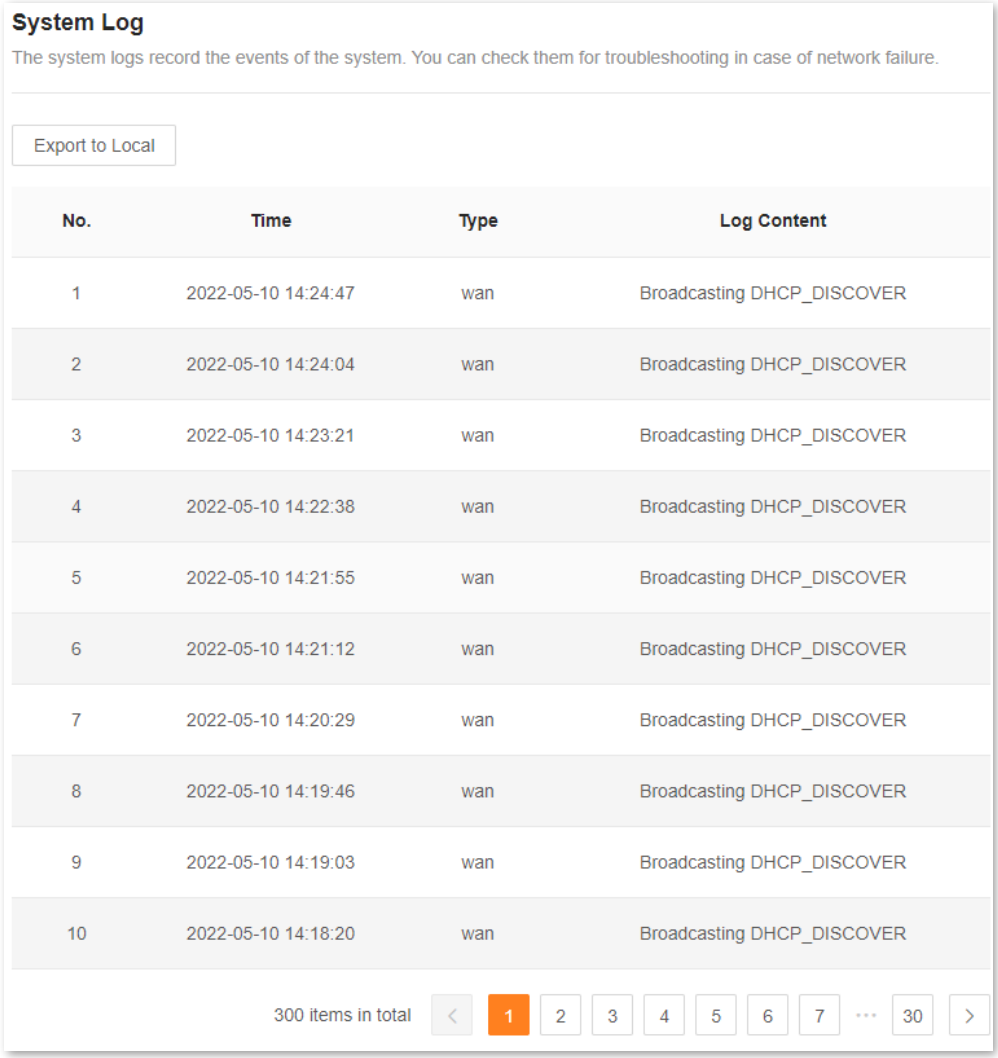
Parameter	Description
Auto System Maintenance	Used to enable or disable the auto system maintenance function.
Reboot At	Specifies the time when the router reboots automatically every day.
Delay Reboot	Used to enable or disable the reboot delay function. • Ticked: The function is enabled. When the time for rebooting approaches, if there is any user connected to the router and the traffic over the router's WAN port exceeds 3 KB/s, the router will delay rebooting. • Unticked: The function is disabled. The router reboots immediately when the specified time for rebooting approaches.

9.11.6 System log

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

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



TIP

Rebooting the router will clear all previous system logs.

10 FAQ

10.1 Failed to access the web UI

Use the following method to troubleshoot the fault, and then try again.

- If you are using a wireless device, such as a smartphone:
  - Ensure that it is connected to the Wi-Fi network of the router.
  - Ensure that the cellular network (mobile data) of the client is disabled.
  - Use another smartphone or tablet to log in to the web UI.
- If you are using a wired device, such as a computer:
  - Ensure that the Ethernet cable between your computer and the router is connected properly.
  - Ensure that your computer is set to **Obtain an IP address automatically**.
  - Ensure that the login IP address (**192.168.0.1** by default) you entered is correct.
  - Clear cache of your browser, or use another browser.
  - Use another computer to log in to the web UI.
  - Hold down the **Reset** button for about 8 seconds to restore the router to factory settings.

10.2 Internet detection failed upon the first setup

Use the following method to troubleshoot the fault, and then try again.

- Ensure that the Ethernet cable for internet connection is connected to the WAN port of the router.
- Ensure that the Ethernet cable is well-connected and not damaged, and the modem is powered on.
- If the problem persists, please contact your ISP.

10.3 Failed to find or connect my wireless network

Use the following method to troubleshoot the fault.

- If you cannot find any wireless network:
  - Check that the wireless function is enabled when you are using a laptop with a built-in wireless adapter.
  - Check that the wireless adapter is installed properly and enabled successfully.
- If you can find other wireless networks except yours, ensure that your device is in the Wi-Fi network coverage range of your routers.

10.4 Forgot my password

Use the following method to troubleshoot the fault.

- If you used the same password for Wi-Fi login and web UI login, reset the router by holding down the **Reset** button with a needle-like item (such as a pin) for about 8 seconds, and perform settings again.
- If you used different passwords for Wi-Fi login and web UI login:
  - If you forgot the web UI login password, reset the primary node by holding down the **Reset** button with a needle-like item (such as a pin) for about 8 seconds, and perform settings again.
  - If you remember the web UI login password but forget the Wi-Fi login password, log in to the web UI and navigate to **WiFi Settings** to check the Wi-Fi login password.

Appendixes

A.1 Factory settings

Parameter		Default value
Login	IP address	192.168.0.1
	Password	No login password by default
LAN parameters	IP address	192.168.0.1
	Subnet mask	255.255.255.0
DHCP server	DHCP server	Enabled
	Start IP address	192.168.0.100
	End IP address	192.168.0.200
	Preferred DNS server	192.168.0.1
Operating mode		Router mode
Wireless settings	Wi-Fi name	See the label on the bottom of the router.
IPv6		Disabled
Unify 2.4 GHz & 5 GHz		Disabled
Unify 2.4 GHz & 5 GHz & 6GHz		Disabled
Guest Wi-Fi		Disabled
VPN		Disabled
IPTV		Disabled
App remote management		Disabled
MAC address filter		Disabled

Parameter	Default value
DMZ host	Disabled
Remote web management	Disabled
DDNS	Disabled
UPnP	Enabled
Time sync mode	Sync with internet time
DST	Disabled
Auto system maintenance	Enabled Default reboot time: 02:00

A.2 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
MPPE	Microsoft Point-to-Point Encryption
MTU	Maximum Transmission Unit
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point to Point Tunneling Protocol

Acronym or Abbreviation	Full Spelling
RA	Router Advertisement
SSID	Service Set Identifier
STB	Set-top box
TCP	Transmission Control Protocol
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
WPA-PSK	WPA Pre-shared Key
WPA3-SAE	WPA3-Simultaneous Authentication of Equals
WPS	Wi-Fi Protected Setup