AX3000 Whole Home Mesh Wi-Fi6 System

User Guide

V1.0

Copyright Statement

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, Tenda reserves the right to make changes to the products without obligation to notify any person or organization of such revisions or changes. Tenda does not assume any liability that may occur due to the use or application of the product described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute a warranty of any kind, express or implied.

Preface

Thank you for choosing Tenda!

This user guide walks you through all functions on the AX3000 Whole Home Mesh Wi-Fi6 System, which can be managed on both the web UI and app. All the screenshots and product figures herein, unless otherwise specified, are taken from MX12.

TIP

- The web UI of different models may differ. The web UI actually displayed shall prevail.
- The AX3000 Whole Home Mesh Wi-Fi6 System may include multiple devices. Each of them may be referred to as a "Mesh device", "device" or "router" in this user guide. The whole of them may be referred to as the "Mesh system".

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 MX12 was introduced.

Version	Date	Description
v1.0	2022-03-28	Original publication.

Contents

1 Get to know your device

This chapter introduces the product in the following sections:

1.1 Product overview

The Whole Home Mesh Wi-Fi6 System provides powerful Wi-Fi coverage and seamless roaming experience with multiple nodes working under one unified network. It features easy installation, free networking, and flexible management on both web UI and app. EasyMesh is also supported for the product to interwork with devices of other brands.

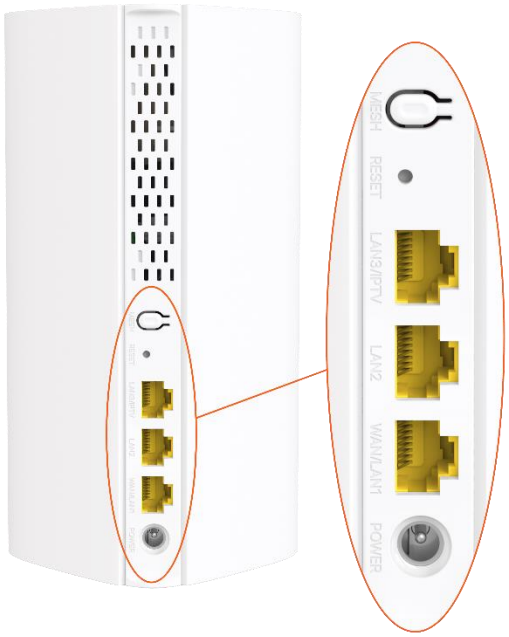
1.2 Appearance

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 started
		Blinking green slowly	Waiting for networking
	During networking	Blinking green slowly	Connecting to other nodes in the same kit or waiting to connect to other nodes TIP This status only exists during the first-time networking.
		Blinking green quickly	Networking by the Mesh button
		Solid on	Networking completed and internet connection succeeded • Solid green: The signal is good. • Solid yellow: The signal is fair. • Solid red: The signal is poor.
		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	Reset completed
	Batch upgrade	Blinking yellow quickly	Batch upgrade succeeded
		Solid yellow	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
MESH	Mesh button. • As a networking button: Press this button on this device for about 1 to 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** button of another device for 1 to 3 seconds to negotiate with this device. • As a de-networking button: Press this button for about 8 seconds and release it when the LED indicator blinks red fast. The node is restored to factory settings, and also removed from the network and no longer automatically joins in again. TIP Do not hold down the **MESH** button for 8 seconds unless necessary.
RESET	Reset button. When the device completes startup, hold down this button using a needle-like item (such as a pin) for about 8 seconds, and then release it when the LED indicator blinks red fast. If the LED indicator blinks green slowly, the device is reset successfully.
LAN3/IPTV	LAN/IPTV multiplexing port, LAN port by default. When the IPTV function is enabled, this port is used as the IPTV port only.
LAN2	LAN port.

Jack/Port/Button	Description
WAN/LAN1	WAN/LAN multiplexing port, WAN port by default. • When the device is used as the primary node, this port is used as the WAN port to connect your optical modem, DSL modem, cable modem or broadband network port. • When the device is used as the secondary node, this port is used as the LAN port to connect your computer, switch, or gaming console.
POWER	Power jack.

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.

Power: Specifies the power of the device.

Login Address: Specifies the default address used to log in to the web UI 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.

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

SN: Specifies the serial number required if you need technical assistance to repair your device.

Password: Specifies the default Wi-Fi password of the device.

2 Web UI operations

This chapter introduces all functions and operations available on the web UI, including:

Some functions and operations are also available on the Tenda WiFi app. For details, see APP operations.

2.1 Quick setup

The device kit you purchased includes multiple devices. You can choose one of them to work as the primary node and others as the secondary nodes to extend your network. This section describes how to connect the devices and enable internet access through the quick setup wizard. It contains the following sections:

2.1.1 Connect your primary node

Connect your primary node with a modem

To connect your primary node with a modem:

Step 1 Power off your modem.

Step 2 Use the included Ethernet cable to connect the **WAN/LAN1** port of the primary node to your modem.

Step 3 Power on your modem.

Step 4 Power on the primary node, and wait until the LED indicator blinks green.

---End

Connect your primary node without a modem

To directly connect your primary node without a modem:

Step 1 Ensure that the network connection status of your Ethernet device is normal.

Step 2 Use an Ethernet cable to connect the **WAN/LAN1** port of the primary node to the LAN port of the Ethernet device.

Step 3 Power on the primary node, and wait until the LED indicator lights solid green.

---End

2.1.2 Connect your primary node to the internet

After connecting your primary node, 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.

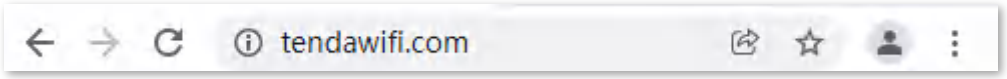
To connect your primary node to the internet through the quick setup wizard:

Step 1 Use an Ethernet cable to connect your computer to the **LAN2** or **LAN3/IPTV** port of the primary node.

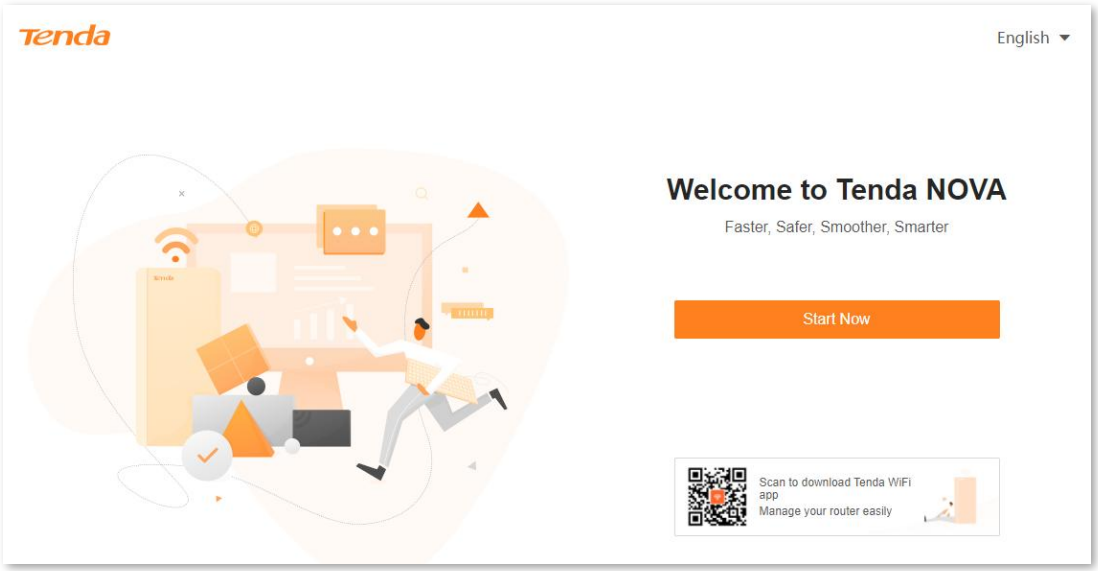
TIP

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

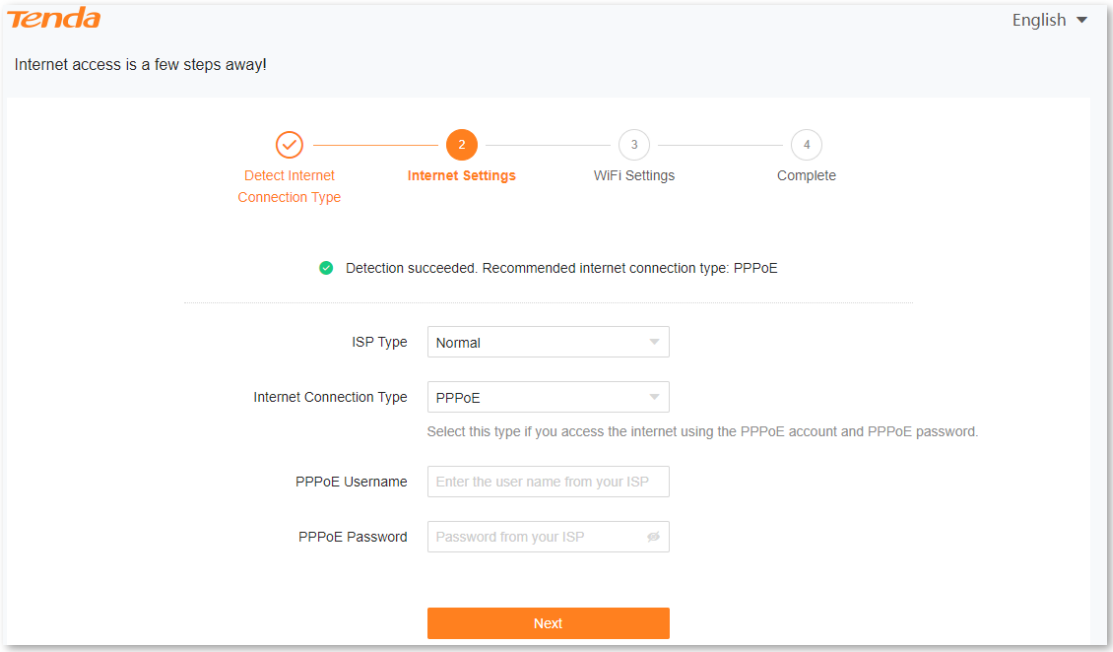
Step 2 Start a browser on the computer and enter **tendawifi.com** in the address bar to access the web UI.



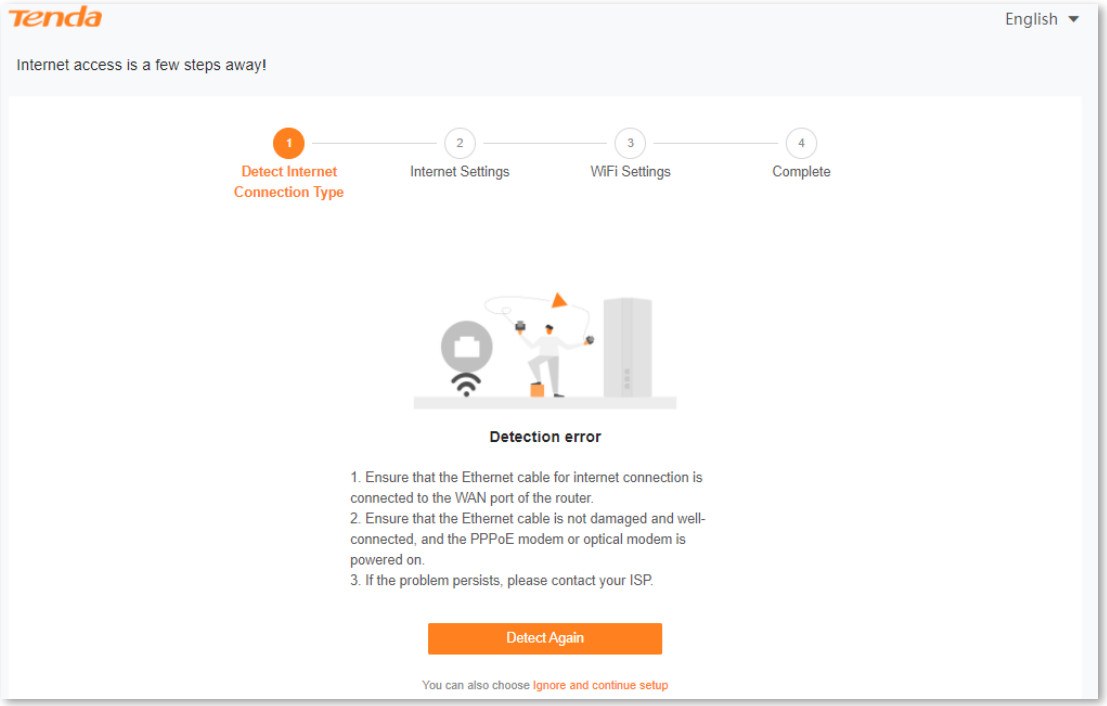
Step 3 Click **Start Now**.



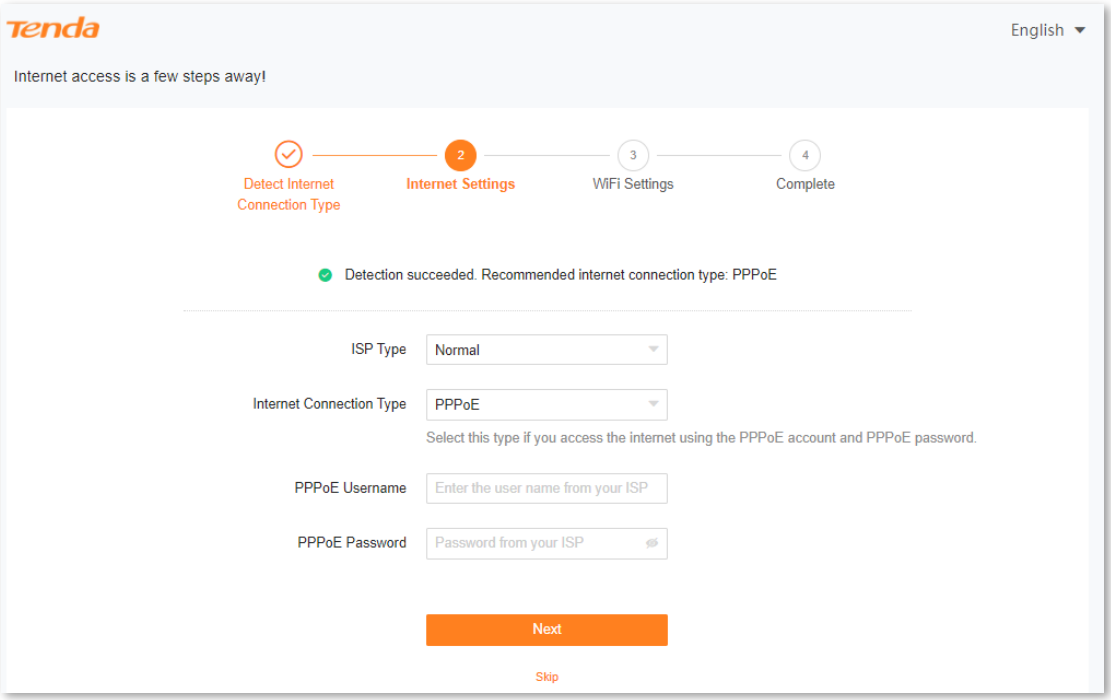
- If your internet connection is normal, the following page is displayed and you can continue the setup in **Step 4**.



- 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**.



The following table describes the parameters displayed on this page.

Parameter description

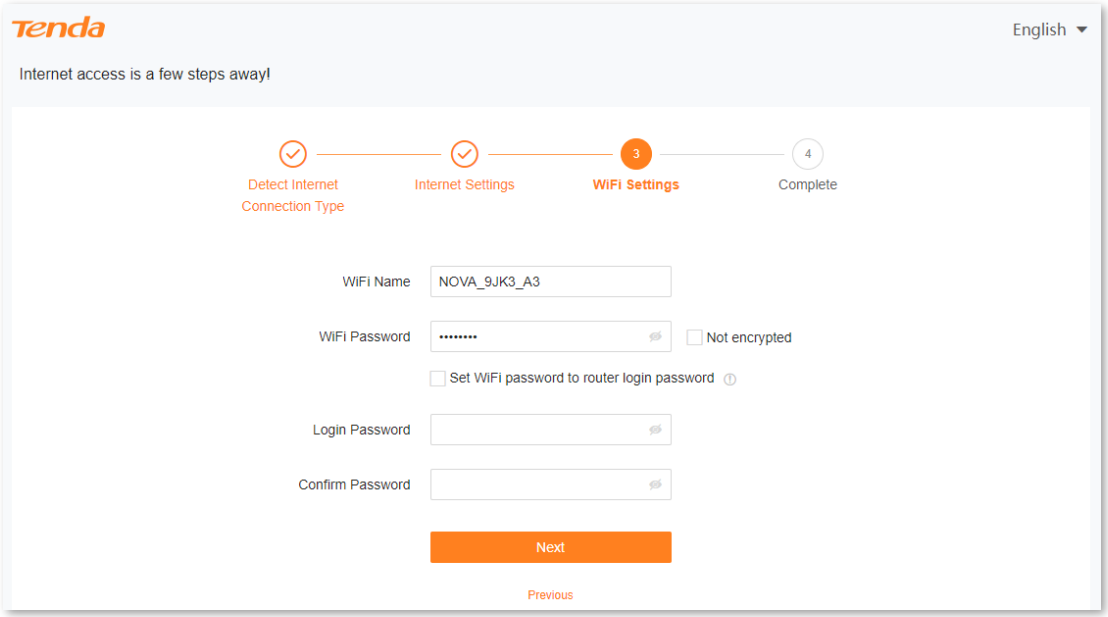
Parameter	Description
ISP Type	Specifies the type of your ISP, such as **Normal**, **Russia**, **Unifi**, **Maxis**, **Maxis-Special**, and **Manual**. Parameters required for each option may differ. Refer to the following to choose your connection type: • **Normal**, **Unifi**, **Maxis**, and **Maxis-Special**: 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.
Internet Connection Type	Specifies how your Mesh device 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**: 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 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.  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 Mesh device obtains a DNS server address from the DHCP server of the upstream network automatically. • **Manual**: The DNS server address is configured manually.

Parameter	Description
Server IP Address/Domain Name	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.
User Name	
Password	
Internet 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.
IPTV VLAN ID	

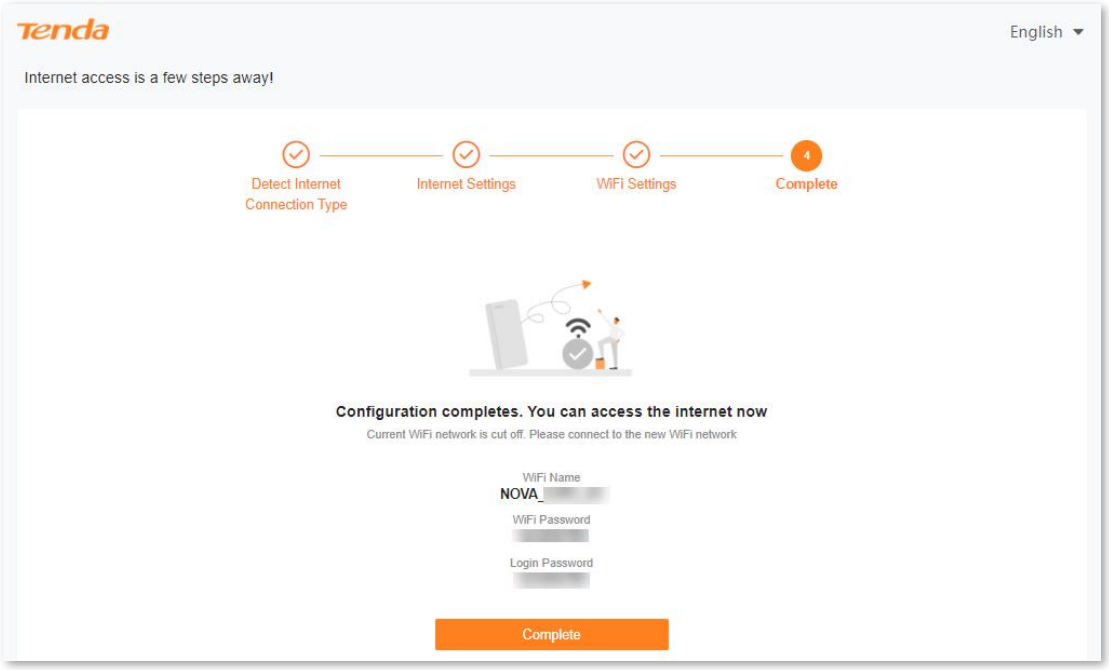
Step 5 Set parameters as required, and click **Next**.

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**.



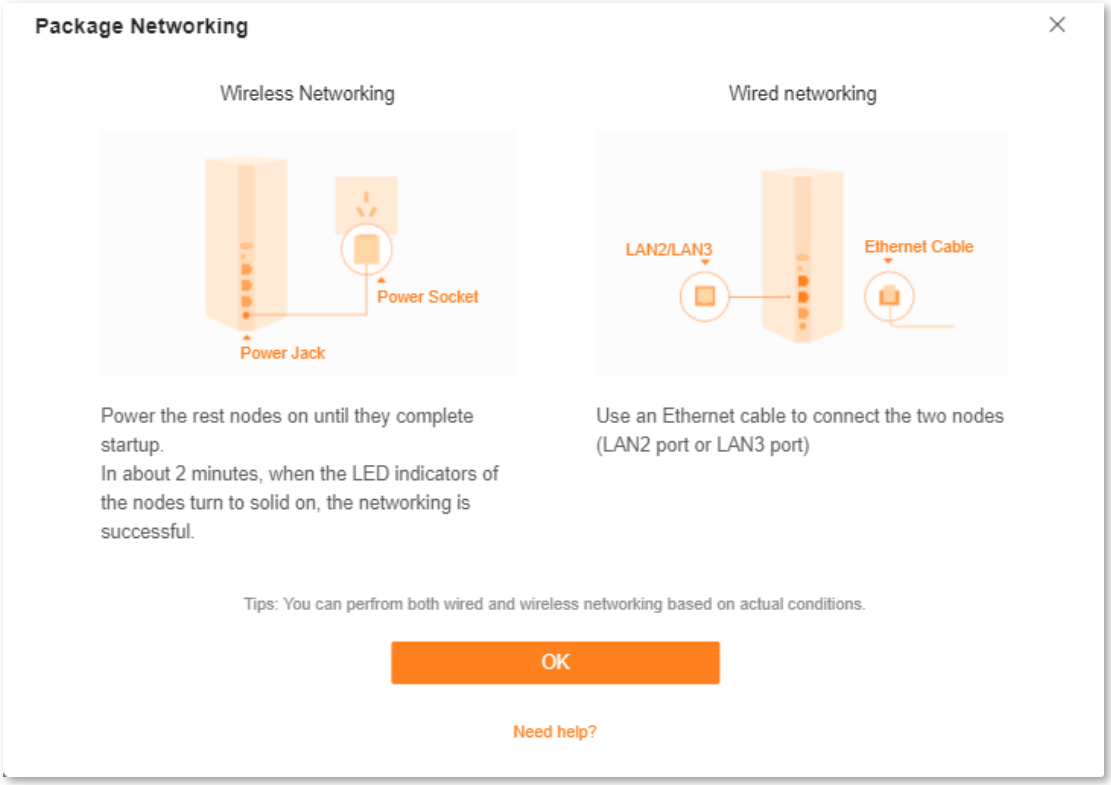
---End

Now you can access the internet with:

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

2.1.3 Extend your network

Upon your first login, the following information is displayed to tell you how to extend the network with secondary nodes in the same kit. To extend the network with other nodes, see Add a node.



To extend your network with secondary nodes in the same kit:

Step 1 Connect secondary nodes by following the instructions displayed, as shown in the preceding figure.

When the LED indicators of secondary nodes light solid green, the networking is successful.

Step 2 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 3 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 4 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.
Solid red	Networking succeeds. Poor connection quality.

If any secondary node's LED indicator lights solid red, relocate it by repeating **Steps 2** to **4**.

---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.)

2.2 Web UI

This section introduces basic information of the web UI, including:

2.2.1 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 **LAN2** or **LAN3/IPTV** port of the primary node, or use your smartphone to access the Wi-Fi network of the primary node.

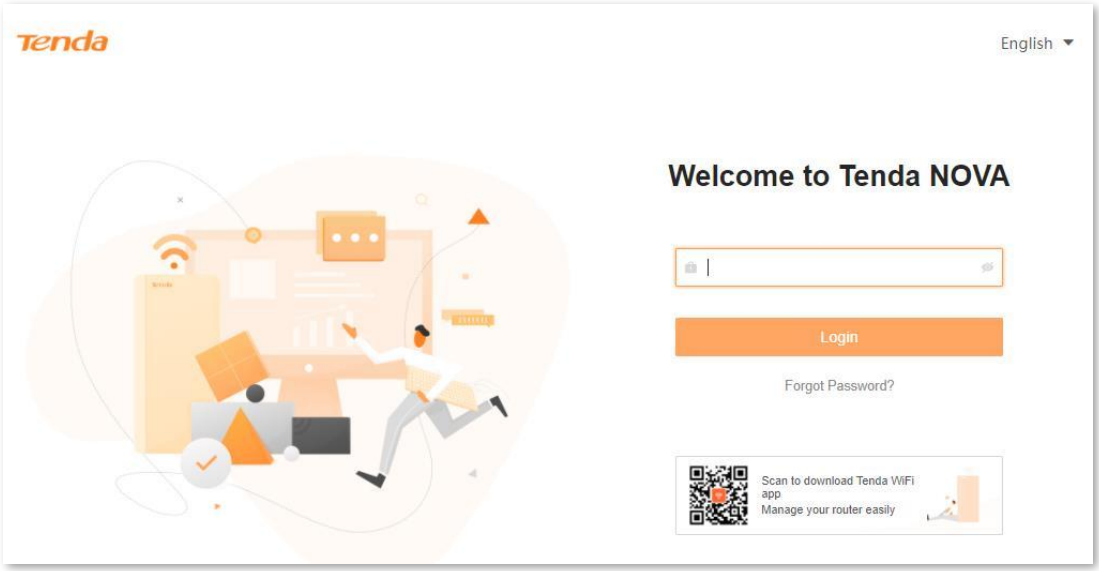
In the following steps, computer connection is used for illustration.

TIP

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

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 your primary node to the internet.
- The password is the one that you specified in Connect your primary node to the internet. It is case-sensitive. If you forgot the password, go to Forgot my password.

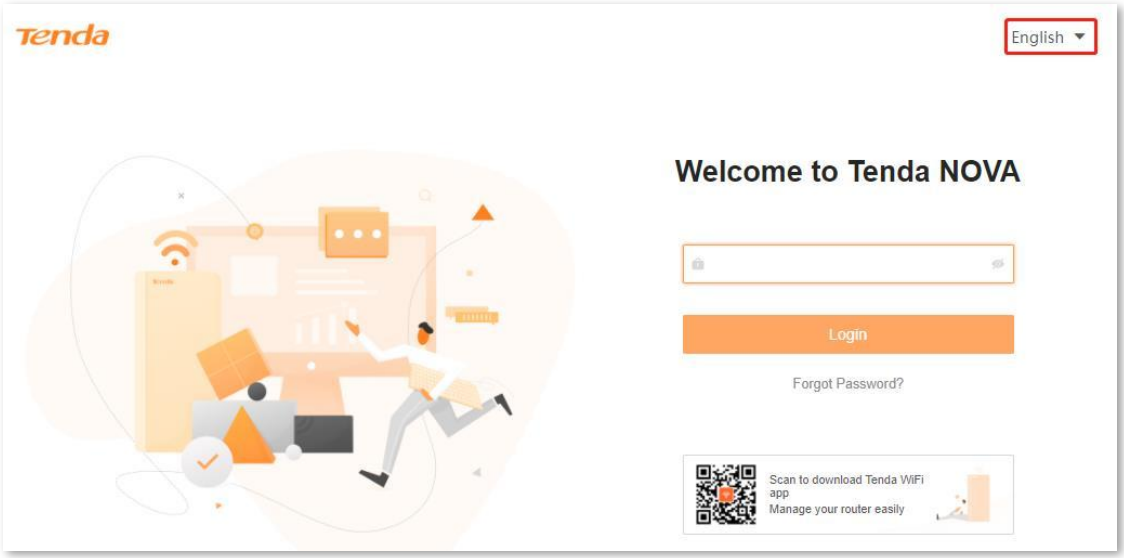
---End

2.2.2 Log out of the web UI

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

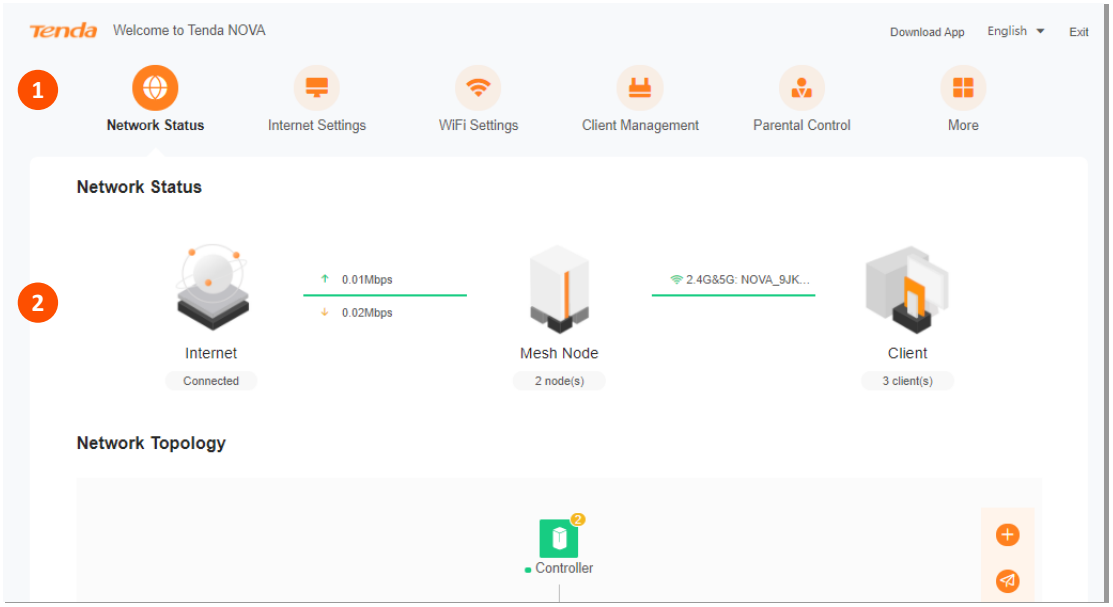
2.2.3 Change the language

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



2.2.4 Web UI layout

The web UI of the Mesh device 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 Mesh device. Users can select functions in the navigation bar.
2	Configuration area	Used to modify or view your configuration.

2.3 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 section includes the following parts:

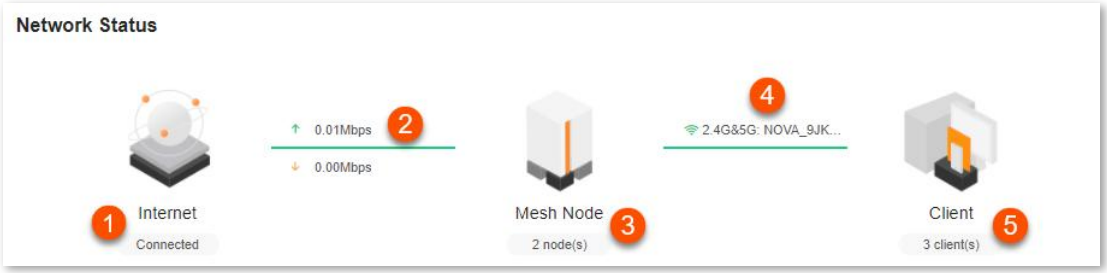
2.3.1 Network status

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 primary node is connected to the internet successfully. • **Disconnected**: The primary node 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 Wi-Fi name and frequency band.
5	Indicates the number of clients connected in the network, including secondary Mesh nodes.

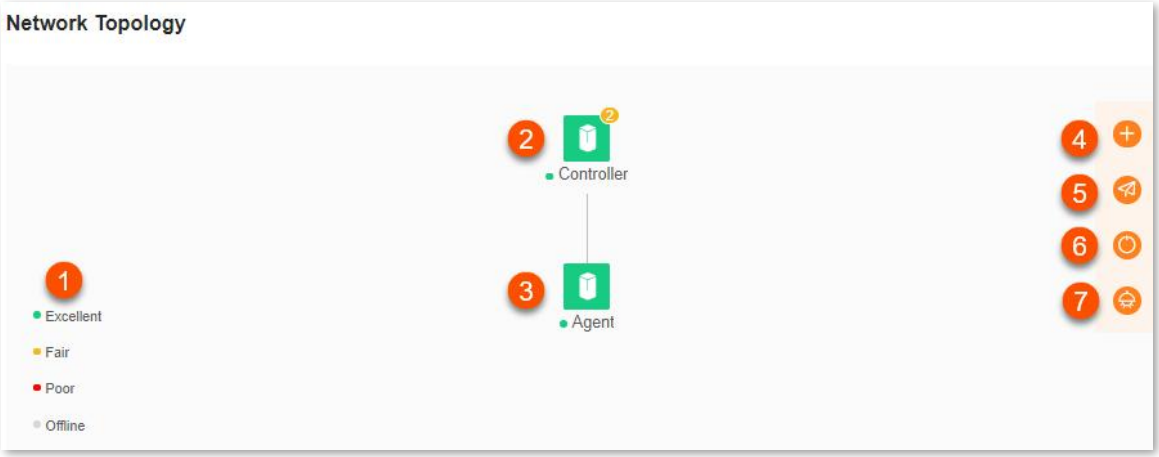
2.3.2 Network topology

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.

Controller information

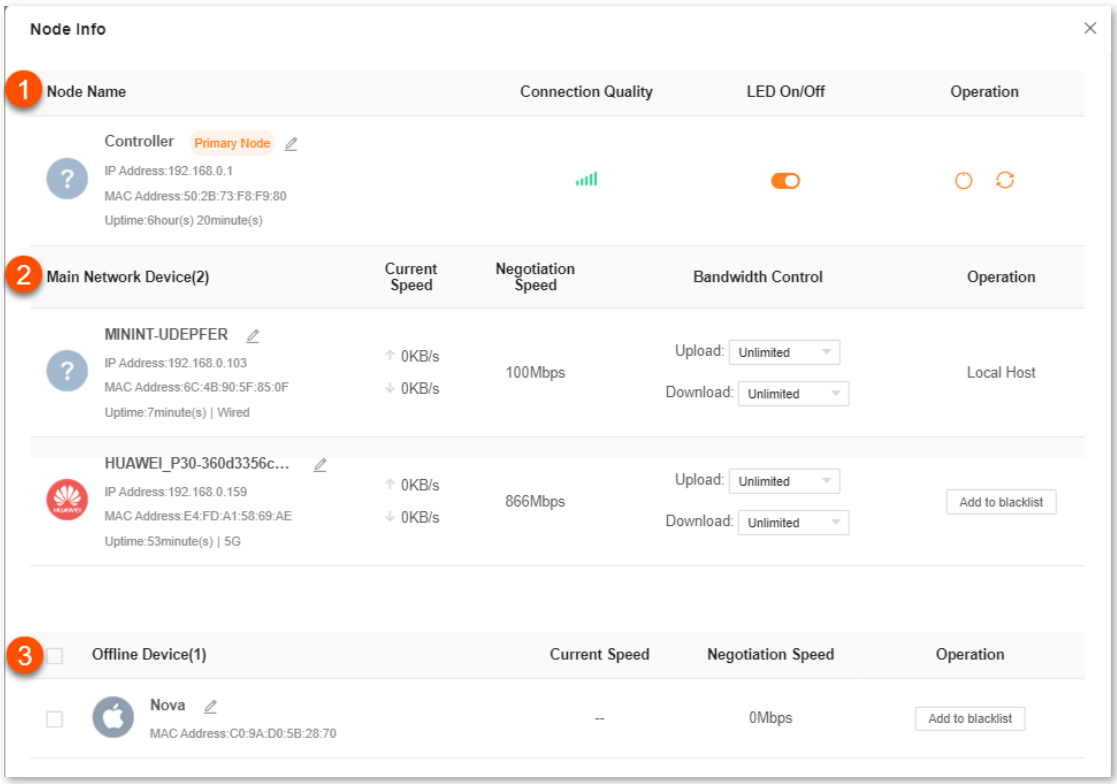
To view the information about and perform quick operations on the controller (primary node) and clients in the network:

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** and **5G**. • **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 20 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).

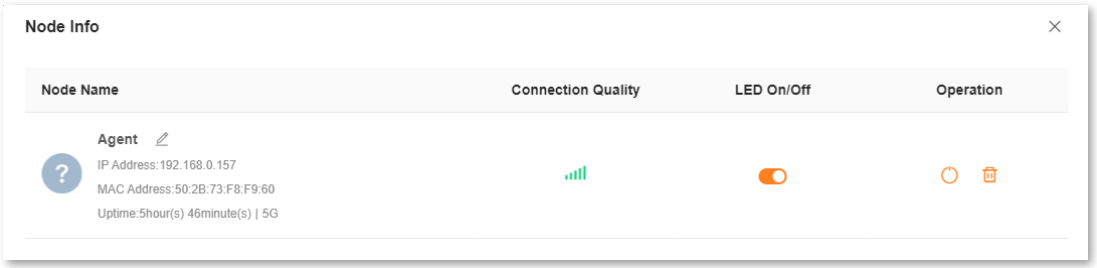
Agent information

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.
Uptime	Indicates the network connection time of the secondary node and the networking mode, such as **Wired**, **2.4G** and **5G**.

Parameter	Description
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.

Add a node

NOTE

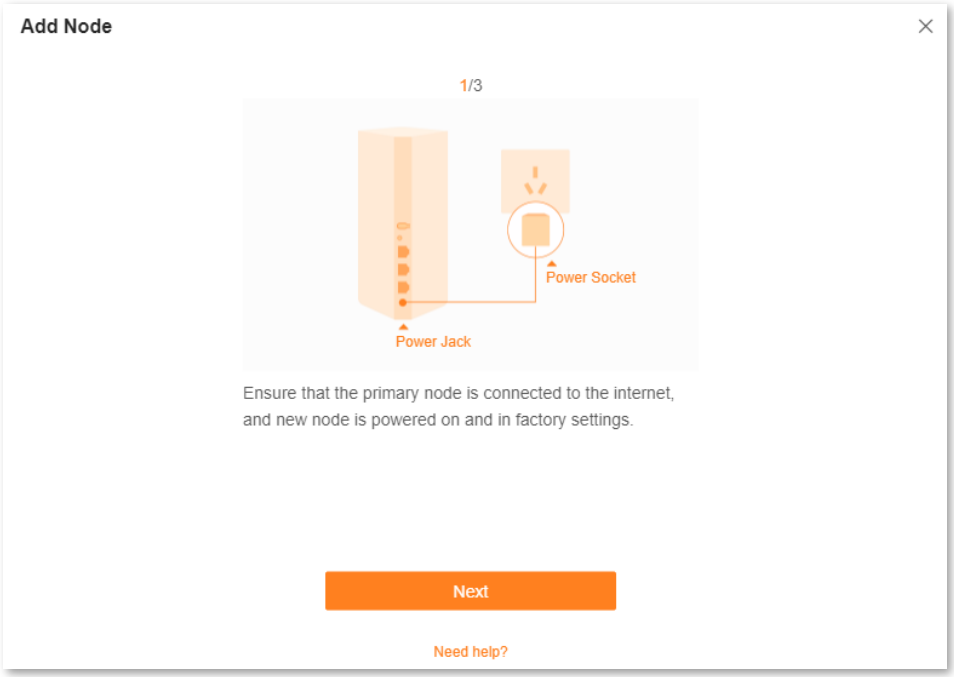
- The node to be added must support the EasyMesh or Xmesh protocol.
- The node to be added must be located within the signal coverage of the primary node.
- A maximum of nine nodes can be added to a Mesh network.

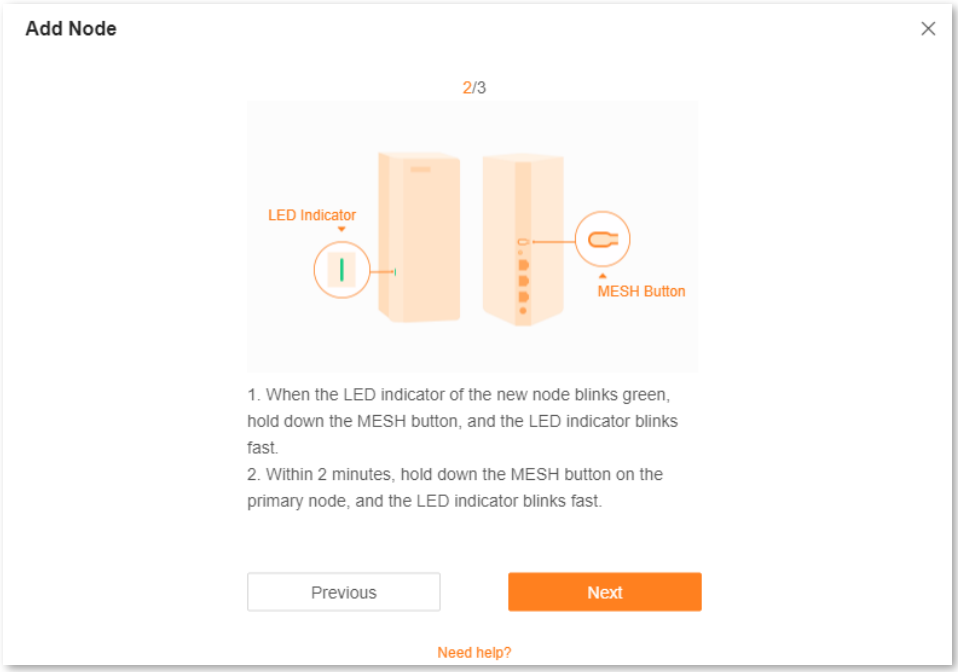
To add a node:

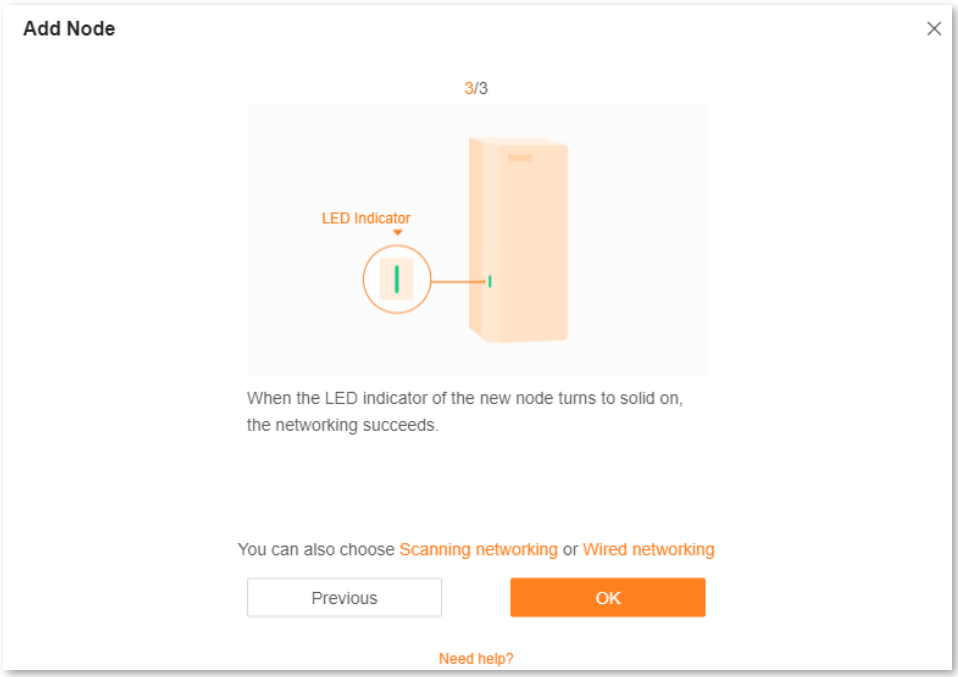
Step 1 Log in to the web UI.

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

Step 3 Follow the instructions displayed.







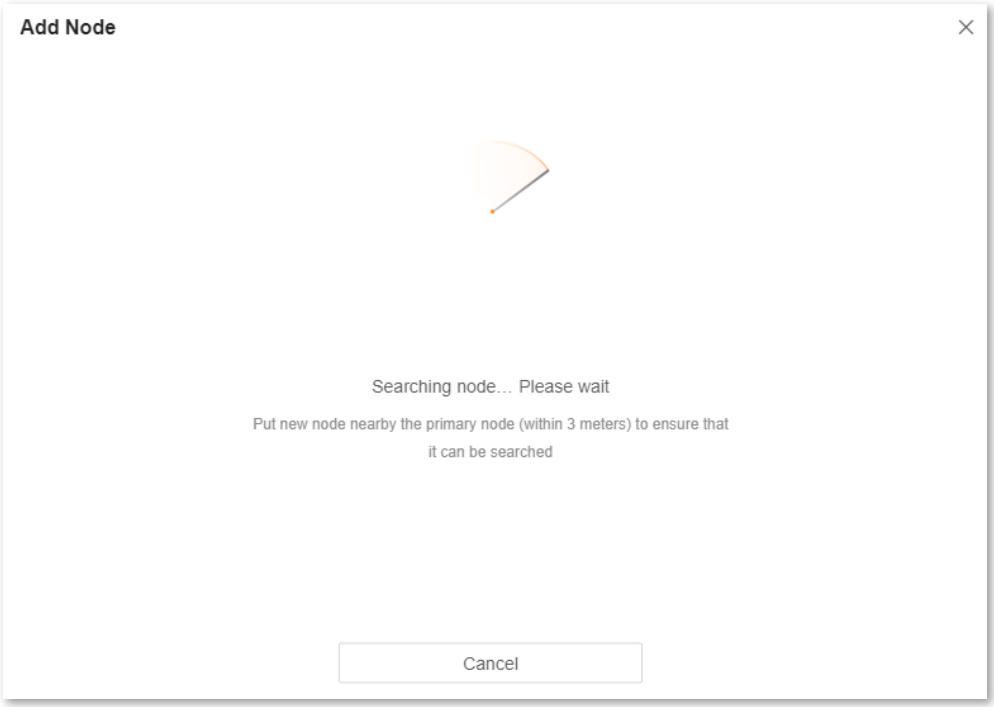
If the LED indicator of new node lights solid on and the new node is displayed in **Network Topology**, the node is added successfully.

---End

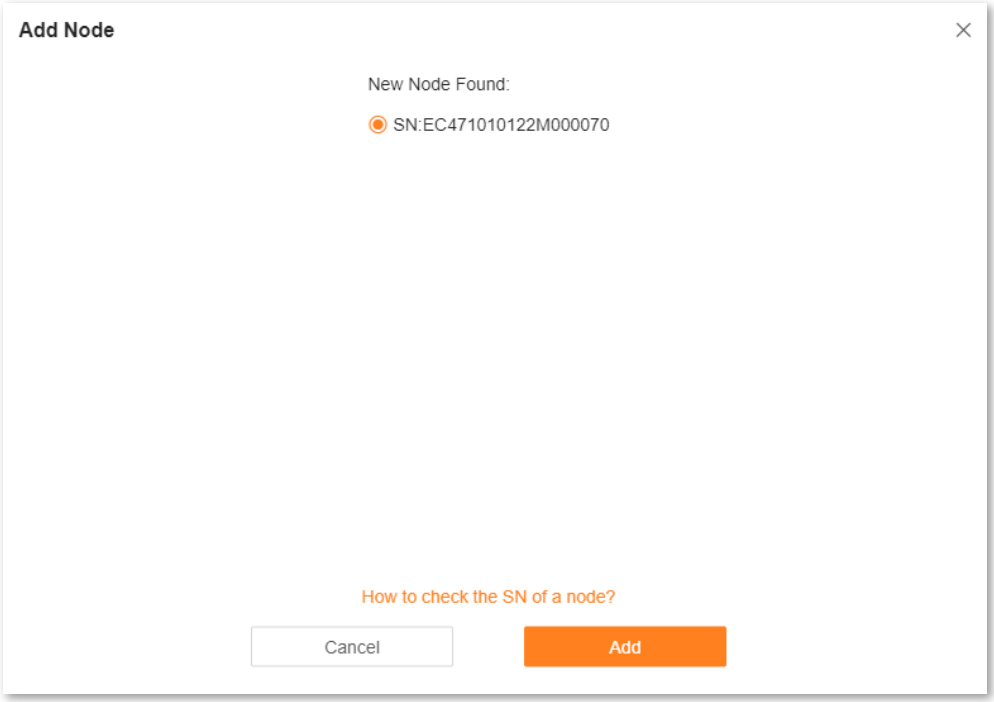
If you cannot add a node by following the preceding instructions, try the following two methods by clicking **Scanning networking** or **Wired networking** shown in the preceding figure:

- To scan a new node:

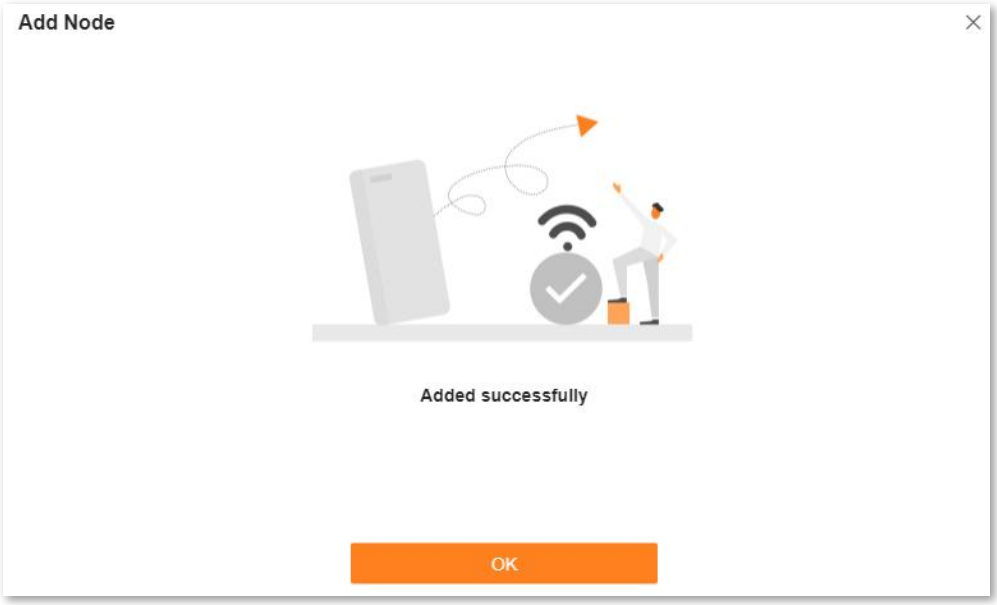
Step 1 Click **Scanning networking**.



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



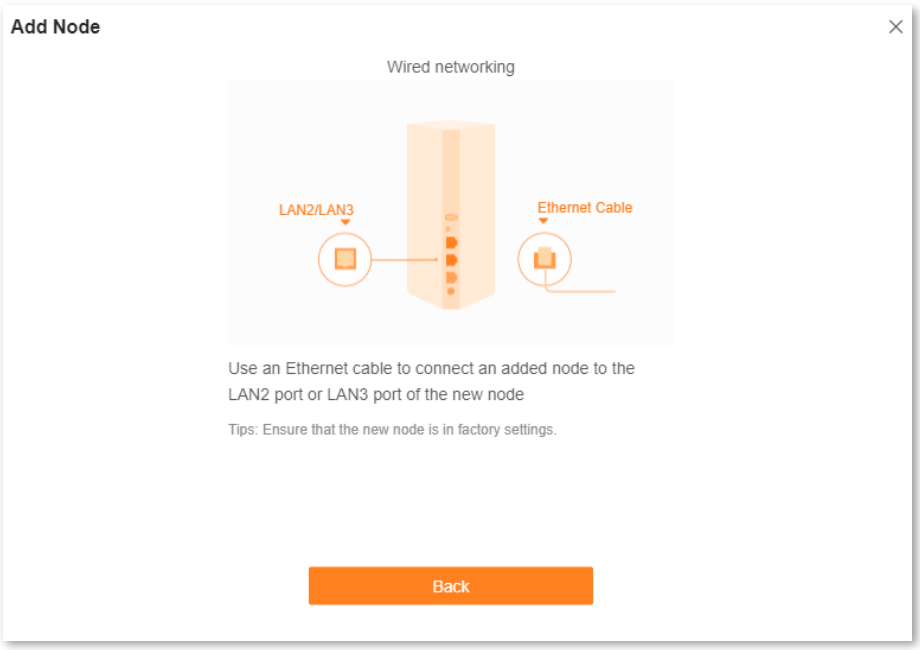
Step 3 Wait until the ongoing process is complete.



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.

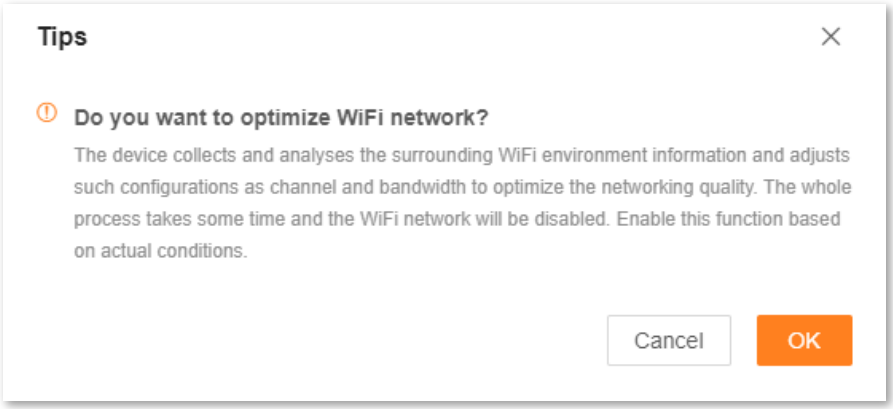
One-click optimization

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

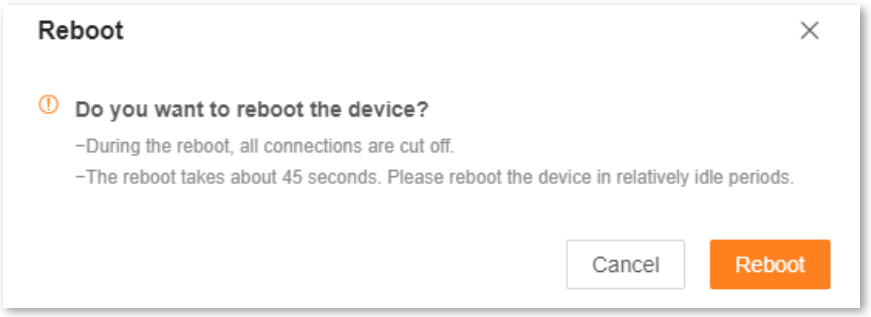
Reboot all nodes

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

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  under **Network Topology**.

The indicators turn on/off immediately.

---End

2.4 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 Mesh device for the first time or after restoring it to factory settings, refer to Connect your primary node to the internet to configure the internet access. After that, you can change the internet settings by following the instructions in this chapter.

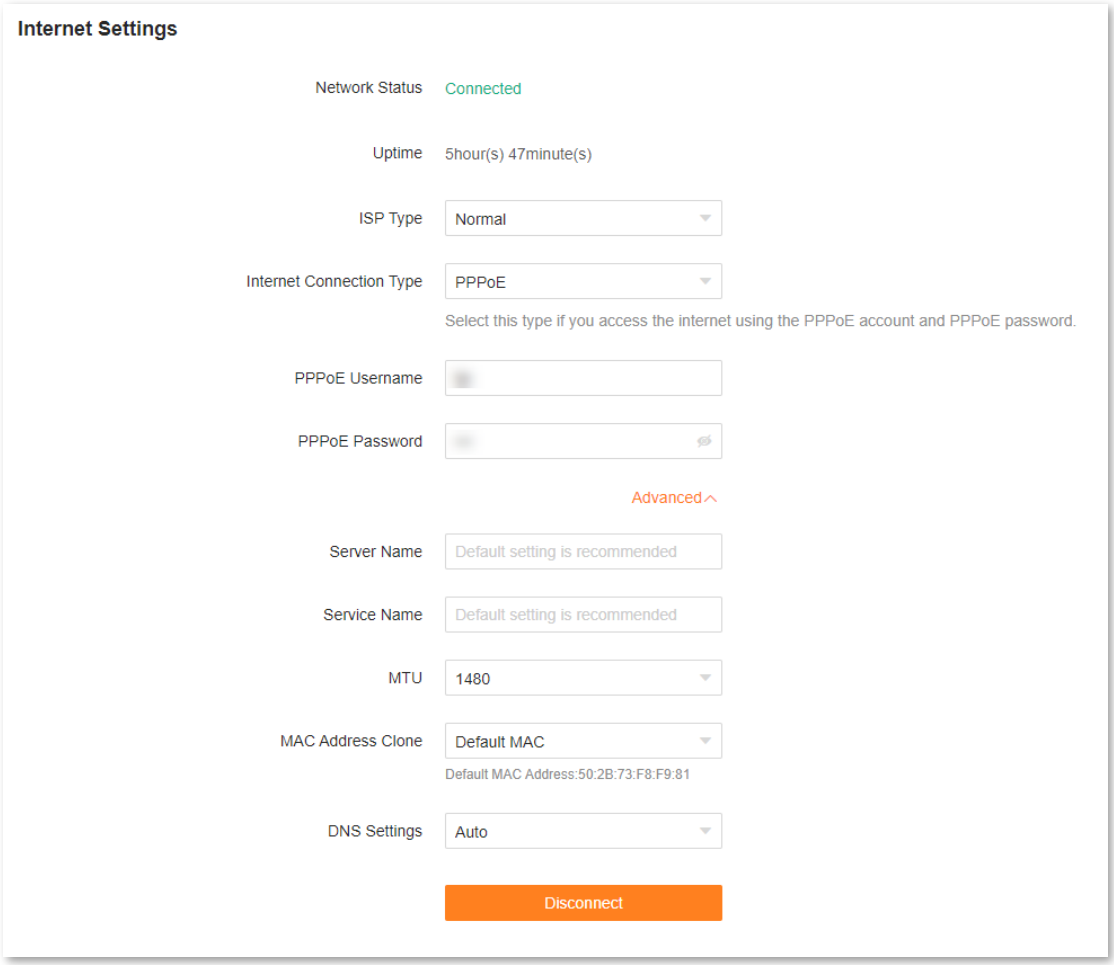
This section includes the following parts:

2.4.1 Overview

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

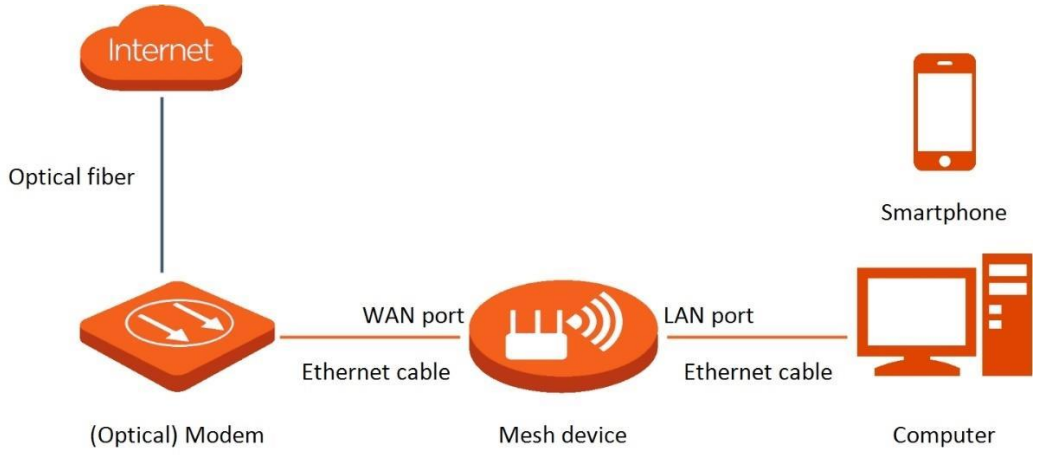
Parameter	Description
Network Status	Indicates the internet connection status. • **Connected**: The internet connection is successful. • Other information (for example, **No Ethernet cable is connected to the WAN port**): The internet connection failed. Perform troubleshooting according to the tips displayed.
Uptime	Indicates the network connection time of the Mesh device.
ISP Type	See Parameter description in Connect your primary node to the internet.
Internet Connection Type	
PPPoE Username	
PPPoE Password	
IP Address	
Subnet Mask	
Gateway	

Parameter	Description
Primary DNS	
Secondary DNS	
Address Type	
DNS Settings	
Server IP Address/Domain Name	
User Name	
Password	
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.
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.

Parameter	Description
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 Mesh device to the same as that of the device which is configuring the Mesh device. • **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.

2.4.2 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**.

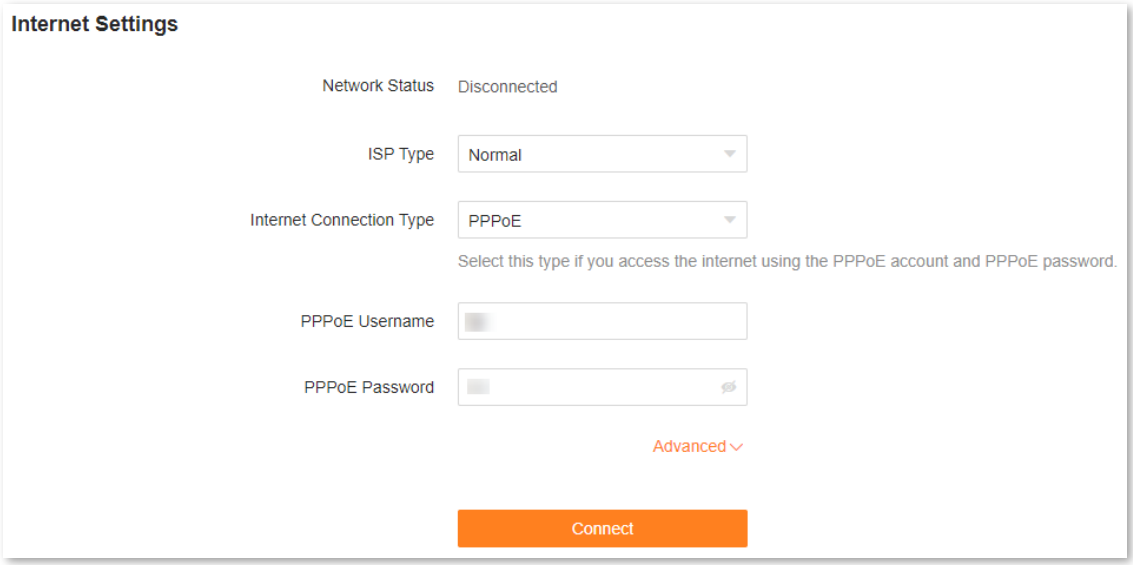
TIP

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.

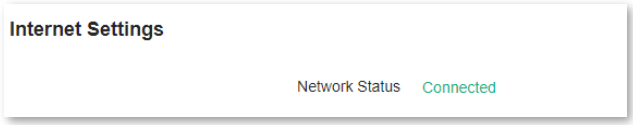
Step 3 Set **Internet Connection Type** to **PPPoE**.

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

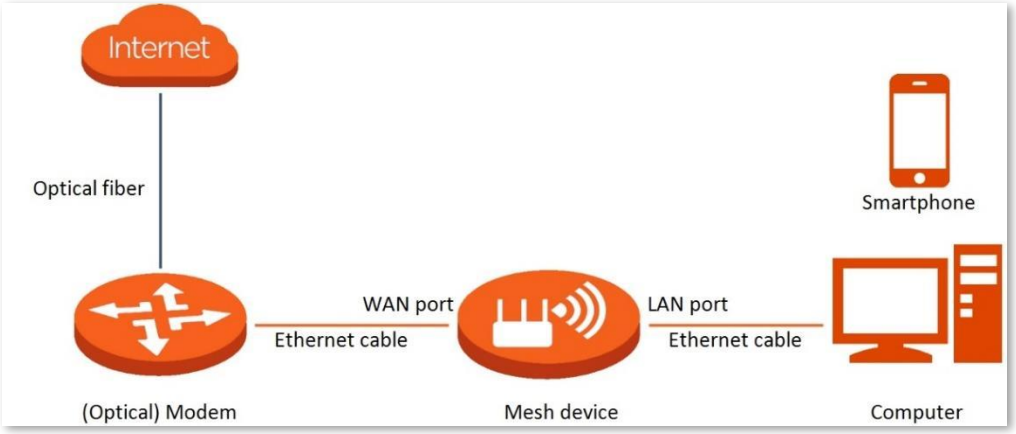
If there is no response from the remote server, troubleshoot as prompted under **Network Status** on the **Internet Settings** page.

2.4.3 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**.

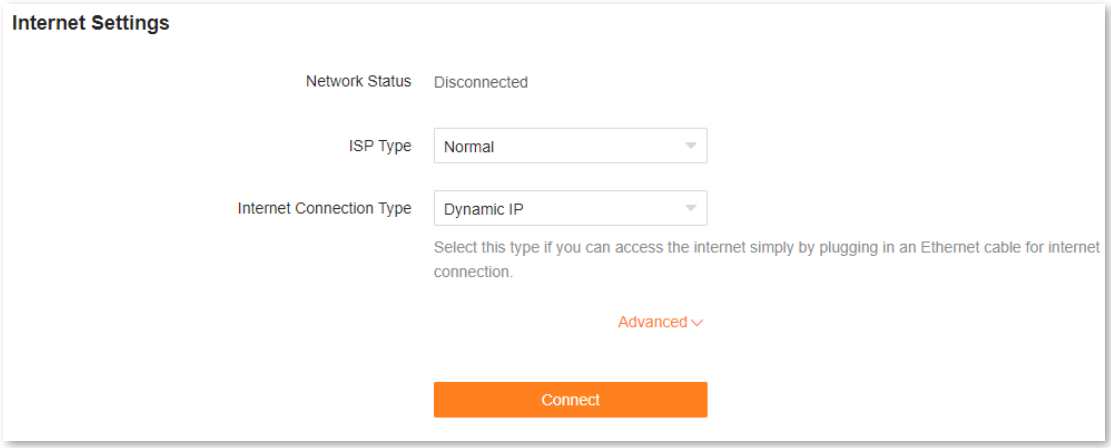
Step 2 Set **ISP Type**.

TIP

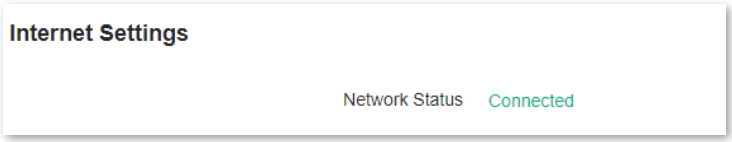
If you select **Manual** for **ISP Type**, enter **Internet VLAN ID** and **IPTV VLAN ID** (if any) provided by your ISP. Blank VLAN ID indicates that the IPTV function is disabled.

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

2.4.4 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**.

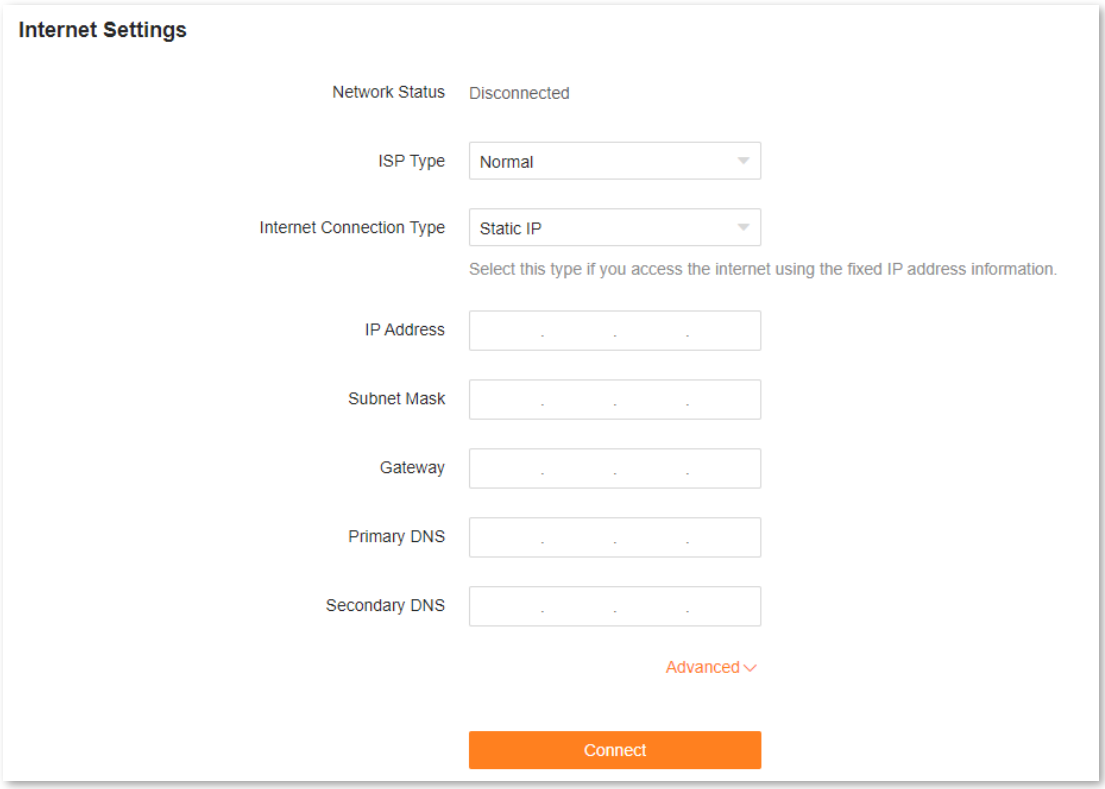
TIP

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.

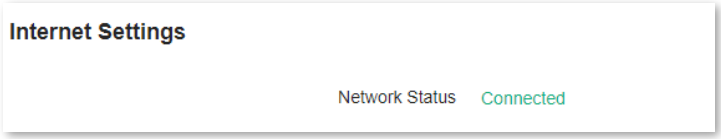
Step 3 Set **Internet Connection Type** to **Static IP**.

Step 4 Set **IP Address**, **Subnet Mask**, **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

2.4.5 Set up dual access connection

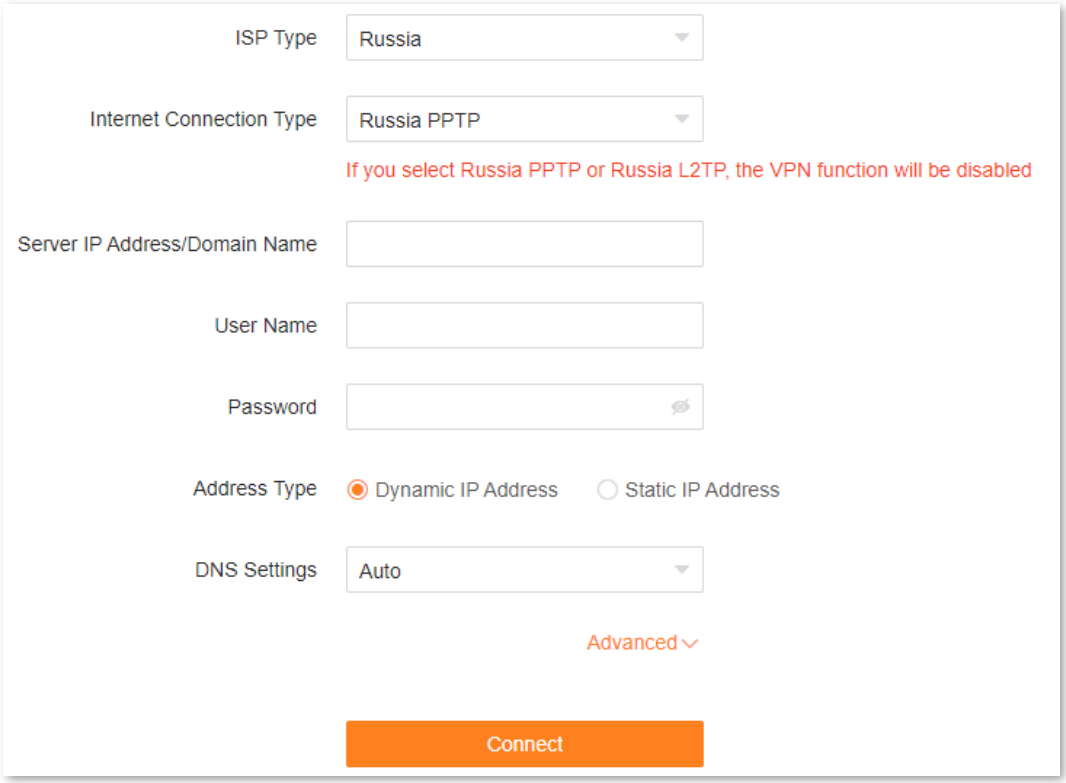
In countries like Russia, the ISP may require you to set up dual access. One is for access to the internet through PPPoE, PPTP or L2TP, and the other is for access to the “local” resources where the ISP is located through DHCP or static IP address. If your ISP provides such connection information, you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

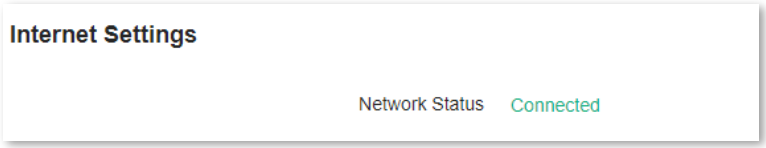
Step 3 Set **Internet Connection Type**, which is **Russia PPTP** in this example, and fill in required parameters.



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

2.5 Wi-Fi settings

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

This section includes the following parts:

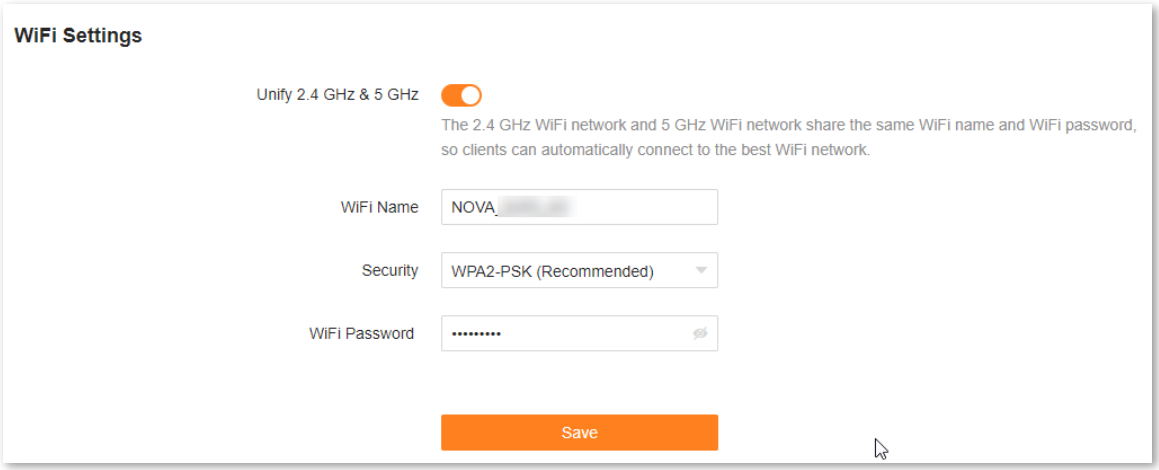
Basic settings

Separate the 2.4 GHz and 5 GHz Wi-Fi networks

2.5.1 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 and 5 GHz Wi-Fi networks.
WiFi Name	Specifies the Wi-Fi network name (SSID) of the corresponding Wi-Fi network.
Security	Specifies the encryption mode supported by the Mesh device, 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 WiFi 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.

2.5.2 Separate the 2.4 GHz and 5 GHz Wi-Fi networks

The Mesh device supports both 2.4 GHz and 5 GHz Wi-Fi networks, which are unified and only one Wi-Fi name is displayed by default.

To separate the Wi-Fi names of the two networks:

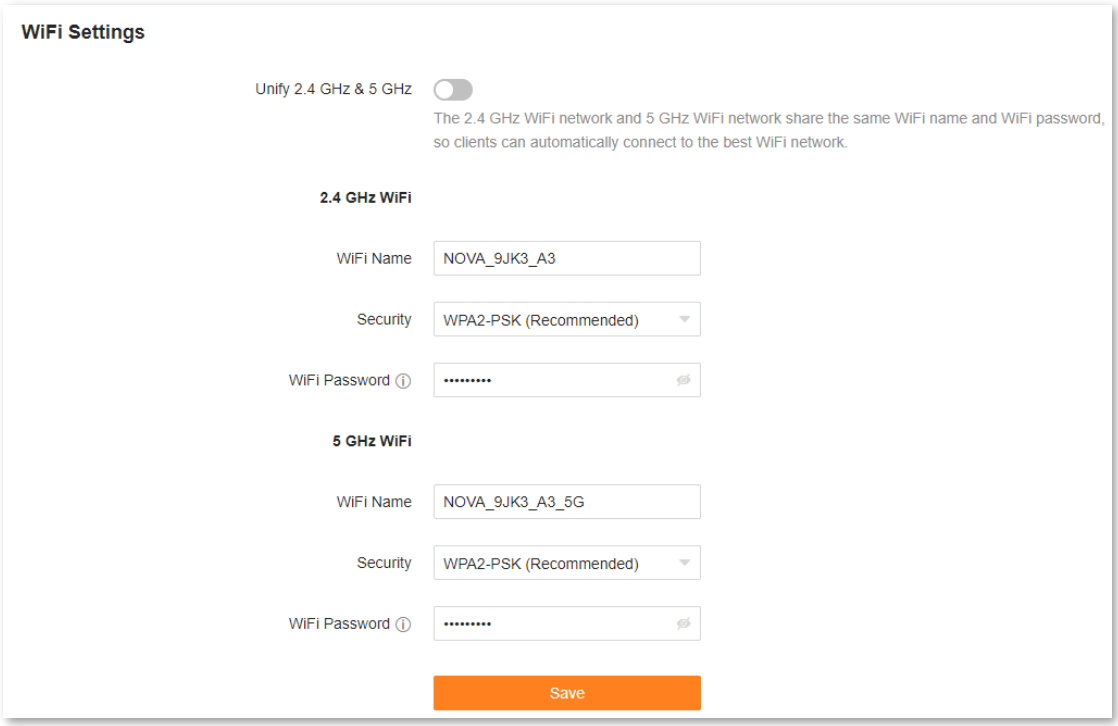
Step 1 Log in to the web UI, and choose **WiFi Settings**.

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

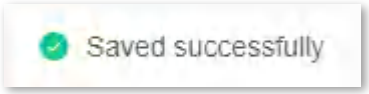
Step 3 Set **WiFi Name** and **WiFi Password** of each WiFi network.

In this example, the 2.4 GHz Wi-Fi network is named **NOVA_9JK3_A3** and the 5 GHz Wi-Fi network is named **NOVA_9JK3_A3_5G**.

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.

2.6 Client management

This section describes how to manage your clients, including:

2.6.1 View client information

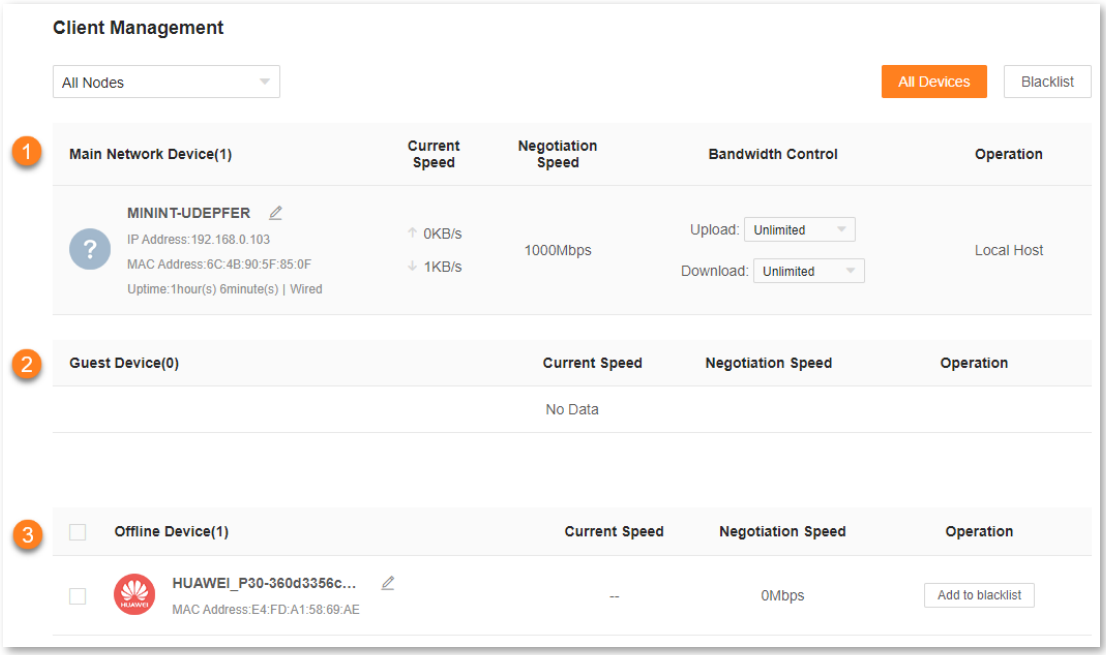
To view information of clients:

Step 1 Log in to the web UI.

Step 2 Choose **Client Management**.

- 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**.

No.	Description
1	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** and **5G**. • **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
2	This area 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 Mesh system.
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**: 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 Mesh system. A maximum of 20 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.

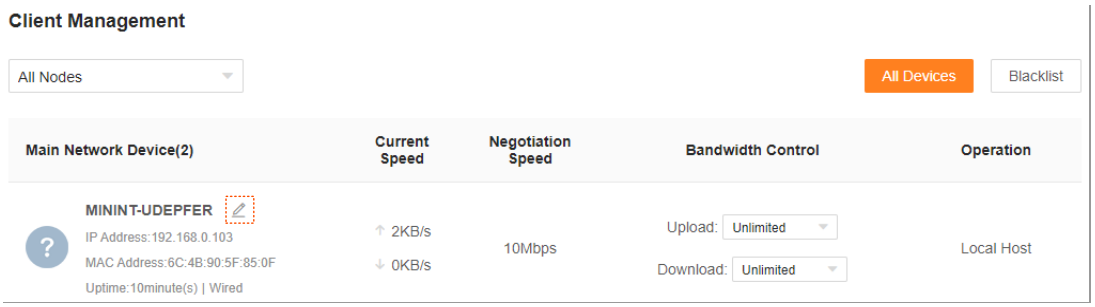
2.6.2 Change a client name

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.

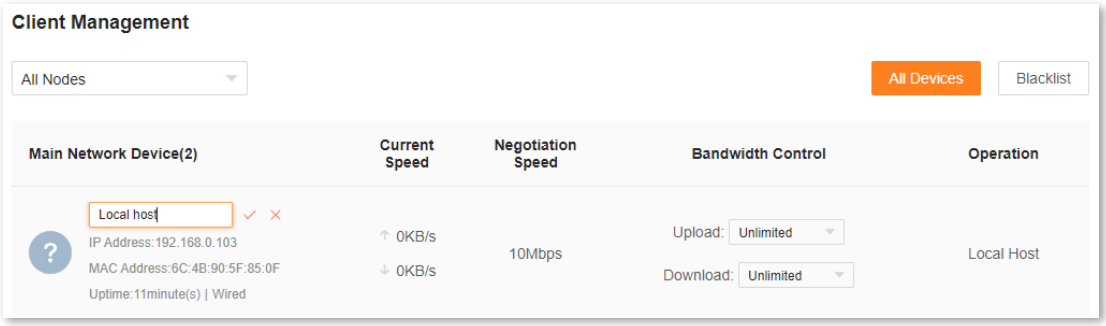
To change the name of a client:

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

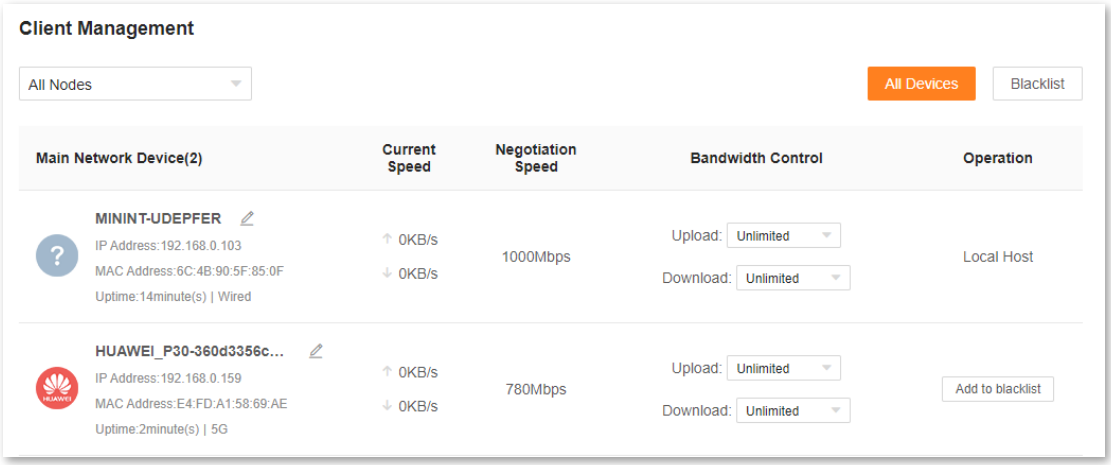
2.6.3 Add a client to the blacklist

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.

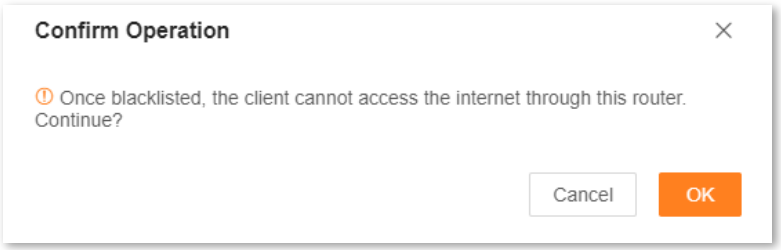
To blacklist a client:

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

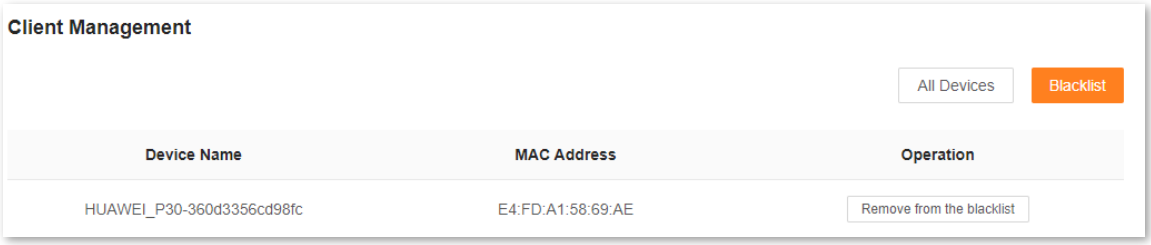
Step 2 Click **Add to blacklist** under **Operation** in the line of the client to be blacklisted.



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 Mesh device again.
- A maximum of 80 clients can be blacklisted.
- The blacklist rule prevails when conflicting with the parent control rule.

---End

2.6.4 Remove a client from the blacklist

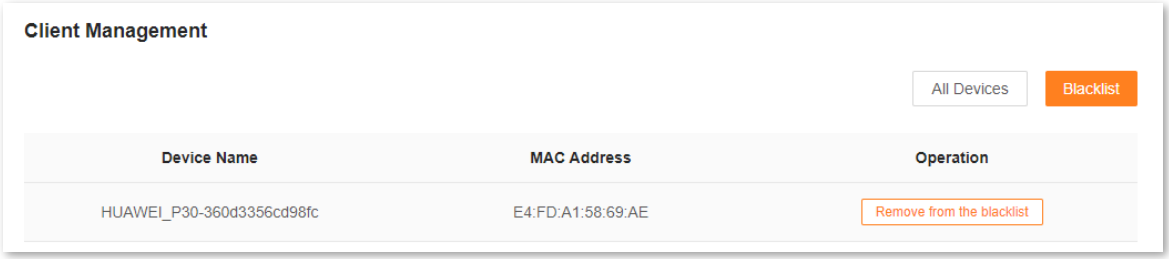
If you blacklist a client by mistake, you can remove it from the blacklist.

To remove a client from the blacklist:

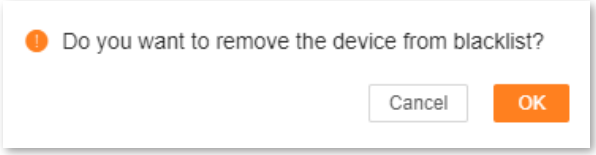
Step 1 Log in to the web UI, and choose **Client Management**.

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

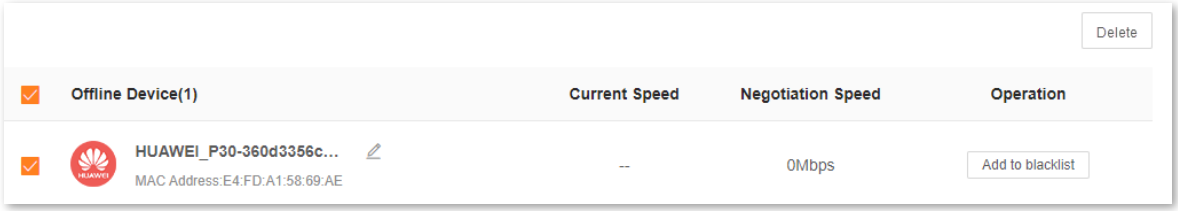
2.6.5 Delete an offline client

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

2.7 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 section includes the following parts:

Create a parental control rule

Other operations on the parental control rules

2.7.1 Create a parental control rule

Add a parental control rule

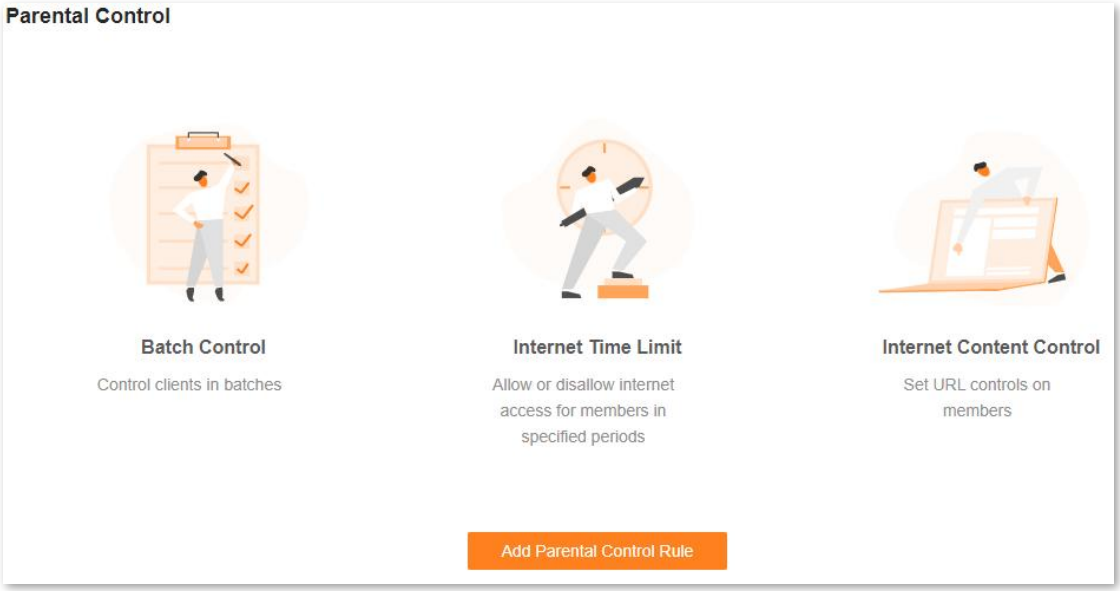
NOTE

- 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.

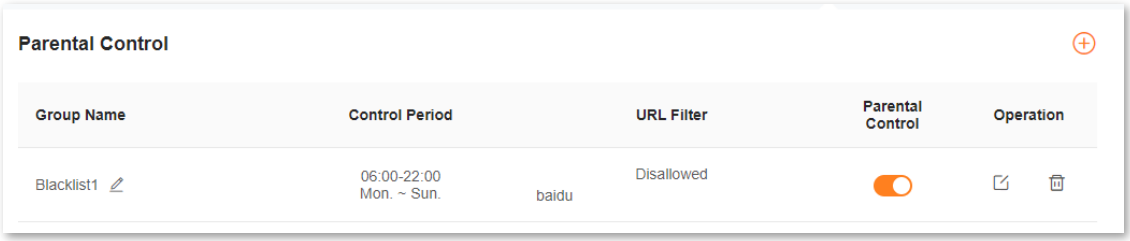
To add a parental control rule:

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.

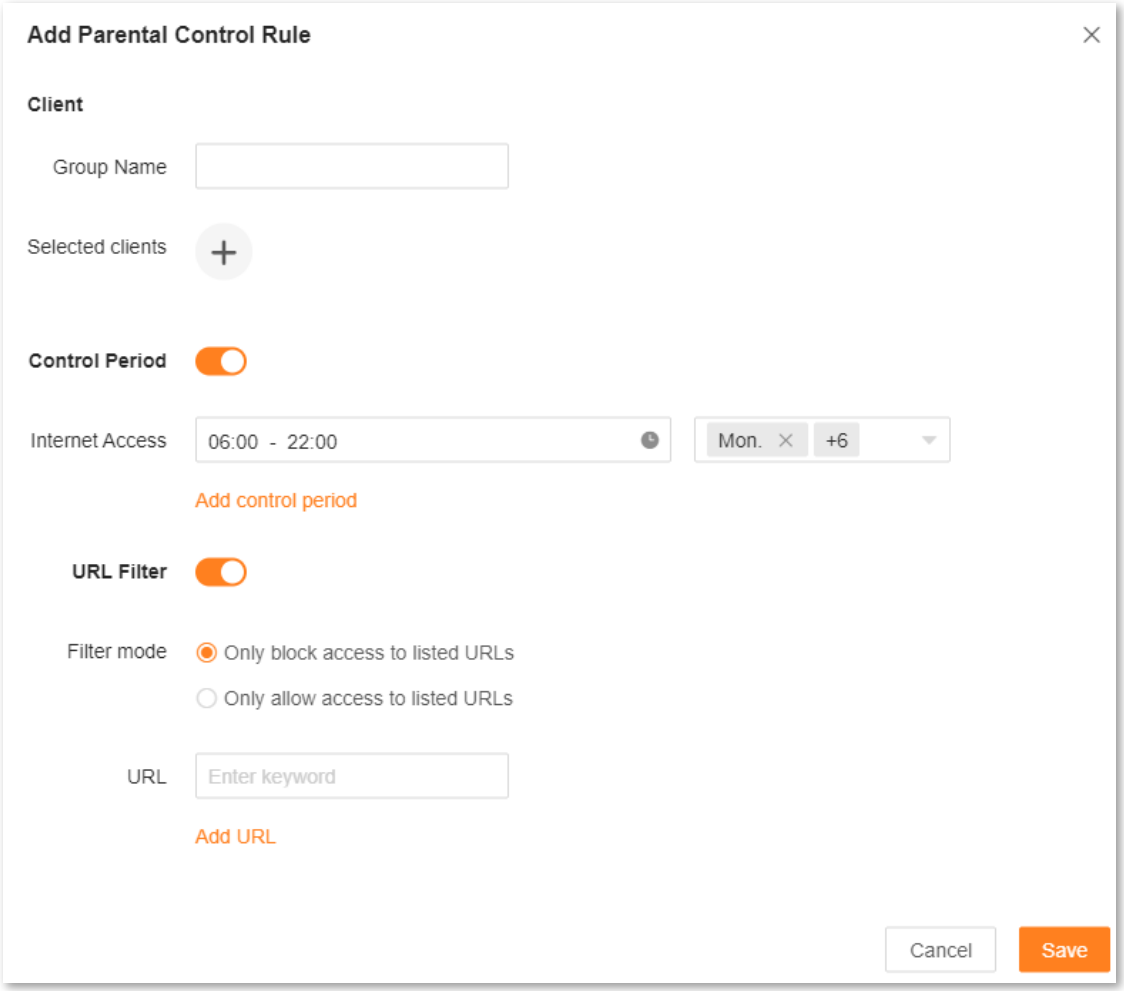


Step 2 Click **Add Parental Control Rule** or .

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.

Parameter	Description
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.
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.

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 Mesh device.

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:

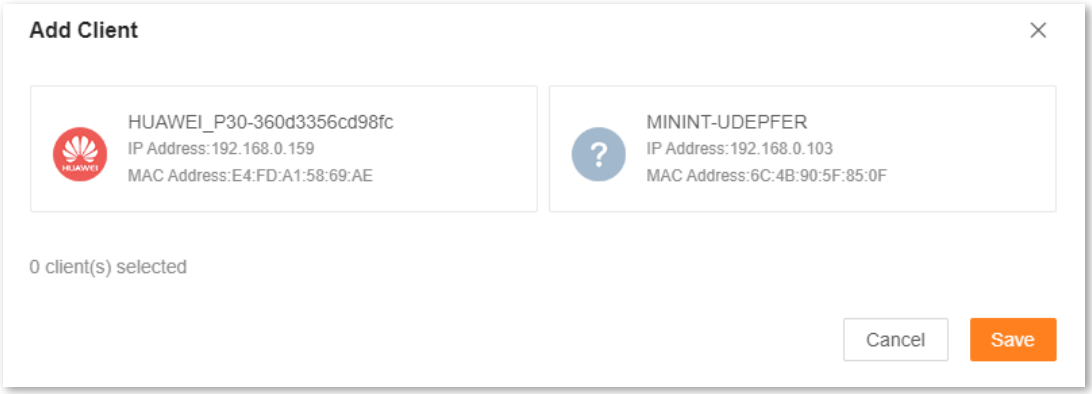
Step 1 Log in to the web UI, and choose **Parental Control**.

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.

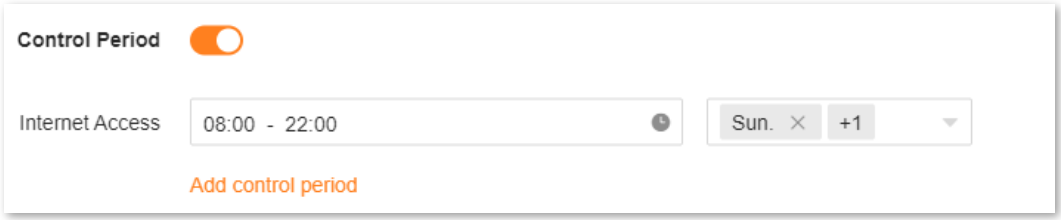


Step 5 Select the clients to which this parental control rule is applied, and click **Save**.

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.

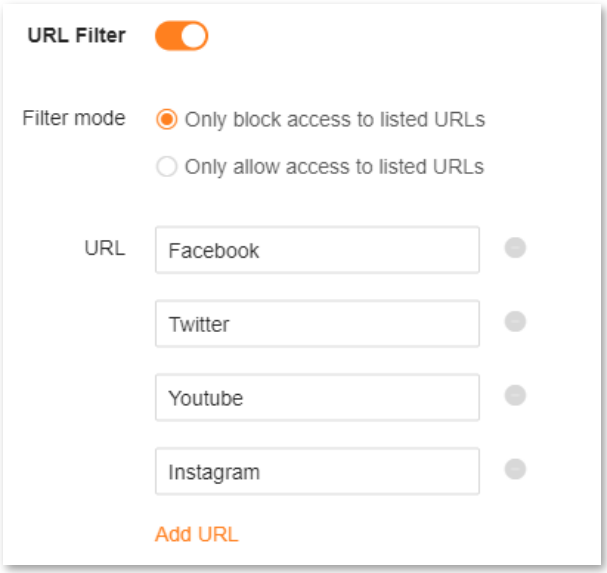
1. Click the left field to set **Start Time** to **08:00** and **End Time** to **22:00**.
2. Select **Sat.** and **Sun.** from the right drop-down list box.



Step 8 Toggle on **URL Filter**.

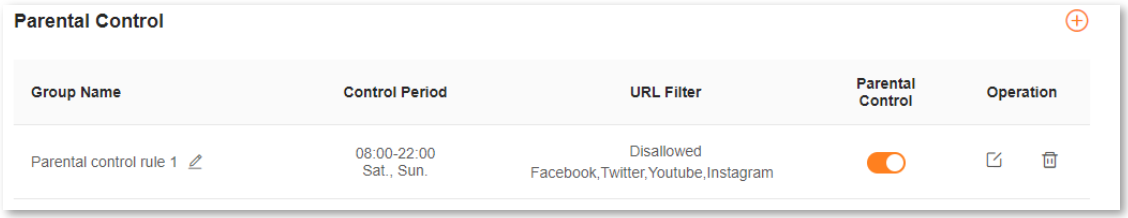
Step 9 Select **Only block access to listed URLs** for **Filter mode**.

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



Step 11 Click **Save**.

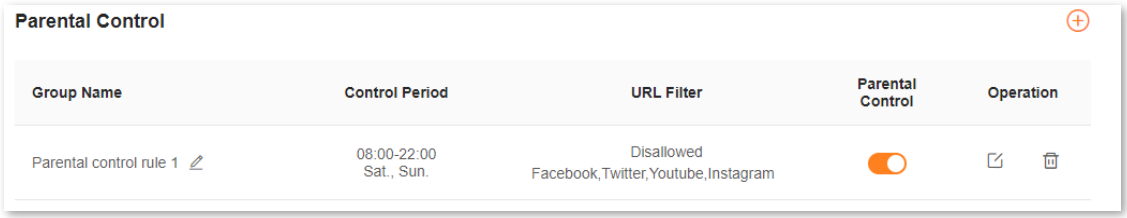
The following page is displayed, and your kid can access any websites except for Facebook, Twitter, Youtube and Instagram from 8:00 to 22:00 on weekends and cannot access the internet at all between 22:00 to 8:00 on weekends.



---End

2.7.2 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 Mesh device 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.

2.8 More

This section describes other settings you may need when using the Mesh device, including:

Router information

Guest Wi-Fi

Working mode

IPv6

Smart power saving

Advanced Wi-Fi Settings

Network settings

Advanced

System settings

2.8.1 Router information

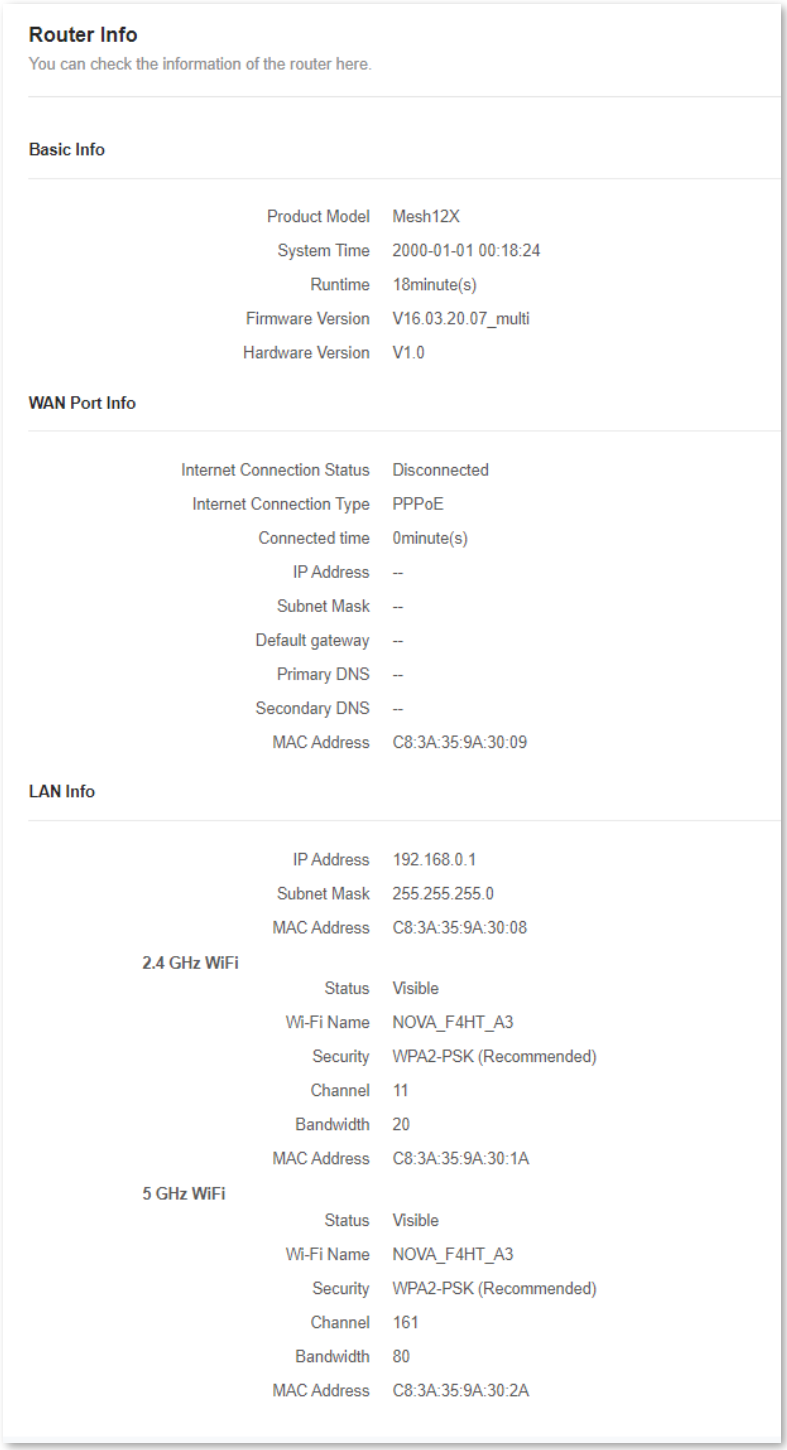
On this page, you can view the information of the primary node, including Basic information, WAN port information, and LAN information.

To view the information of the primary node:

Step 1 Log in to the web UI.

Step 2 Choose **More** > **Router Info**.

The following page is displayed.



---End

Basic information

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

Parameter description

Parameter	Description
Product Model	Specifies the model of the primary node. **Mesh12X** is used as an example here.

Parameter	Description
System Time	Specifies the current system time.
Uptime	Specifies the network connection time of the primary node.
Firmware Version	Specifies the firmware version of the primary node.
Hardware Version	Specifies the hardware version of the primary node.

WAN port information

This part is displayed only in the router mode.

In this part, you can view WAN port information of the primary node, 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.
Uptime	Specifies the internet connection time of the primary node.
IP Address	Specifies the WAN IP address of the primary node.
Subnet Mask	Specifies the WAN subnet mask of the primary node.
Gateway	Specifies the gateway IP address of the primary node.
Primary DNS	Specify the IP address of primary and secondary DNS servers of the primary node.
Secondary DNS	
MAC Address	Specifies the WAN MAC address of the primary node.

LAN information

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

Parameter description

Parameter	Description
IP Address	Specifies the LAN IP address of the primary node, which is also the IP address for logging in to the web UI of the primary node.

Parameter	Description
Subnet Mask	Specifies the LAN subnet mask of the primary node.
MAC Address	Specifies the LAN MAC address of the primary node.
Status	Specifies the visibility of the Wi-Fi network.
WiFi Name	Specifies the Wi-Fi name of the respective Wi-Fi network.
Security	Specifies the security mode of the respective Wi-Fi network.
Channel	Specifies the channel that the respective Wi-Fi network works in.
Bandwidth	Specifies the bandwidth of the respective Wi-Fi network.
MAC Address	Specifies the MAC address of the respective Wi-Fi network.

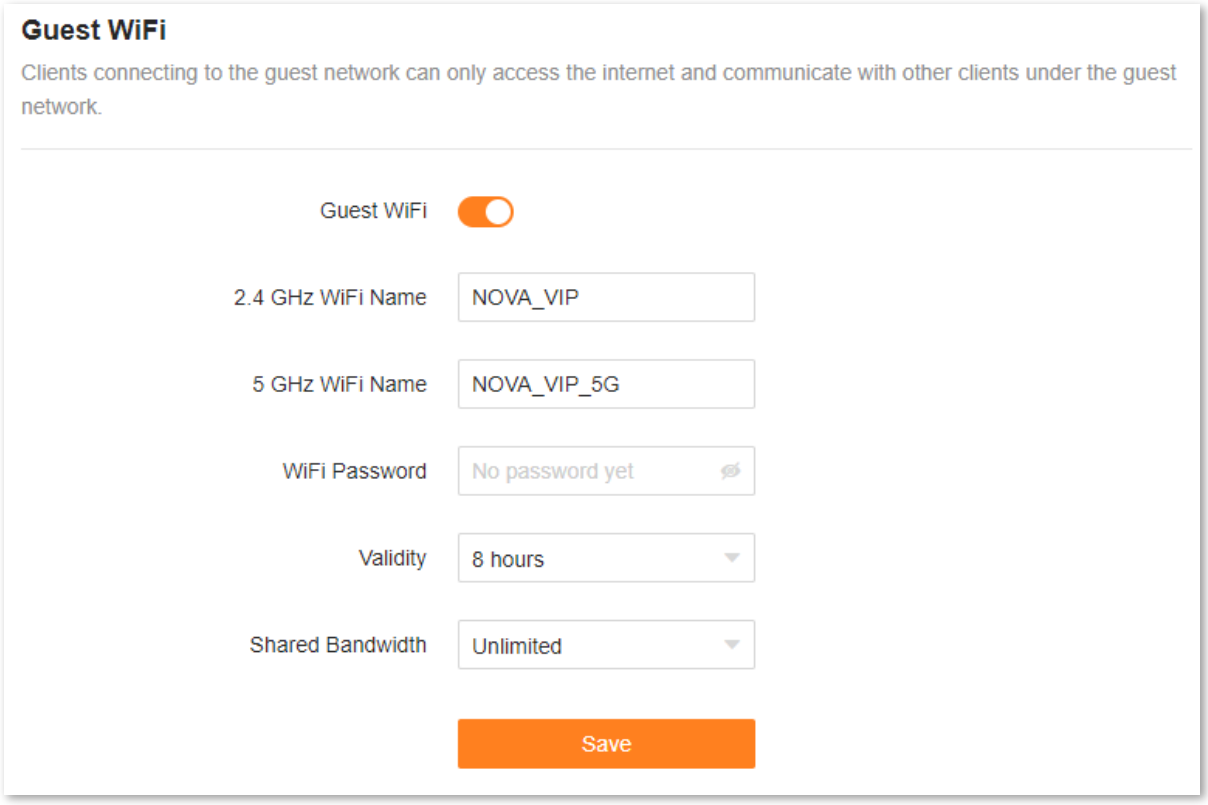
2.8.2 Guest Wi-Fi

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 Mesh device 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 Mesh system's guest network. By default, **NOVA_VIP** is for the 2.4 GHz Wi-Fi network and **NOVA_VIP_5G** for the 5 GHz Wi-Fi network. You can change the Wi-Fi names (SSIDs) as required. To distinguish the guest network from the main network, you are recommended to set different Wi-Fi network names.
5 GHz WiFi Name	
WiFi Password	Specifies the password for the Mesh device'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**.

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 and 5 GHz networks: **John_Doe** and **John_Doe_5G**.
- Wi-Fi password for 2.4 GHz and 5 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 **WiFi Password**, which is **Tenda+245** in this example.

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

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

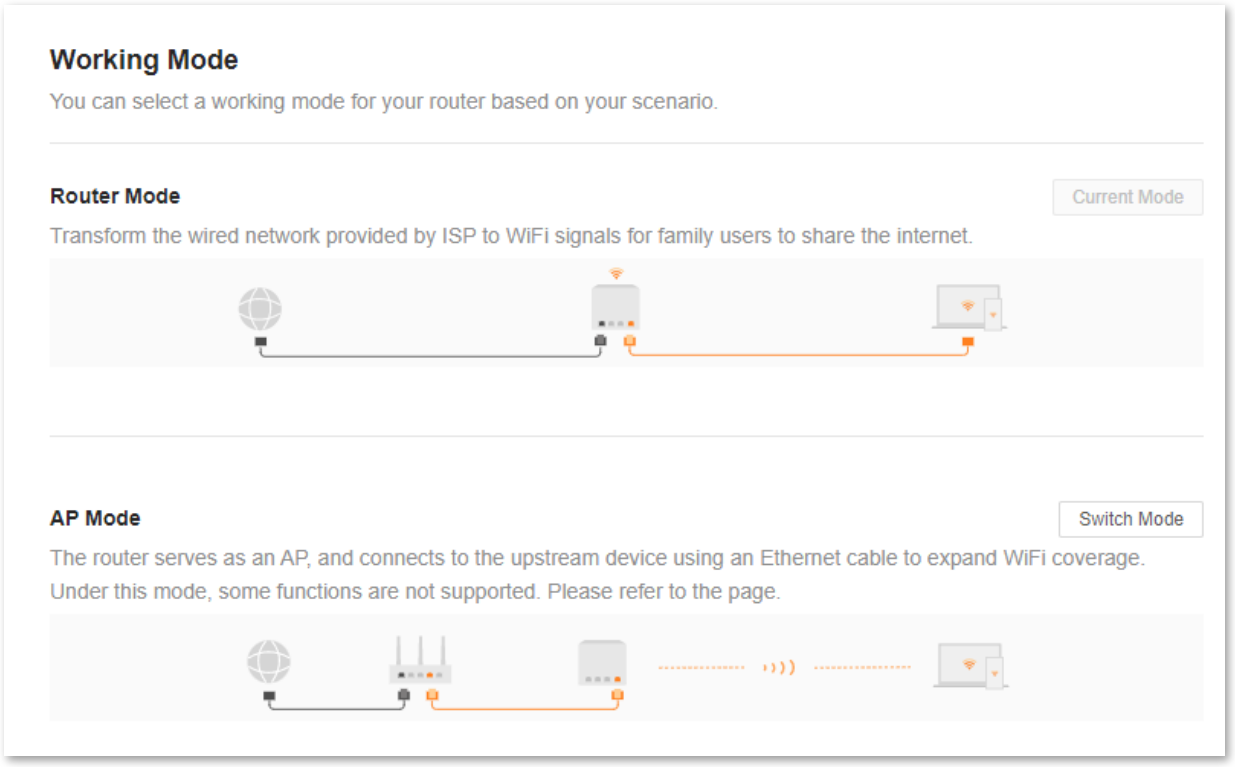
Step 9 Click **Save**.

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

---End

2.8.3 Working mode

You can select a working mode for the Mesh device on this page. The Mesh device can work in the router mode and access point (AP) mode. **Current Mode** is displayed after the working mode currently adopted by the Mesh device, as shown in the following figure. In this example, the current working mode is router mode.



For users who need to specify the network connection mode, select the router mode. For users who use an upstream router, select the AP mode.

Router mode

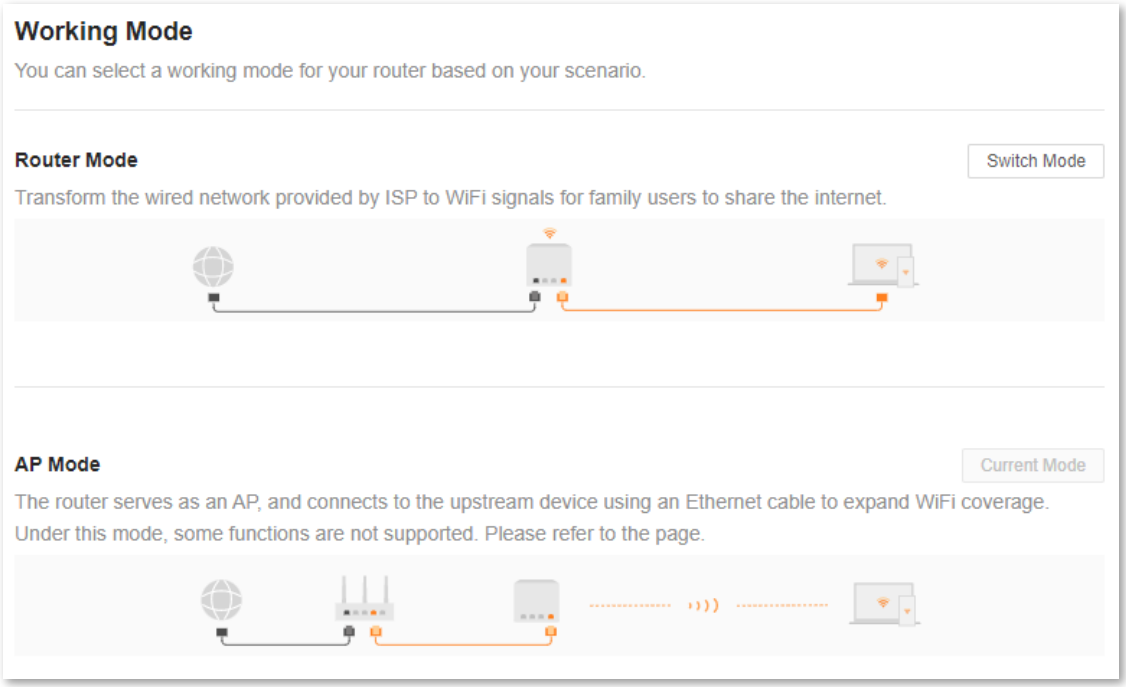
By default, all nodes work in the router mode. All functions are available in this mode. If you want to switch from the router mode to AP mode, see AP mode.

To switch the working mode from the AP mode to router mode:

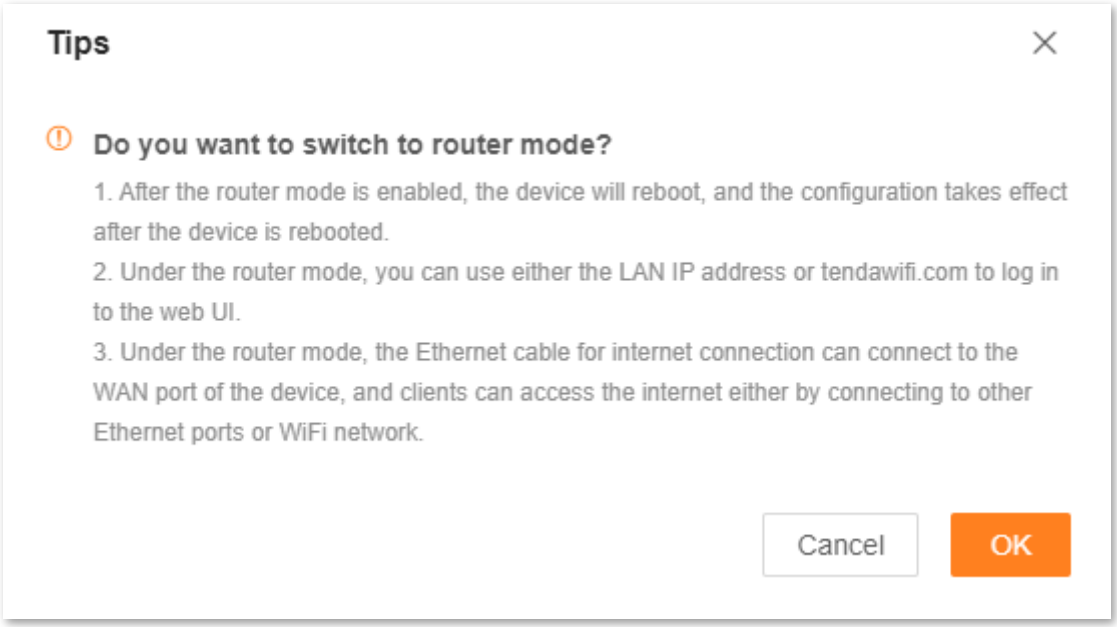
Step 1 Log in to the web UI.

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

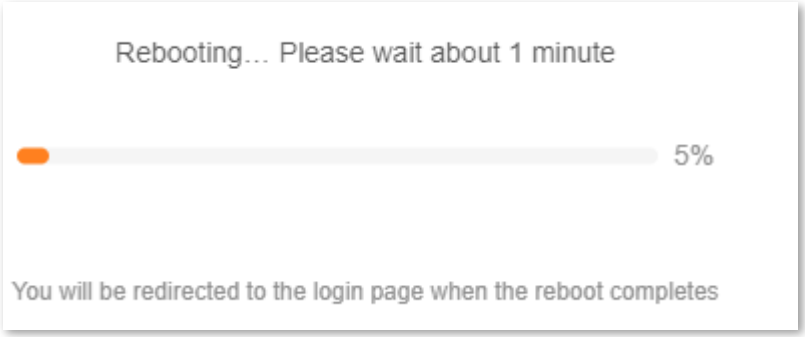
Step 3 Click **Switch mode**.



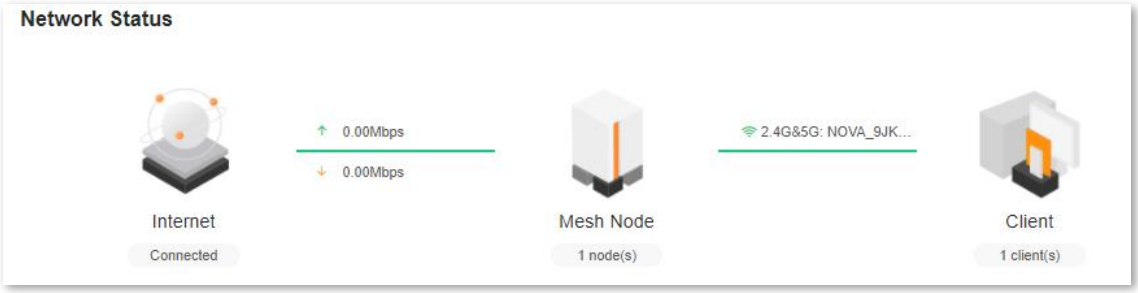
Step 4 Click **OK**.



Step 5 Wait until the devices are restarted.



Step 6 Log in to the web UI of the Mesh device again, and navigate to **Network Status** to check whether the router mode is configured successfully as shown below.



---End

AP mode

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

TIP

When the Mesh device is set to AP mode:

- Every physical port can be used as a LAN port.
- The LAN IP address of the Mesh device will be changed. Please log in to the web UI of the Mesh device 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:

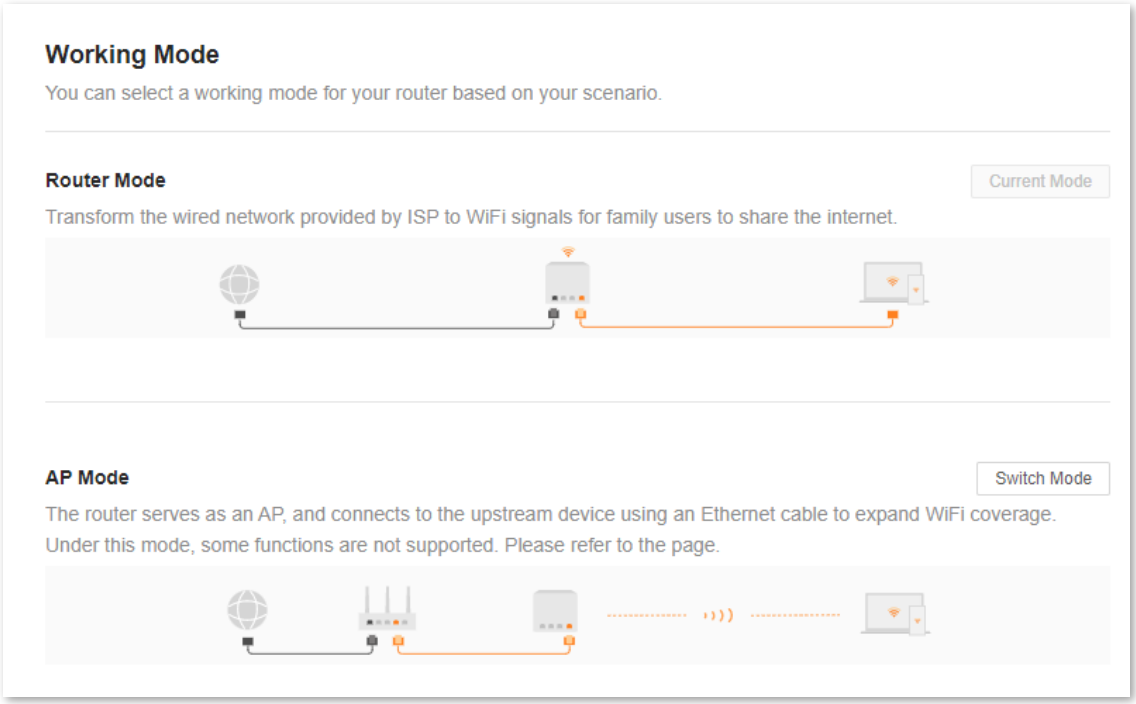
TIP

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.

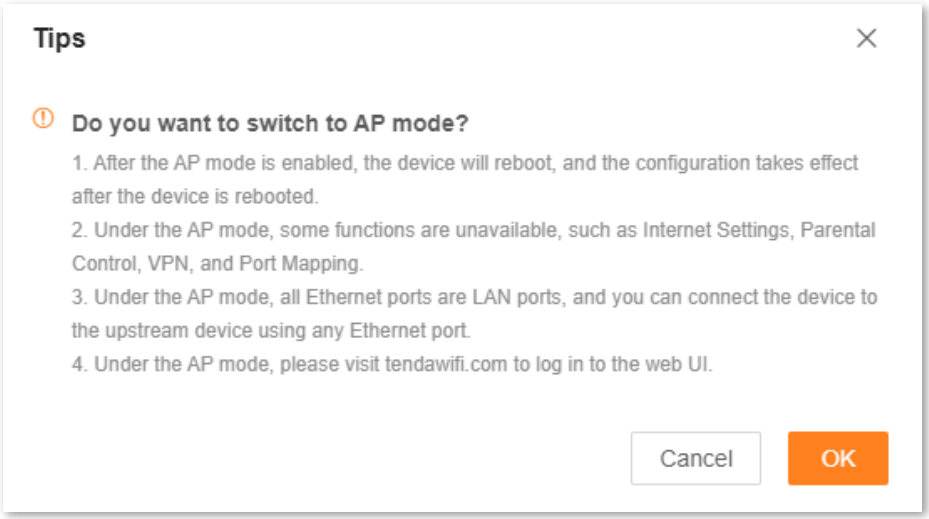
Step 1 Log in to the web UI.

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

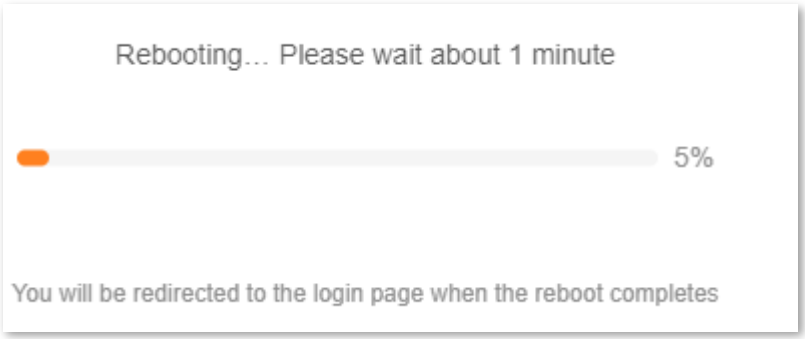
Step 3 Click **Switch mode**.



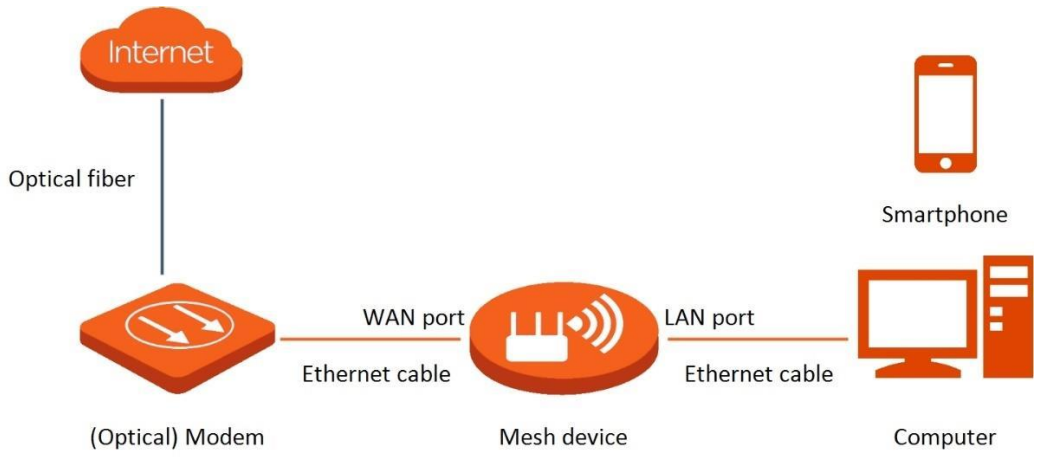
Step 4 Click **OK**.



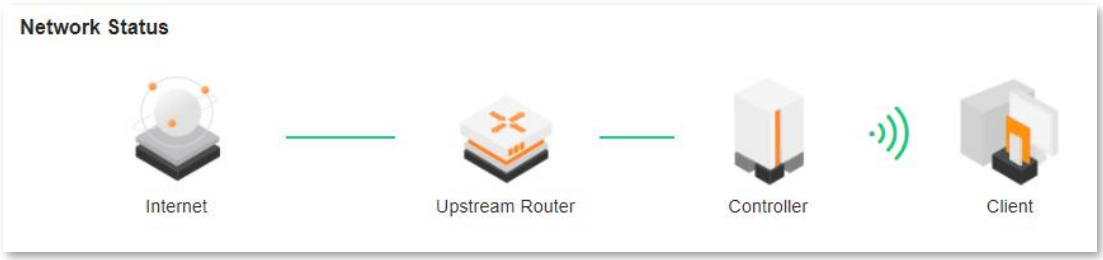
Step 5 Wait until the devices are restarted.



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



Step 7 Log in to the web UI of the Mesh device again, and navigate to **Network Status** to check whether the AP mode is configured successfully as shown below.



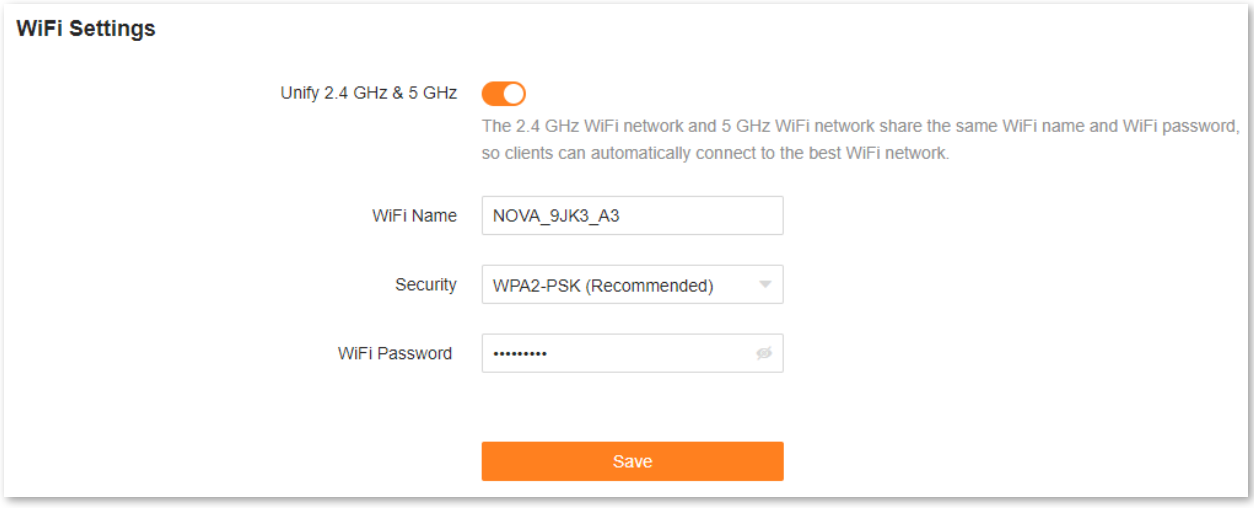
---End

NOTE

If there is another network device with the same login domain name (**tendawifi.com**) as the Mesh device, log in to the upstream router and find the IP address obtained by the Mesh device in the client list. Then you can log in to the web UI of the Mesh device 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 Mesh device.
- If the computer connected to the Mesh device cannot access the internet, ensure that the computer is configured to obtain an IP address and DNS server automatically.

2.8.4 IPv6

TIP

This function is only available in the router mode.

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

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

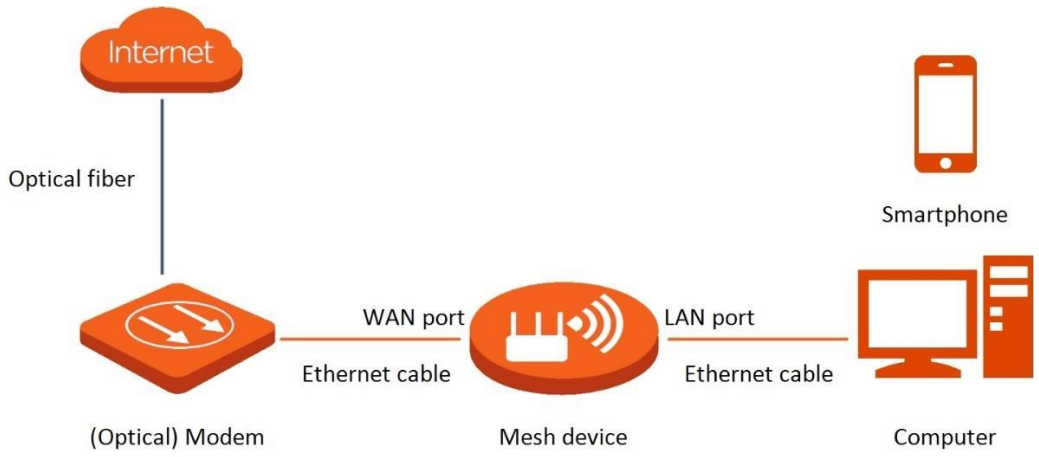
TIP

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.

DHCPv6

DHCPv6 enables the Mesh device 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:

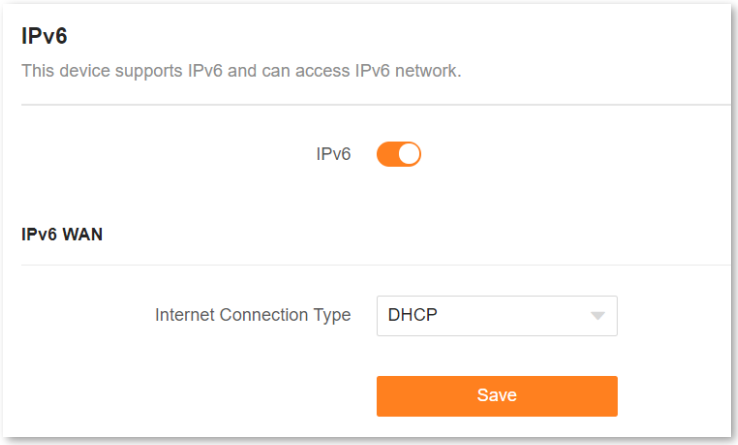
Step 1 Log in to the web UI.

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

Step 3 Enable the **IPv6** function.

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

Step 5 Click **Save**.



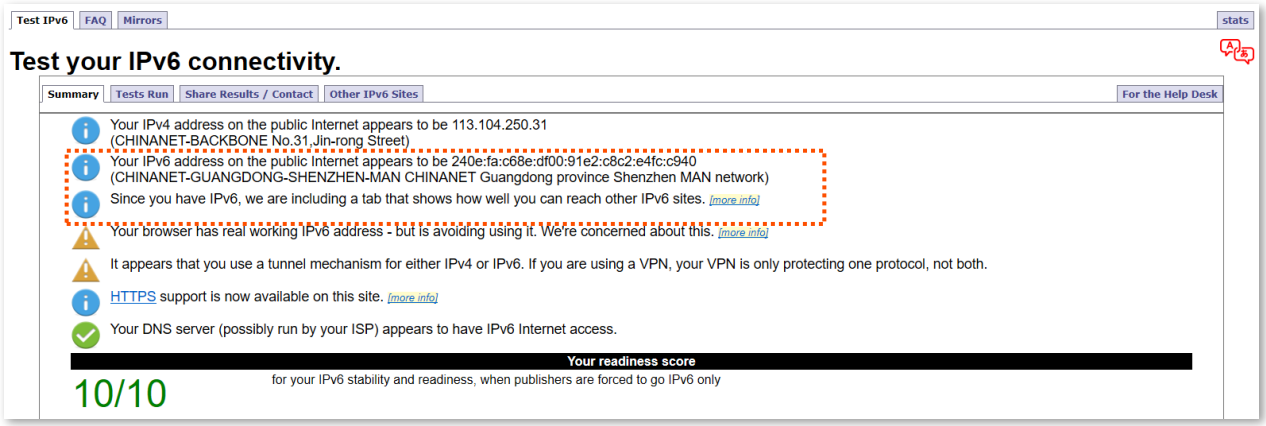
The following message is displayed, indicating that the settings are saved successfully.

---End

IPv6 network test:

Start a web browser on a phone or a computer that is connected to the Mesh device, 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.

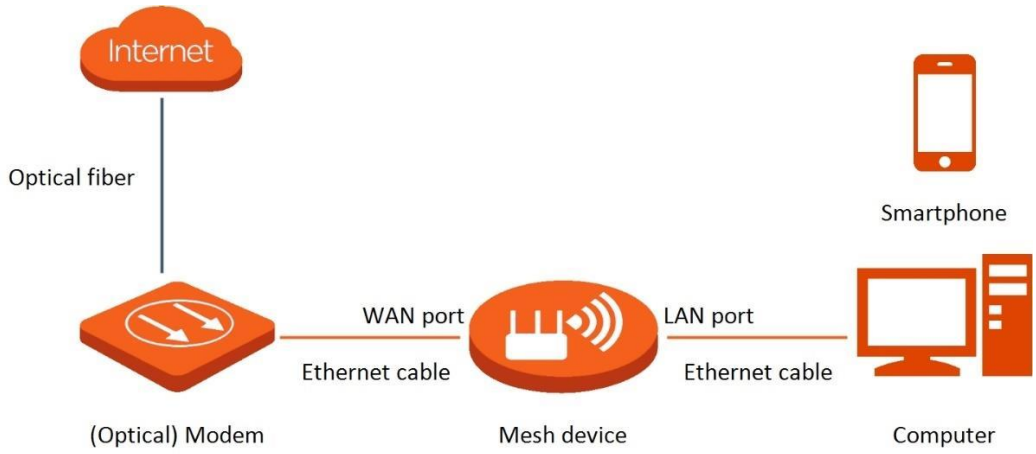


If the IPv6 network test fails, try the following solutions:

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

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:

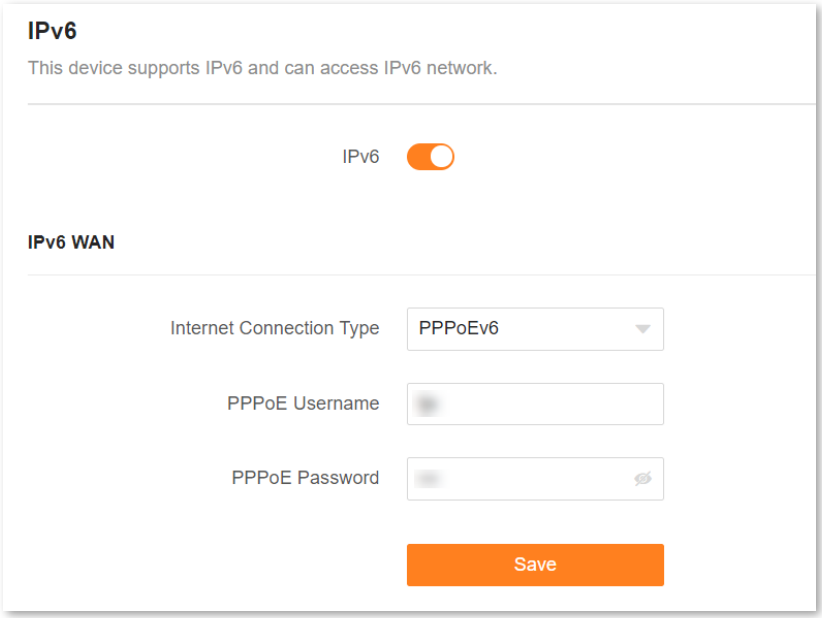
Step 1 Log in to the web UI.

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 Mesh device, 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 Mesh device obtain their IPv6 address through PPPoEv6.
- Consult your ISP for help.

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.

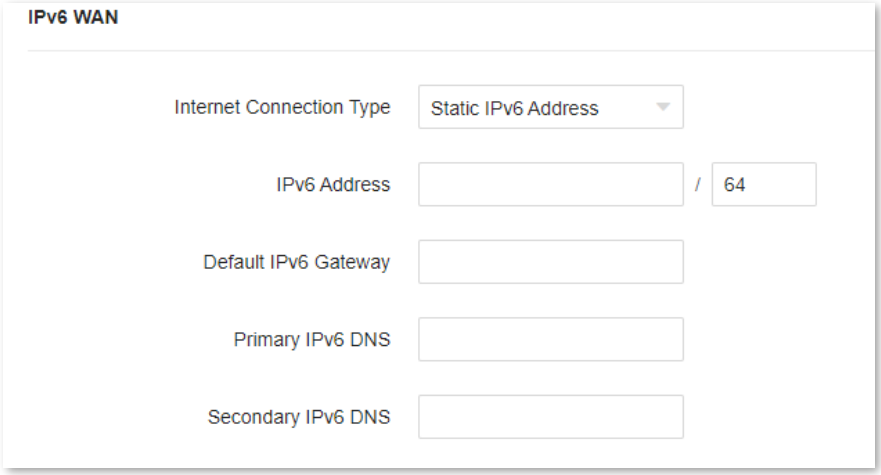
Step 2 Choose **More** > **IPv6**.

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.
Default IPv6 Gateway	TIP
Primary IPv6 DNS	If your ISP only provides one DNS address, leave the secondary IPv6 DNS blank.
Secondary IPv6 DNS	

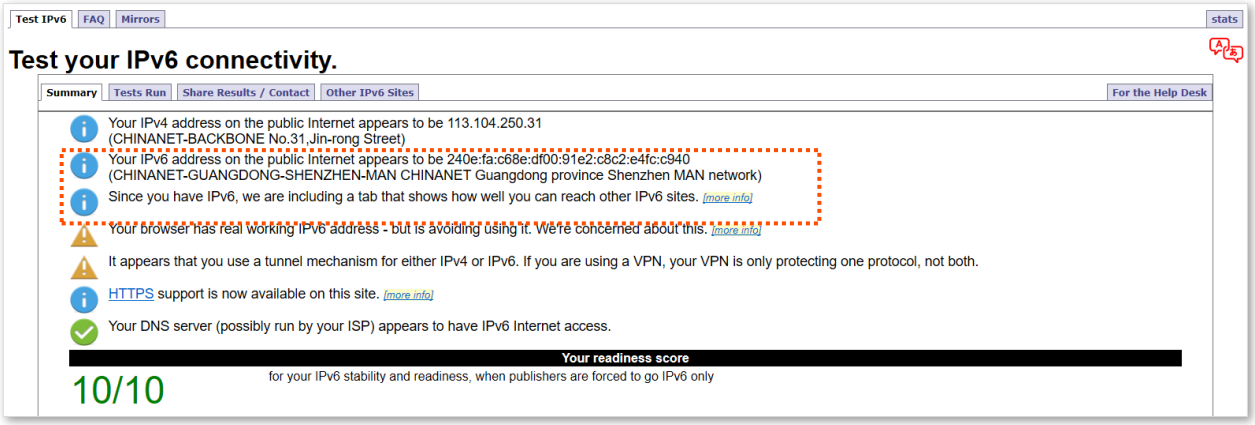
The following message is displayed, indicating that the settings are saved successfully.

---End

IPv6 network test:

Start a web browser on a phone or a computer that is connected to the Mesh device, 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 Mesh device obtain their IPv6 address through DHCPv6.
- Consult your ISP for help.

2.8.5 Smart power saving

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:

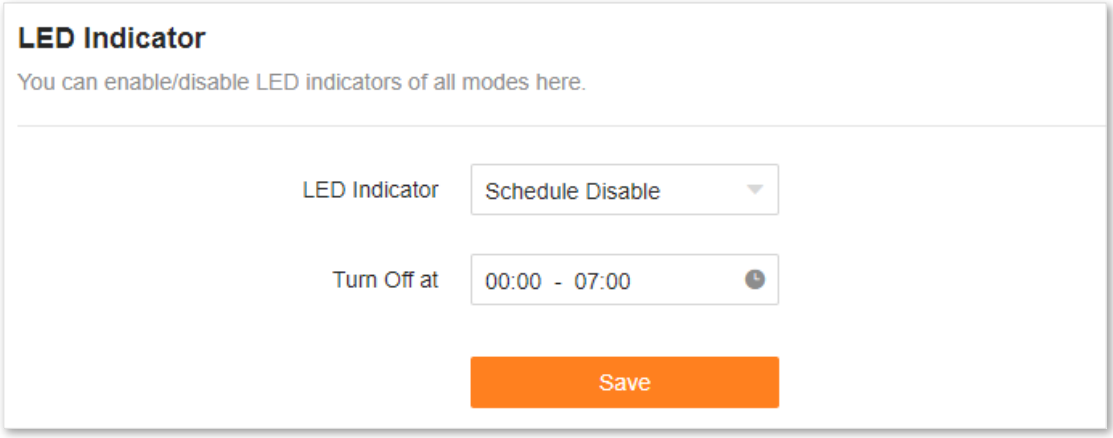
Step 1 Log in to the web UI.

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

2.8.6 Advanced Wi-Fi settings

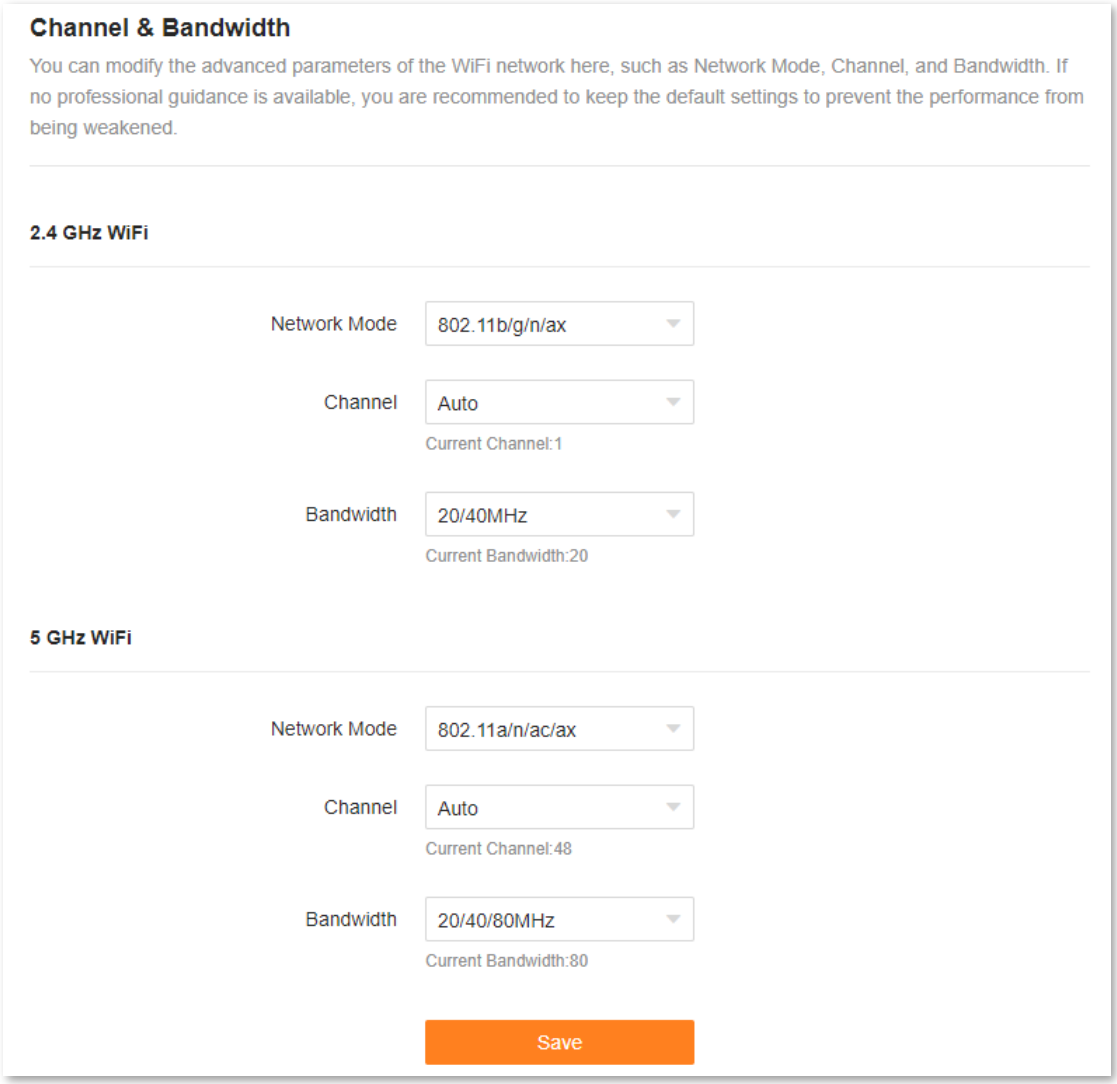
Channel & bandwidth

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

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

TIP

In order not to influence 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 WiFi network of the Mesh device. • **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 Mesh device. 5 GHz WiFi 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 Mesh device. • **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 Mesh device. • **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 Mesh device.
Channel	Specifies the channel in which the Wi-Fi network works. By default, the wireless channel is **Auto**, which indicates that the Mesh device selects a channel for the Wi-Fi network automatically. You are recommended to choose a channel with less interference for better wireless transmission efficiency. You can use a third-party tool to scan the Wi-Fi signals nearby to understand the channel usage situations.
Bandwidth	Specifies the bandwidth of the wireless channel of a Wi-Fi network. Please change the default settings only when necessary. • **20MHz**: Indicates that the channel bandwidth used by the Mesh device is 20 MHz. • **40MHz**: Indicates that the channel bandwidth used by the Mesh device is 40 MHz. • **20/40MHz**: Specifies that a Mesh device 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 Mesh device is 80 MHz. This option is available only at 5 GHz. • **160MHz**: Indicates that the channel bandwidth used by the Mesh device is 160 MHz. This option is available only at 5 GHz. • **20/40/80/160MHz**: Specifies that a Mesh device 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.

WPS

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

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

TIP

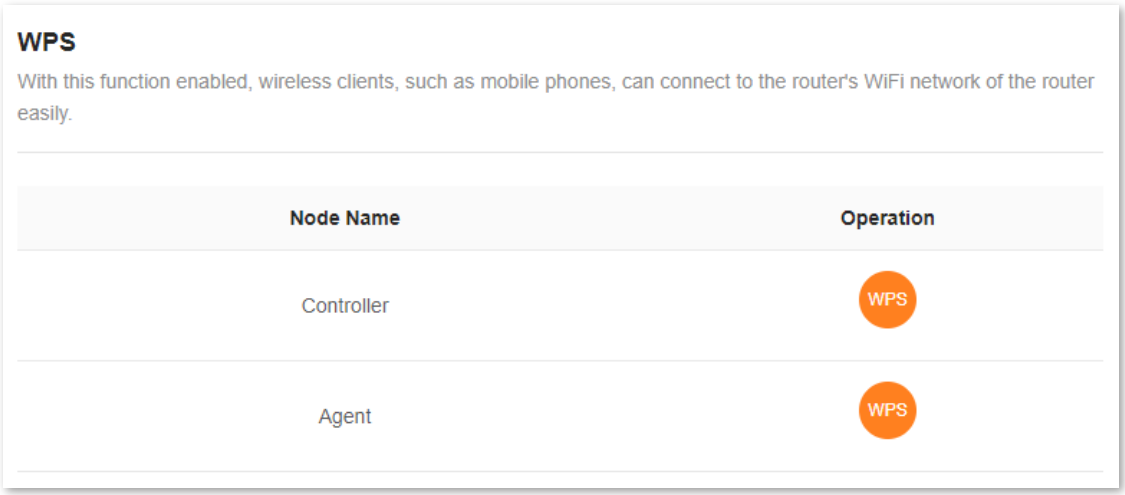
- This function only applies to WPS-enabled Wi-Fi devices. It is enabled by default and cannot be disabled.
- Wi-Fi networks encrypted with WPA3 cannot be connected through WPS.
- The WPS negotiation times out in 120 seconds. The **WPS** button is disabled during WPS negotiation.

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

Step 1 Log in to the web UI.

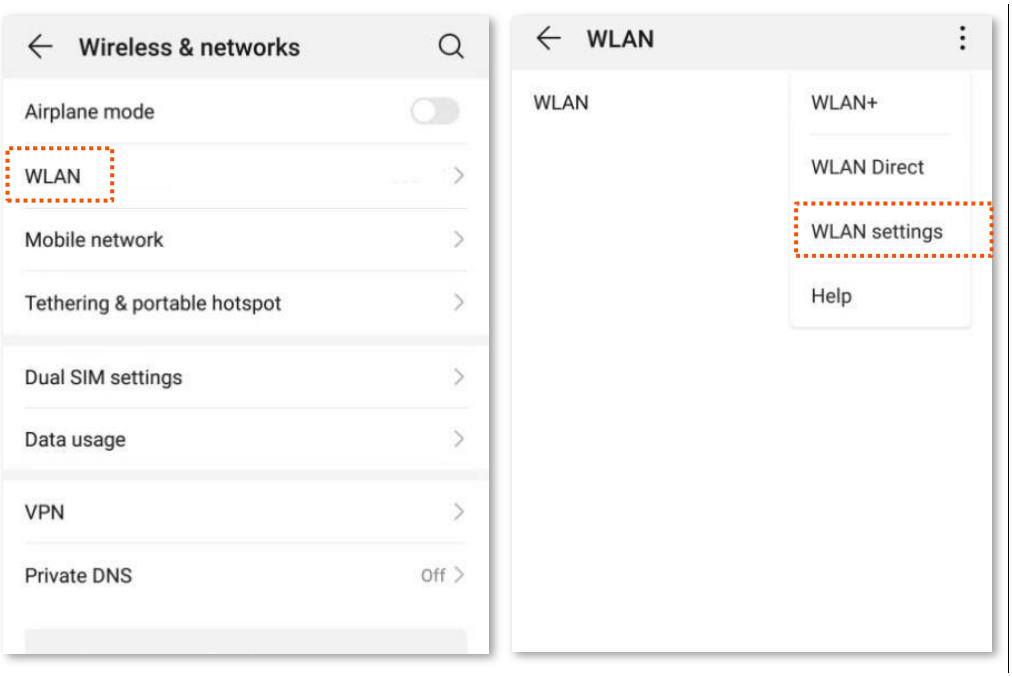
Step 2 Choose **More** > **WiFi Settings** > **WPS.**

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

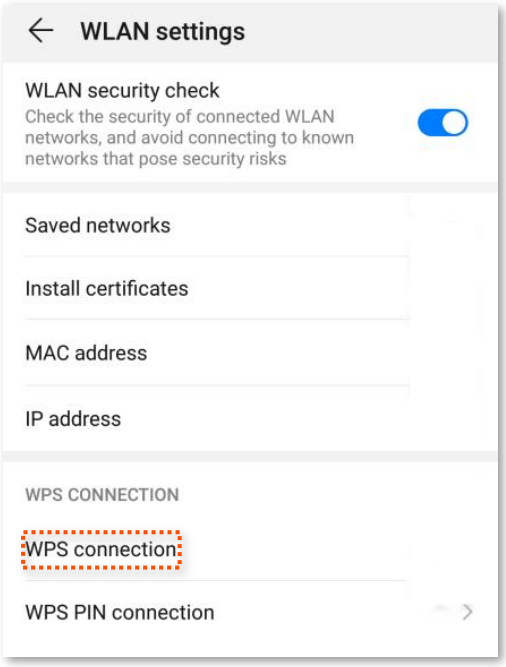


Step 4 Configure the WPS function on your WiFi-enabled devices **within 2 minutes**. Configuration on various devices may differ (Example: HUAWEI P10).

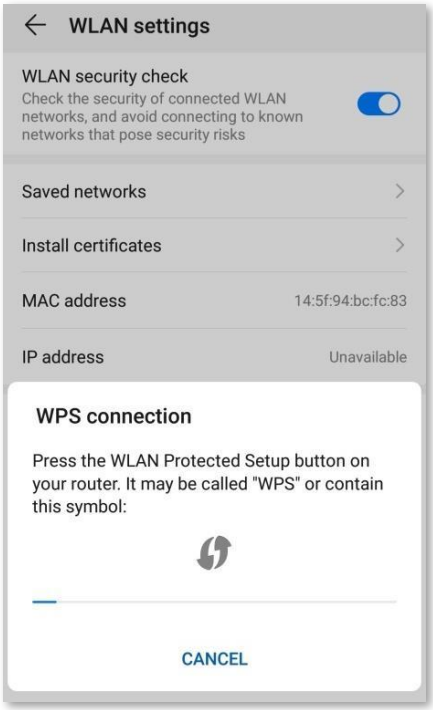
1. Find **WLAN** settings on your phone.
2. Tap ⋮, and choose **WLAN settings**.



3. Choose **WPS connection**.



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



---End

MESH button

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

TIP

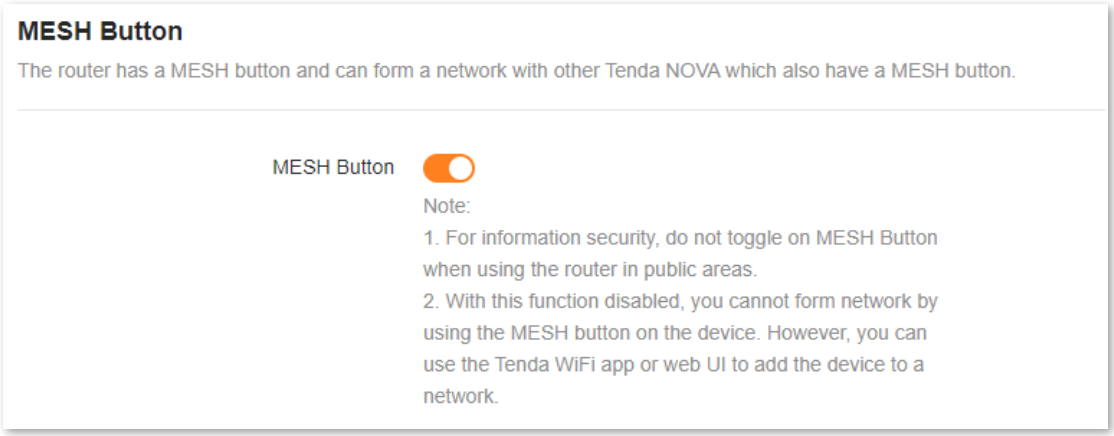
- For information security, do not toggle on **MESH Button** when using the Mesh device in public areas.
- With this function disabled, you cannot form a network by using the **MESH** button on the device. However, you can use the Tenda WiFi app or web UI to add the device to a network.

To enable or disable the **MESH** button:

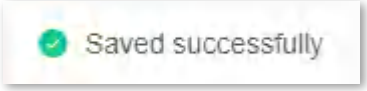
Step 1 Log in to the web UI.

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

2.8.7 Network settings

LAN Settings

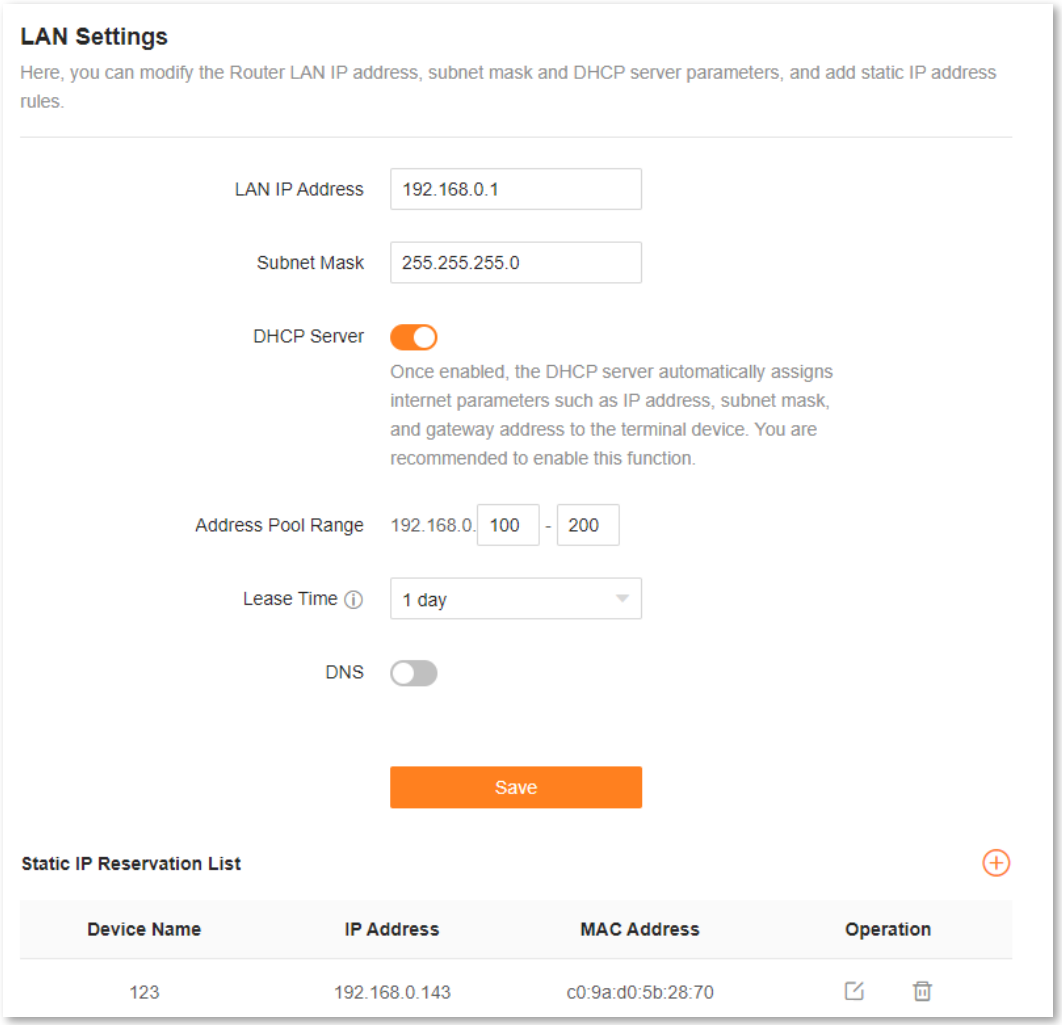
To access the configuration page, log in to the web UI of the Mesh device, and choose **More** > **Network Settings** > **LAN Settings**.

Overview

On this page, you can:

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

  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 Mesh device, which is also the management IP address for logging in to the web UI of the Mesh device.
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 Mesh device. The default range is 192.168.0.100 to 192.168.0.200.

Parameter		Description
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 Mesh device 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 Mesh device has the DNS proxy function.
Primary DNS		Specifies the primary DNS address allocated to the client by the Mesh device. 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 Mesh device 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.
	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.

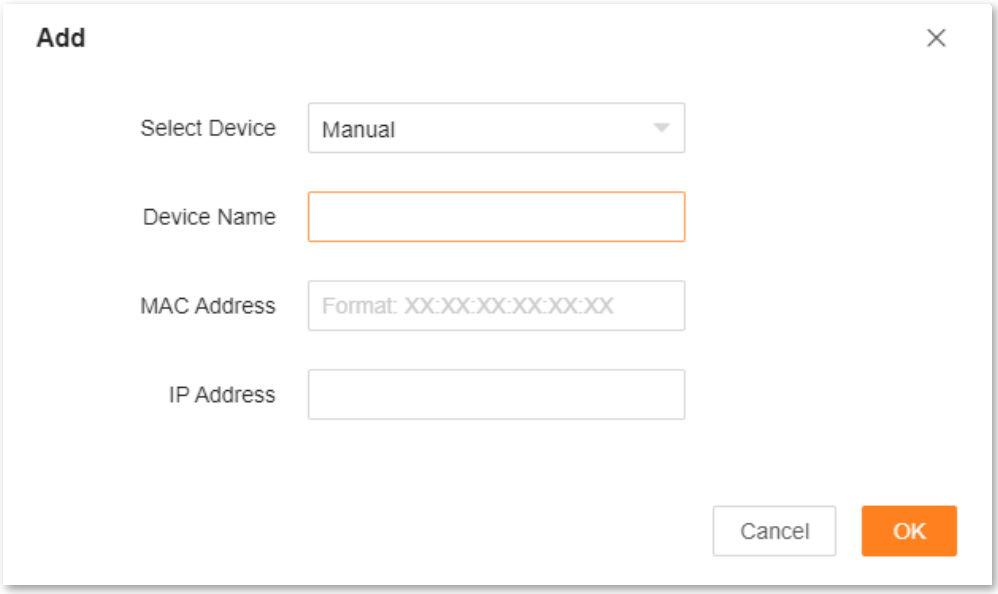
Step 2 Choose **More** > **Network Settings** > **LAN Settings**.

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

Step 4 Set **Select Device**.

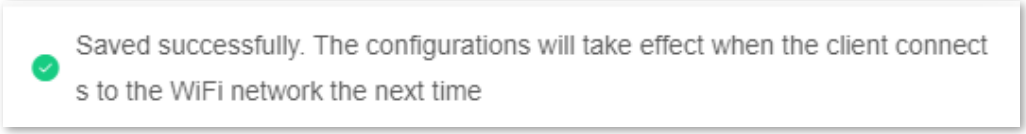
- You can directly select a client from the drop-down list box, which requires no further settings on **MAC Address** and **IP Address**.

- 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.

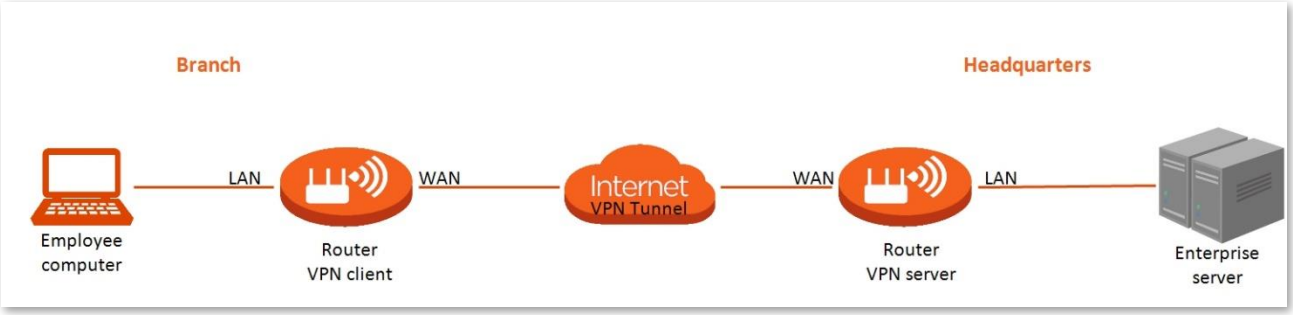


---End

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.

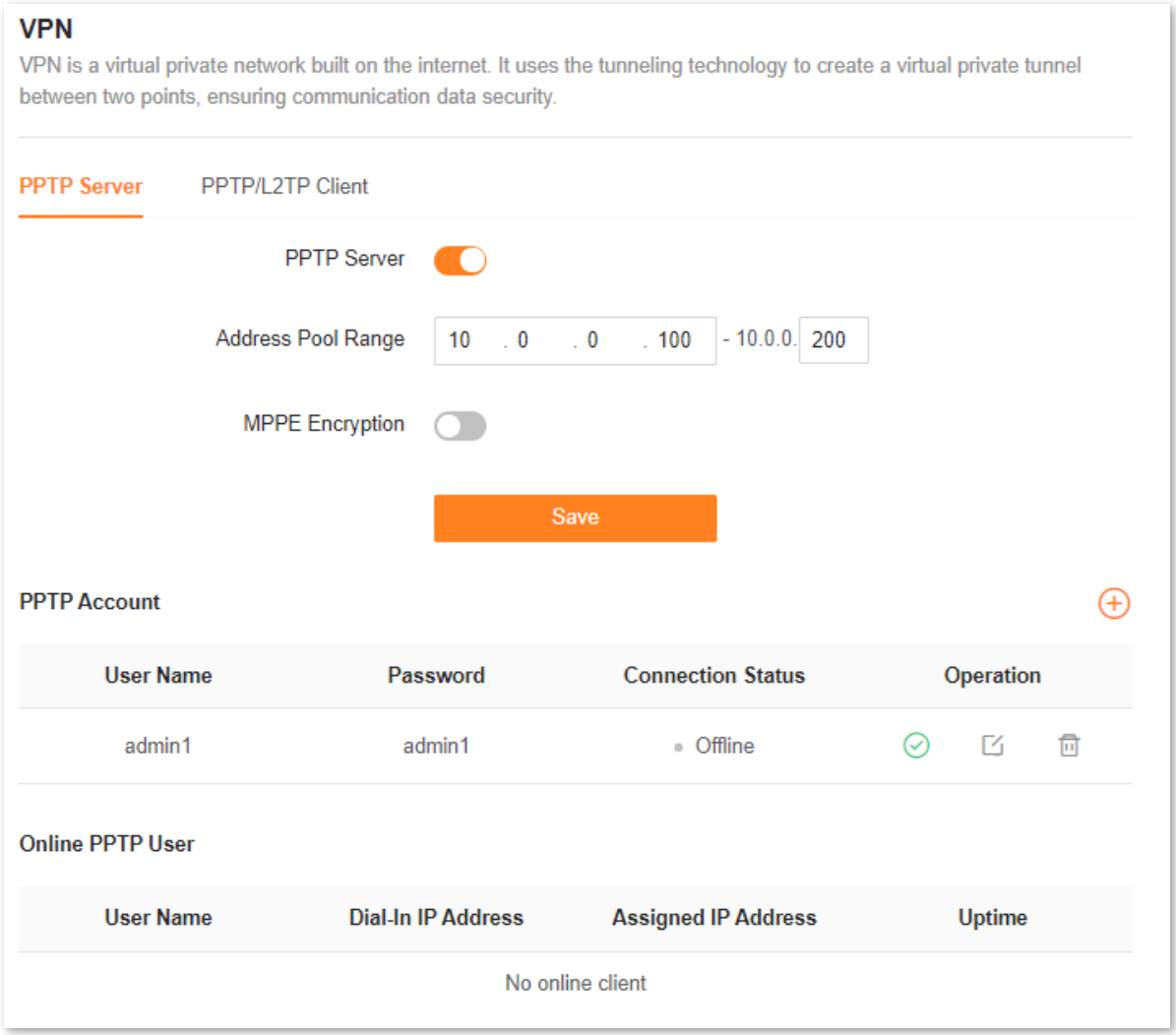
The typology of a VPN network is shown below.



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 Mesh device, 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

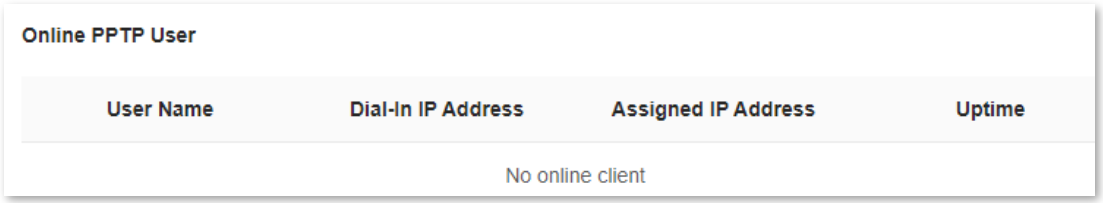
Parameter		Description
PPTP Server	PPTP Server	Used to enable or disable the PPTP server. When it is enabled, the Mesh device functions as a PPTP server, which can accept the connections from PPTP clients.
	Address Pool Range	Specifies the IP address range within which the PPTP server can assign to PPTP 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.

Parameter		Description
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 Mesh device, 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 Mesh device, 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 Mesh device.

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 Mesh device 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 Mesh device 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:

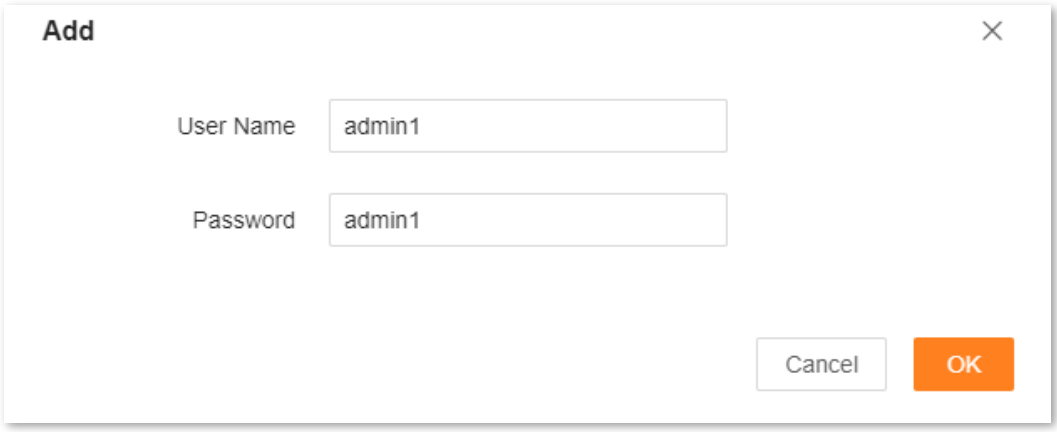
Step 1 Log in to the web UI.

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.**

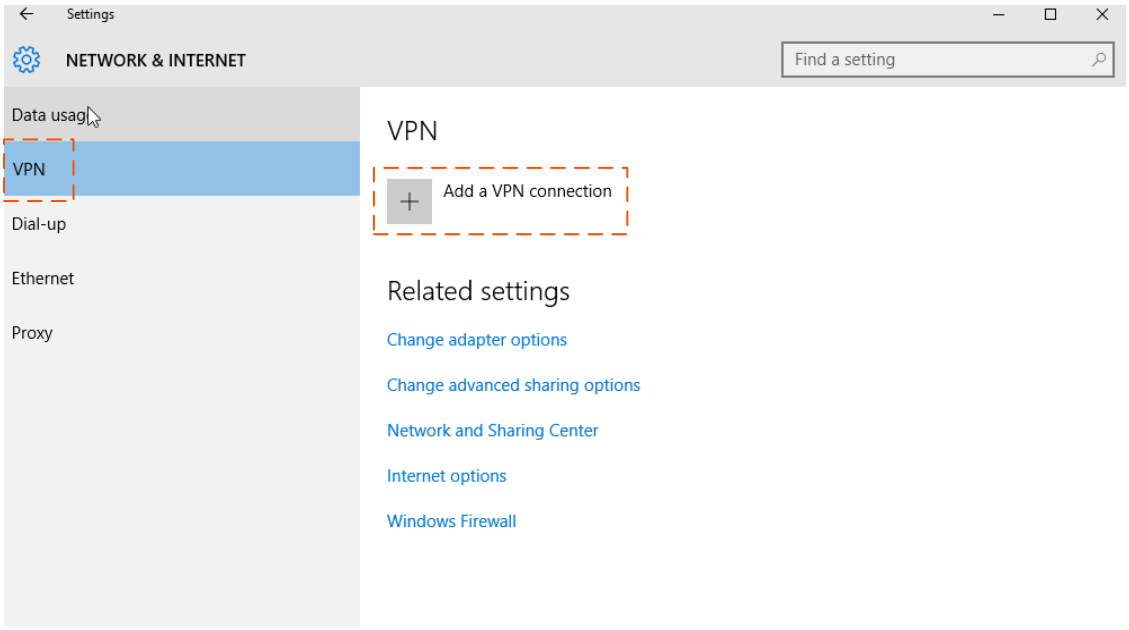
The following message is displayed, indicating that the settings are saved successfully.

---End

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

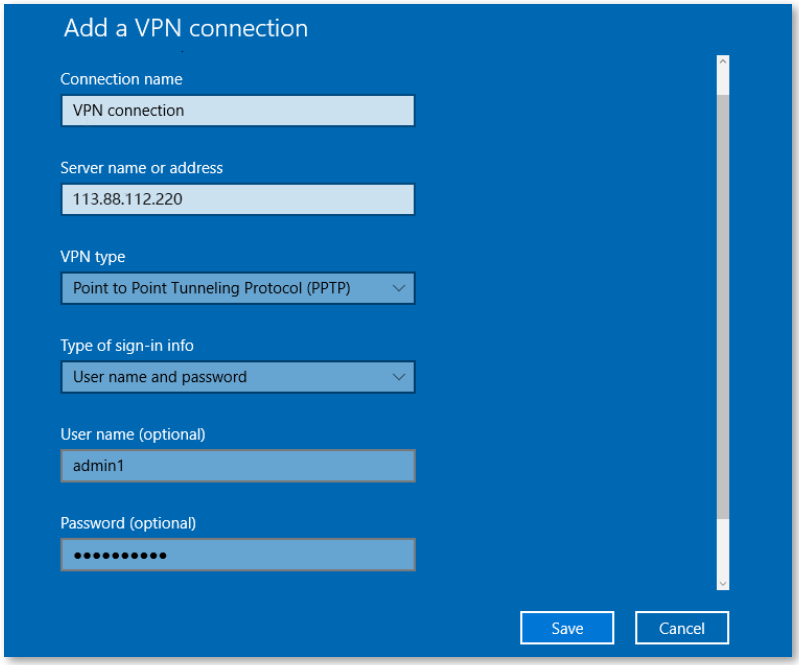
Step 1 Click the icon at the bottom right corner on the desktop of another computer with internet access, and then click **Network settings**.

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

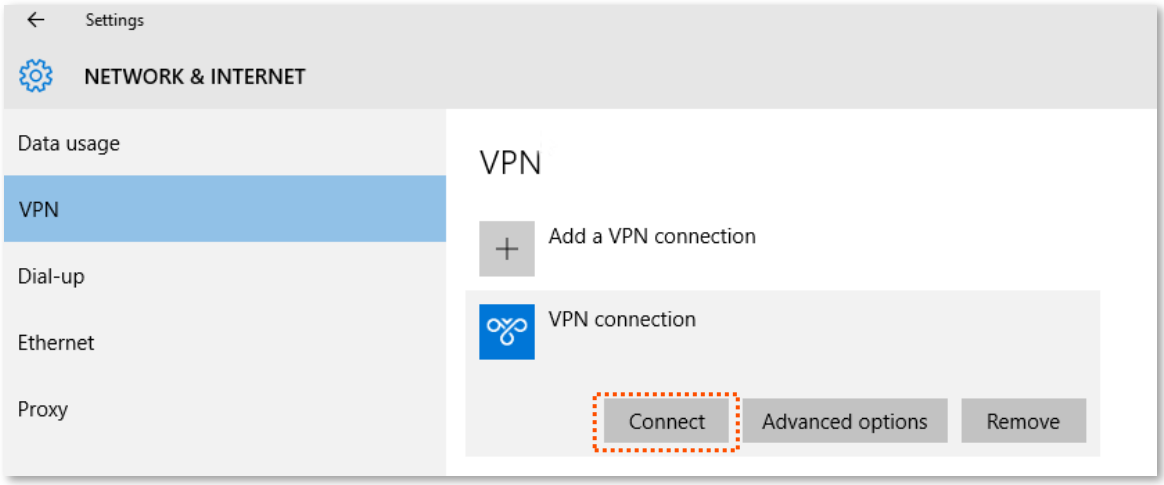


Step 3 Configure the VPN parameters.

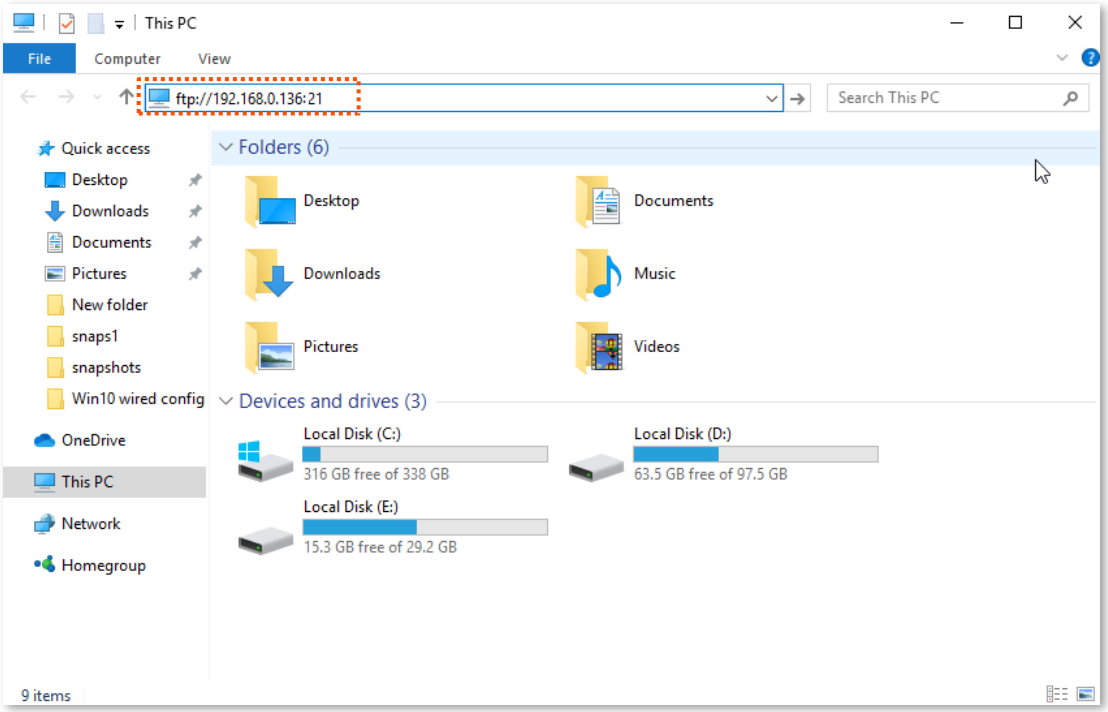
1. Enter a connection name, such as **VPN connection**.
2. Enter the server address, which is **113.88.112.220** in this example.
3. Select a VPN type, which is **Point to Point Tunneling Protocol (PPTP)** in this example.
4. Select a type of sign-in info, which is **User name and password** in this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



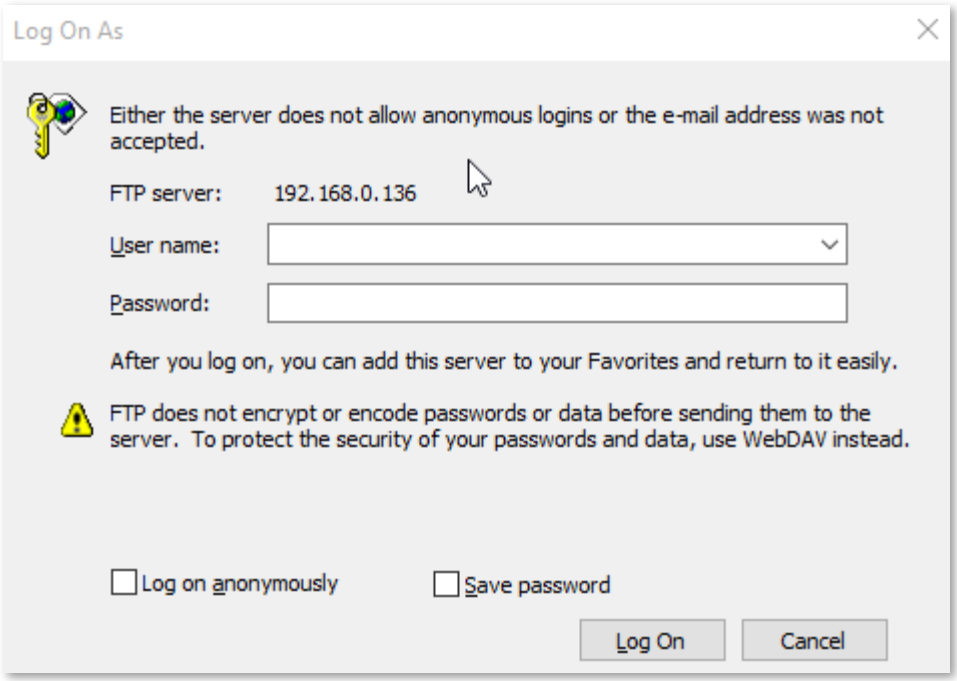
Step 4 Find the VPN connection added, and click **Connect**.



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**.



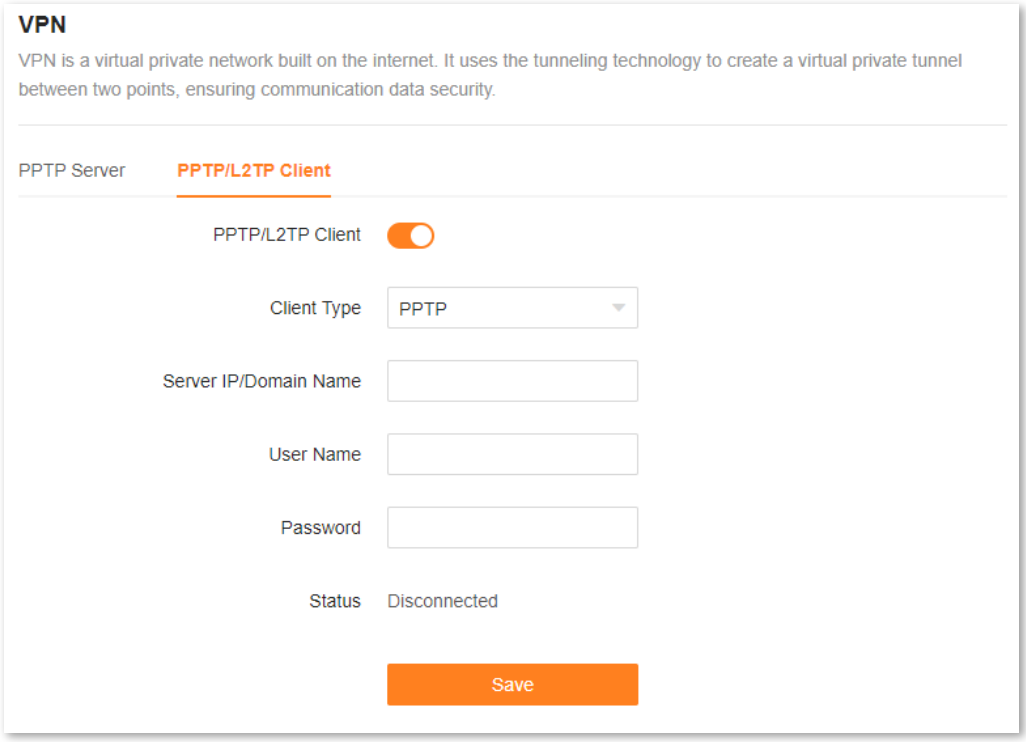
---End

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

PPTP/L2TP client

This series of Mesh devices 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 Mesh device serves as, either PPTP or L2TP. • **PPTP**: When the Mesh device is connecting to a PPTP server, select this option. • **L2TP**: When the Mesh device 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 Mesh device connects to. Generally, when a Mesh device 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	Specifies 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 Mesh device**

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**.

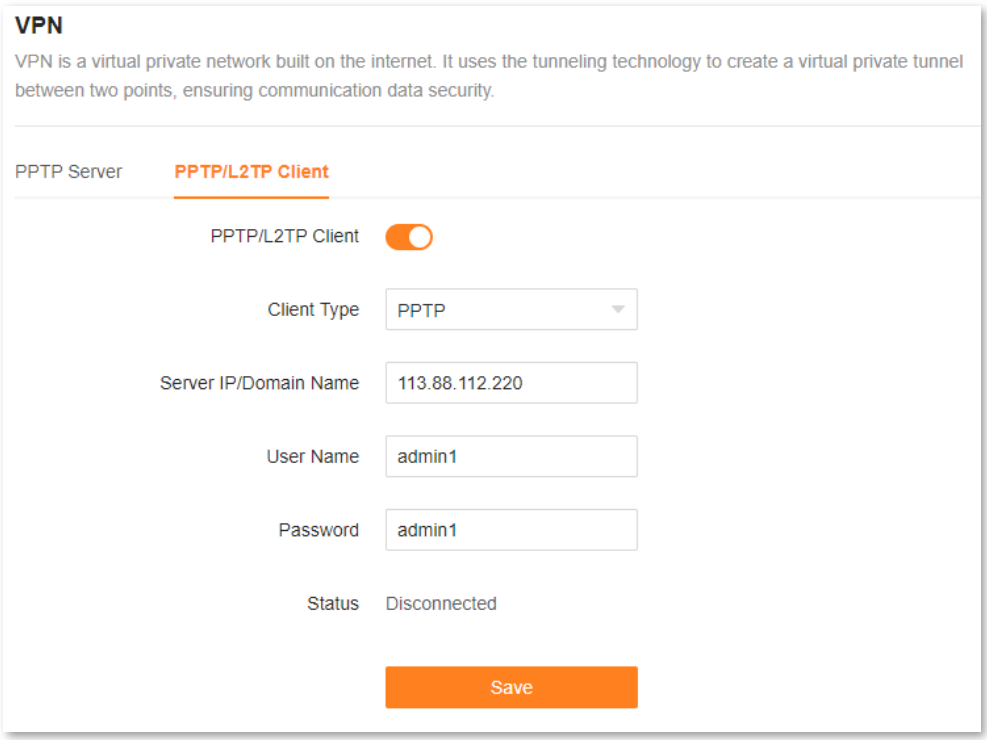
Step 3 Enable **PPTP/L2TP Client.**

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.

IPTV

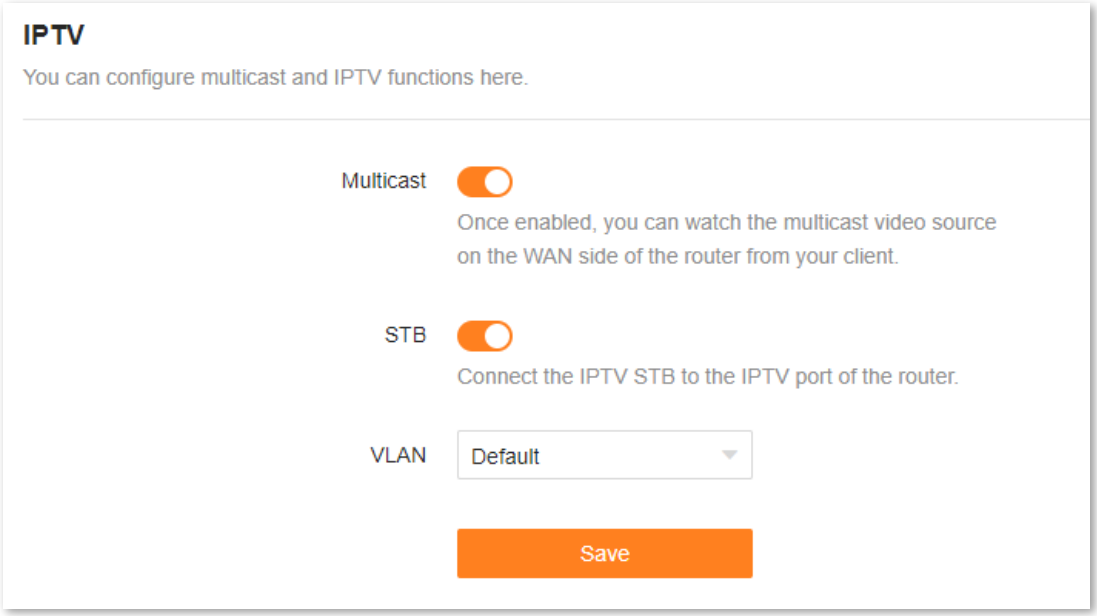
IPTV is the technology integrating internet, multimedia, telecommunication and many other technologies to provide interactive services, including digital TV, for family users by internet broadband lines.

You can set the multicast and STB functions here.

- **Multicast**: If you want to watch multicast videos from the WAN side of the Mesh device on your computer, you can enable the multicast function of the Mesh device.
- **STB** (set-top box): If the IPTV service is included in your broadband service, you can enjoy both internet access through the Mesh device 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 Mesh device 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

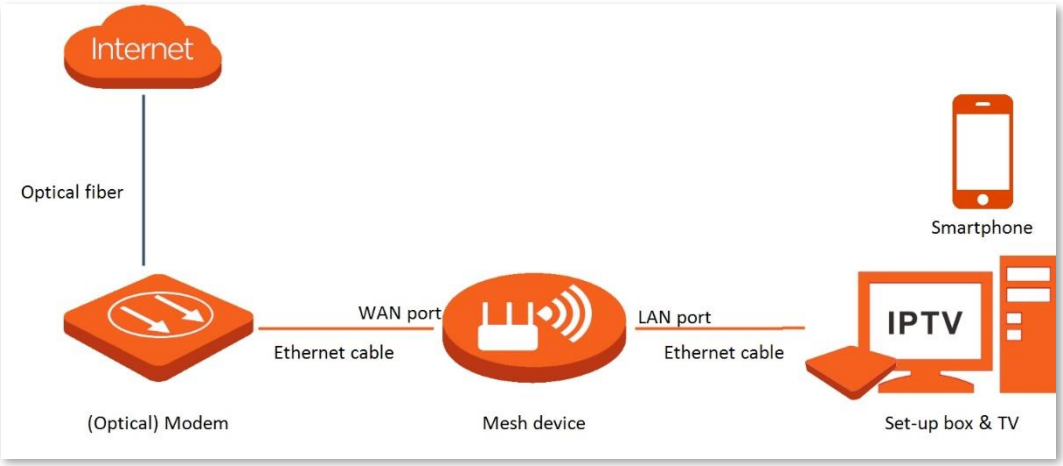
Parameter	Description
Multicast	Used to enable or disable the multicast function.
STB	Used to enable or disable the IPTV function of the Mesh device. When this function is enabled, the port **LAN3/IPTV** can be used only as an IPTV port and be connected to an IPTV set-top box.
VLAN	Specifies the VLAN ID of your IPTV service. • 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 Mesh device

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 Mesh device.

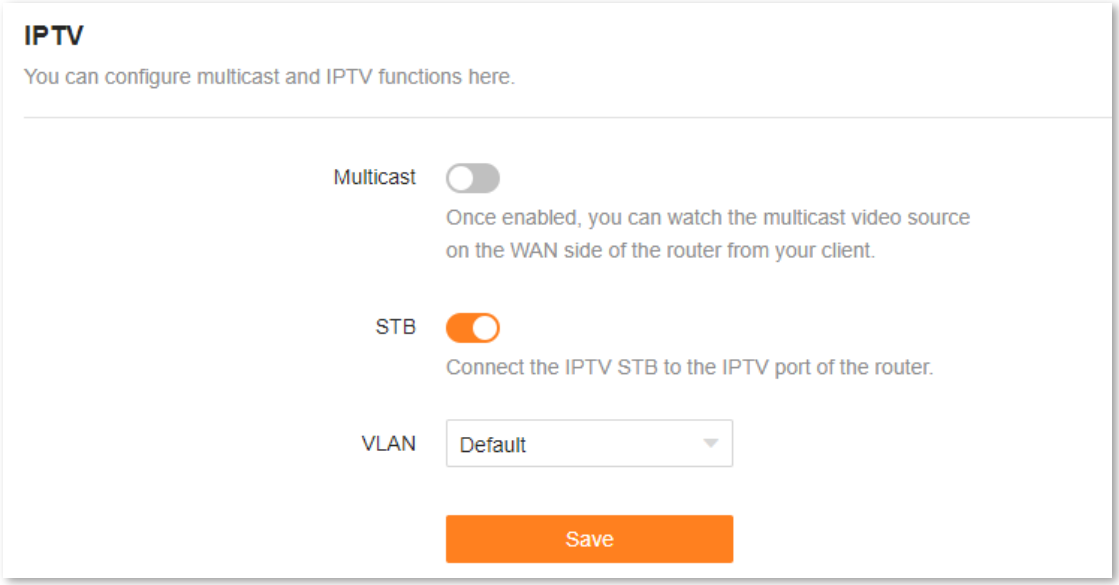
Solution: You can configure the IPTV function to reach the goal.



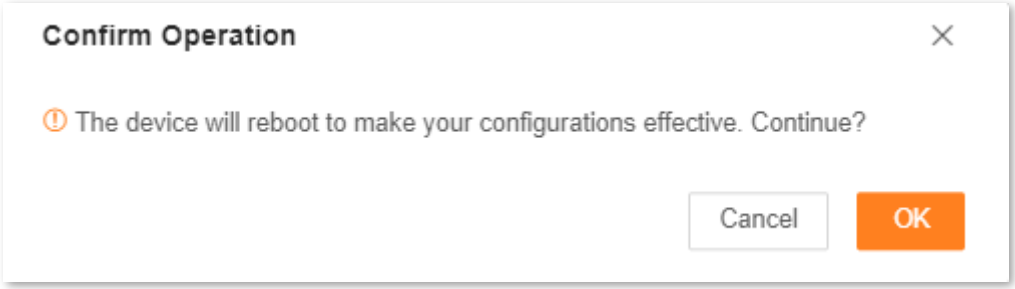
Configuration procedure:

Step 1 Set your Mesh device.

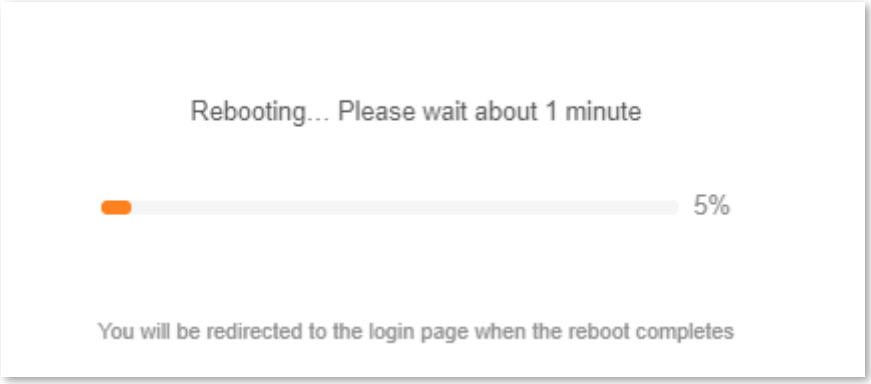
1. Log in to the web UI.
2. Choose **More** > **Network Settings** > **IPTV**.
3. Enable the **STB** function.
4. Click **Save**.



5. Click **OK**.



Wait until the Mesh device 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

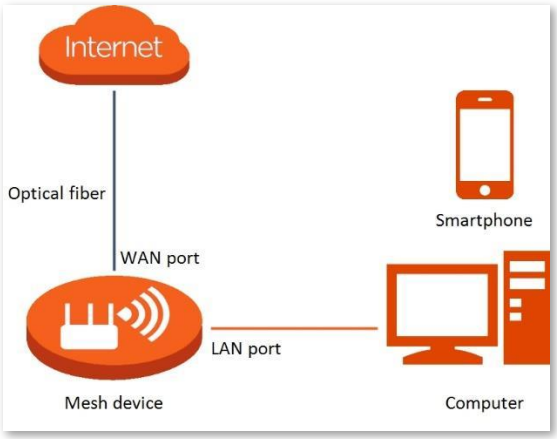
After completing the configuration, you can watch IPTV programs on your TV.

Watch multicast videos through the Mesh device

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.



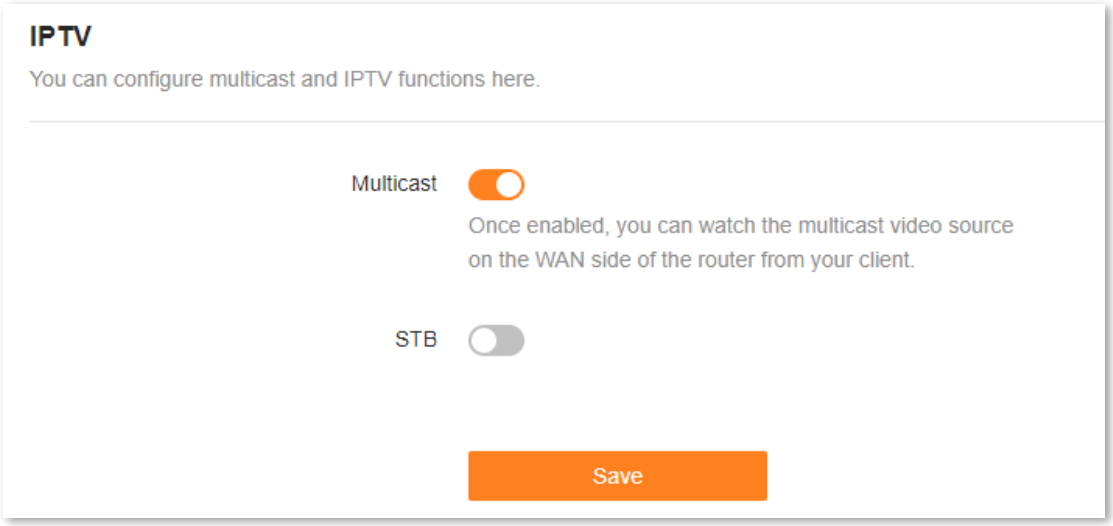
Configuration procedure:

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**.



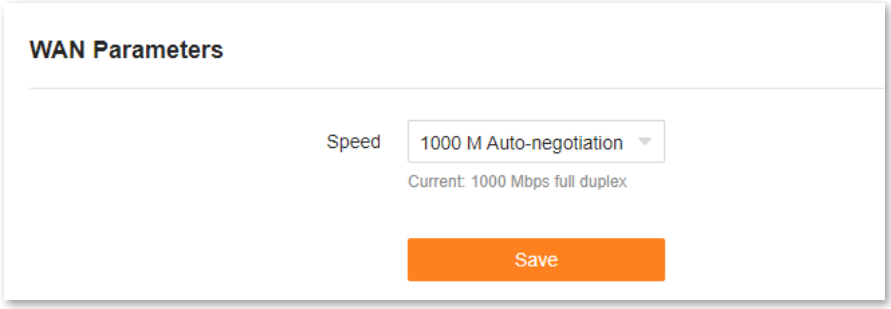
---End

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

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 Mesh device, 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.

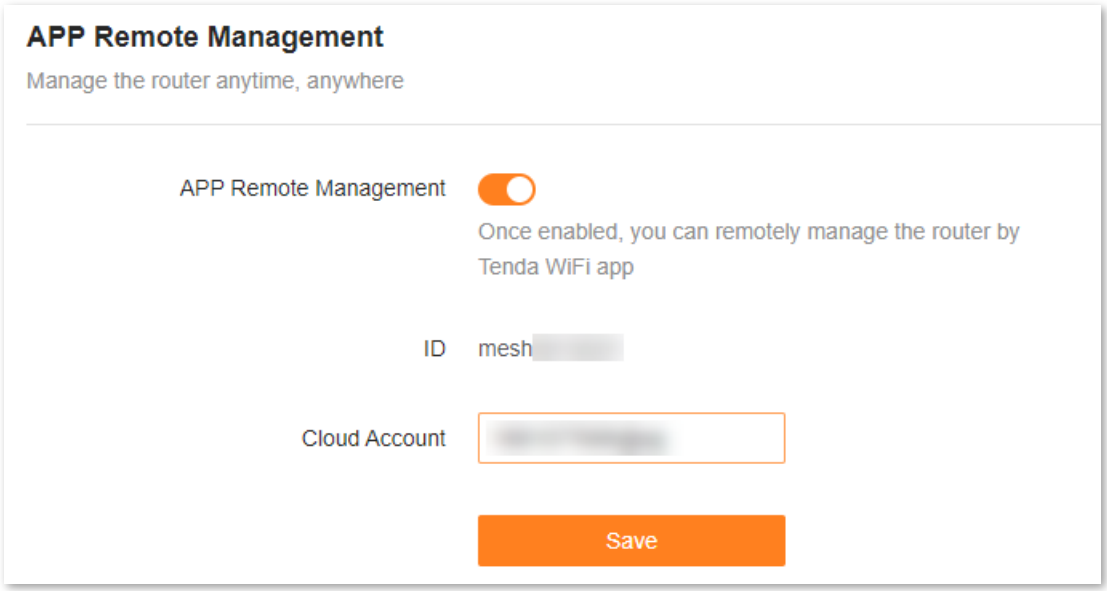
Speed	Application
10 Mbps full duplex	Indicates that the WAN port is working at the speed of 10 Mbps, and the port can receive and send data packets at the same time.
10 Mbps half duplex	Indicates that the WAN port is working at the speed of 10 Mbps, but the port can only receive or send data packets alternately.

2.8.8 Advanced

App remote management

The Mesh device can be managed remotely using the Tenda WiFi app. The app remote management function is enabled by default. You can disable this function as required.

To access the configuration page, log in to the web UI of the Mesh device, 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 Mesh node, which is automatically allocated.
Cloud Account	Specifies the account bound on your Tenda WiFi app.

MAC address filter

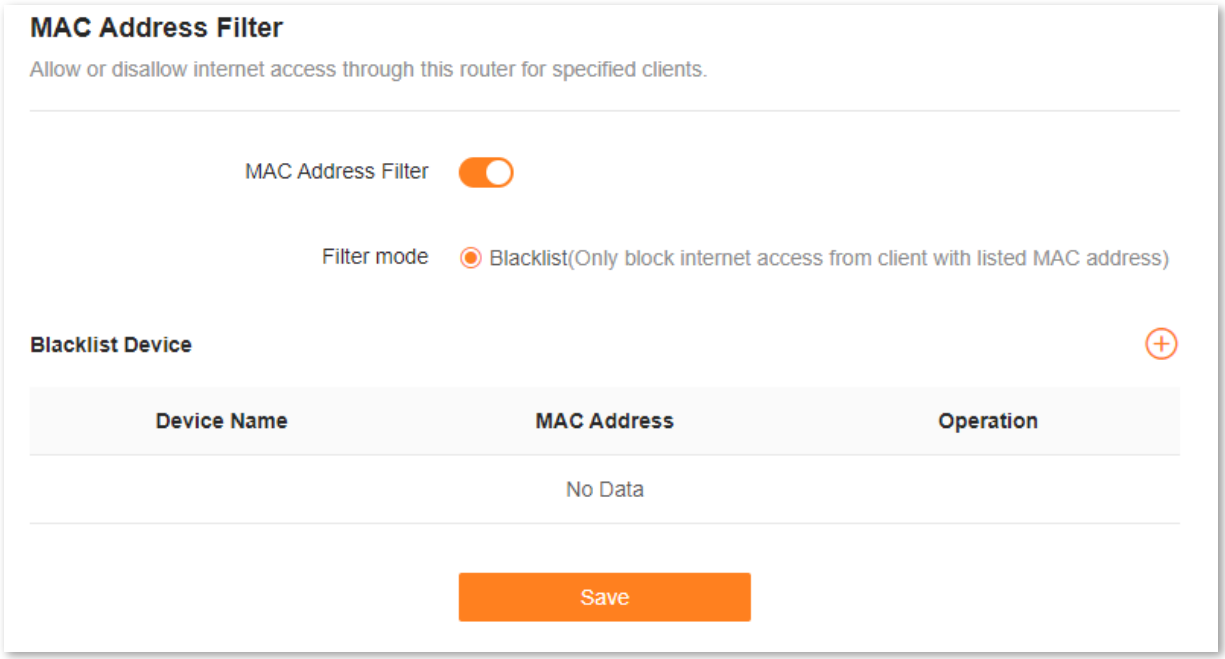
Overview

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

TIP

- If you blacklist a wired client, the client will fail to access the network, but it can still connect to the Mesh device.
- If you blacklist a wireless device, the client will be kicked offline and cannot connect to the Mesh device again.

To access the configuration page, log in to the web UI of the Mesh device, 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 Mesh device.
Blacklist Device	Device Name	Specifies the name of the blacklisted client.
	MAC Address	Specifies the MAC address of the blacklisted client.

Parameter	Description
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

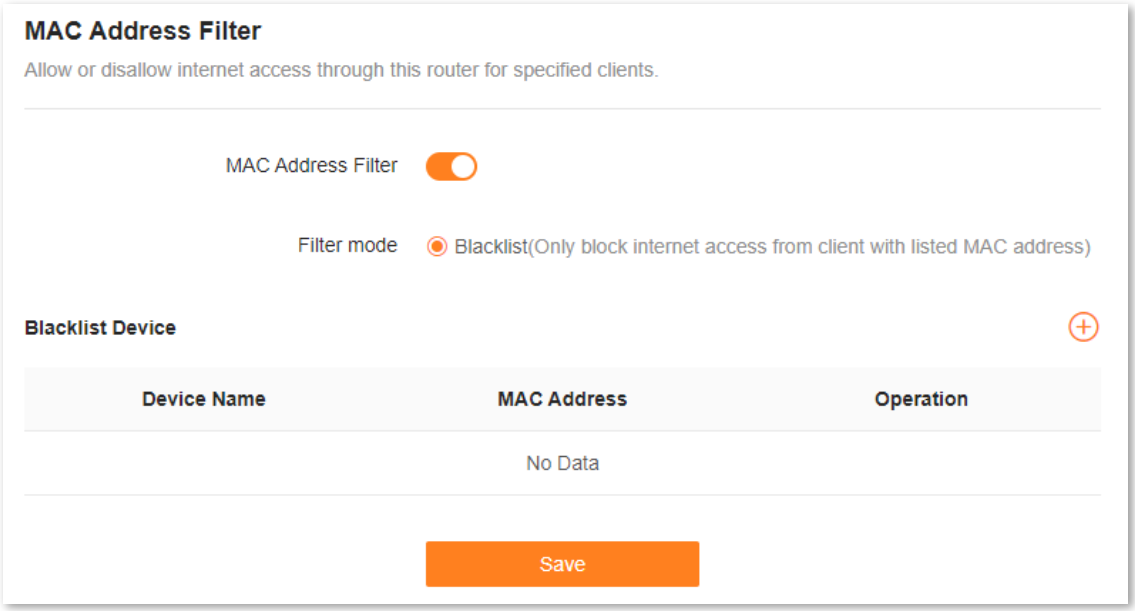
Configuration procedure:

Step 1 Log in to the web UI.

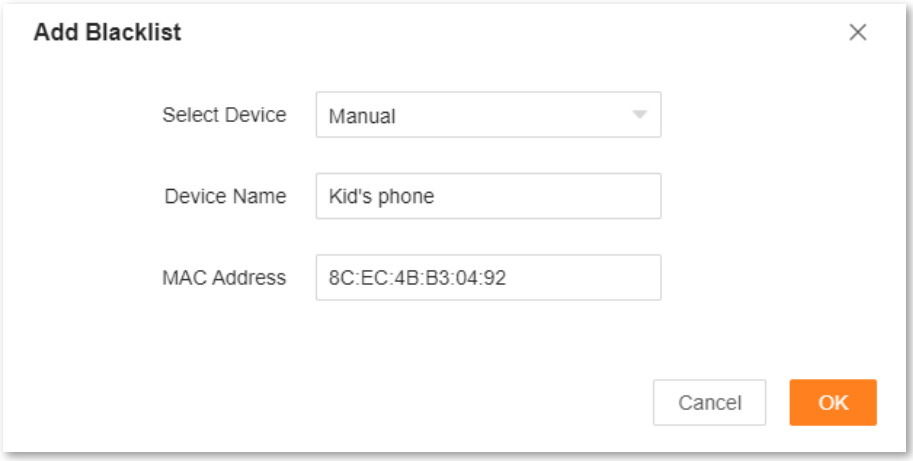
Step 2 Choose **More** > **Advanced** > **MAC Address Filter**.

Step 3 Enable **MAC Address Filter**.

Step 4 Click .

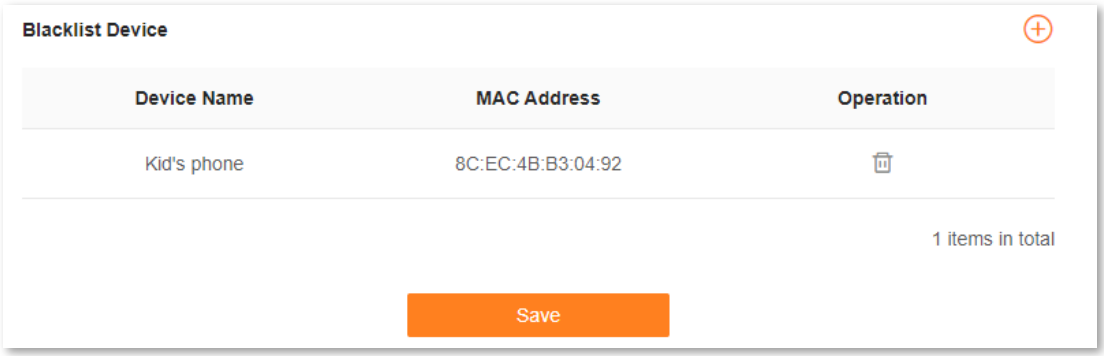


Step 5 Set **Device Name**. Enter **MAC Address** of the client, which is **8C:EC:4B:B3:04:92** in this example.



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.

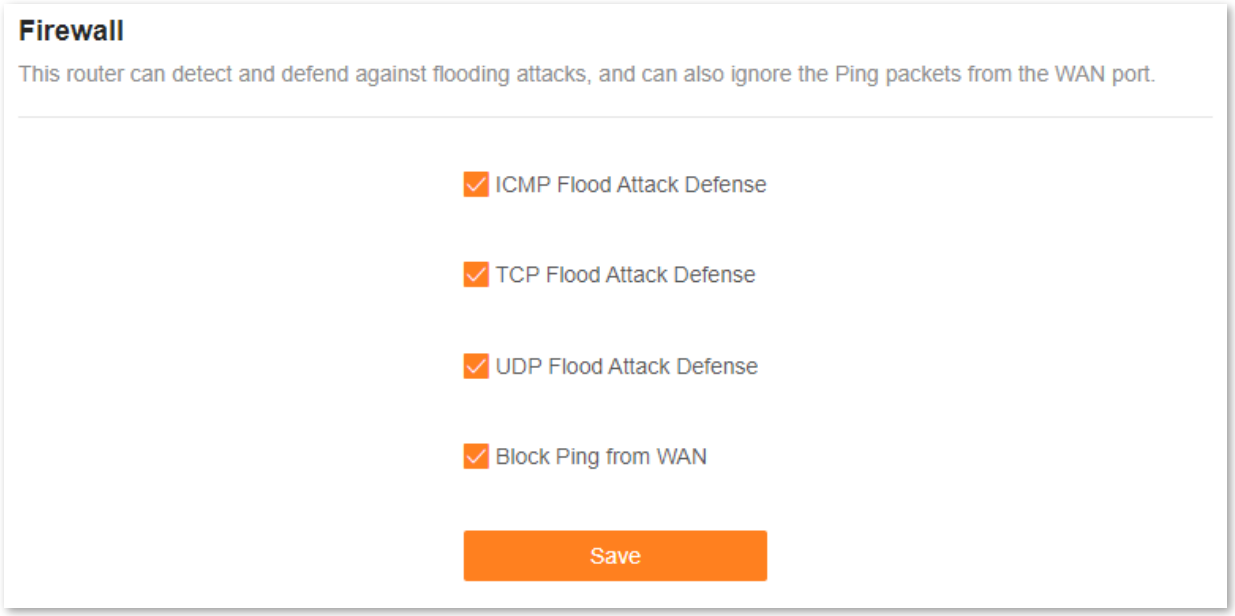
---End

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

Firewall

The firewall function helps the Mesh device 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 Mesh device, 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 Mesh device automatically ignores the ping to its WAN from hosts from the internet and prevents itself from being exposed, while preventing external ping attacks.

DMZ host

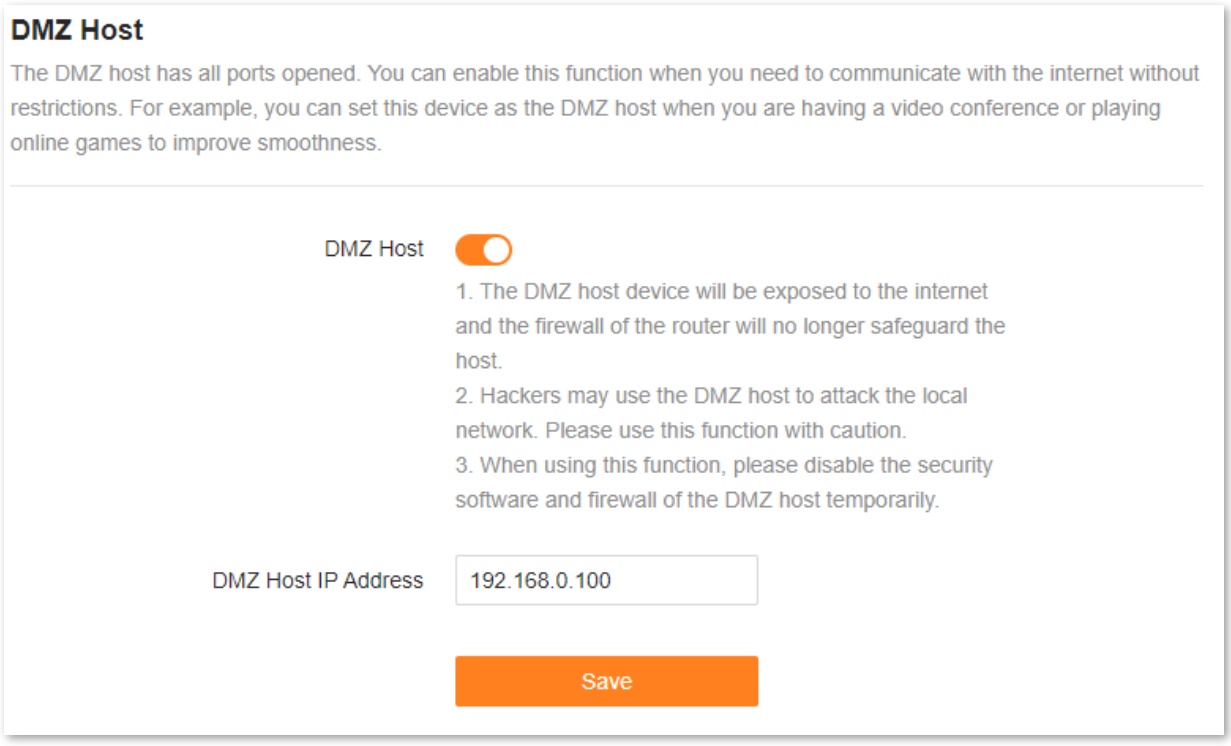
Overview

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 Mesh device. 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 Mesh device, 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.

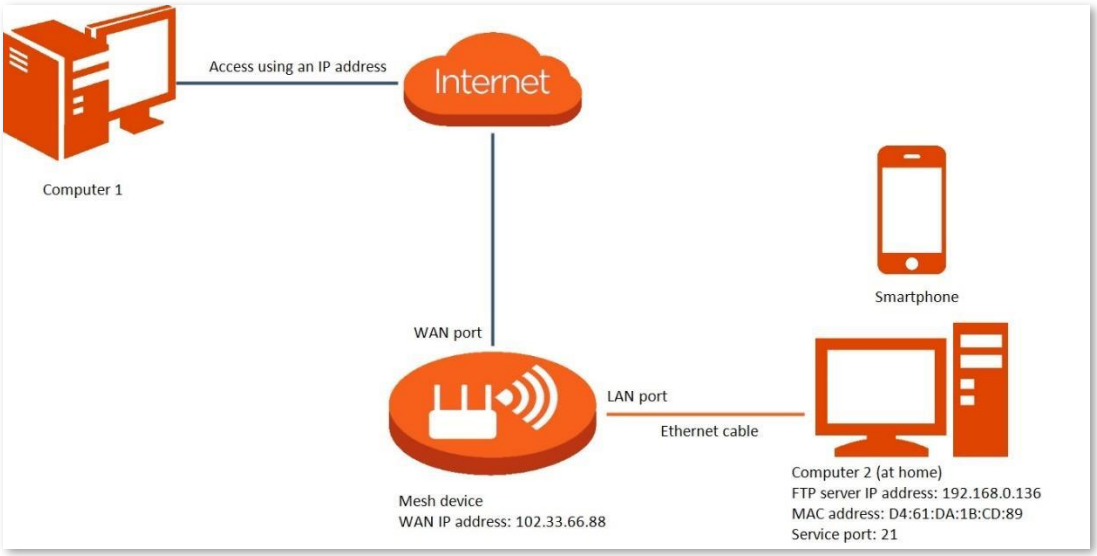
Solution: You can configure the DMZ host function to reach the goal.

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 Mesh device: **102.33.66.88**

TIP

Ensure that the Mesh device 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.

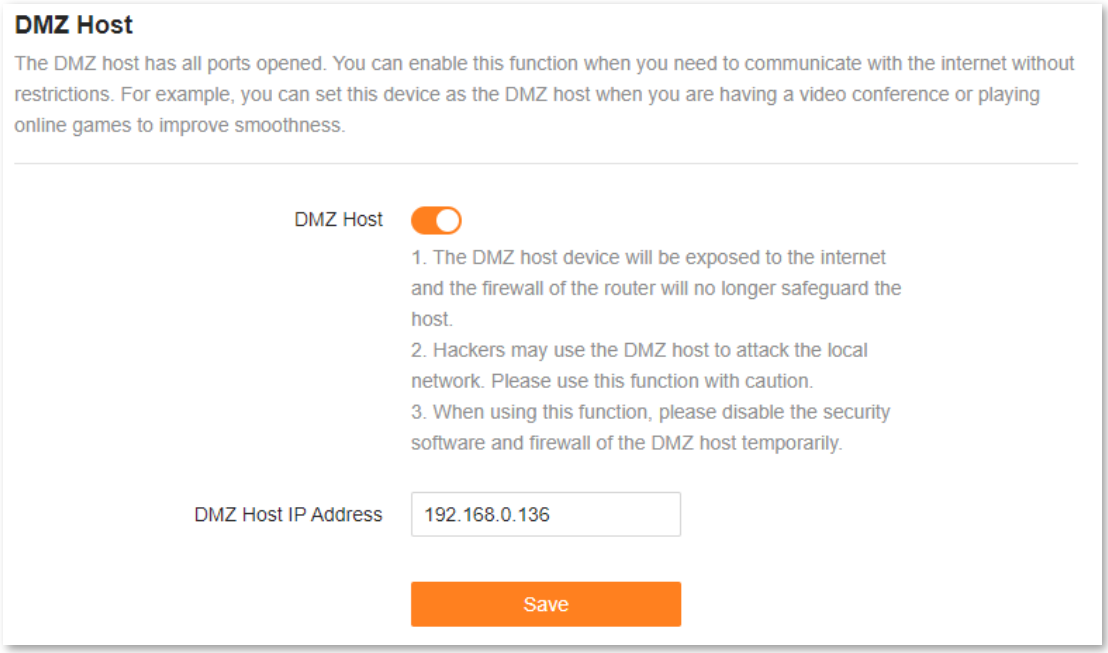


Configuration procedure:

Step 1 Log in to the web UI.

Step 2 Set the server host as the DMZ host.

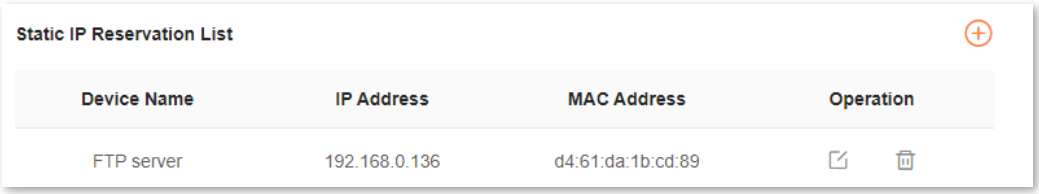
1. Choose **More** > **Advanced** > **DMZ Host**.
2. Enable **DMZ Host**.
3. Enter the IP address of the host, which is **192.168.0.136** in this example.
4. Click **Save**.



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**.



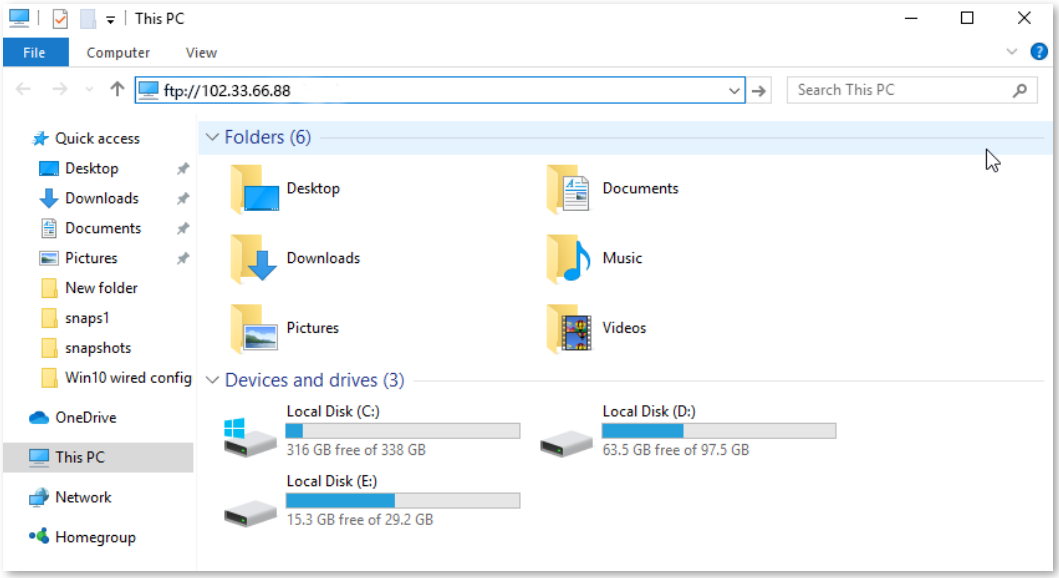
----End

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 Mesh device*". 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 Mesh device:Intranet service port number*".

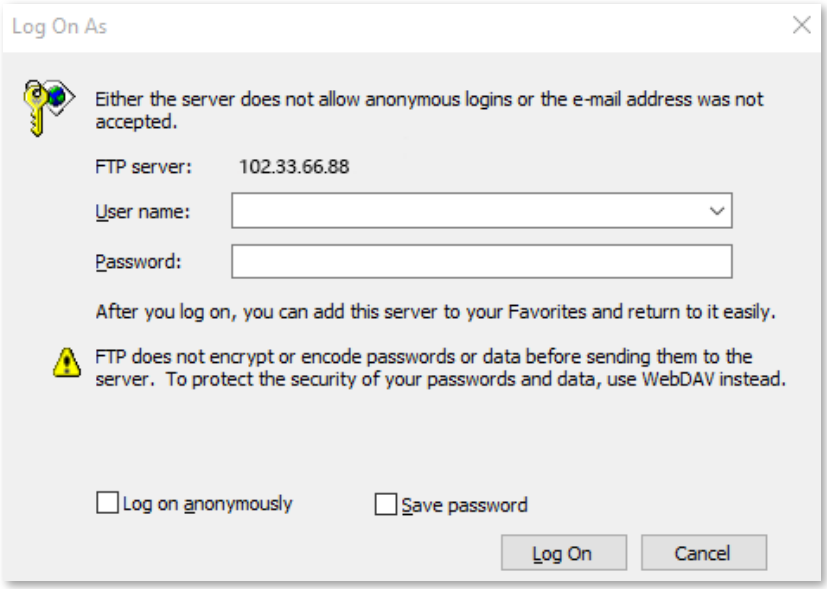
In this example, the address is "**ftp://102.33.66.88**". You can find the WAN IP address of the Mesh device in WAN port information.

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.

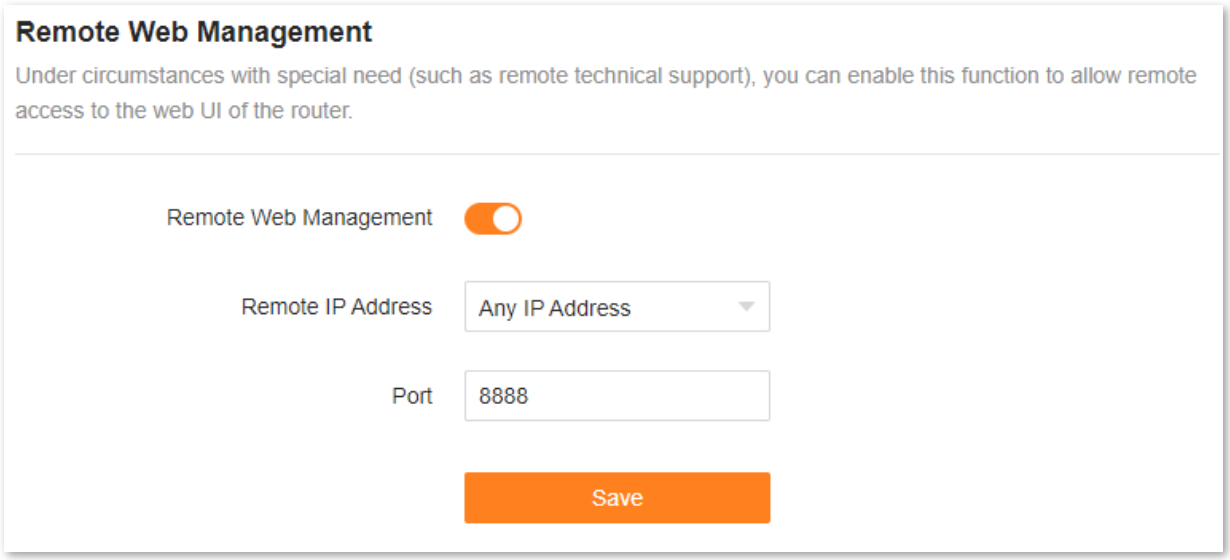
Remote web management

Overview

Generally, the web UI of the Mesh device can only be accessed on clients that are connected to the Mesh device 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 Mesh device, 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 Mesh device.
Remote IP Address	Specifies the IP address of the host which can access the web UI of the Mesh device remotely. • **Any IP Address**: Indicates that hosts with any IP address from the internet can access the web UI of the Mesh device. It is not recommended for security. • **Specified IP Address**: Only the host with the specified IP address can access the web UI of the Mesh device remotely. If the host is under a LAN, ensure that the IP address is the IP address of the gateway of the host (a public IP address).

Parameter	Description
Port	Specifies the port number of the Mesh device 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 Mesh device*:*Port number*". If the DDNS host function is enabled, the web UI can also be accessed through "http://*Domain name of the Mesh device's WAN port*:*Port number*".

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

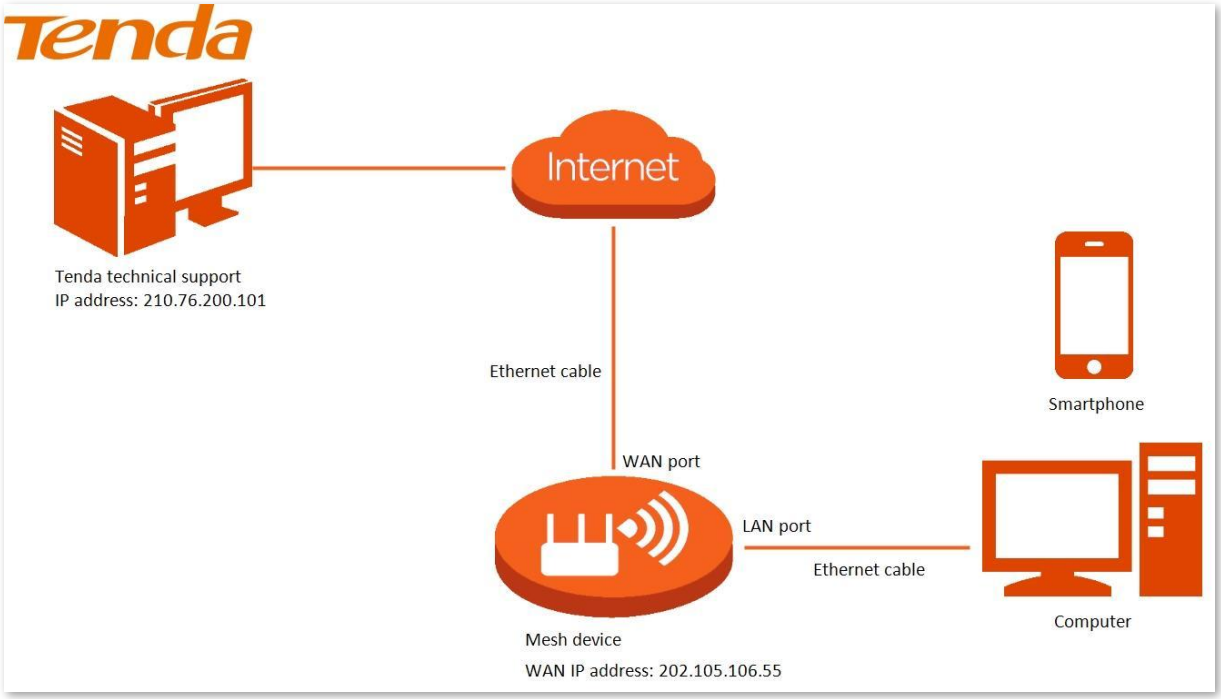
Scenario: You encounter a problem in configuring the Mesh device, and the Mesh device can access the internet.

Goal: Ask the Tenda technical support to help you configure the Mesh device 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 Mesh device: **202.105.106.55**



Configuration procedure:

Step 1 Log in to the web UI.

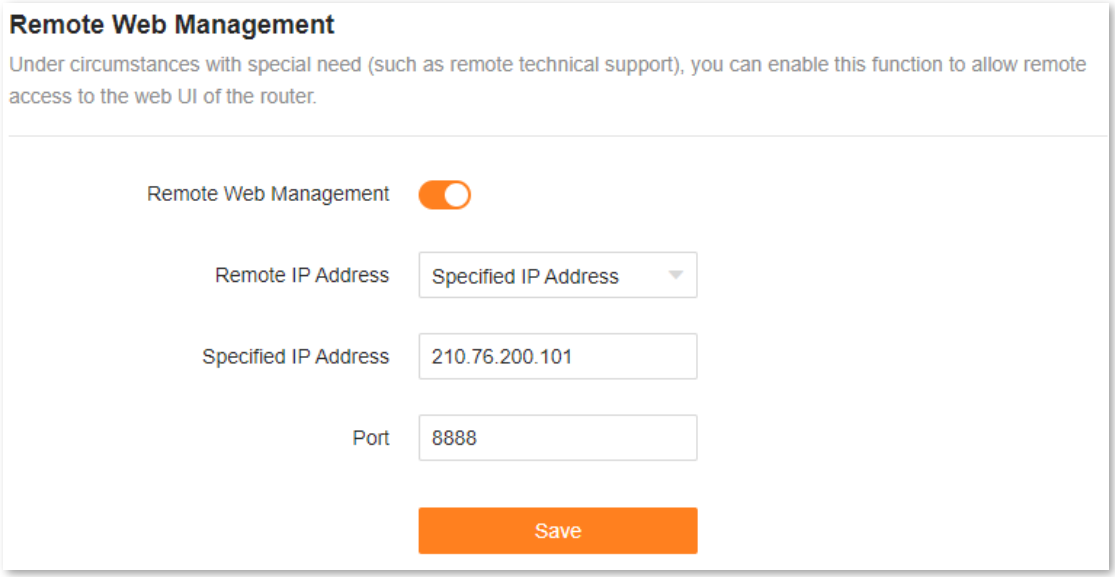
Step 2 Choose **More** > **Advanced** > **Remote Web Management**.

Step 3 Enable **Remote Web Management**.

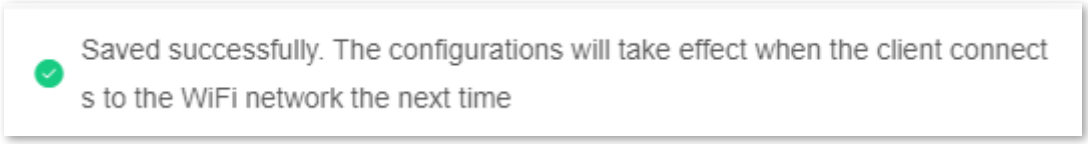
Step 4 Select **Specified IP Address** for **Remote Web Management**.

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 Mesh device by visiting "**http://202.105.106.55:8888**" on the computer.

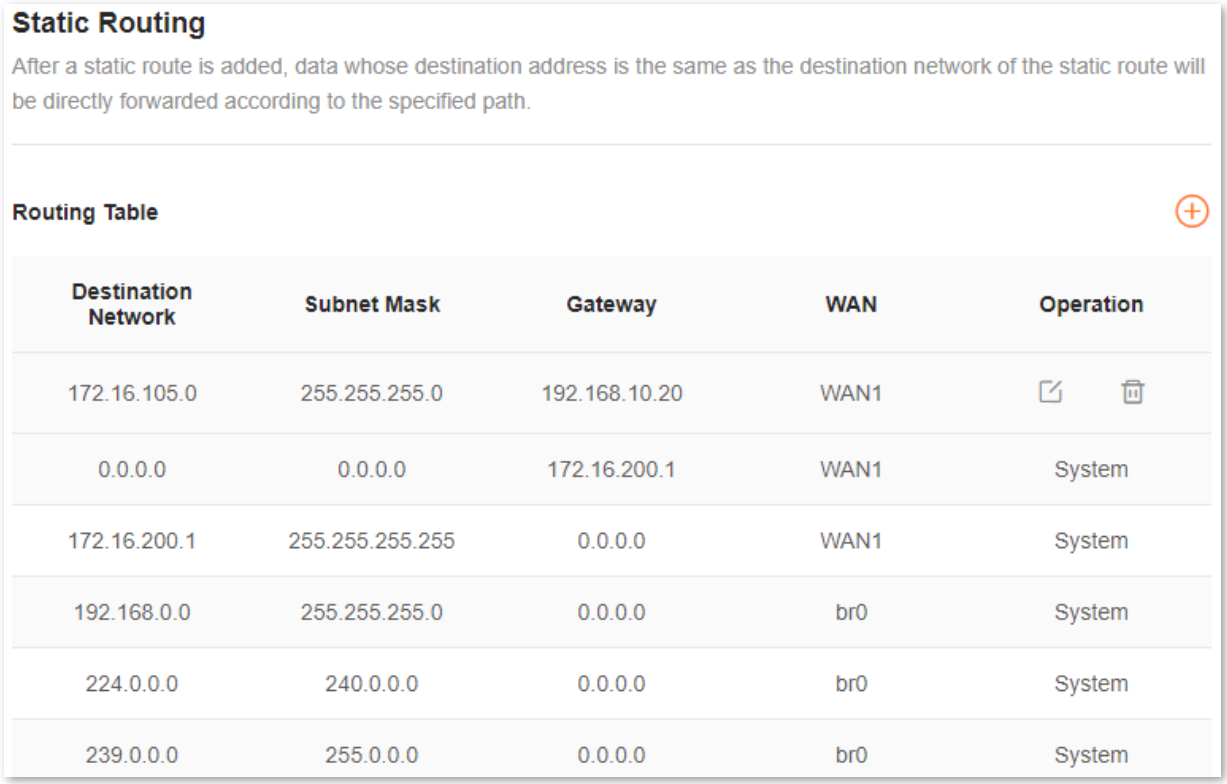
Static routing

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 Mesh device, and choose **More** > **Advanced** > **Static Routing**.



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 Mesh device 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 Mesh device. **0.0.0.0** indicates that the destination network is directly connected to the Mesh device.
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 Mesh device 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.

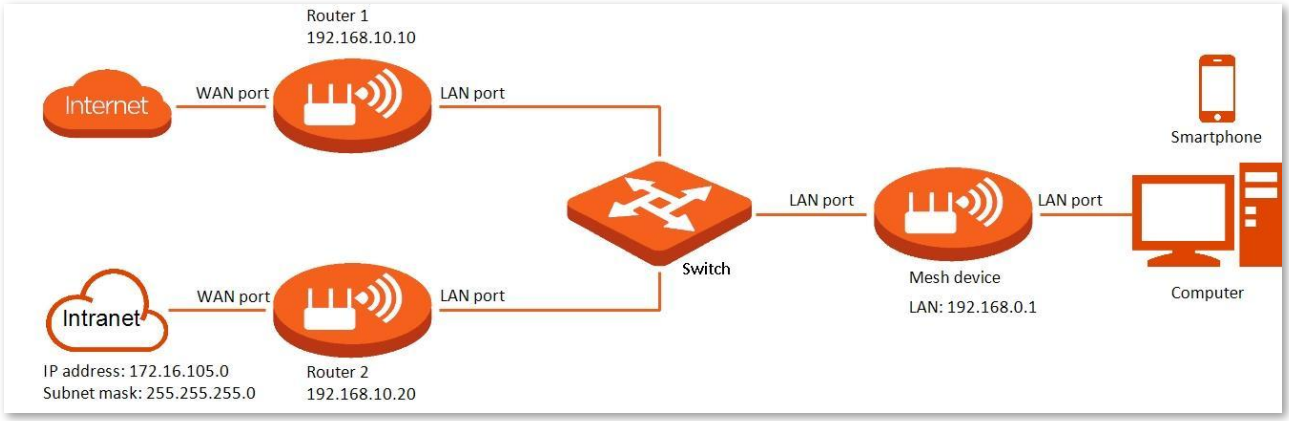
Solution: You can configure the static routing function to reach the goal.

Assume the LAN IP addresses of these devices are:

- Mesh device: 192.168.0.1
- Router1: 192.168.10.10
- Router2: 192.168.10.20

Information about the intranet:

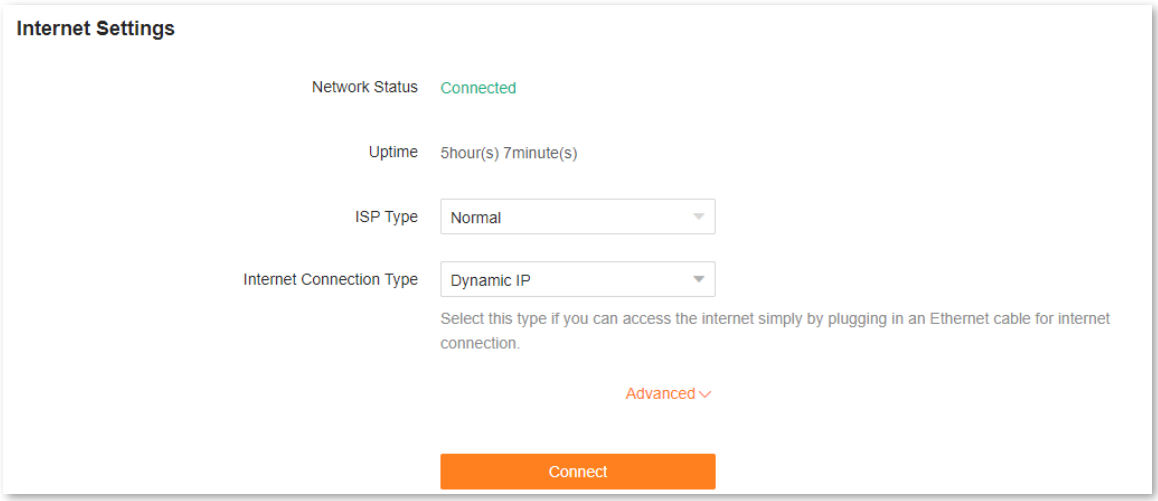
- IP address: 172.16.105.0
- Subnet mask: 255.255.255.0



Configuration procedure:

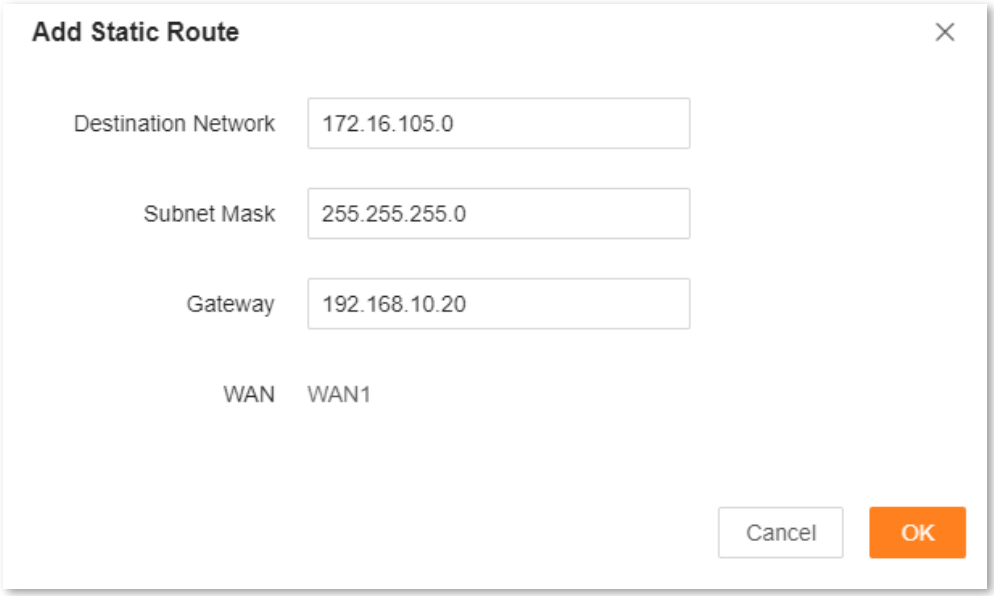
Step 1 Log in to the web UI.

Step 2 Refer to Access the internet through a dynamic IP address to configure the internet access for MX12.

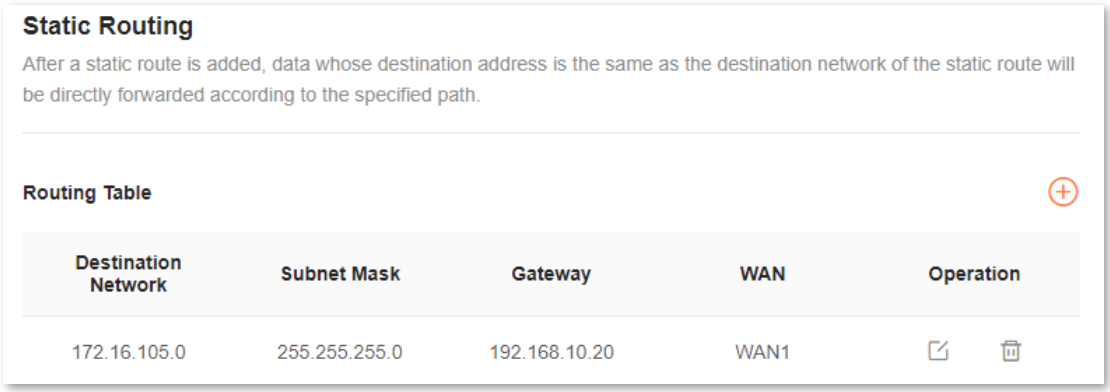


Step 3 Add a static routing rule on MX12.

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

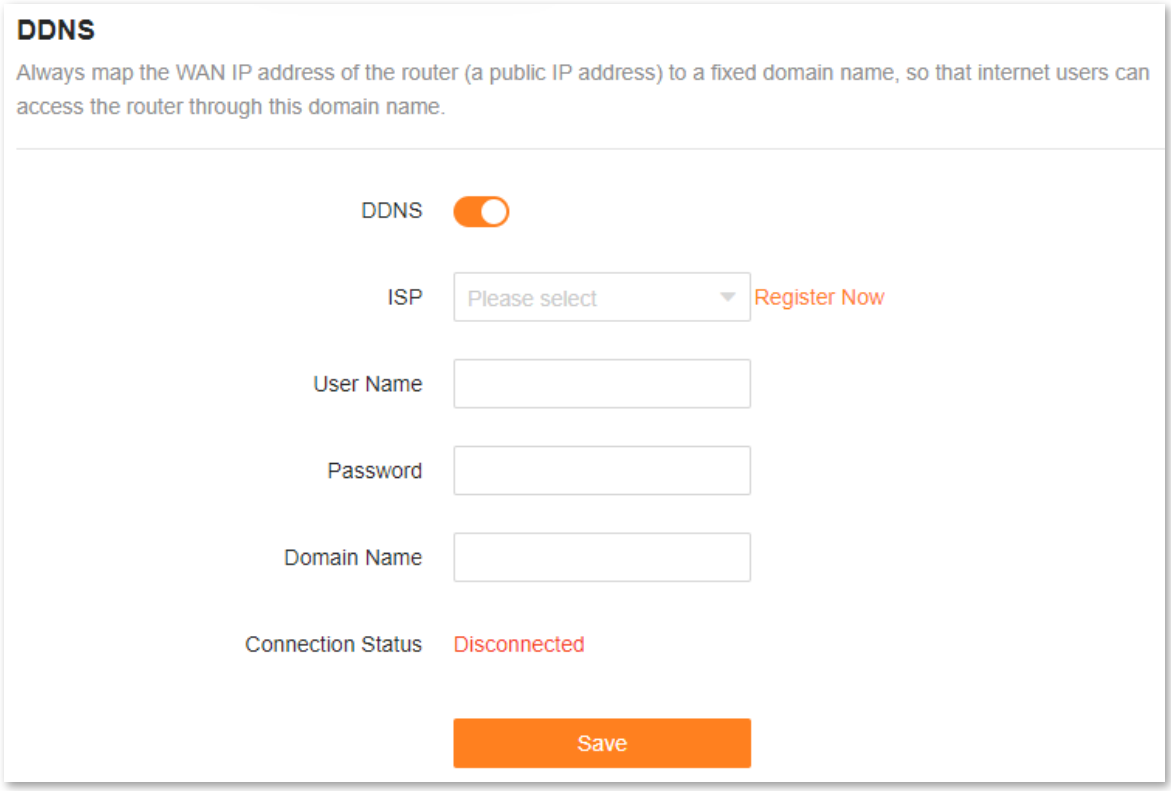
After completing the configuration, you can access both the internet and intranet through MX12 at the same time.

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 Mesh device's web UI with a fixed domain name.

To access the configuration page, log in to the web UI of the Mesh device, 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:

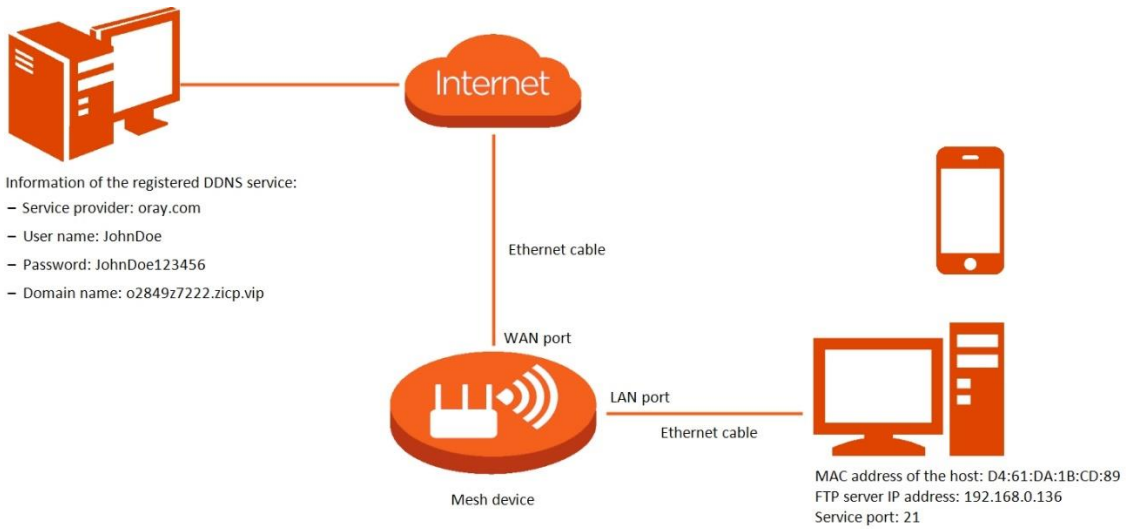
- IP address: **192.168.0.136**
- MAC address of the host: **D4:61:DA:1B:CD:89**
- Service port: **21**

Information of the registered DDNS service:

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

TIP

Ensure that the Mesh device 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.



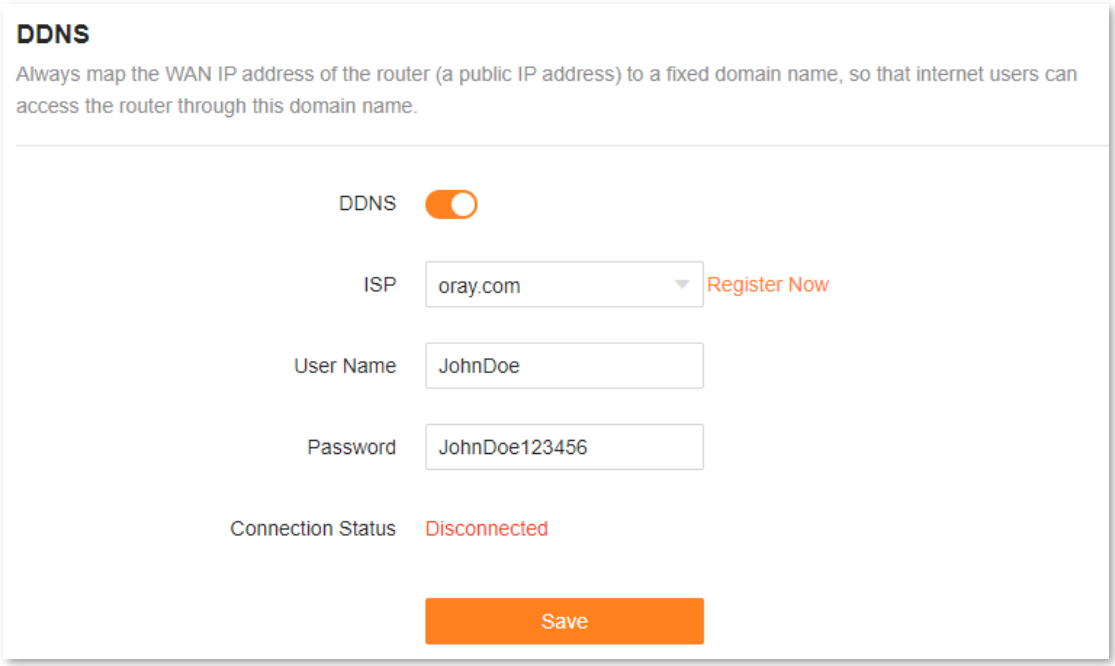
Configuration procedure:

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**.

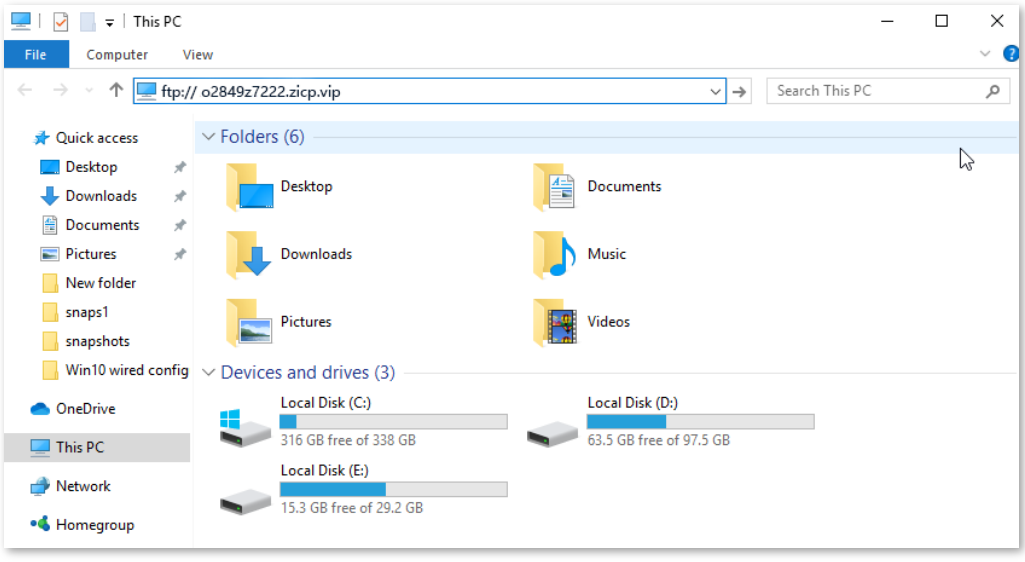


Wait until **Connected** is displayed after **Connection Status**, which indicates that the configuration is successful.

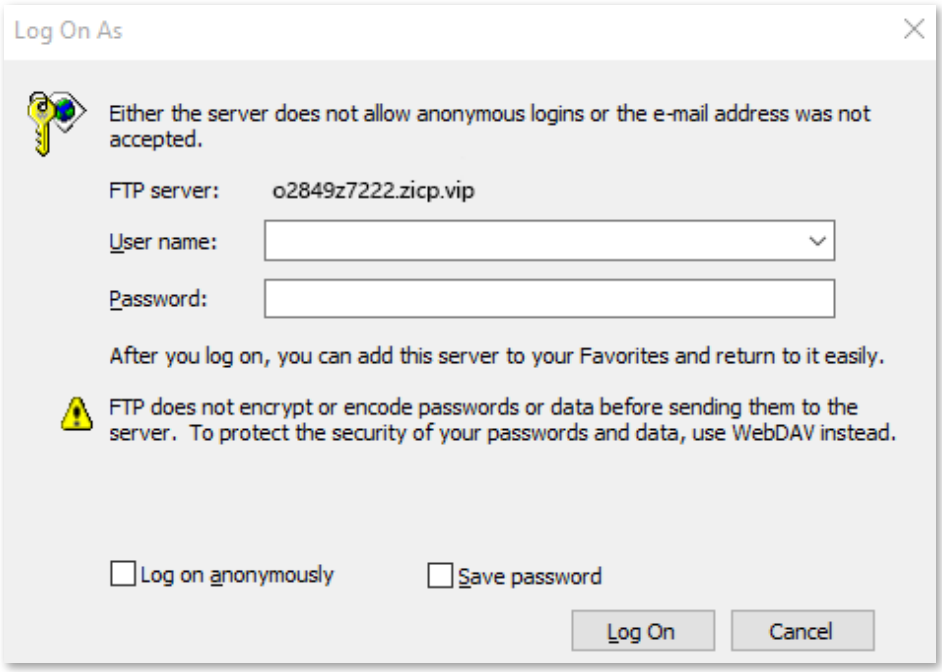
Step 3 Configure the port mapping function by following the steps in Port mapping.

---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.

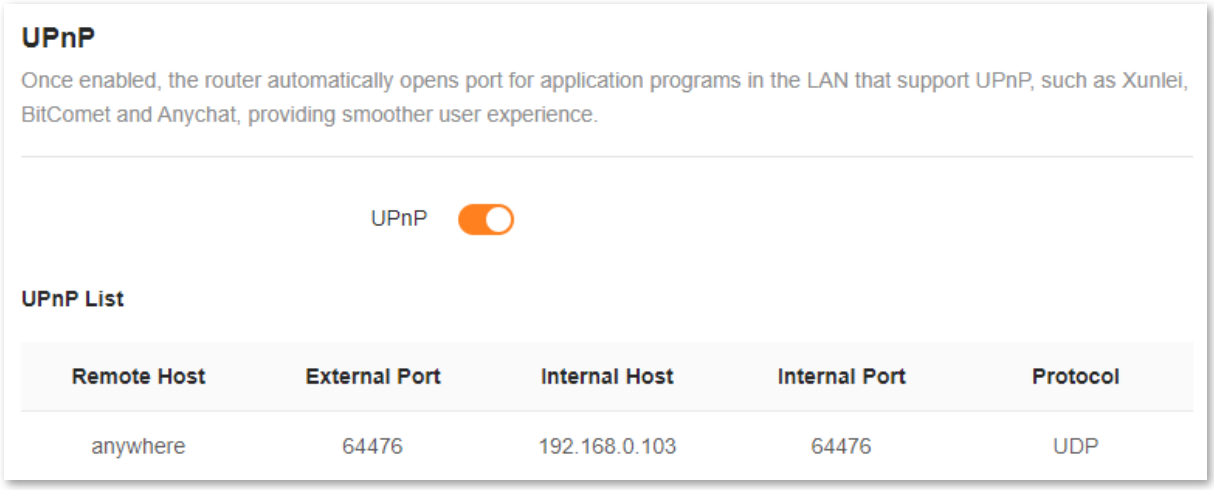
UPnP

UPnP is short for Universal Plug and Play. This function enables the Mesh device 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 Mesh device, 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.

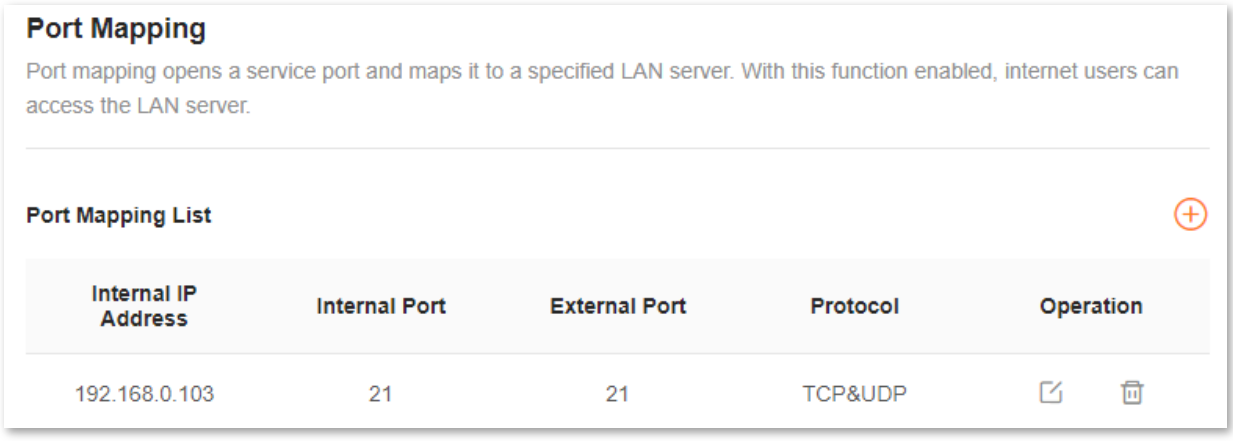
Parameter description

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 Mesh device 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.

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 Mesh device, 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.

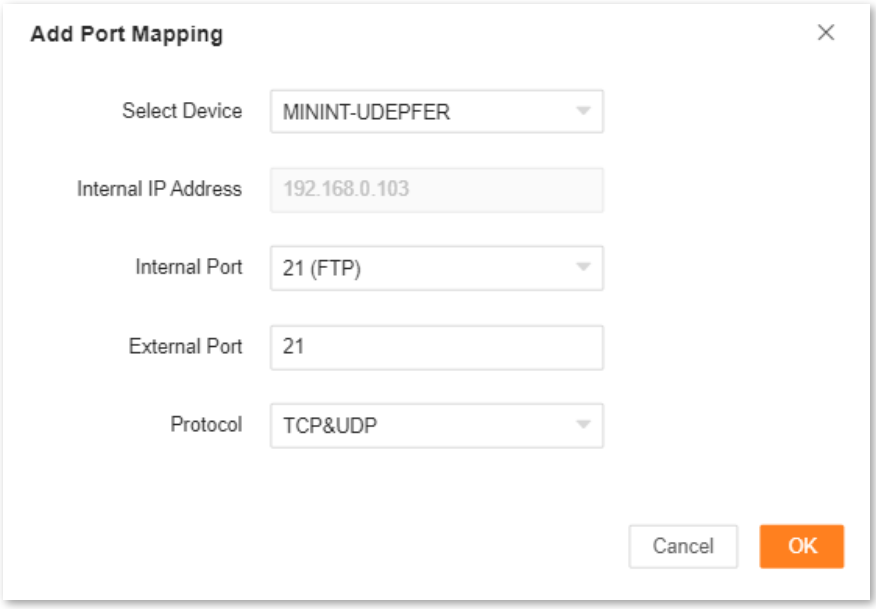
Step 2 Choose **More** > **Advanced** > **Port Mapping**.

Step 3 Click  .

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

- 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.

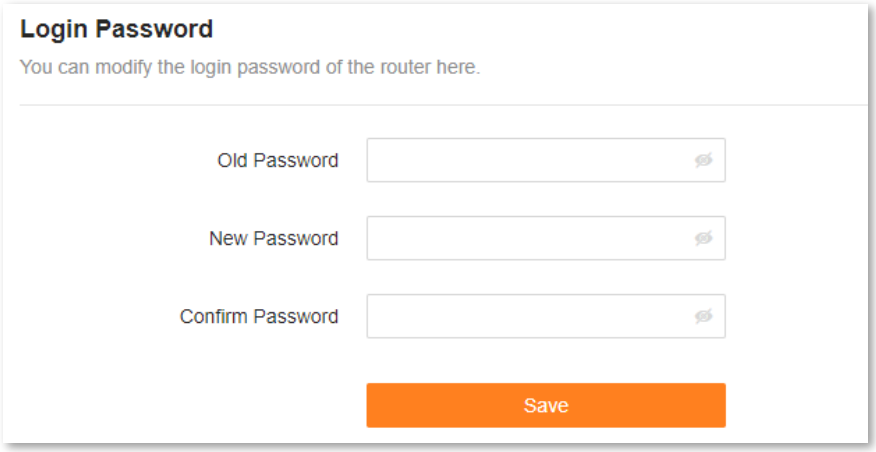
2.8.9 System settings

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	

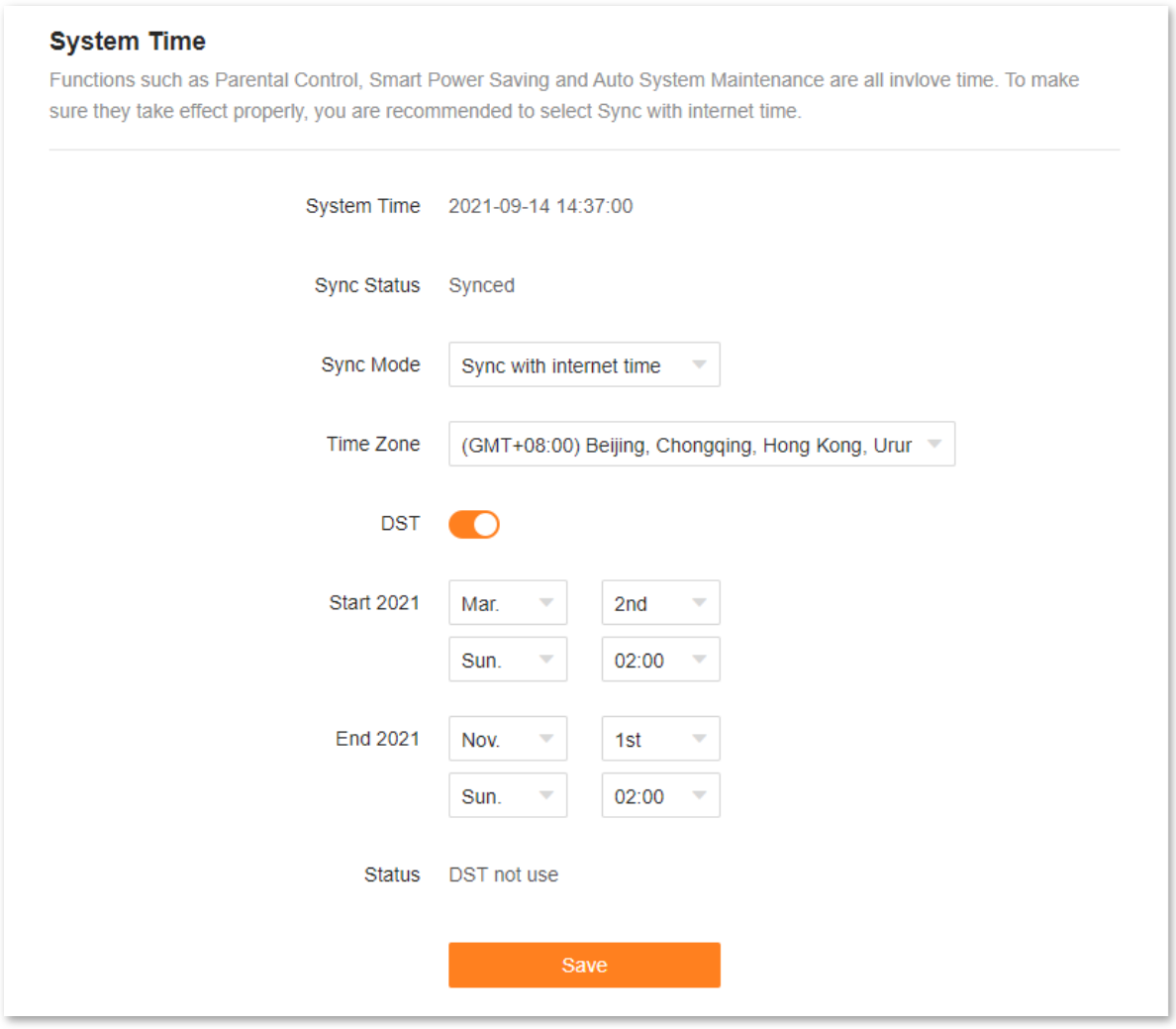
TIP

If you forgot your password, see Forgot my password.

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 Mesh device 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 Mesh device, and choose **More** > **System Settings** > **System Time.**



The following table describes the parameters displayed on this page.

Parameter description

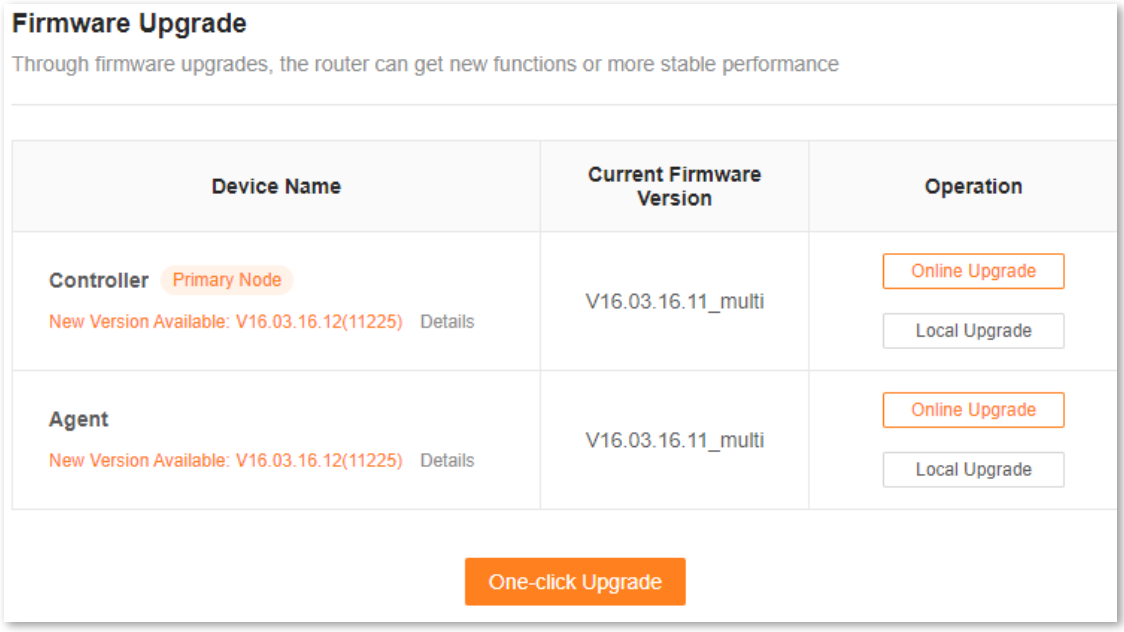
Parameter	Description
System Time	Specifies the current system time.
Sync Status	Specifies whether the system is synced.
Sync Mode	Specifies the sync mode of the system time. • **Sync with internet time**: Indicates that the system time is synced with the internet time. **Time Zone** must be set when 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.
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.

Firmware upgrade

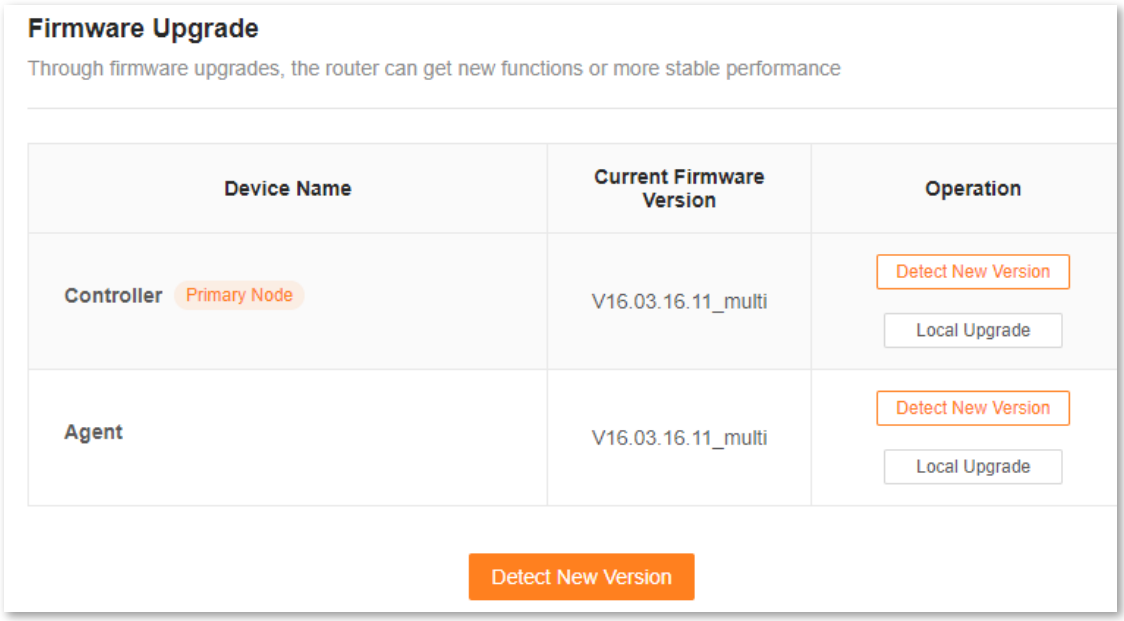
With this function, you can upgrade the firmware of the Mesh device to obtain the latest functions and more stable performance. The Mesh device supports one-click upgrade, online upgrade and local upgrade.

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

When the Mesh device 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

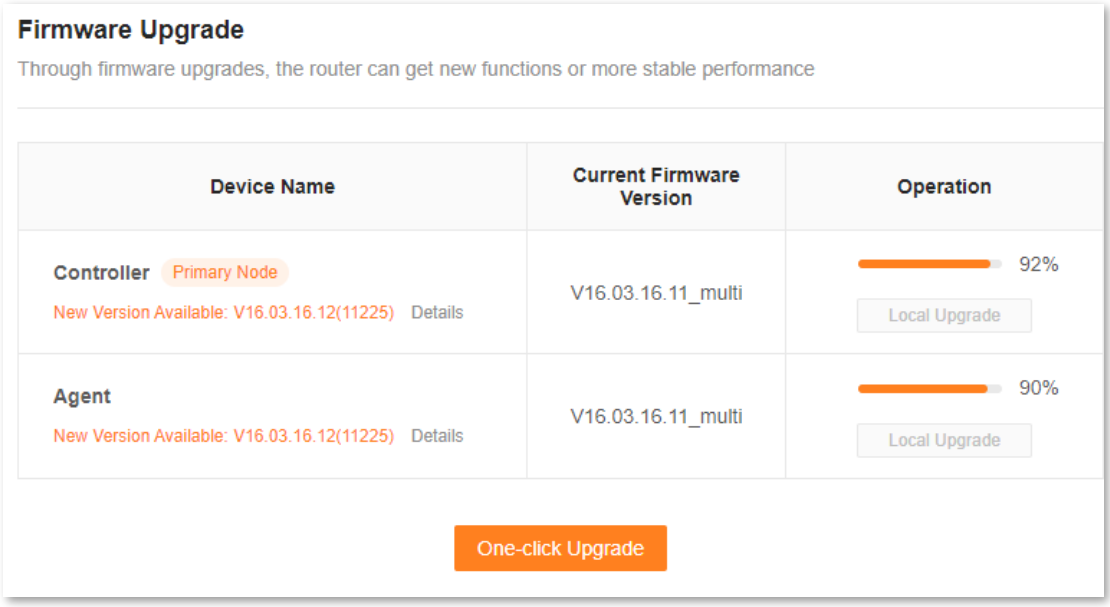
To perform one-click upgrade on all nodes:

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 Mesh device, you are recommended to reset the Mesh device to factory settings and re-configure the Mesh device after the upgrade completes.

Local upgrade

NOTE

To prevent the Mesh device from being damaged:

- Ensure that the firmware is applicable to the Mesh device.
- 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 Mesh device.

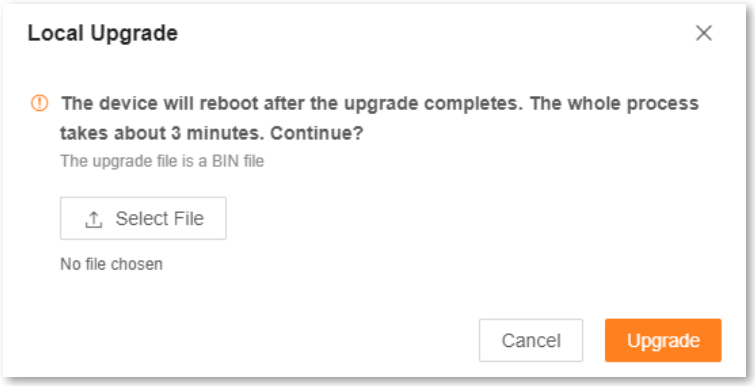
Step 1 Go to www.tendacn.com. Download applicable firmware of the Mesh device to your local computer and unzip it.

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 Mesh device to factory settings and re-configure the Mesh device after the upgrade completes.

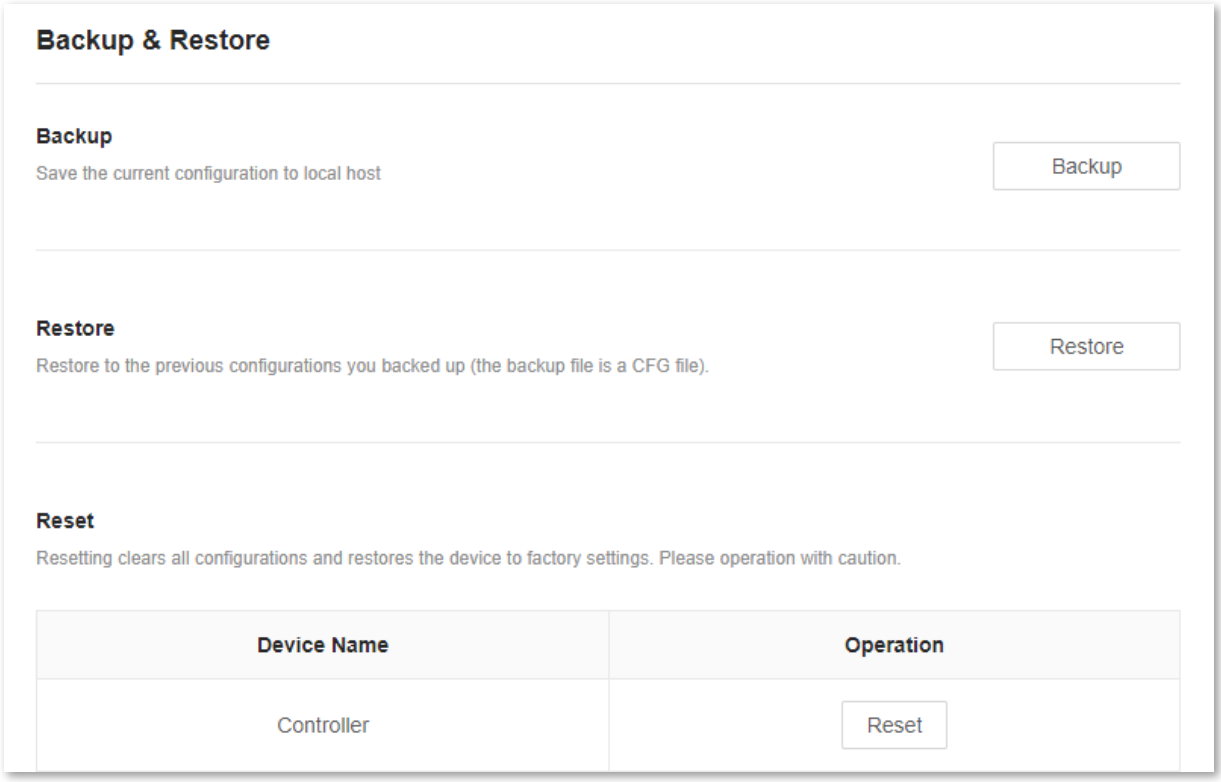
Backup & restore

In this module, you can back up the current configuration of the Mesh device to your computer. You are recommended to back up the configuration after the settings of the Mesh device are significantly changed, or the Mesh device 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 Mesh device to factory settings on this page.

After you restore the Mesh device 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 Mesh device, and choose **More** > **System Settings** > **Backup & Restore.**



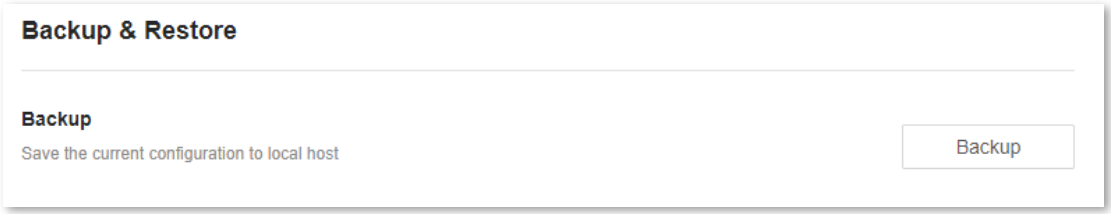
Back up the configuration of the Mesh device

To back up the configuration of the Mesh device:

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

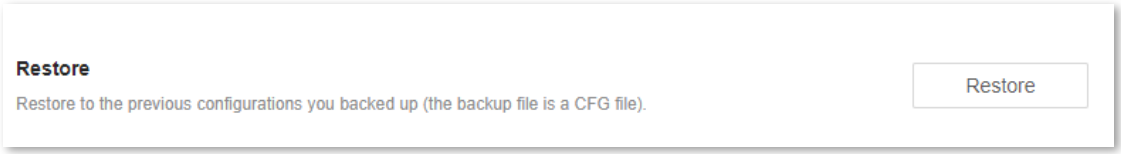
Restore the previous configuration of the Mesh device

To restore the previous configuration of the Mesh device:

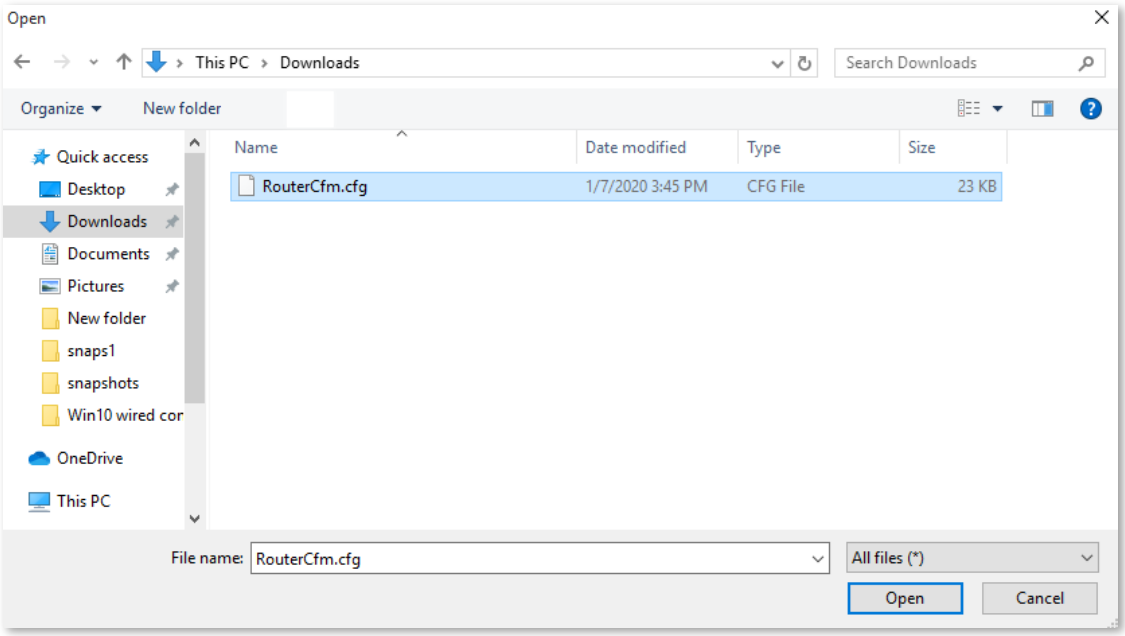
Step 1 Log in to the web UI.

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 Mesh device.

---End

Reset a node

NOTE

- Resetting clears all configurations and restores the Mesh device to factory settings. Please operate with caution.
- Resetting the primary node clears all customized configurations on the primary node. You can configure the network again after resetting. If the Mesh devices in the same kit are in the networking range, automatic networking will be performed after you configure the node as the primary node again.
- Resetting a secondary node clears all customized configurations on the secondary node. If the secondary node is in the networking range of the primary node in the same kit, automatic networking with the primary node will be performed after you reset the secondary node.

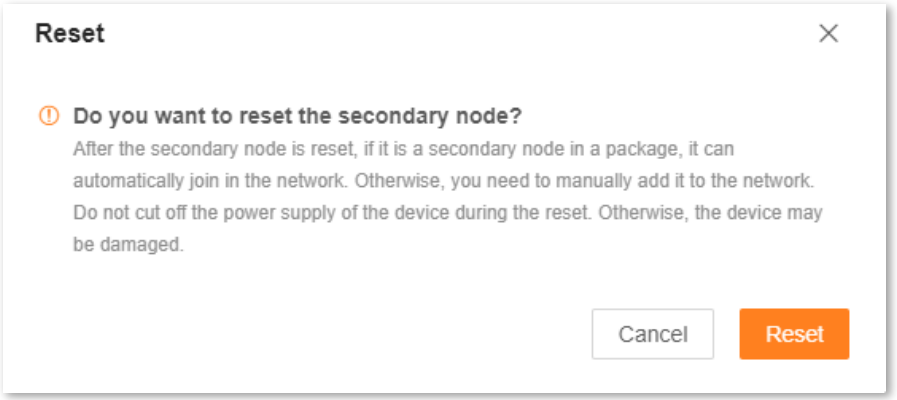
To reset a node:

Step 1 Log in to the web UI.

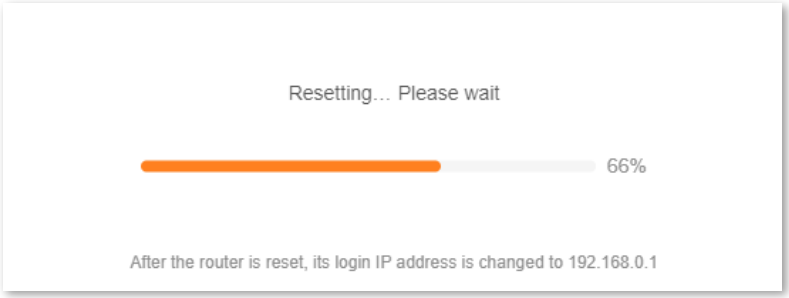
Step 2 Choose **More** > **System Settings** > **Backup & Restore.**

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.

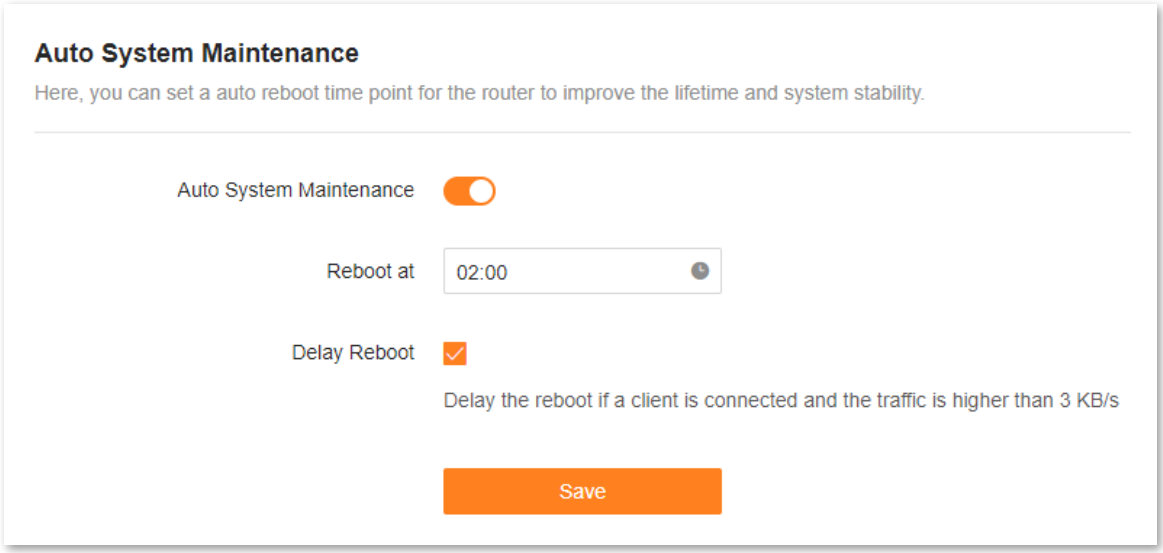


---End

Auto system maintenance

Auto system maintenance enables you to restart the Mesh device regularly. It helps improve the stability and service life of the Mesh device.

To access the configuration page, log in to the web UI of the Mesh device, and choose **More** > **System Settings** > **Auto System Maintenance.**



The following table describes the parameters displayed on this page.

Parameter description

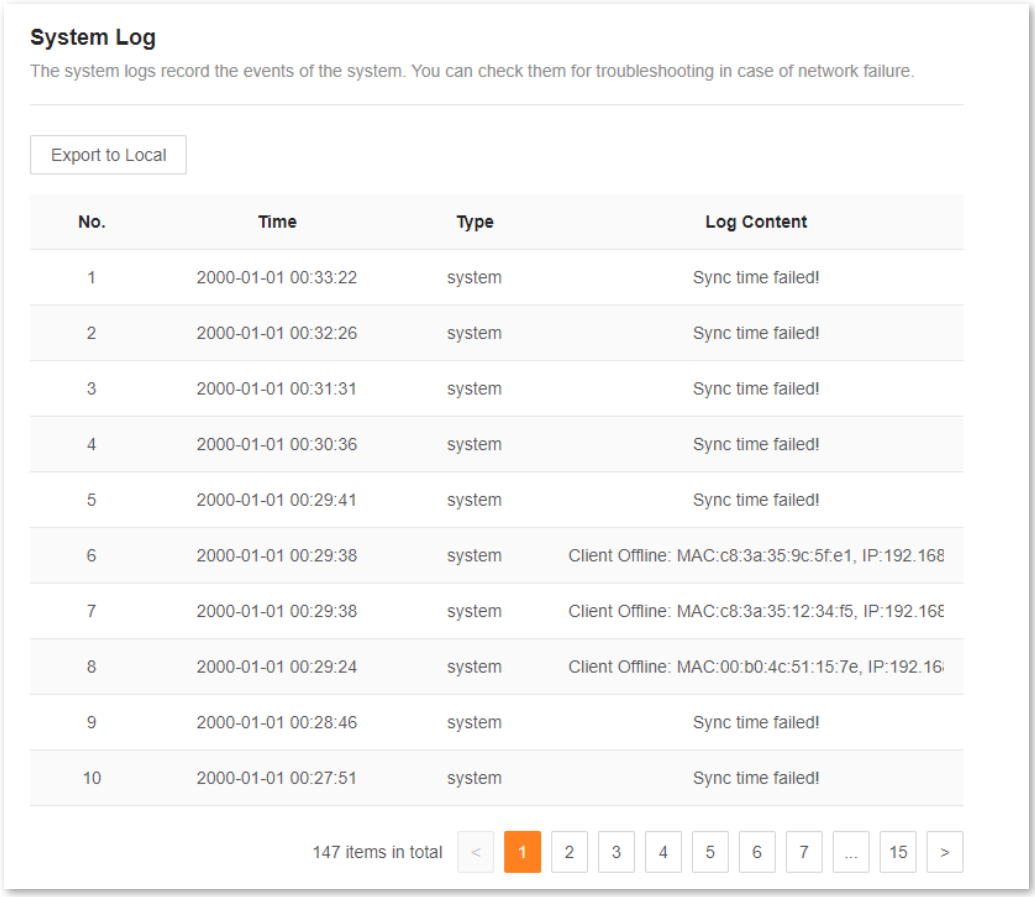
Parameter	Description
Auto System Maintenance	Used to enable or disable the auto system maintenance function.
Reboot At	Specifies the time when the Mesh device reboots automatically every day.
Delay Reboot	Used to enable or disable the reboot delay function. • Ticked: The function is enabled. When the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

System log

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

This function logs all key events that occur after the Mesh device 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 Mesh device will clear all previous system logs.

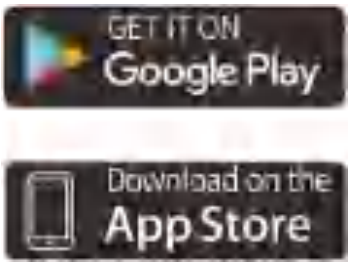
3 APP operations

This chapter introduces the functions and operations available on the Tenda WiFi app, including:
Registration and binding
Quick setup
Management type
My WiFi
My profile
Common Settings
System Settings

To download and install the Tenda WiFi app, see APP download and installation.
More functions and operations are available on the web UI. For details, see Web UI operations.

3.1 APP download and installation

Download the Tenda Wifi App onto your mobile device by searching for **Tenda WiFi** in **Google Play** or **App Store** or by scanning the **QR** code. Then install the **Tenda WiFi** App.



Or

Tenda WiFi

3.2 Registration and binding

3.2.1 Register a Tenda account

You can register a Tenda account and log in with it to manage the Mesh devices.

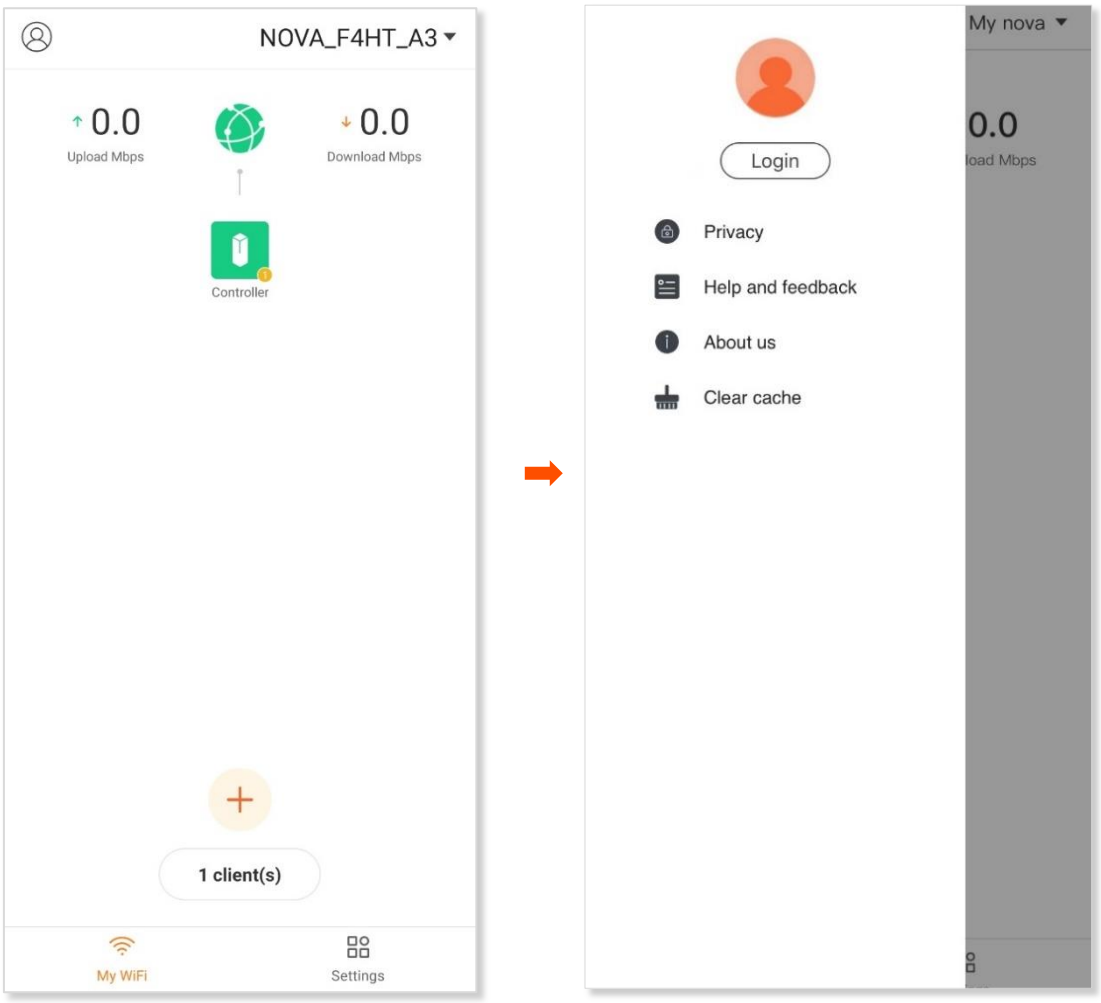
TIP

To log in to the Tenda Wifi App using a third-party account without registering a Tenda account, see Log in to Tenda WiFi App.

Procedure:

Step 1 Run the Tenda WiFi App, and tap in the upper-left corner.

Step 2 Tap **Login**.



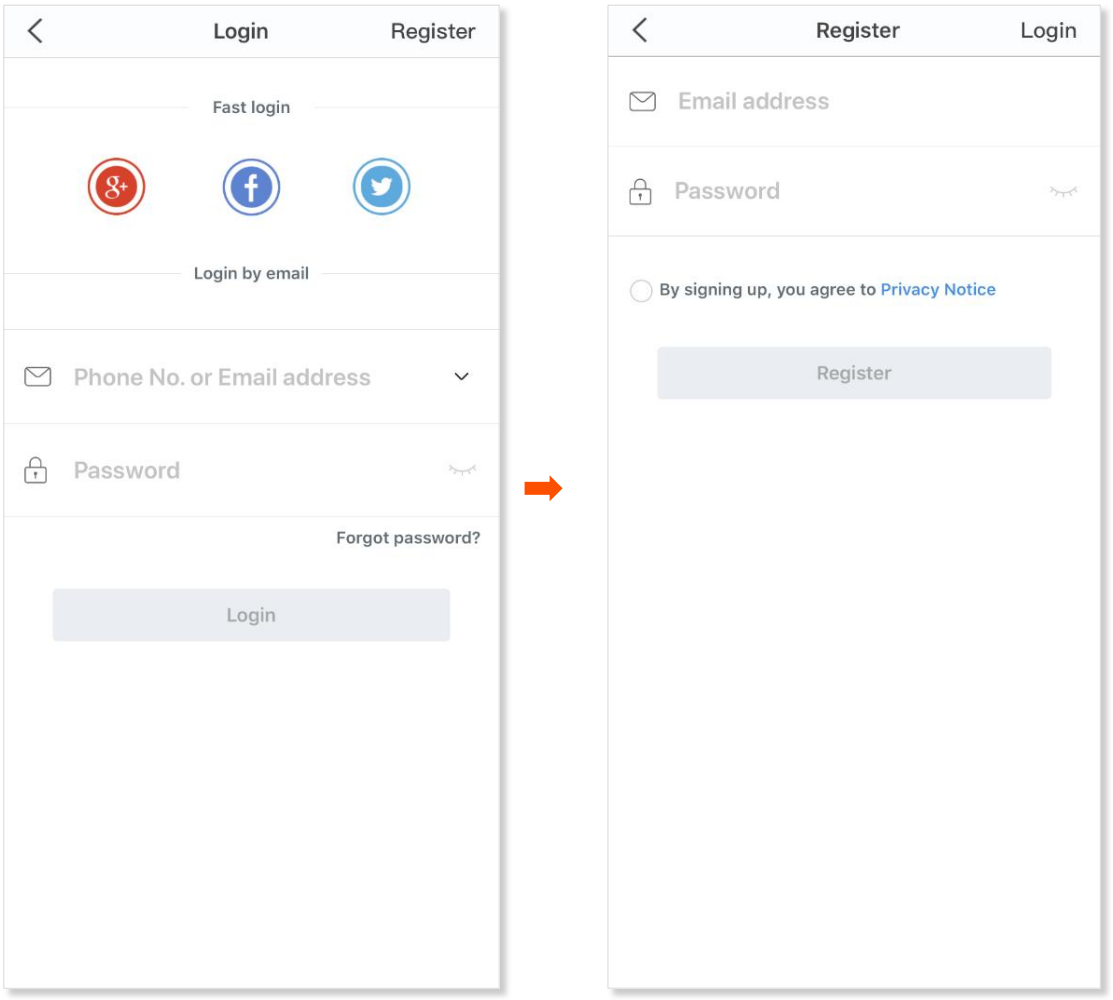
Step 3 Tap **Register** in the upper right corner.

Step 4 Enter an email address.

Step 5 Customize a password for your Tenda account.

Step 6 Tick **By signing up, you agree to Privacy Notice**.

Step 7 Tap **Register**.

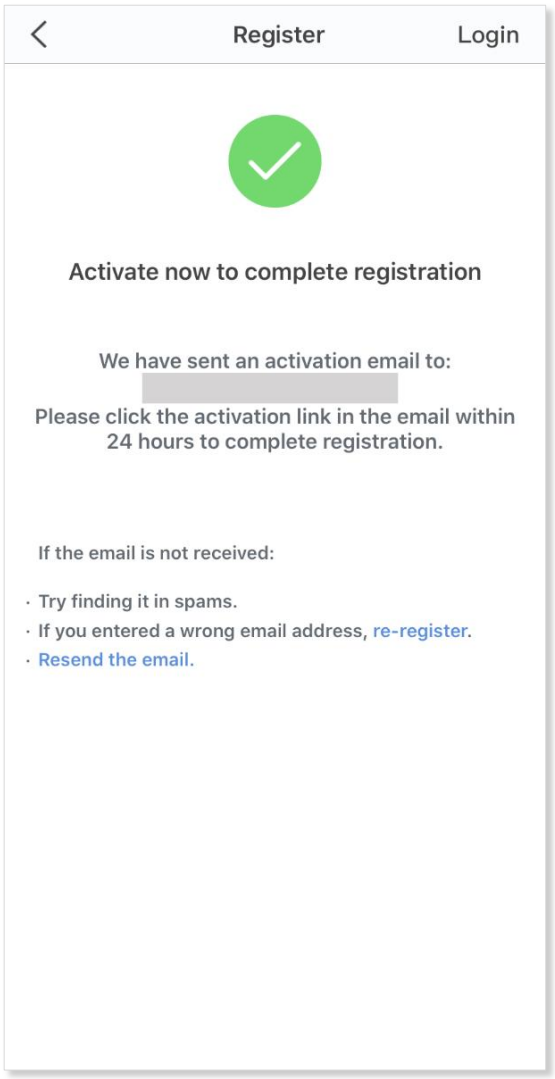


Step 8 An activation email is sent to the email account you entered. Check the email and activate the account as instructed in the email.

---End

Registration completes.

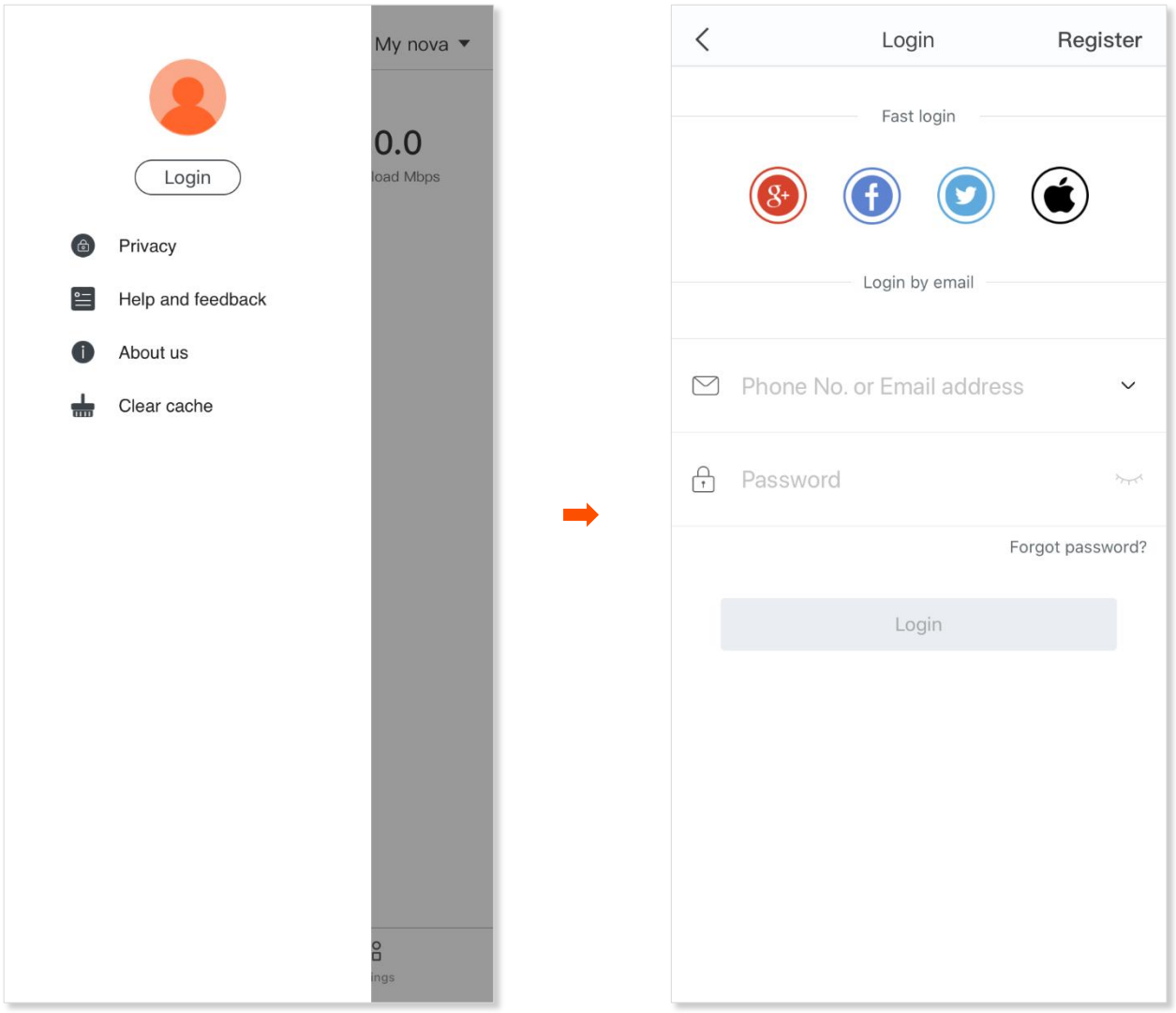
You can tap **Login** in the upper right corner to log in with the registered account.



3.2.2 Log in to Tenda WiFi App

After you completed installation and setup using the Tenda WiFi App, a login prompt page appears. You can authorize the Tenda WiFi App to use a third party account, including **Google+**, **Facebook**, and **Twitter**, or a registered account to log in.

You can also tap in the upper-left corner and tap **Login**. Then choose a login method as required.



3.2.3 Bind the administrator account

When an account is bound to the Mesh device, it becomes the administrator account of the Mesh device.

Procedure:

Step 1 Connect your smartphone to the Wi-Fi network of your Mesh device, and run the Tenda WiFi App.

Step 2 Log in to the Tenda WiFi App, and your account is bound with the Mesh device.

---End

TIP

If the Mesh device is already bound with an account, it cannot be bound again with another account.

3.3 Quick setup

3.3.1 Connect your primary node to the internet

Before you start, download the **Tenda WiFi** App on your mobile device (smartphone or tablet). A smartphone is used for illustration here.

Procedure:

Step 1 Connect your primary node.

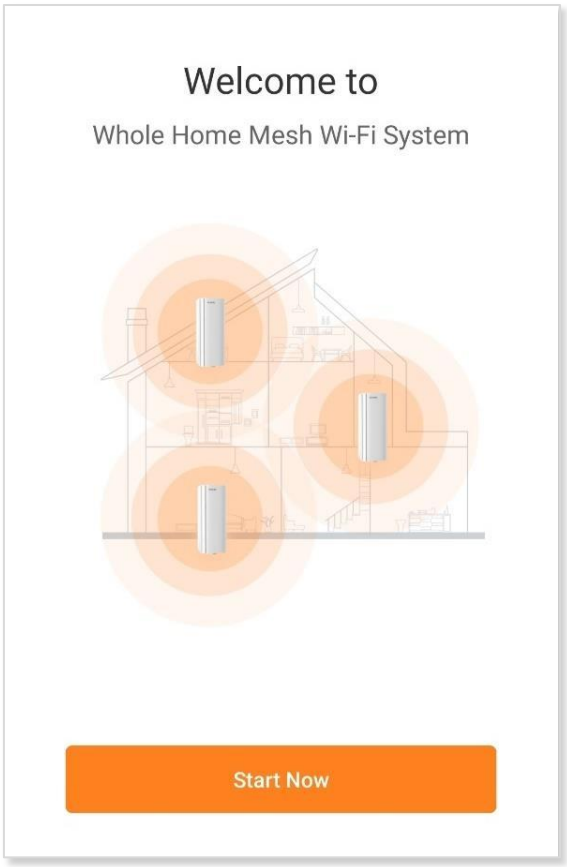
Step 2 Connect your smartphone to the Wi-Fi network of the primary node.

TIP

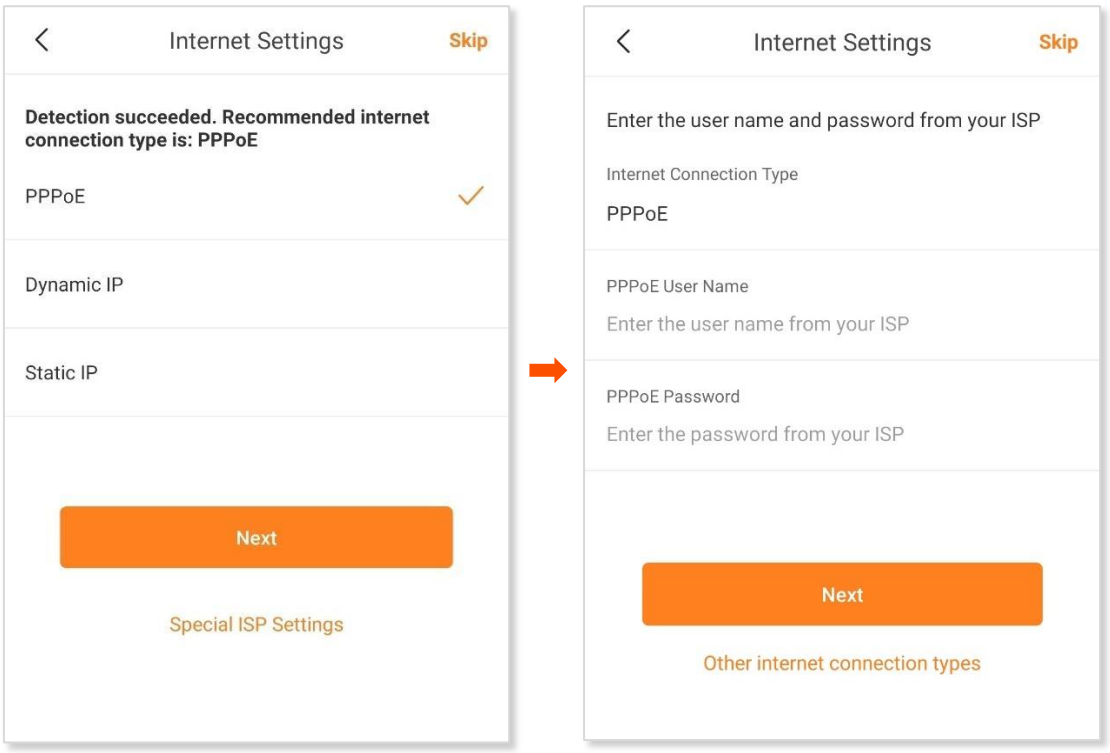
The default Wi-Fi name and password can be found on the bottom label of the device.

Step 3 Run the Tenda WiFi App.

Step 4 Tap **Start Now**.



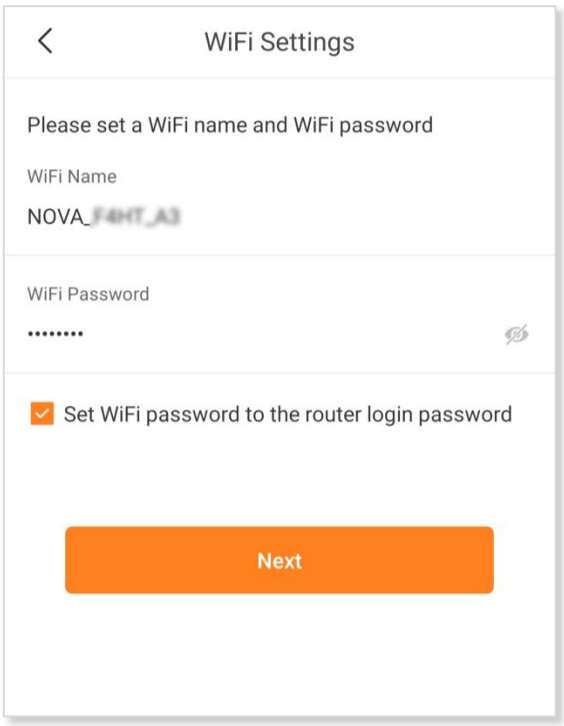
Step 5 Set required parameters (PPPoE is used for illustration here) and tap **Next**.



TIP

Tenda WiFi App will detect the connection type of WAN port of the Mesh device. If the WAN port is not connected properly, follow the instructions on the App to complete the connection.

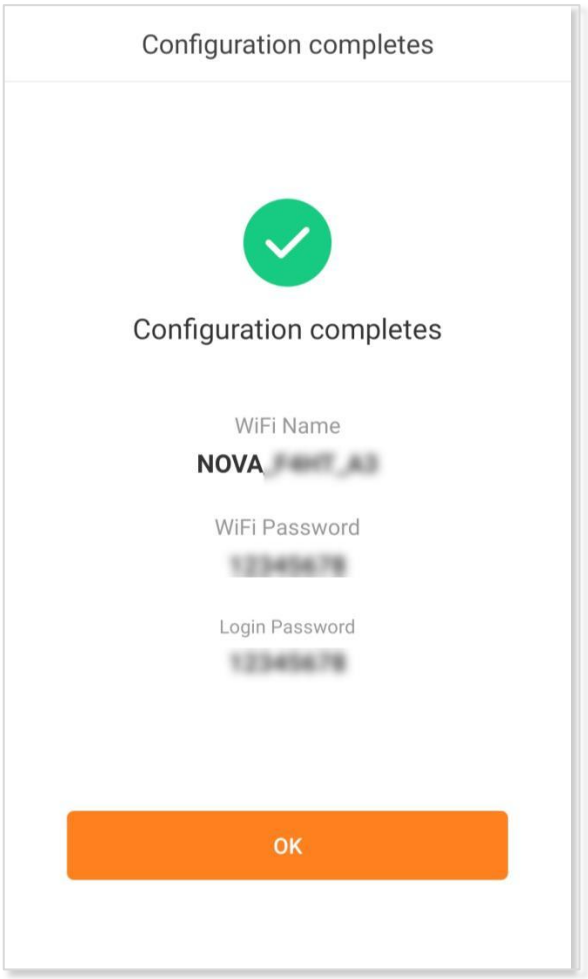
Step 6 Customize the **WiFi Name** and **WiFi Password**.



TIP

- 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** for web UI login.

Step 7 Tap **OK**.



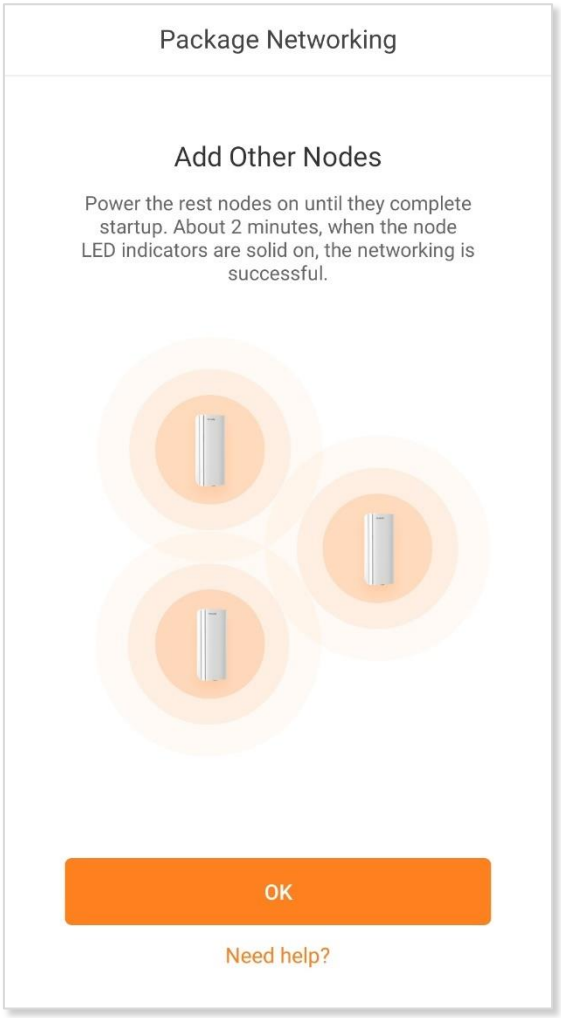
---End

After the quick setup, if you use the default Wi-Fi password, Android phones will connect to the Wi-Fi network you set automatically, whereas iOS phones need to be connected to the Wi-Fi network manually.

If you want to add any new node, go back to the App and add new nodes according to the onscreen instructions.

3.3.2 Extend your network

Upon your first login, the following information is displayed to tell you how to extend the network with secondary nodes in the same kit. To extend the network with other nodes, see Add a node.



For detailed steps, see Extend your network in Web UI operations.

3.4 Management type

Mesh devices support local management and remote management with the Tenda WiFi App. You can choose either of the management types as needed.

3.4.1 Local management

TIP

If your nodes are bound to a Tenda account, you can manage them only after logging in to the App with the administrator account.

Local management indicates that you can use the Tenda WiFi App to manage your Mesh network after connecting your smartphone to the Wi-Fi network of the Mesh device.

Procedure:

Step 1 Connect your smartphone to the Wi-Fi network of your Mesh device.

Step 2 Run the Tenda WiFi App on the smartphone, and then you can use the App to manage your Mesh network.

---End

3.4.2 Remote management

Remote management indicates that you can use the Tenda WiFi App to manage your Mesh network anytime and anywhere without connecting to the WiFi network of the Mesh device.

Prerequisites:

- Your Mesh nodes are connected to the internet.
- You have logged in with the administrator account of the Mesh device.

Procedure:

Step 1 Run the Tenda WiFi App on the smartphone.

Step 2 Tap in the upper-left corner.

Step 3 Log in with the administrator account of the Mesh device.

---End

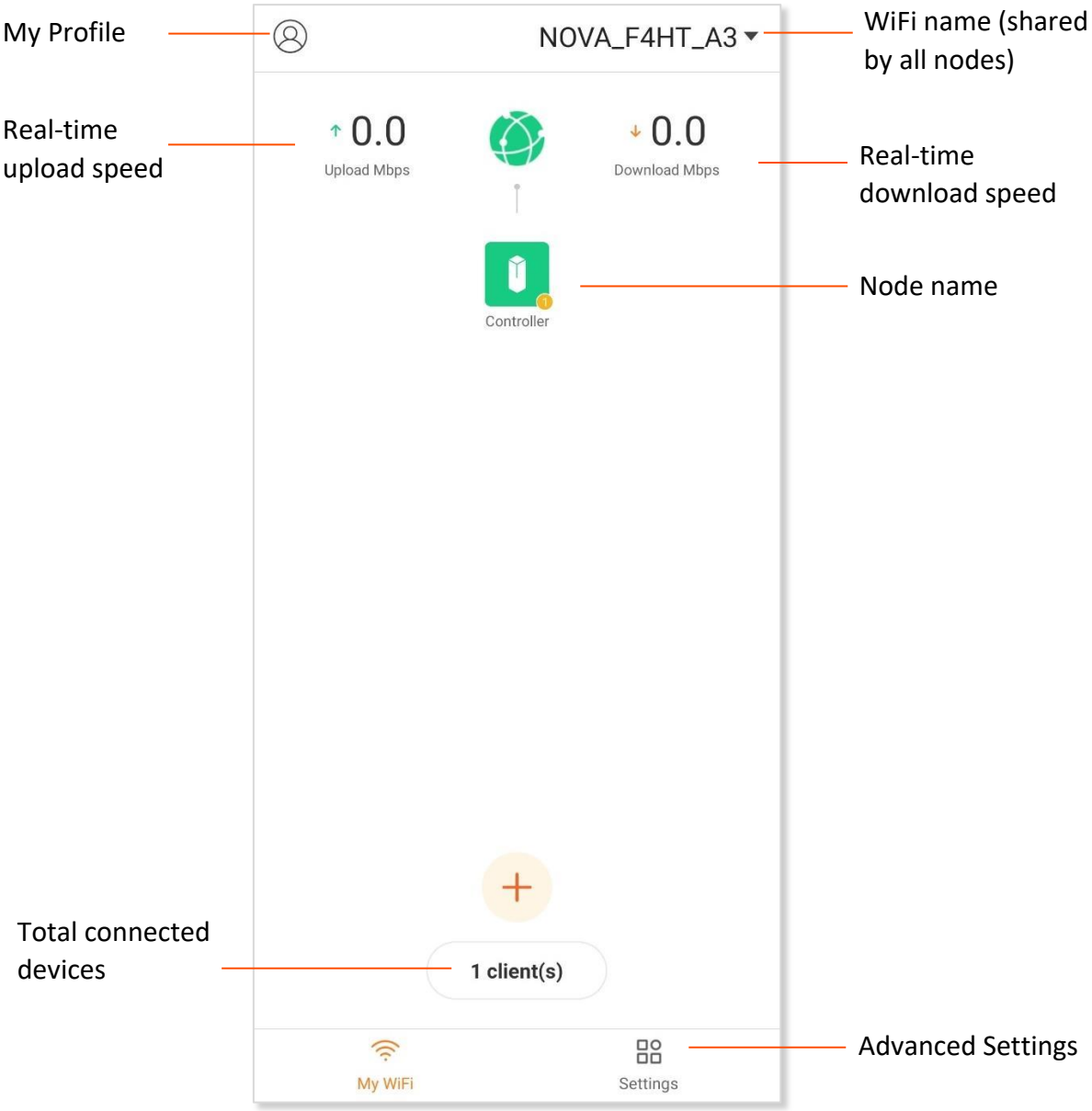
Now, you can manage your Mesh network remotely.

3.5 My WiFi

After completing the quick setup, the following page appears.

You can:

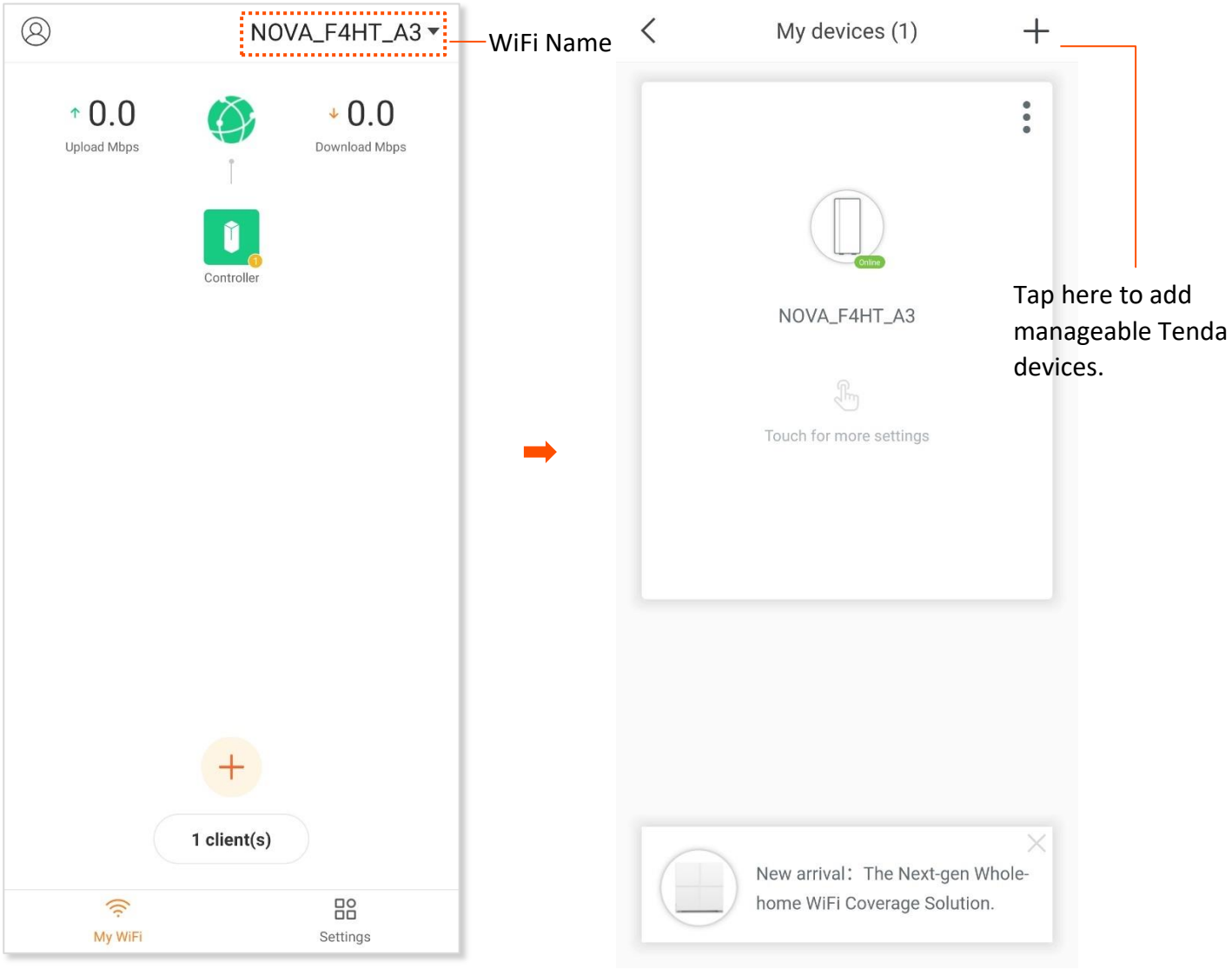
- View managed nodes
- View the internet status
- Add a node
- Manage nodes
- Manage connected clients



3.5.1 View managed nodes

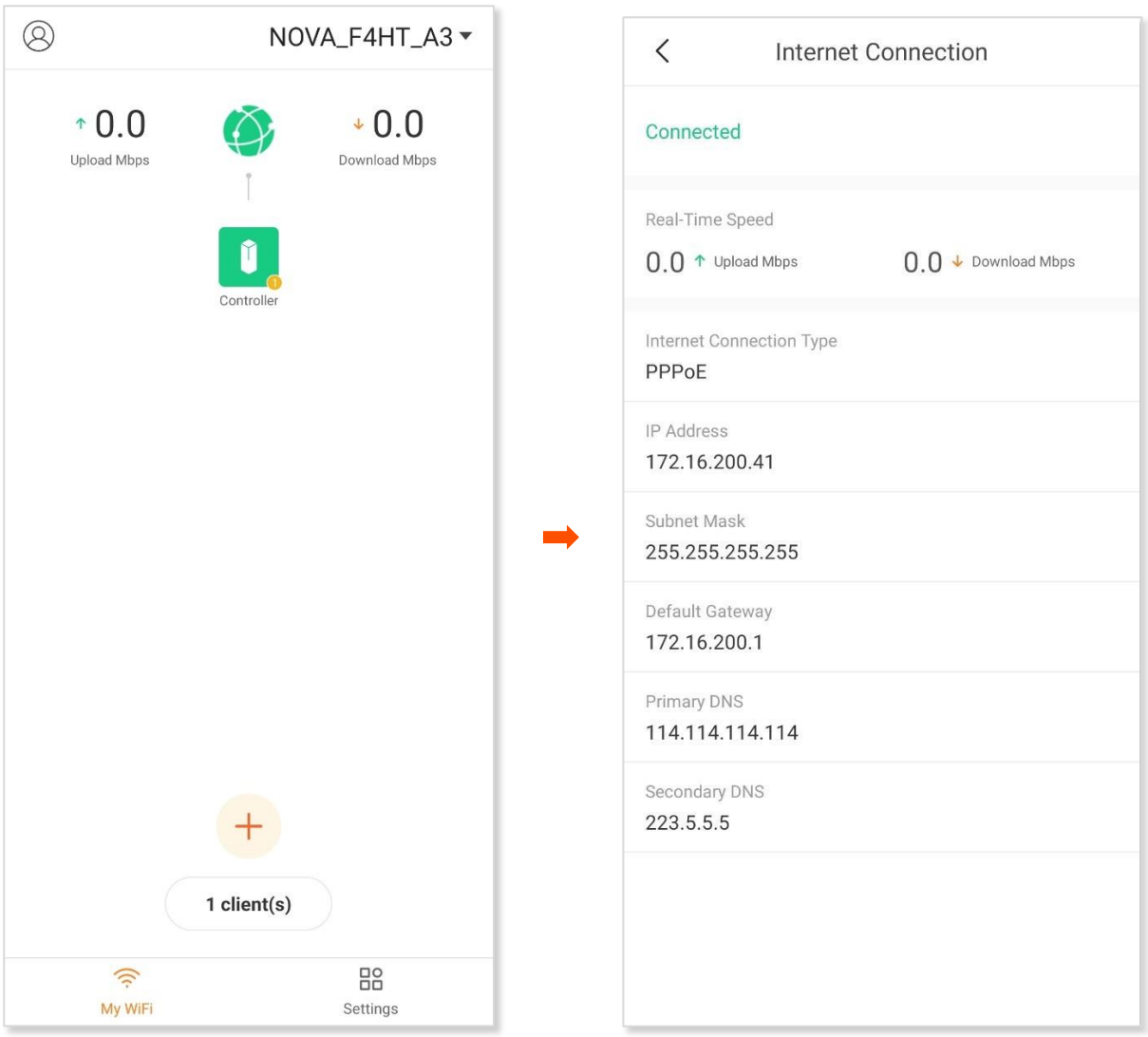
Tap the WiFi name in the upper-right corner of the **My WiFi** page to enter the following page.

All nodes in a network share the same WiFi name.



3.5.2 View internet status

Tap the icon on the **My WiFi** page. Information such as connection status and other basic internet connection parameters is displayed, as shown in the following figure.



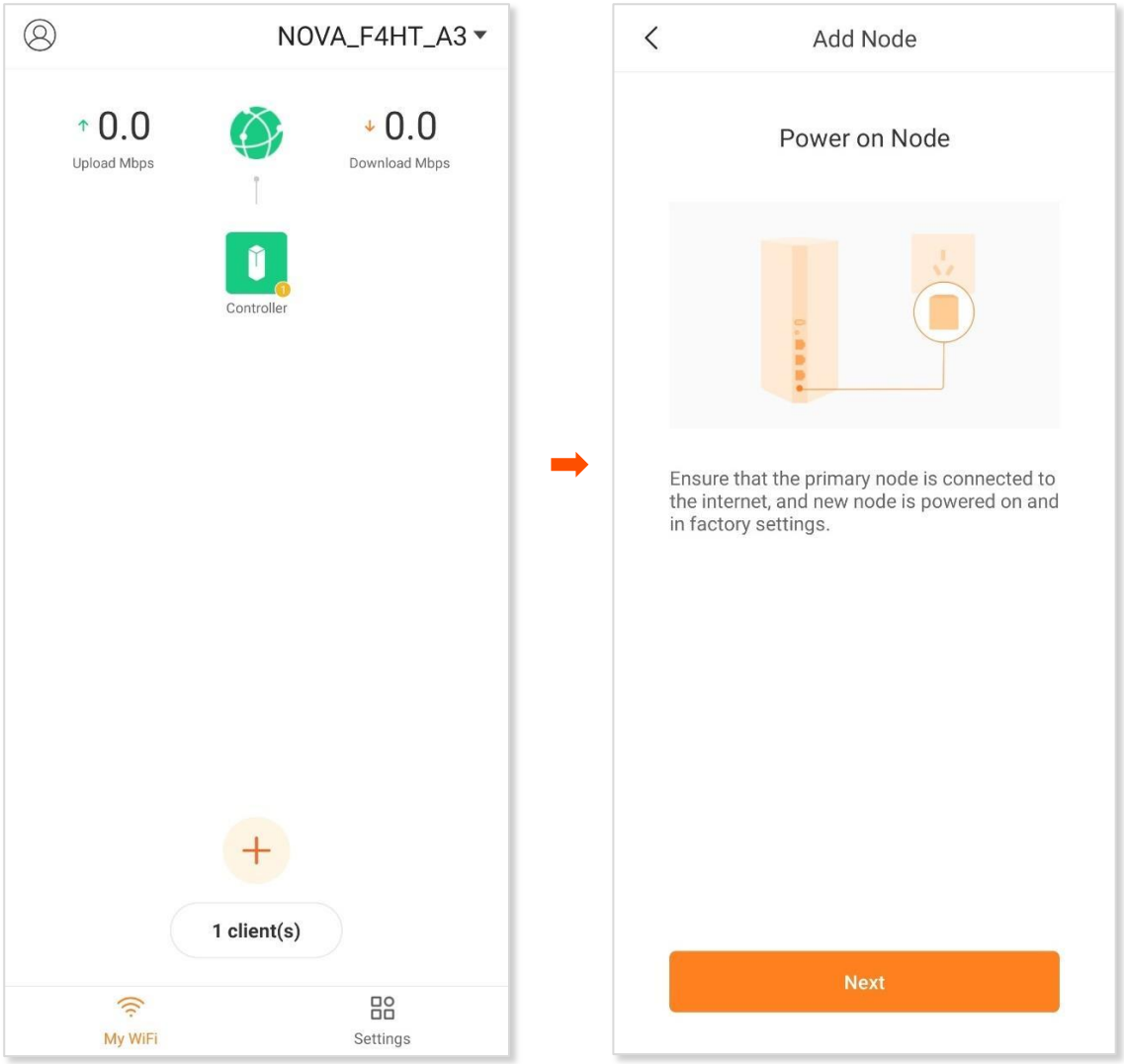
Parameter description

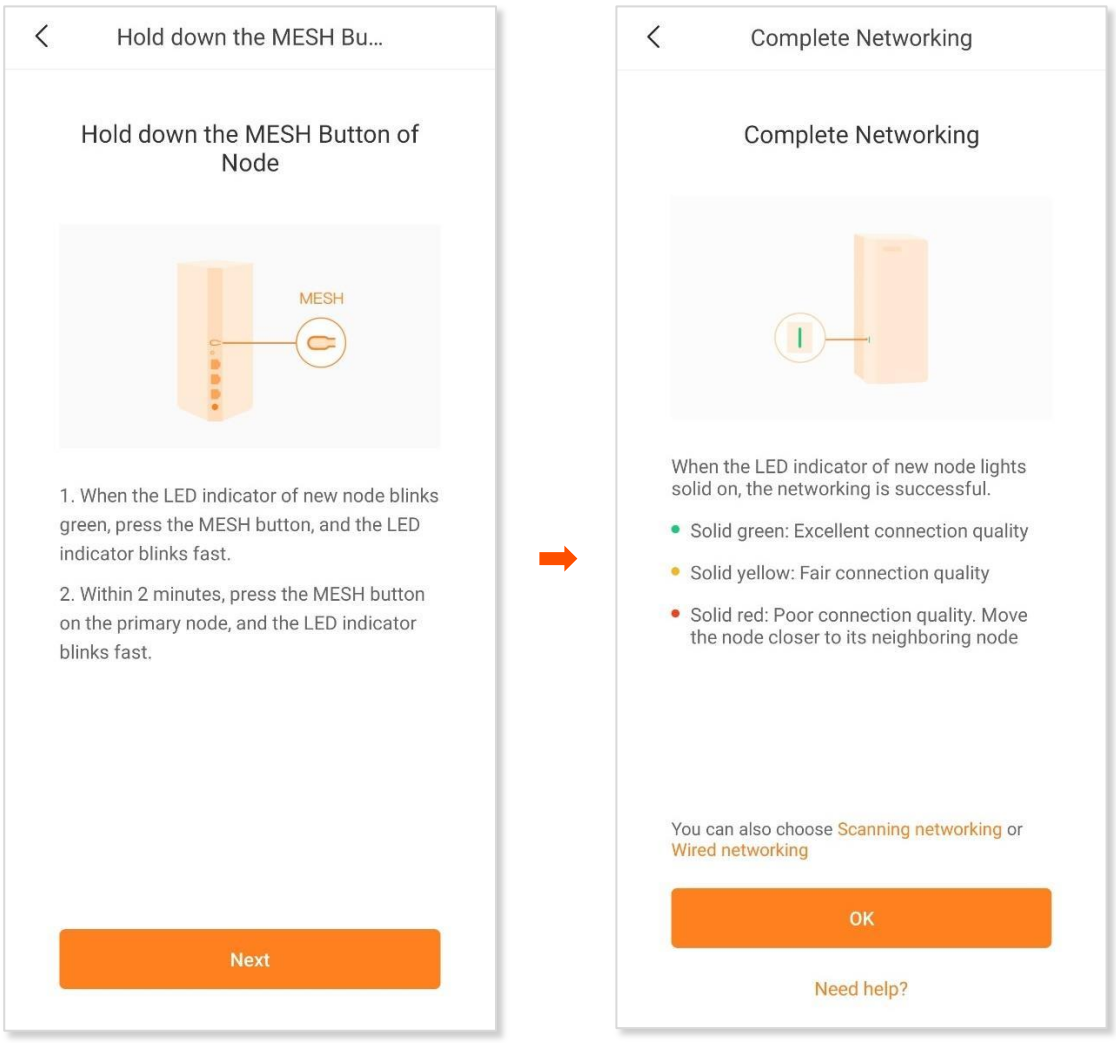
Parameter	Description
Connected/Disconnected	Specifies the internet connection status of the WAN port.
Real-Time Speed	Specifies the real-time upload and download speed in the unit of Mbps.
Internet Connection Type	Specifies the internet connection type of the WAN port. **PPPoE** is used as an example here.
IP Address	Specifies the WAN IP address of the primary node.
Subnet Mask	Specifies the WAN subnet mask of the primary node.

Parameter	Description
Default Gateway	Specifies the gateway IP address of the primary node.
Primary DNS	Specify the IP address of primary and secondary DNS servers of the primary node.
Secondary DNS	

3.5.3 Add a node

Tap the + icon on the **My WiFi** page, and follow the instructions displayed.

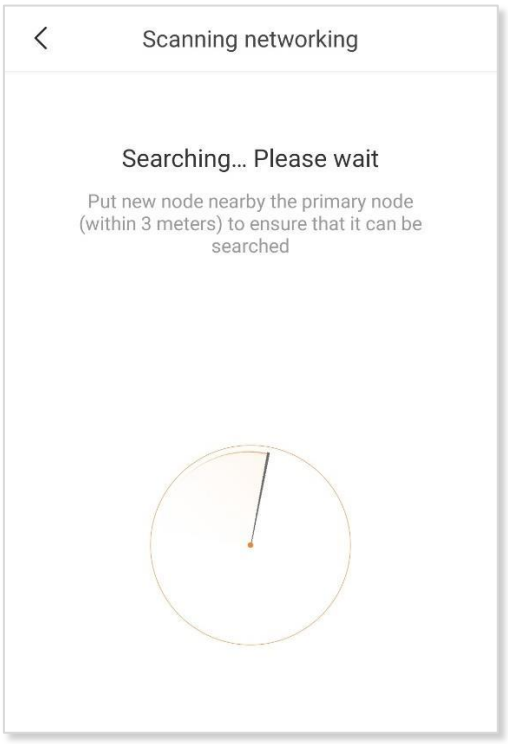




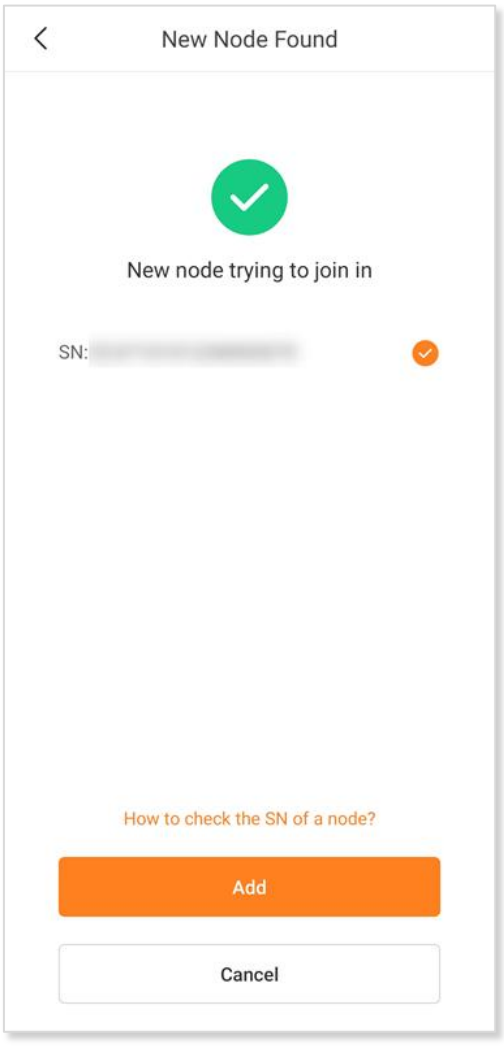
If you cannot add a node by following the preceding instructions, try the following two methods by tapping **Scanning networking** or **Wired networking** shown in the preceding figure:

- To scan a new node:

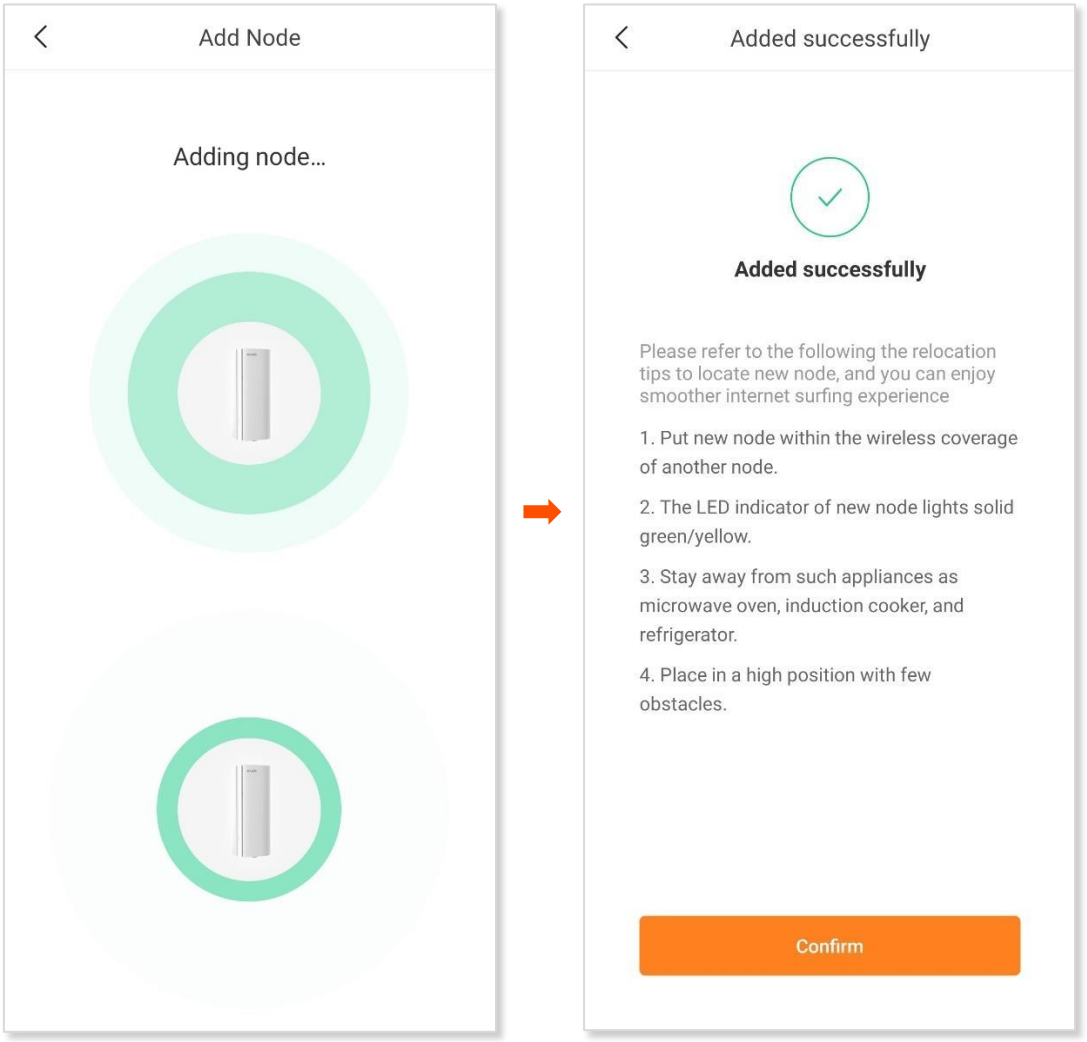
Step 1 Tap **Scanning networking**.



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



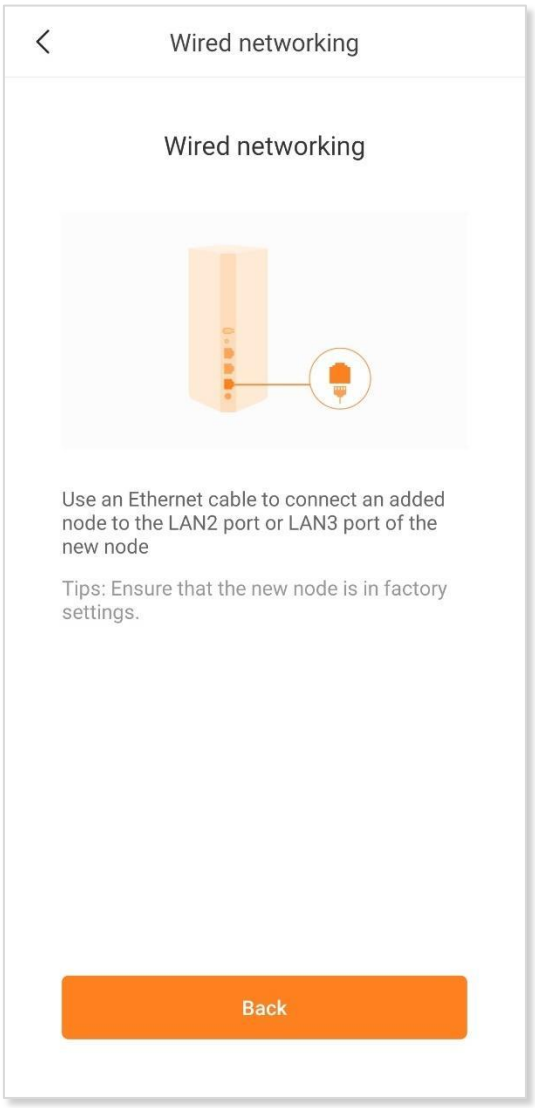
Step 3 Wait until the ongoing process is complete and tap **Confirm**.



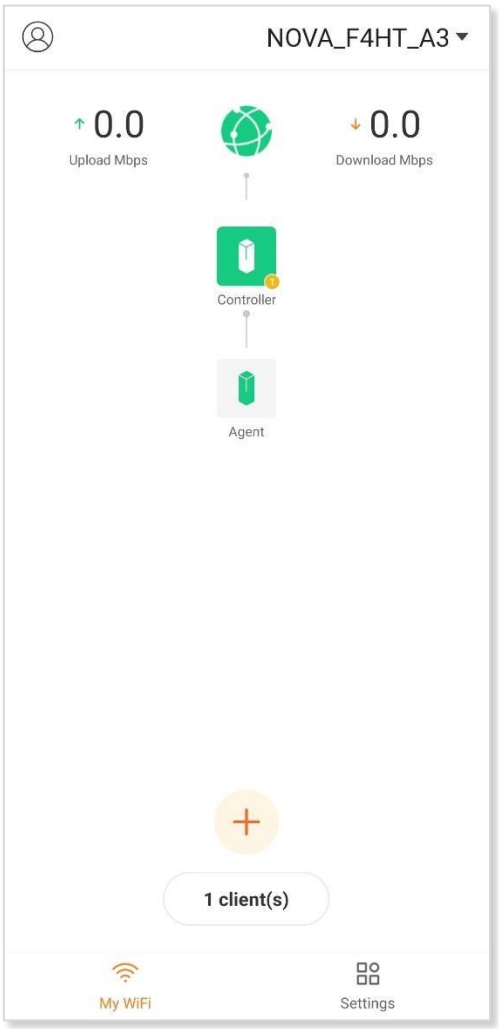
If the LED indicator of new node lights solid on and the new node is displayed in **Network Topology**, the node is added successfully.

---End

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

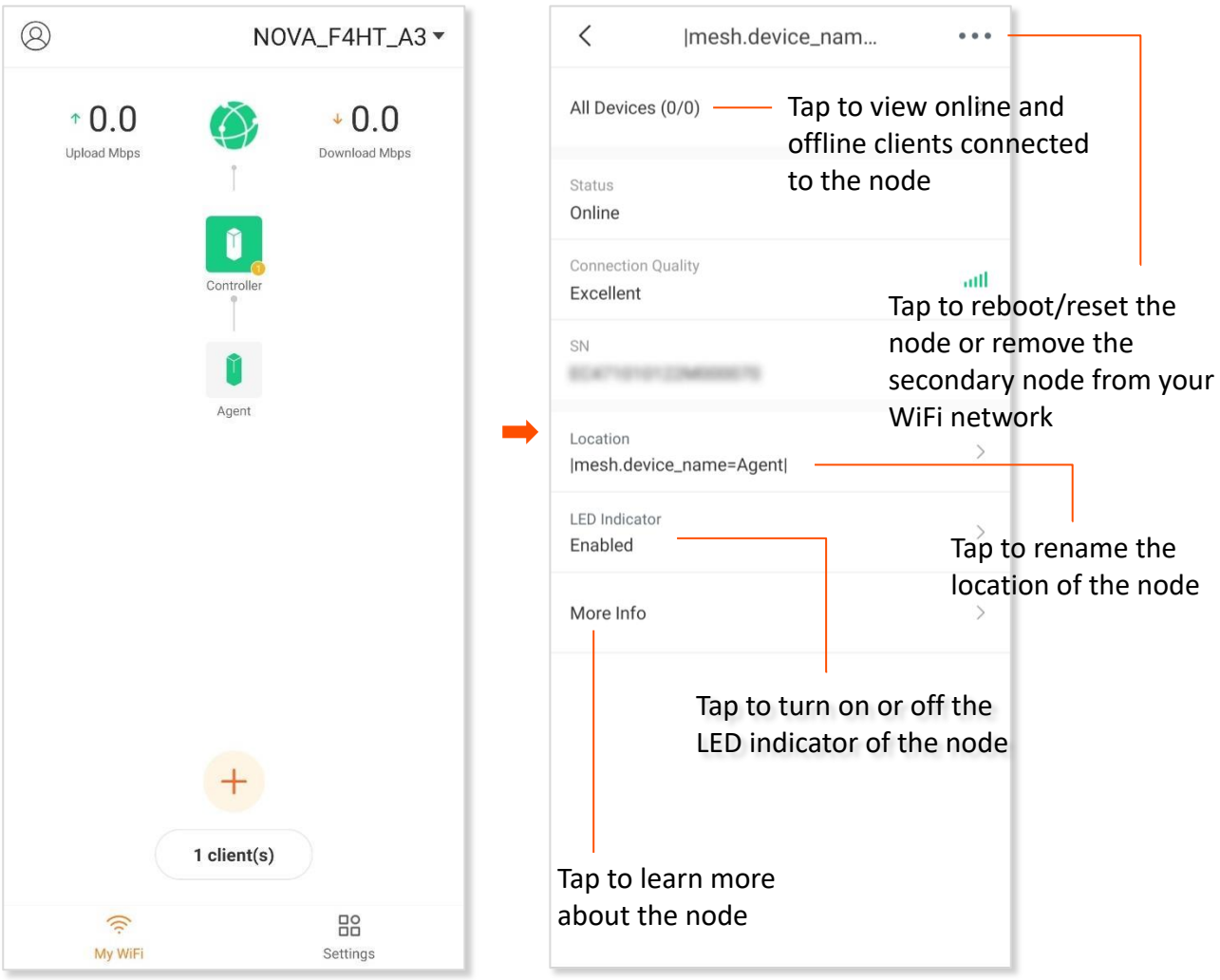


If the LED indicator of new node lights solid on and the new node is displayed on the **My WiFi page**, the node is added successfully.



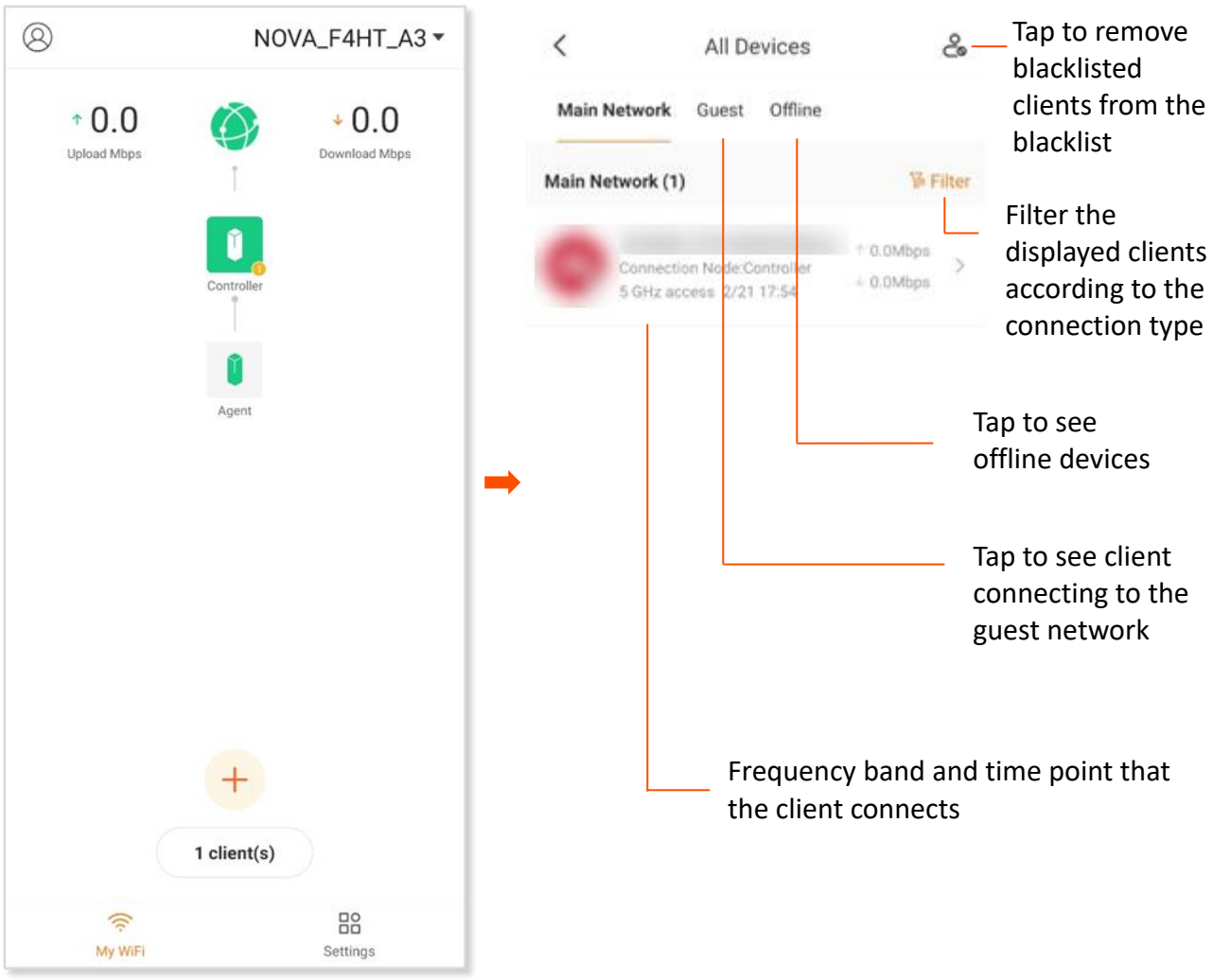
3.5.4 Manage nodes

Tap the  or  icon on the **My WiFi** page. The following figure shows the information of an agent as an example.

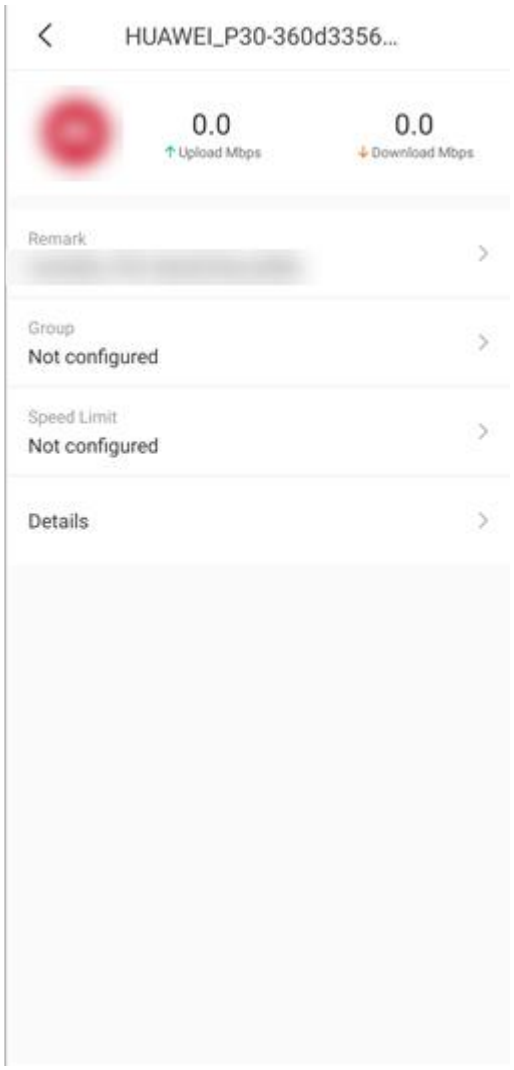

NOVA_F4HT_A3
0.0
Upload Mbps
0.0
Download Mbps
Controller
Agent
1 client(s)
My WiFi
Settings
|mesh.device_nam...
All Devices (0/0)
Tap to view online and offline clients connected to the node
Status
Online
Connection Quality
Excellent
SN
Tap to reboot/reset the node or remove the secondary node from your WiFi network
Location
|mesh.device_name=Agent|
Tap to rename the location of the node
LED Indicator
Enabled
Tap to turn on or off the LED indicator of the node
More Info
Tap to learn more about the node

3.5.5 Manage connected clients

Tap the ***X* client(s)** (*X* indicates the number of connected clients) icon on the **My WiFi** page.



Tap any connected clients and the following page appears.



Tap to rename the client, such as Jack's Phone

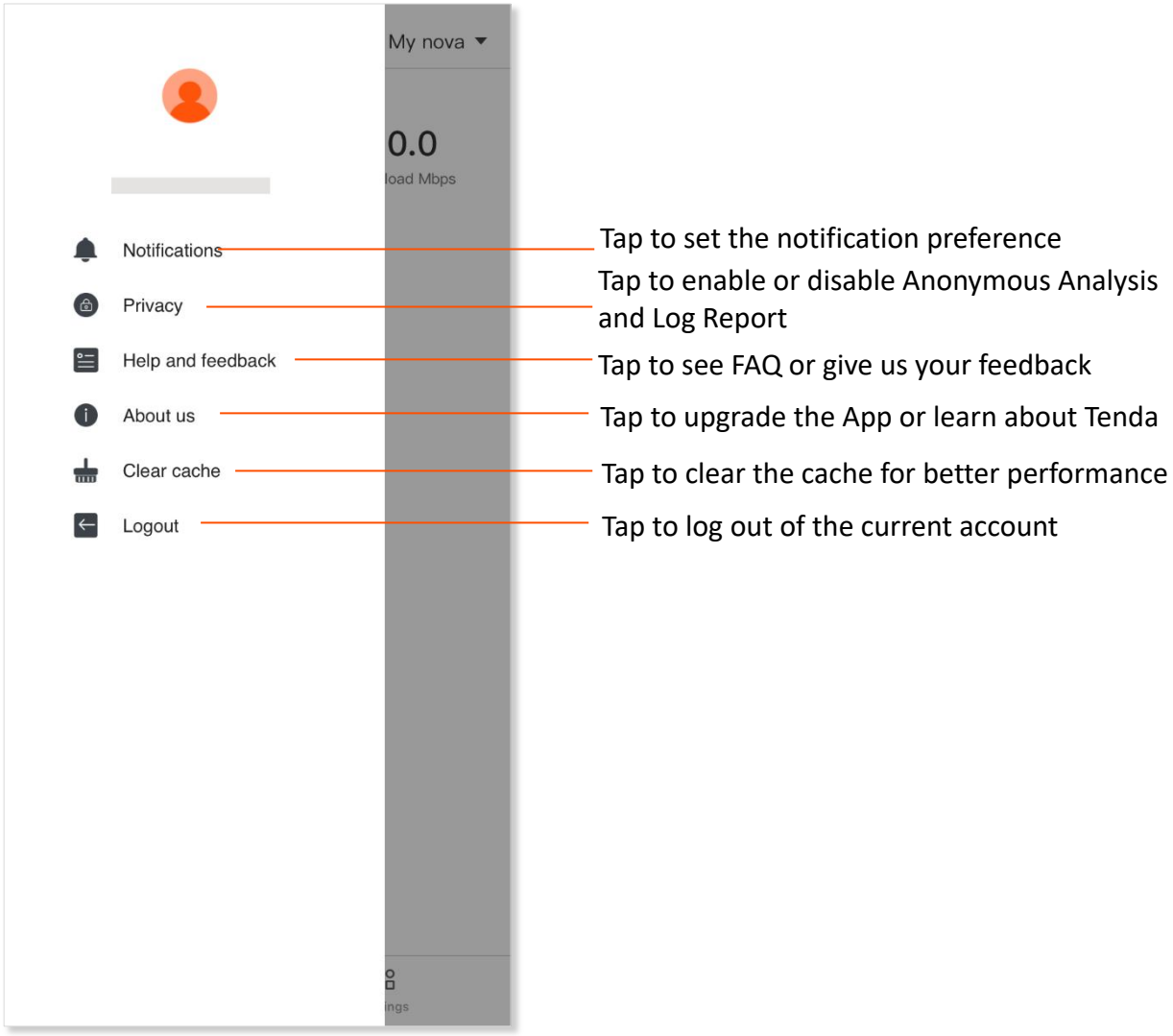
Tap to create a group or add the connected client to a group for the parental control

Tap to set upload and download speed of the client

Tap to check the details of the connected client

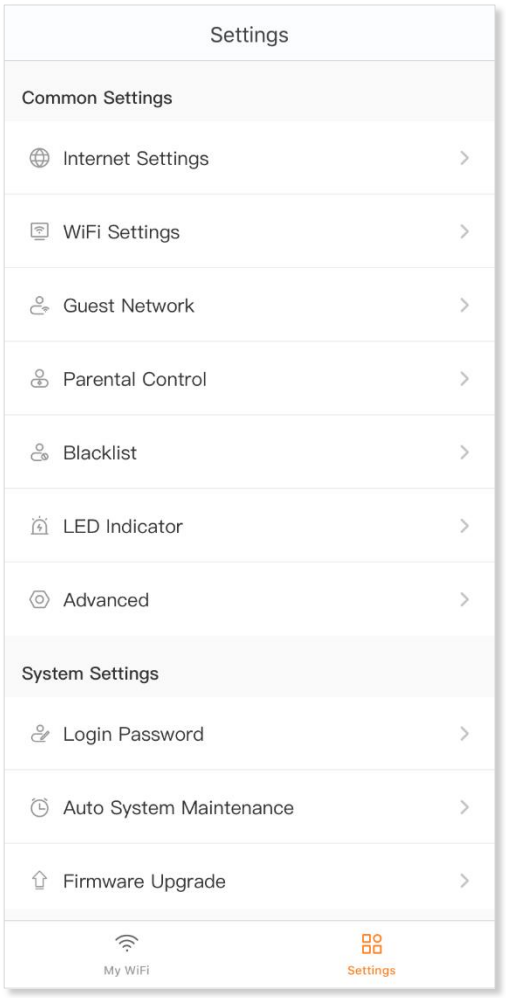
3.6 My profile

Tap the icon in the upper-left corner of **My WiFi** page to enter the page.



3.7 Common Settings

You can change common internet settings or set up more parameters here.
Tap **Settings** to enter the page.



3.7.1 Internet settings

Generally, you can complete the internet settings by following the quick setup wizard of the Tenda WiFi App when you set the nodes for the first time. If your internet connection type or parameters changed, you can set them here again to enable your nodes to access the internet. The nodes support the following connection types:

- **PPPoE:** If this type is selected, you need to enter the PPPoE user name and password provided by your ISP for internet access.
- **Dynamic IP:** If this type is selected, no parameter is required. The node obtains the dynamic IP address and other related parameters automatically from your ISP.
- **Static IP:** If this type is selected, you need to enter the static IP address and other related parameters provided by your ISP for internet access.

Context of use	Information provided by the ISP	Connection type
Connect the node to a modem or Ethernet jack using an Ethernet cable.	PPPoE user name and password	PPPoE
	IP address, subnet mask, default gateway and DNS server address	Static IP
	/	Dynamic IP

The following three connection types are available only when you select **Russia** in **Special ISP Settings**.

- **Russia PPPoE:** If this type is selected, you need to enter the PPPoE user name, PPPoE password, service name, server name, MTU value, and IP address information (if any) provided by your ISP for internet access.
- **Russia PPTP:** If this type is selected, you need to enter the IP address, user name and password of the PPTP server, MTU value, and IP address information (if any) provided by your ISP for internet access.
- **Russia L2TP:** If this type is selected, you need to enter the IP address, user name and password of the L2TP server, MTU value, and IP address information (if any) provided by your ISP for internet access.

Set up a PPPoE connection

Procedure:

Step 1 Run the Tenda WiFi App, and choose **Settings** > **Internet Settings**.

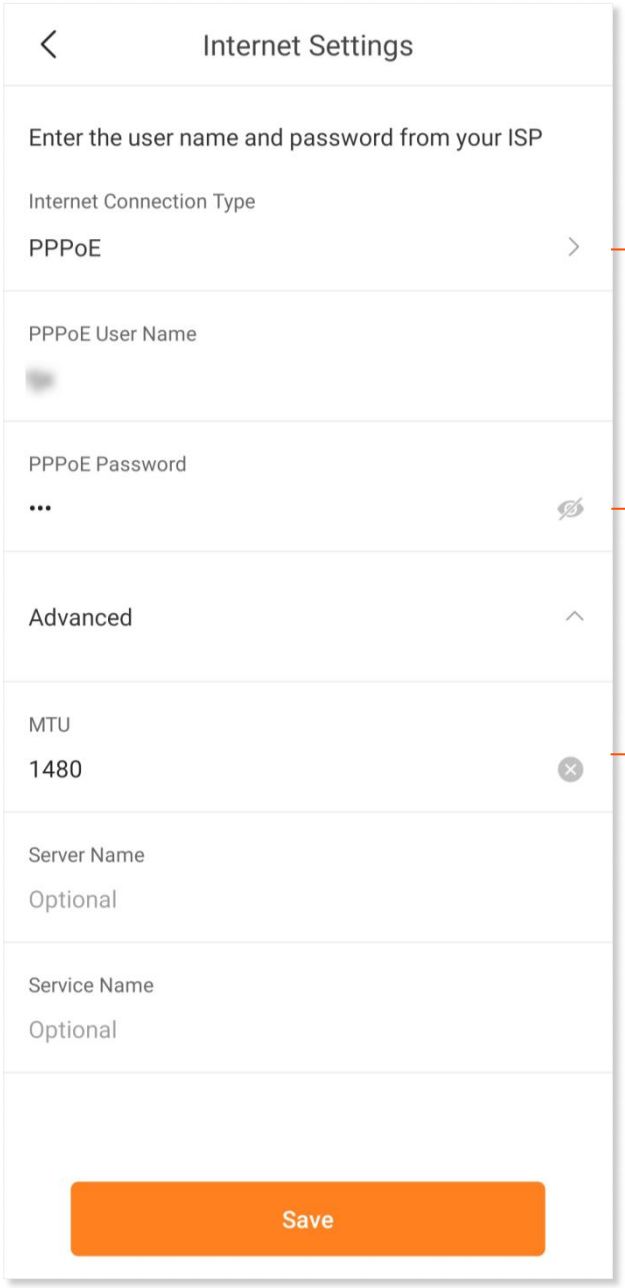
Step 2 Tap **Internet Connection Type**.

Step 3 Select **PPPoE**.

Step 4 Enter the PPPoE user name and password provided by your ISP.

If a service name and a server name are provided, tap **Advanced** to enter them in the target fields.

Step 5 Tap **Save**.



Tap to select an internet connection type

Tap to hide or show the PPPoE password

See MTU for detailed settings.

---End

Set up a dynamic IP address connection

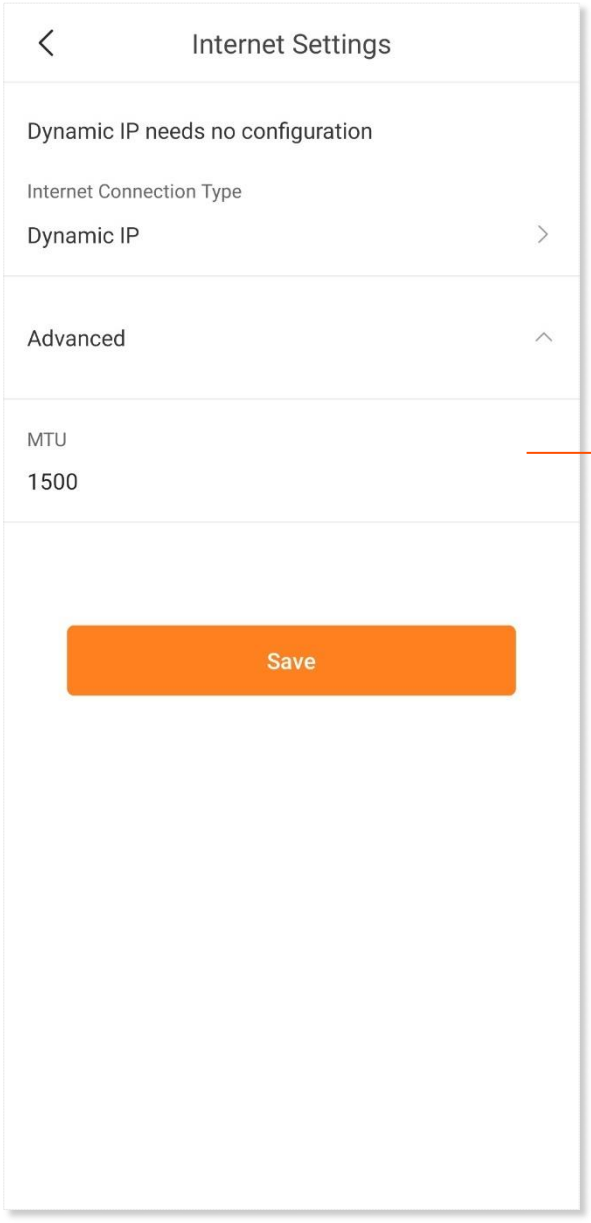
Procedure:

Step 1 Run the Tenda WiFi App, and choose **Settings** > **Internet Settings**.

Step 2 Tap **Internet Connection Type**.

Step 3 Select **Dynamic IP**.

Step 4 Tap **Save**.



See MTU for detailed settings.

---End

Set up a static IP address connection

Procedure:

Step 1 Run the Tenda WiFi App, and choose **Settings** > **Internet Settings**.

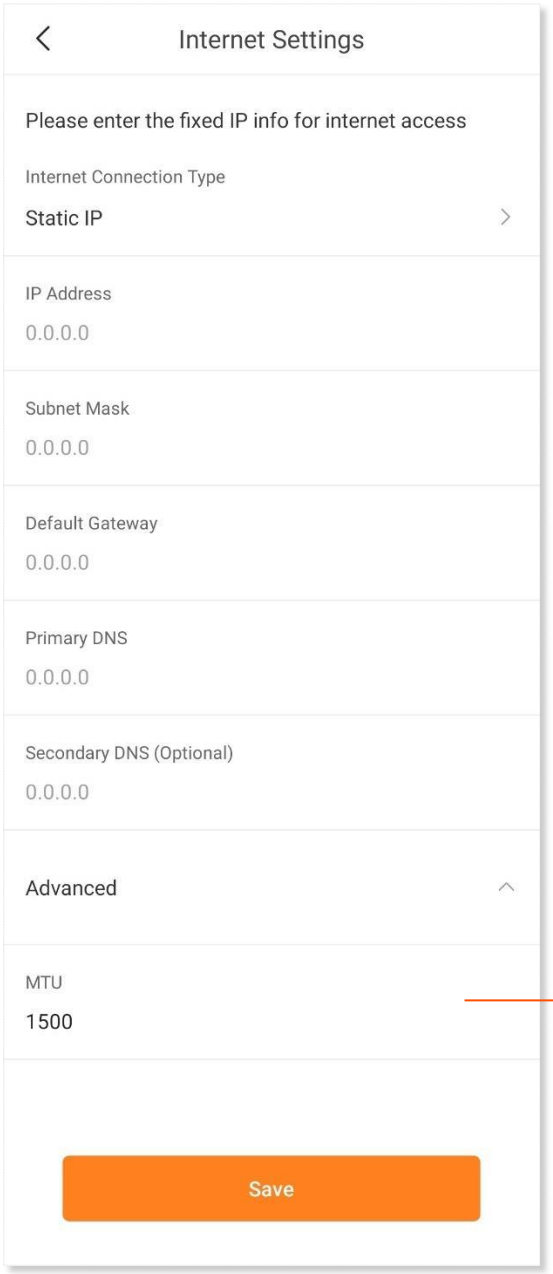
Step 2 Tap **Internet Connection Type**.

Step 3 Select **Static IP**.

Step 4 Enter **IP Address**, **Subnet Mask**, **Default Gateway** and **Primary DNS**.

If a secondary DNS server is provided, enter it as well.

Step 5 Tap **Save**.



See MTU for detailed settings.

---End

Set up dual access connection

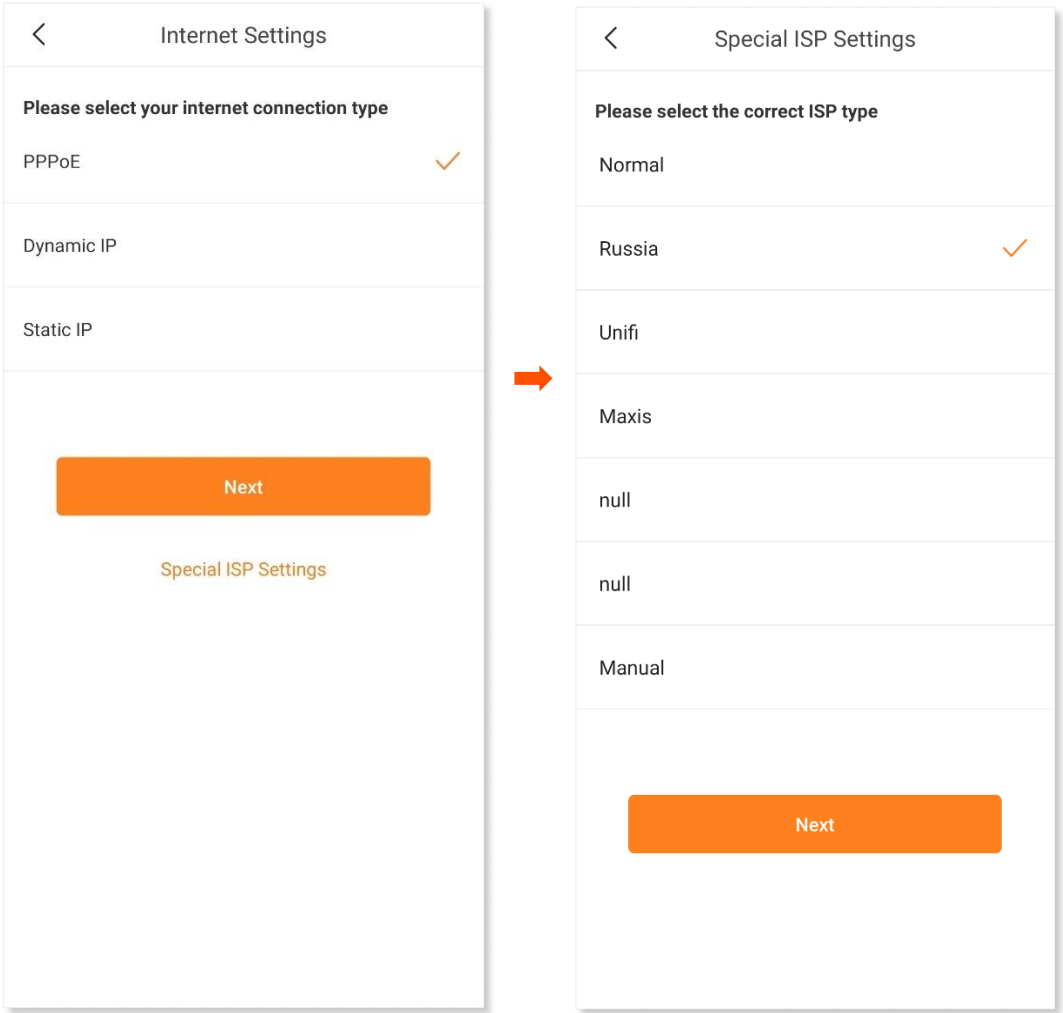
In countries like Russia, the ISP may require you to set up dual access. One is for access to the internet through PPPoE, PPTP or L2TP, and the other is for access to the “local” resources where the ISP is located through DHCP or static IP address. If your ISP provides such connection information, you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

Procedure:

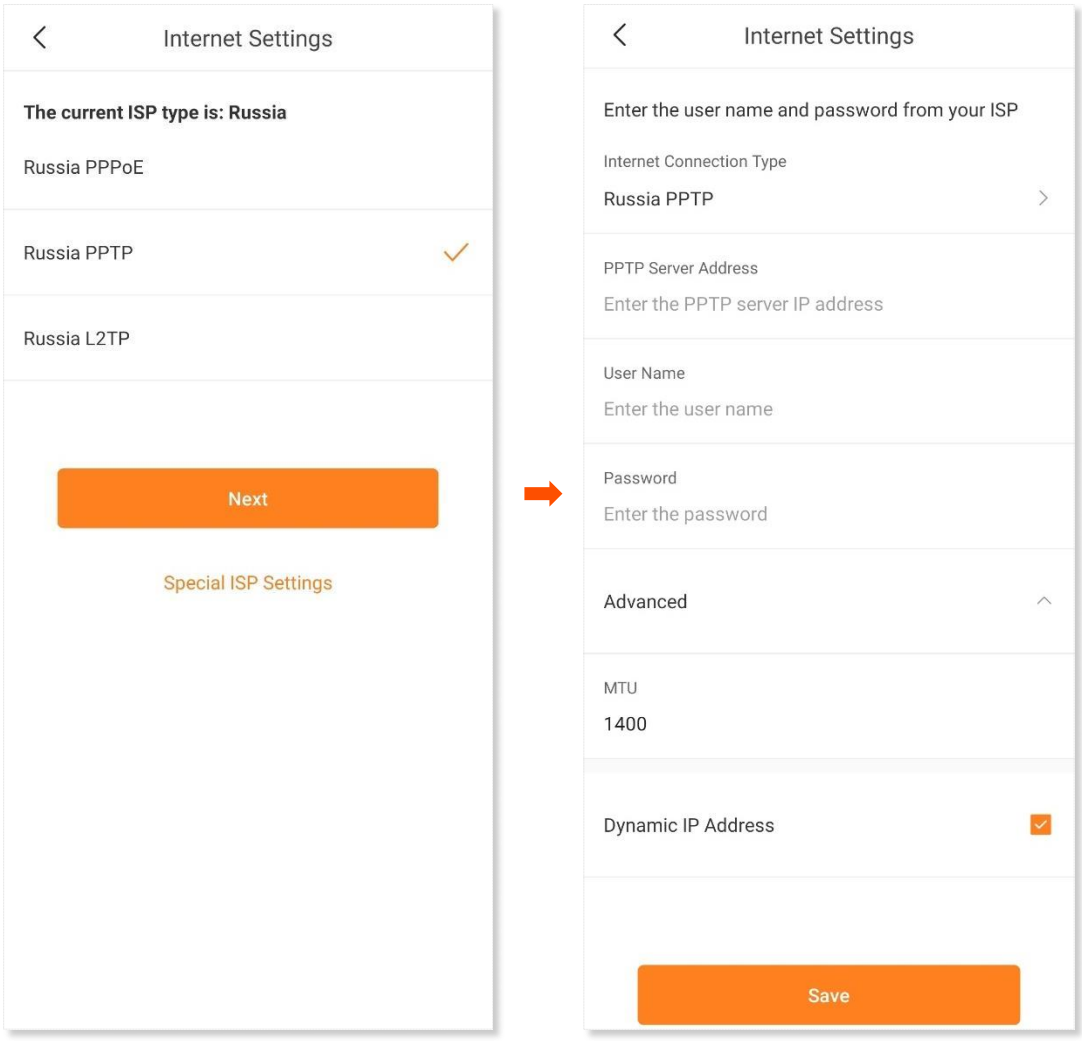
Step 1 Run the Tenda WiFi App, and choose **Settings** > **Internet Settings**.

Step 2 Tap **Internet Connection Type** and then **Special ISP Settings**.

Step 3 Select **Russia** and tap **Next**.



Step 4 Select an internet connection type, which is **Russia PPTP** in this example, fill in required parameters, and tap **Save**.



---End

3.7.2 WiFi (Wireless) settings

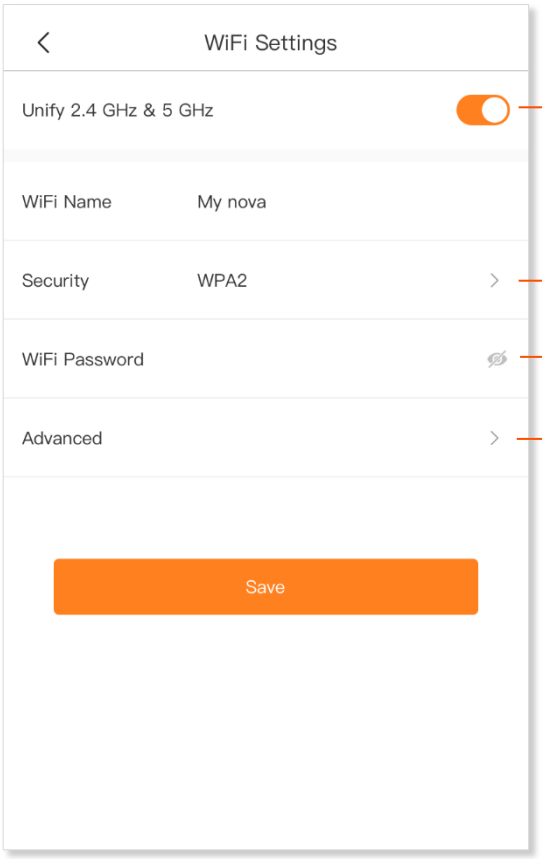
In this module, you can change the WiFi name and WiFi password of your WiFi network.

Procedure:

Step 1 Run the Tenda WiFi App, and choose **Settings** > **WiFi Settings.**

Step 2 Customize the **WiFi Name** and **WiFi Password**.

Step 3 Tap **Save**.



Tap to enable the **Unify 2.4 GHz & 5 GHz** function, which means that the 5 GHz WiFi name and password will be synchronized with those of the 2.4 GHz, and cannot be changed.

Tap to select the encryption type

Tap to hide or show the WiFi password

Tap to set the **Channel**, **Network Mode** and **Bandwidth** of the 2.4 GHz WiFi and 5 GHz WiFi

---End

3.7.3 Guest network

The guest network function enables you to create a separate network for your guests to ensure the security of the main network.

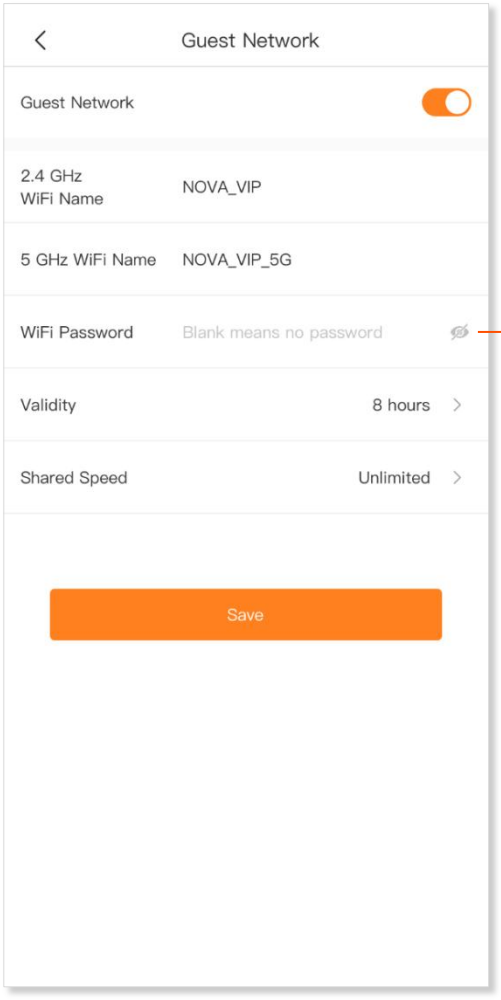
Procedure:

Step 1 Run the Tenda WiFi App, and choose **Settings** > **Guest Network**.

Step 2 Enable the **Guest Network** function.

Step 3 Customize the **WiFi Name** and **WiFi Password**, select a **Validity**, and set a **Shared Speed.**

Step 4 Tap **Save**.



---End

3.7.4 Parental control

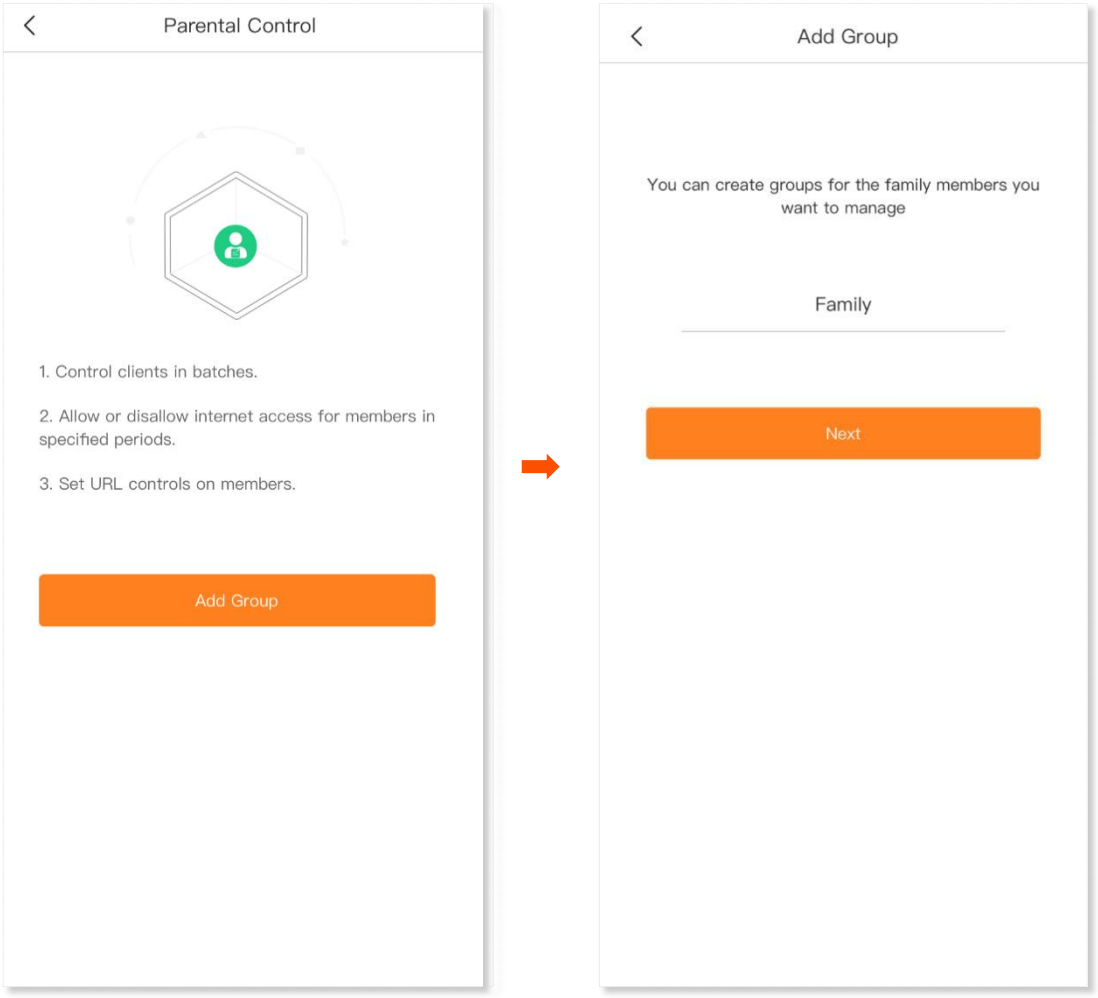
The parental control function enables you to create an appropriate time session for internet access for your family members.

Procedure:

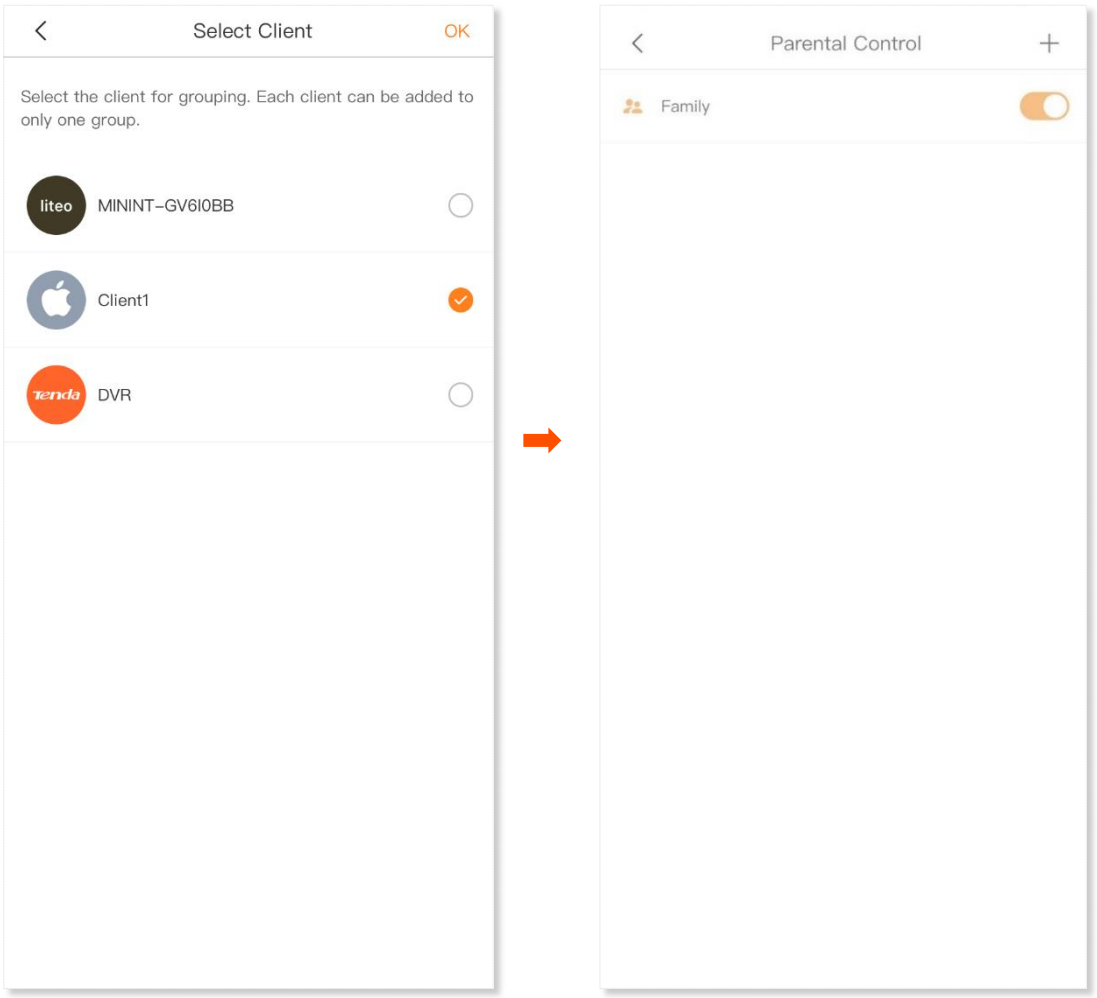
Step 1 Run the Tenda WiFi App, and choose **Settings** > **Parental Control**.

Step 2 Create a group.

1. Tap **Add Group**.
2. Specify a group name, which is **Family** in this example, and tap **Next**.



3. Select target clients. **Client1** is used as an example here.
4. Tap **OK**.



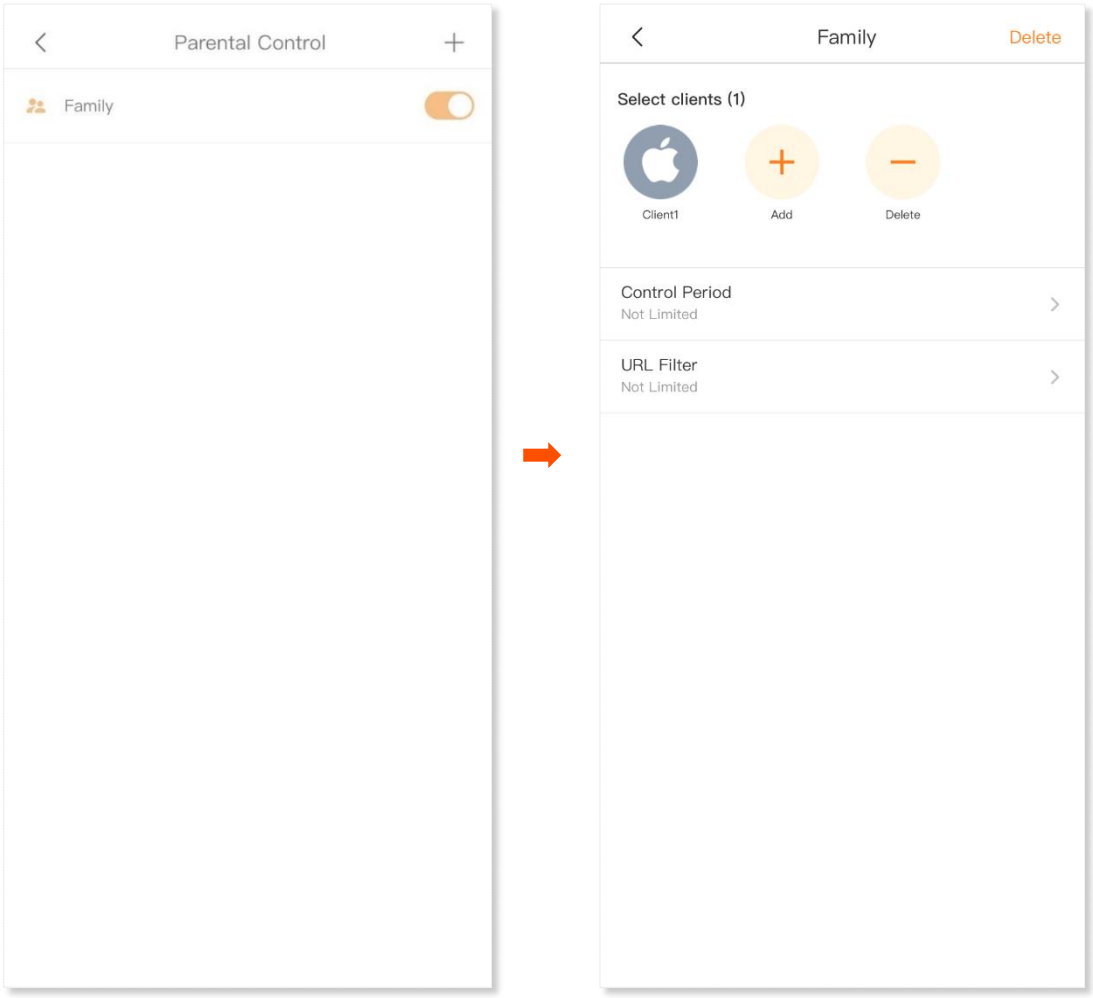
Step 3 Tap  or to enable or disable the function of parental control.

 indicates that the parental control is enabled.

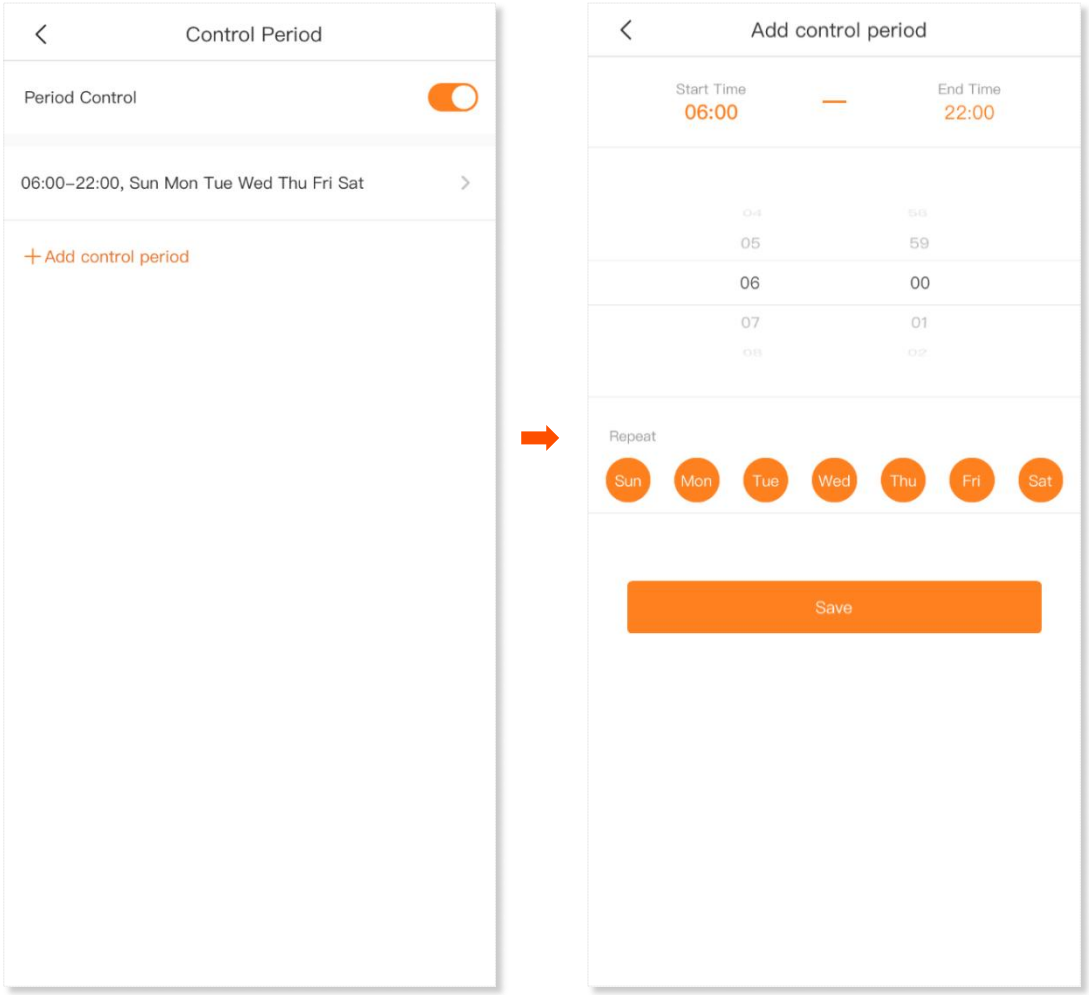
 indicates that the parental control is disabled.

Step 4 Customize the period of internet inaccessibility for the group.

1. Tap the group. **Family** is used as an example here.
2. Tap **Control Period**.

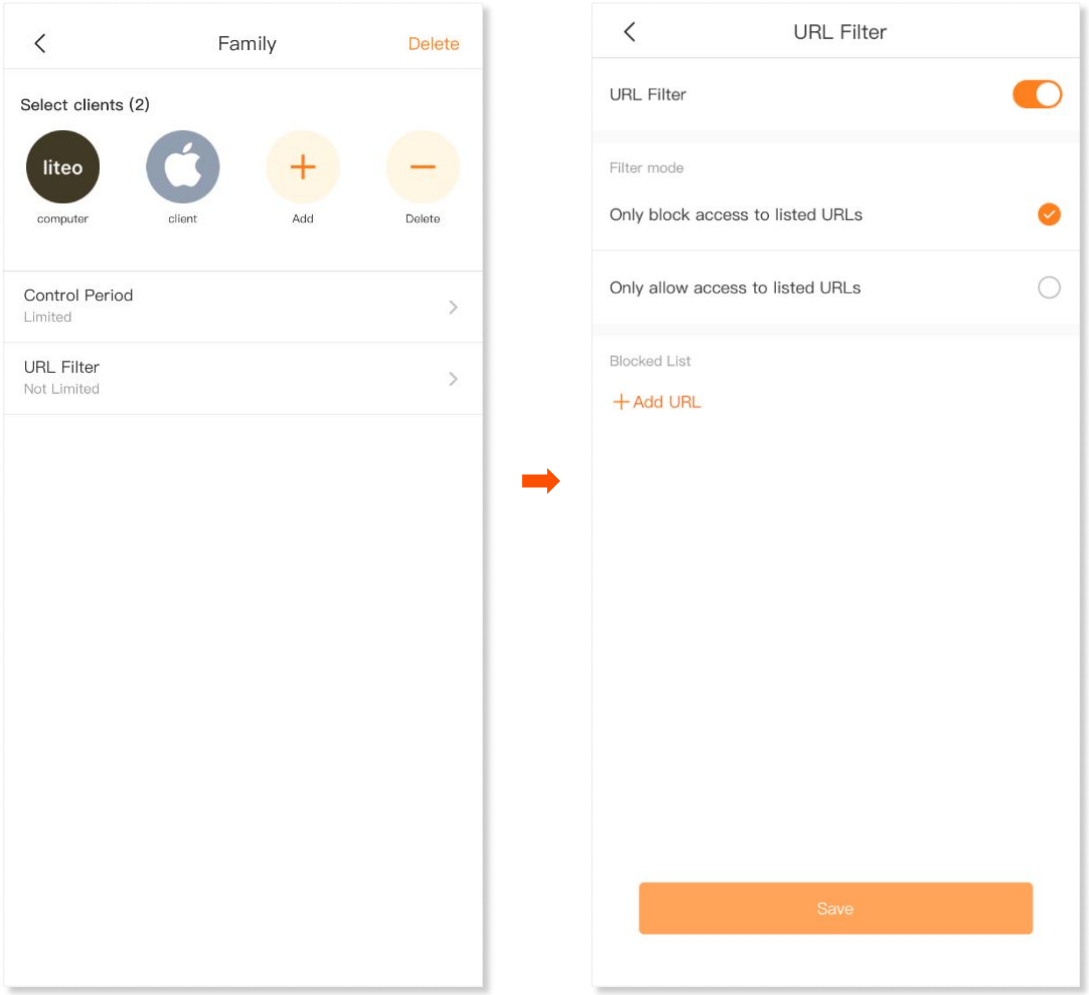


3. Enable the **Period Control** function.
4. Tap **Add control period**.
5. Specify a **Start Time**, **End Time**, and the days on which the rule takes effect.
6. Tap **Save**.

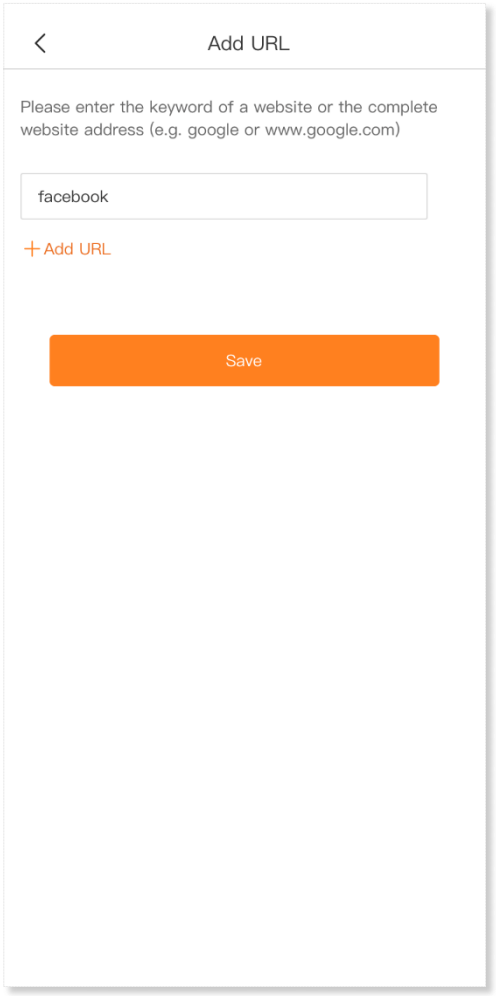


Step 5 Customize the URL filter rule for the group.

1. Tap **URL Filter**.
2. Enable the **URL Filter** function.
3. Select **Filter mode**, and tap **Add URL**.



4. Enter a website you want to block, which is **facebook** in this example.



TIP

Tap **+Add URL** to add other websites you want to block.

5. Tap **Save**.

---End

3.7.5 Blacklist

The blacklist function enables you to add a client into the blacklist or remove a client from 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.

Add a client to the blacklist

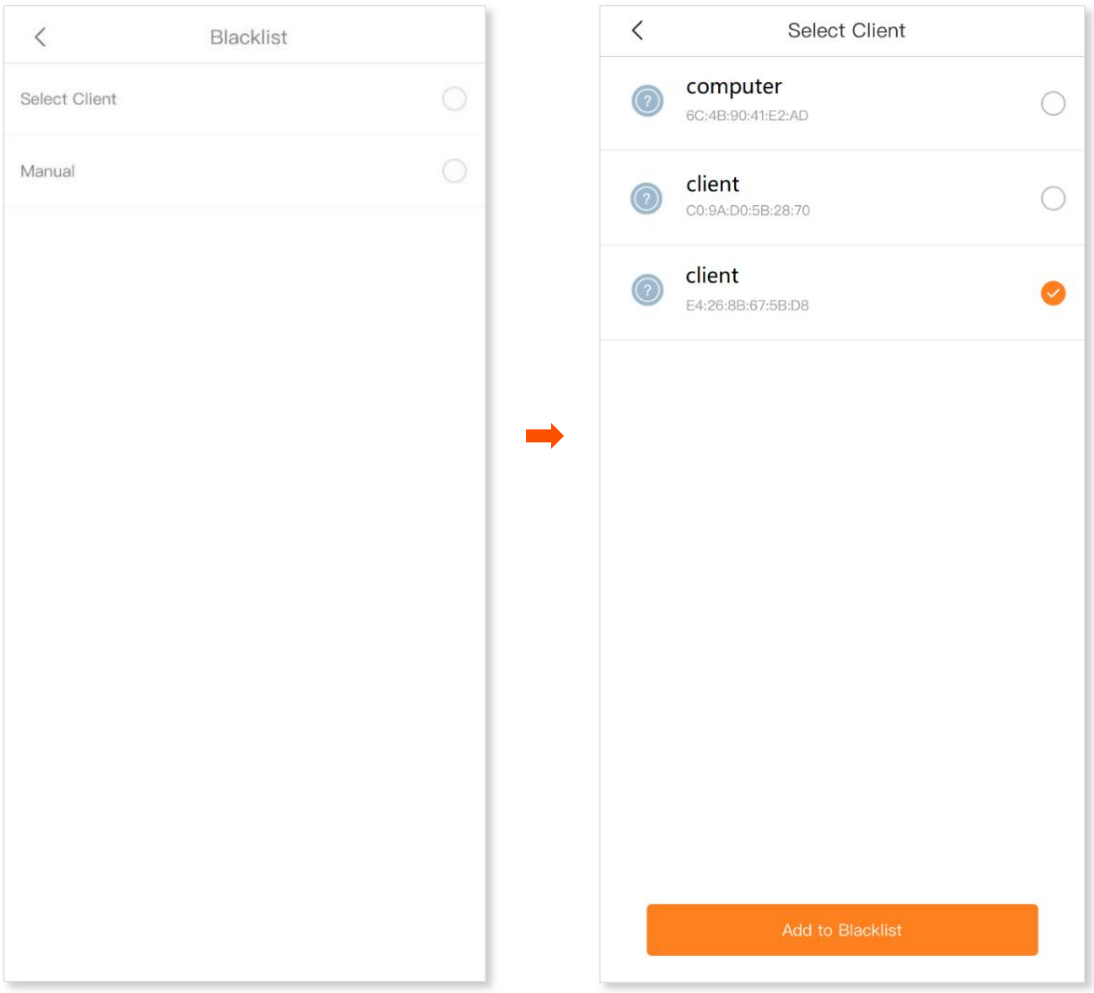
You can add the client into the blacklist to block the internet access.

Procedure:

Step 1 Run the Tenda WiFi App, and choose **Settings** > **Blacklist**.

Step 2 Tap **Add to Blacklist**, and choose **Select Client** or **Manual**, which is **Select Client** in this example.

Step 3 Select a client that you want to add it into blacklist, then tap **Add to Blacklist**.



---End

Remove a client from the blacklist

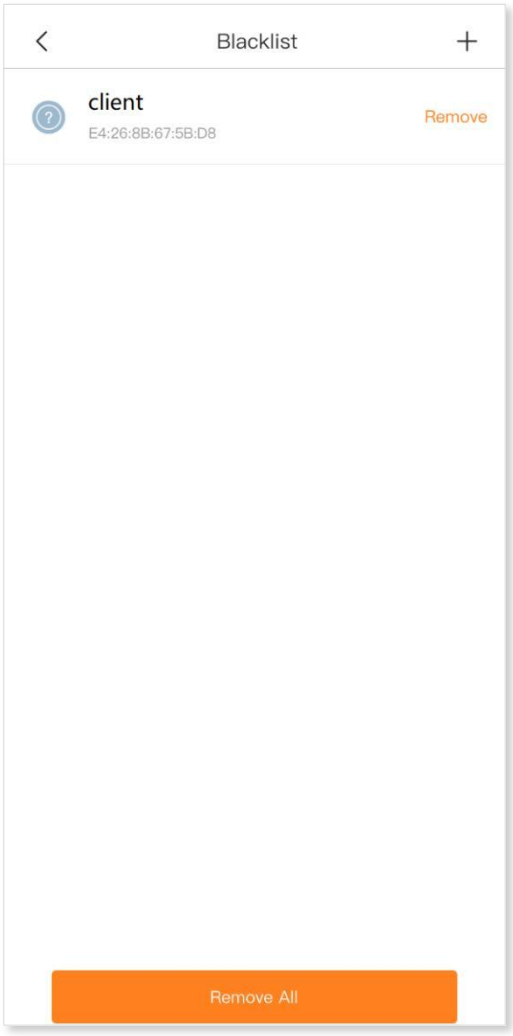
After adding the client into the blacklist, the client cannot access the internet through the Mesh device.

You can remove the client from the blacklist as required.

Procedure:

Step 1 Run the Tenda WiFi App, and choose **Settings** > **Blacklist**.

Step 2 Find a client that you want to remove from the blacklist, then tap **Remove**, or tap **Remove All** to remove all clients from the blacklist.



---End

After the setting completes, the client removed from the blacklist can access the network upon the next connection.

3.7.6 LED indicator

The LED indicator function enables you to turn on or off the LED indicator of the Mesh devices. You can also set a schedule to turn off the LED indicators. By default, the LED indicators are turned on.

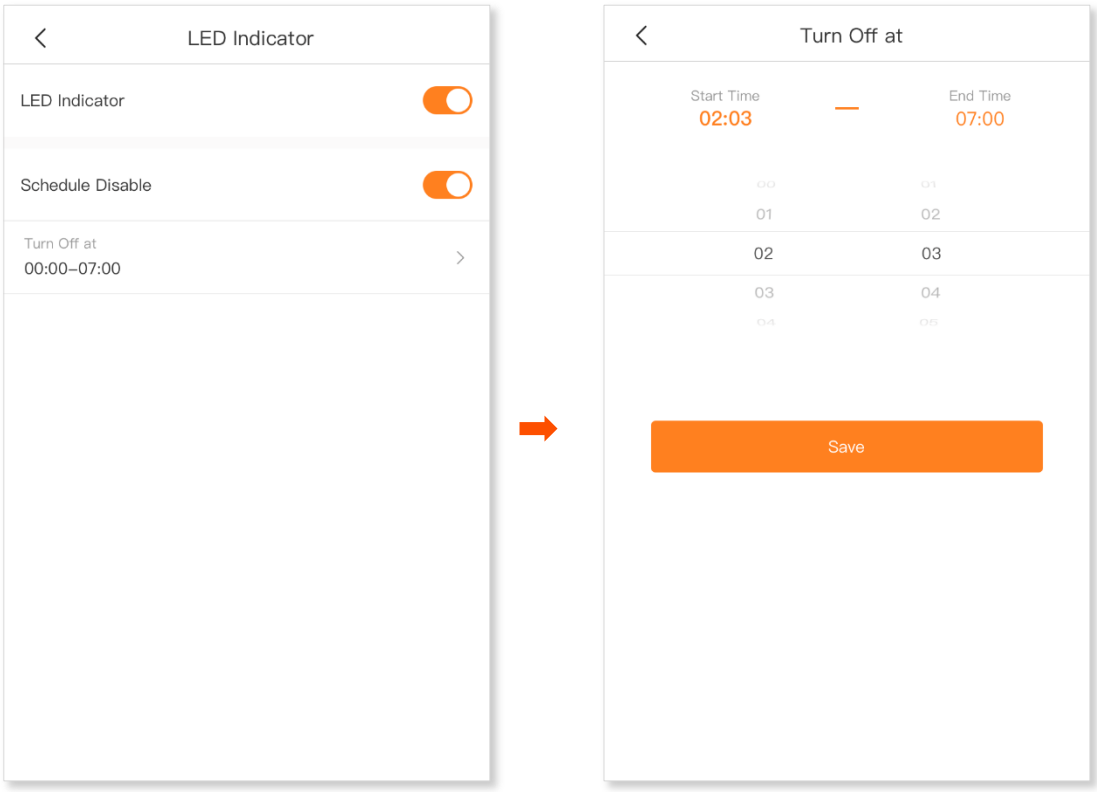
Procedure:

Step 1 Run the Tenda WiFi App, and choose **Settings** > **LED indicator**.

Step 2 Enable **Schedule Disable**.

Step 3 Specify the **Start Time** and **End Time**, which are **02:03** and **07:00** in this example.

Step 4 Tap **Save**.



---End

After the setting completes, the LED indicators of the Mesh devices will turn off at 02:03 to 07:00.

3.7.7 Working mode

This Mesh device can operate in either router mode or access point (AP) mode. **Current Mode** is displayed after the working mode currently adopted by the Mesh device. You can select a working mode for your Mesh device based on your scenario. By default, the Mesh device works in router mode.

For users who need to specify the network connection mode, select the router mode. For users who use an upstream router, select the AP mode.

Router Mode

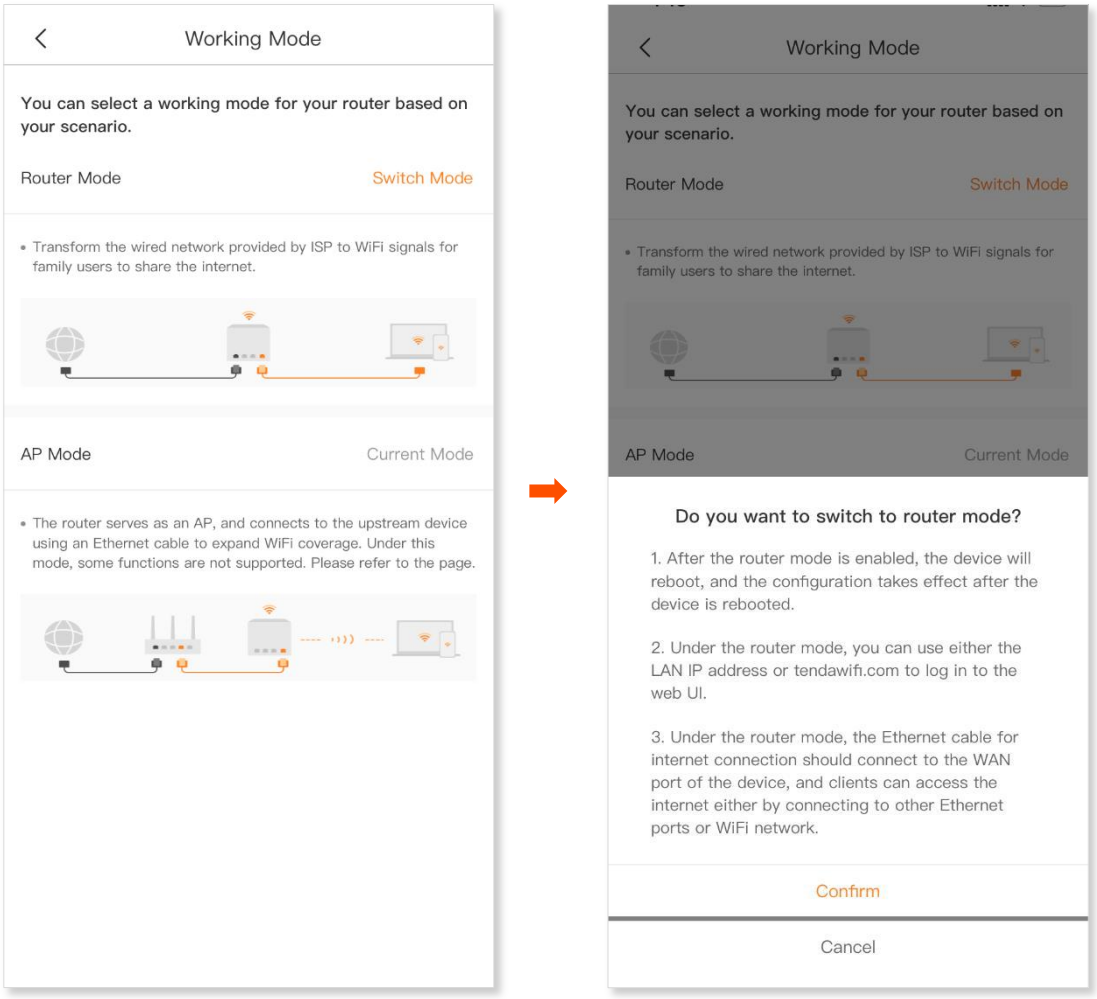
By default, all nodes work in the router mode. All functions are available in this mode. If you want to switch from the router mode to AP mode, see AP mode.

Procedure:

Step 1 Run the Tenda WiFi App, and choose **Settings** > **Advanced** > **Working Mode**.

Step 2 Tap **Switch Mode**.

Step 3 Tap **Confirm** in the pop-up window.


Working Mode
You can select a working mode for your router based on your scenario.
Router Mode
Switch Mode
• Transform the wired network provided by ISP to WiFi signals for family users to share the internet.
AP Mode
Current Mode
• The router serves as an AP, and connects to the upstream device using an Ethernet cable to expand WiFi coverage. Under this mode, some functions are not supported. Please refer to the page.
Working Mode
You can select a working mode for your router based on your scenario.
Router Mode
Switch Mode
• Transform the wired network provided by ISP to WiFi signals for family users to share the internet.
AP Mode
Current Mode
Do you want to switch to router mode?
1. After the router mode is enabled, the device will reboot, and the configuration takes effect after the device is rebooted.
2. Under the router mode, you can use either the LAN IP address or tendawifi.com to log in to the web UI.
3. Under the router mode, the Ethernet cable for internet connection should connect to the WAN port of the device, and clients can access the internet either by connecting to other Ethernet ports or WiFi network.
Confirm
Cancel

---End

AP Mode

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

You can switch the working mode to AP mode here.

TIP

When the Mesh device is set to AP mode:

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

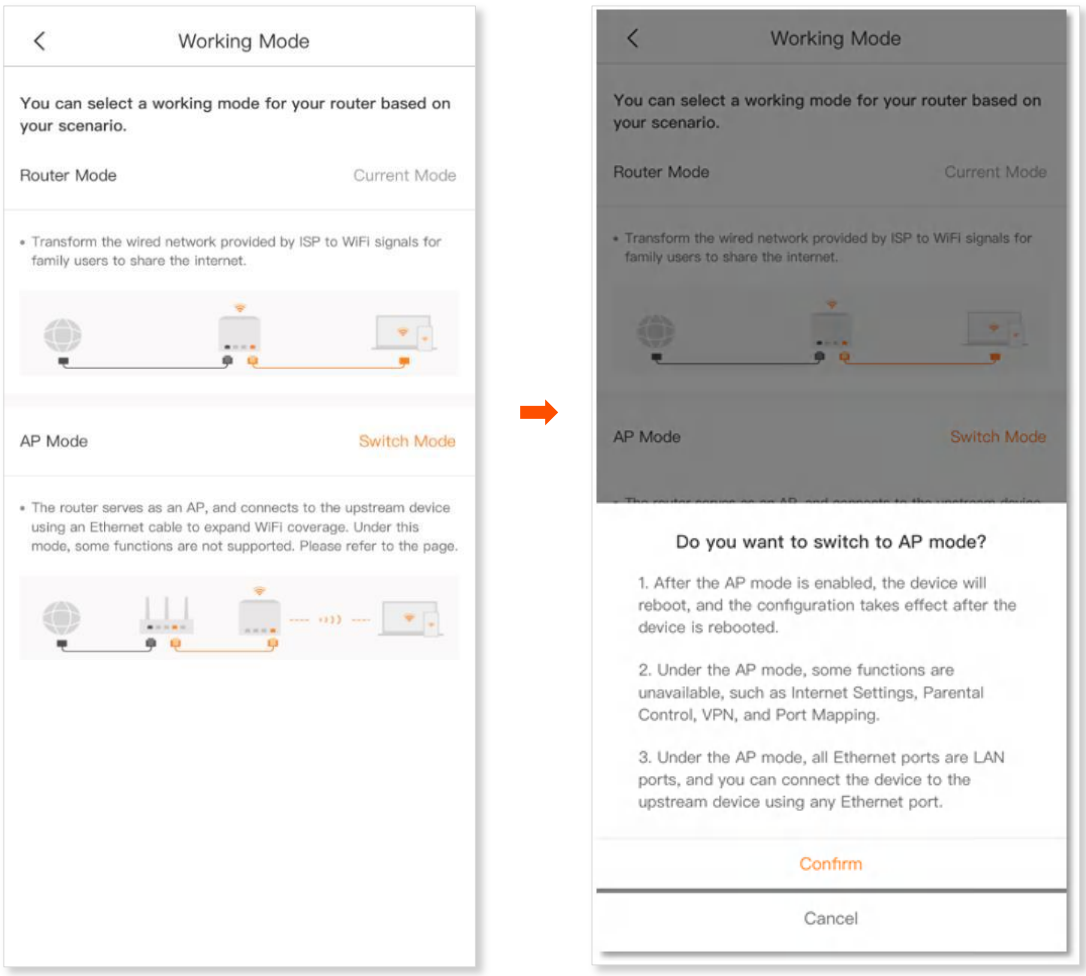
Procedures:

Step 1 Run the Tenda WiFi App, and choose **Settings** > **Advanced** > **Working Mode**.

Step 2 Tap **Switch Mode**.

Step 3 Tap **Confirm** in the pop-up window.

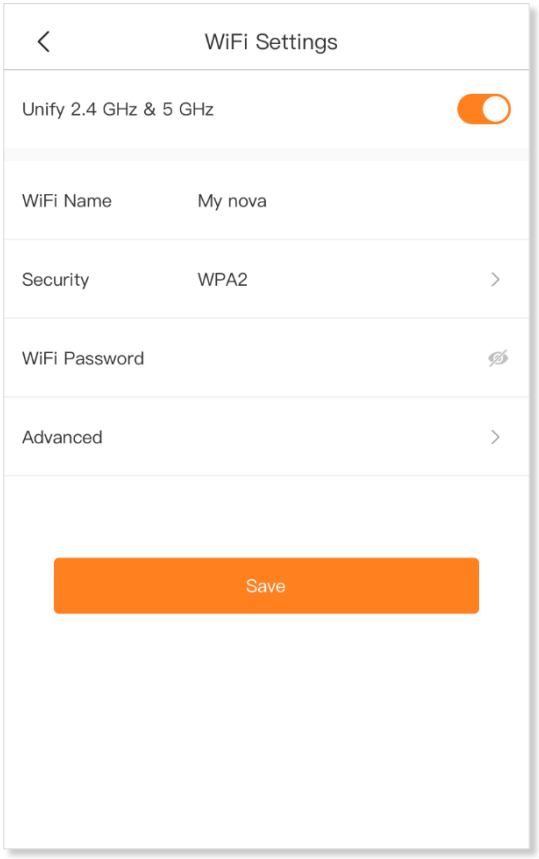
Step 4 Use an Ethernet cable to connect the LAN port of your Mesh device to a LAN port of your upstream router (the router has connected to the internet).



---End

To access the internet, connect your computer to any Ethernet port of the Mesh device, 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 Mesh device.

3.7.8 IPv6

TIP

This function is only available in the router mode.

This Mesh device supports IPv4 and IPv6 dual-stack protocols. In the IPv6 part, you can:

- Perform IPv6 WAN settings
- Change IPv6 LAN settings

IPv6 WAN settings

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

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

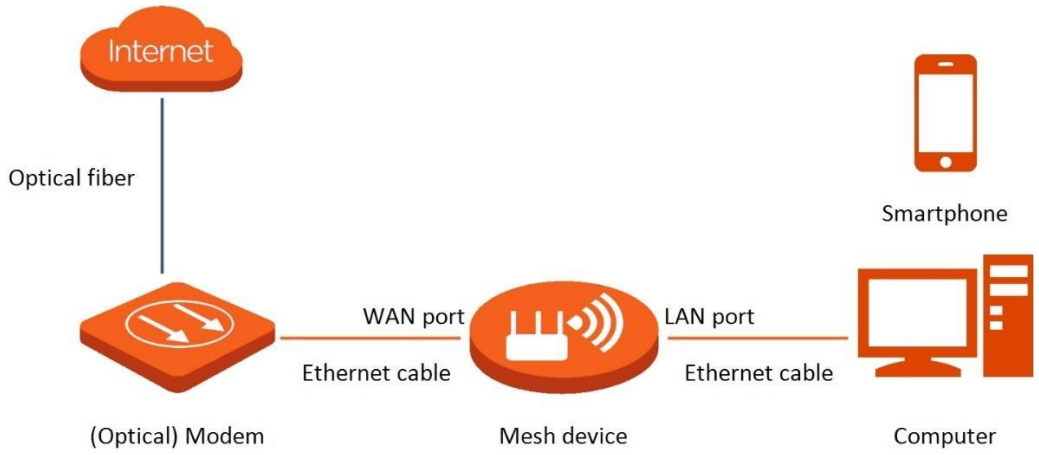
TIP

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.

DHCPv6

DHCPv6 enables the Mesh device 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.



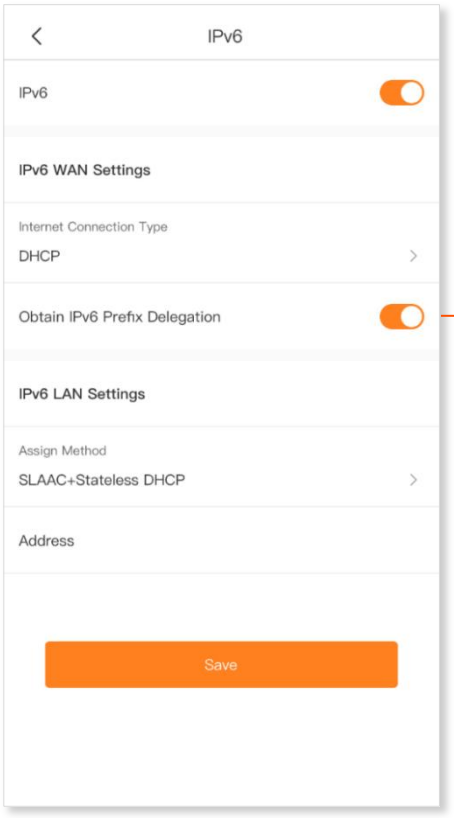
Procedure:

Step 1 Run the Tenda WiFi App, and choose **Settings** > **Advanced** > **IPv6**.

Step 2 Enable the **IPv6** function.

Step 3 Set the **Internet Connection Type** to **DHCPv6**.

Step 4 Tap **Save**.



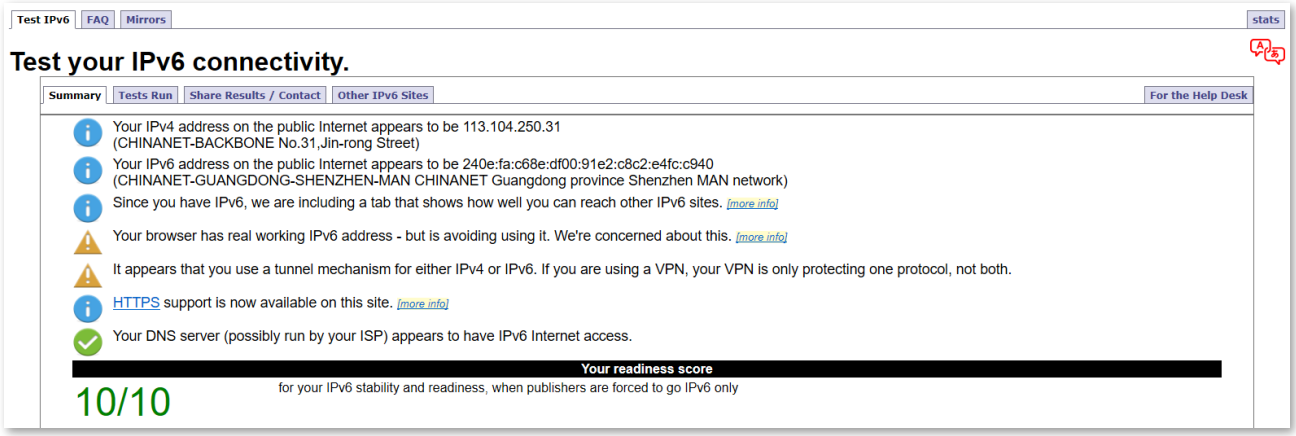
When the option is selected, the LAN port of Mesh device obtains the IPv6 prefix from its upstream device. The LAN port might not obtain the PD prefix if the upstream device does not support PD prefix delivery. Contact your ISP for relevant solutions.

---End

IPv6 network test:

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

When “You have IPv6” is shown on the page, the configuration succeeds and you can access IPv6 services.



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

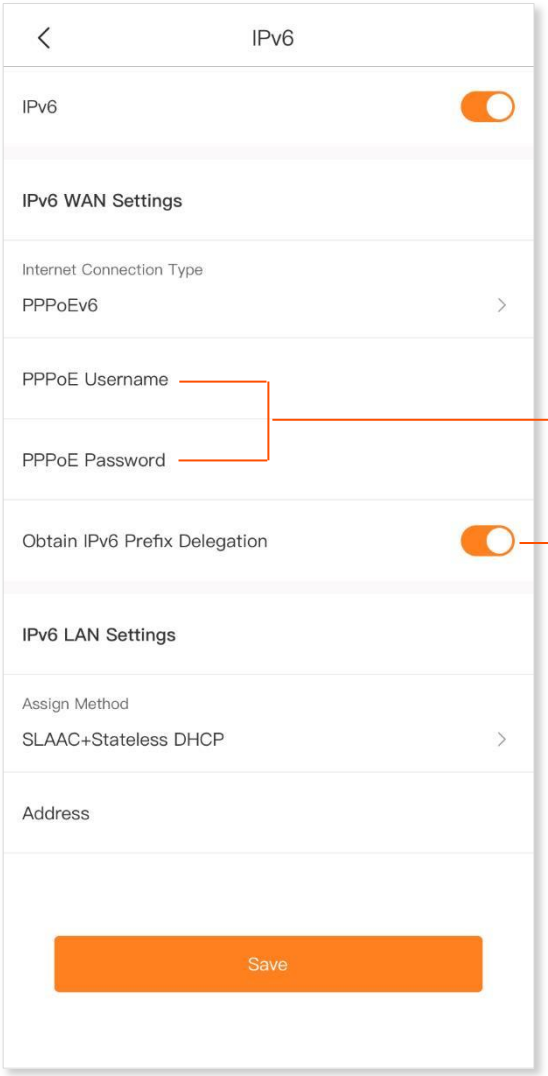
- Ensure that devices connected to Mesh device obtain their IPv6 addresses through DHCP.
- Consult your ISP for help.

PPPoEv6

Overview

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

Run the Tenda WiFi App, and choose **Settings** > **Advanced** > **IPv6**. When the connection type is set to PPPoEv6, the page is shown as below.



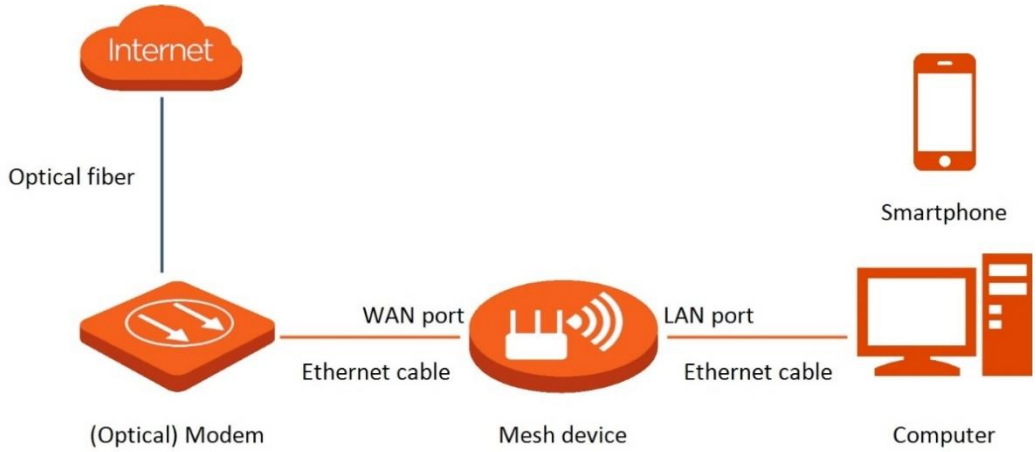
They specify the PPPoE user name and password provided by your ISP.

When the option is enabled, the LAN port of Mesh device obtains IPv6 prefix from its upstream device.

It is recommended to keep the default setting (Enabled). The LAN port might not obtain the PD prefix if the upstream device does not support PD prefix delivery. Contact your ISP for relevant solutions.

Access the internet through PPPoEv6

If the PPPoE account provided by your ISP includes IPv6 service, you can choose PPPoEv6 to access the IPv6 service. The application scenario is shown as below.



Procedure:

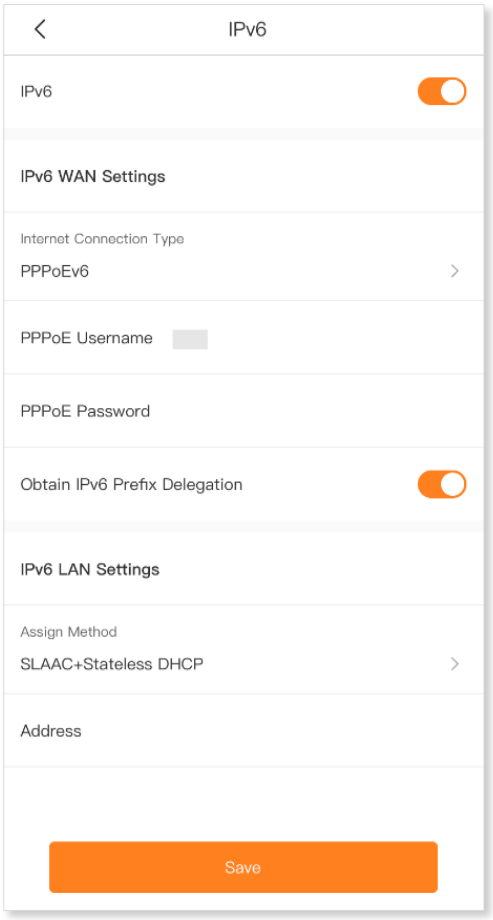
Step 1 Run the Tenda WiFi App, and choose **Settings** > **Advanced** > **IPv6**.

Step 2 Enable the **IPv6** function.

Step 3 Set the **Internet Connection Type** to **PPPoEv6**.

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

Step 5 Tap **Save**.

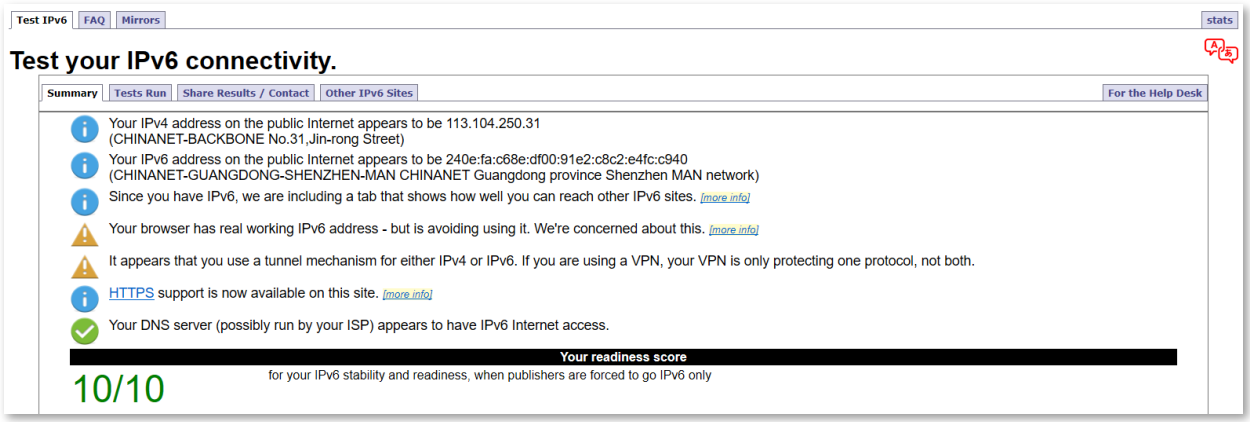


---End

IPv6 network test:

Start a web browser on a phone or a computer that is connected to the Mesh device, 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 succeeds and you can access IPv6 services.



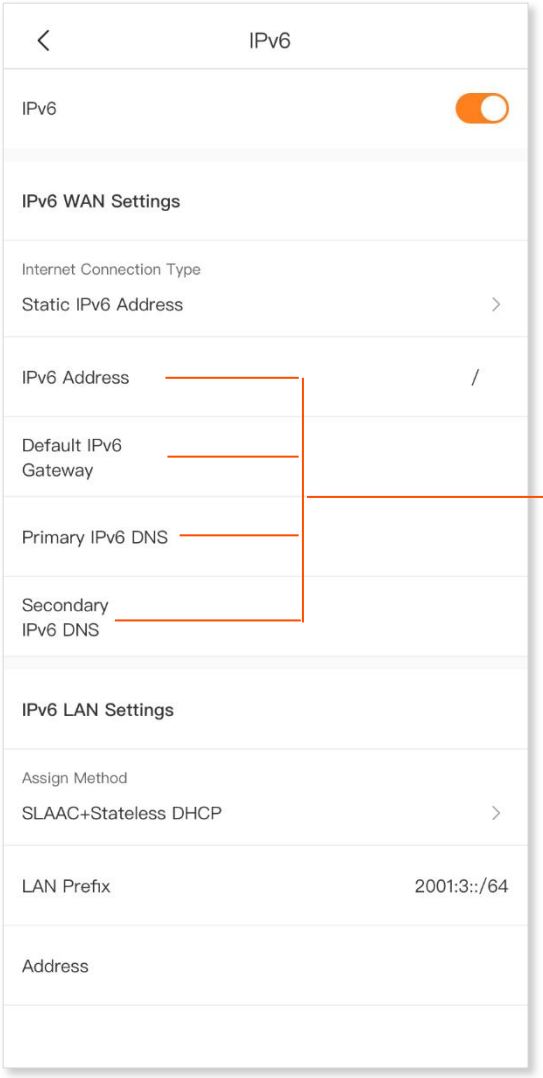
If the IPv6 network test fails, try the following solutions:

- Ensure that devices connected to the Mesh device obtain their IPv6 address through DHCP.
- Consult your ISP for help.

Static IPv6 address

Overview

If 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.
Run the Tenda WiFi App, and choose **Settings** > **Advanced** > **IPv6**. When the connection type is set to **Static IPv6 Address**, the page is shown as below.



They specify the fixed IP address information provided by your ISP.

Access the internet through static IPv6 address

Procedure:

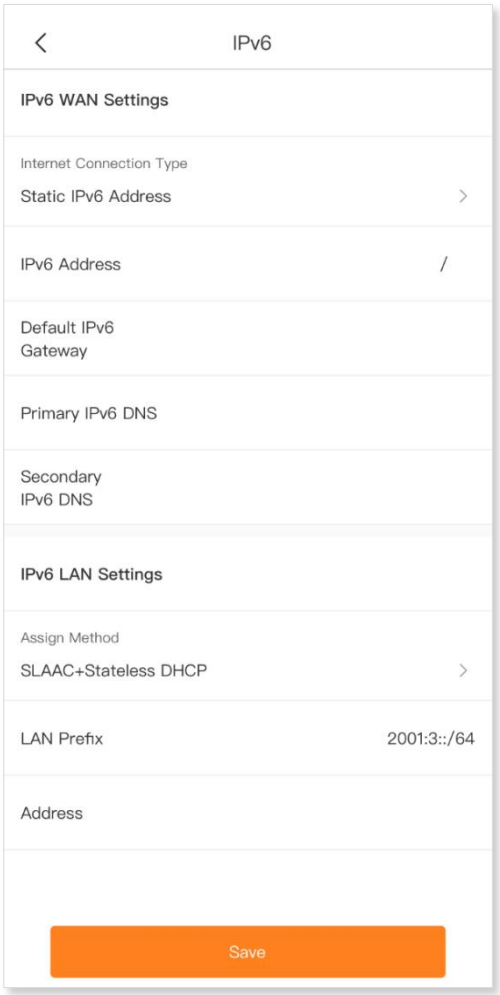
Step 1 Run the Tenda WiFi App, and choose **Settings** > **Advanced** > **IPv6**.

Step 2 Enable the **IPv6** function.

Step 3 Set the connection type to **Static IPv6 Address**.

Step 4 Enter the required parameters under **IPv6 WAN Settings**.

Step 5 Tap **Save**.

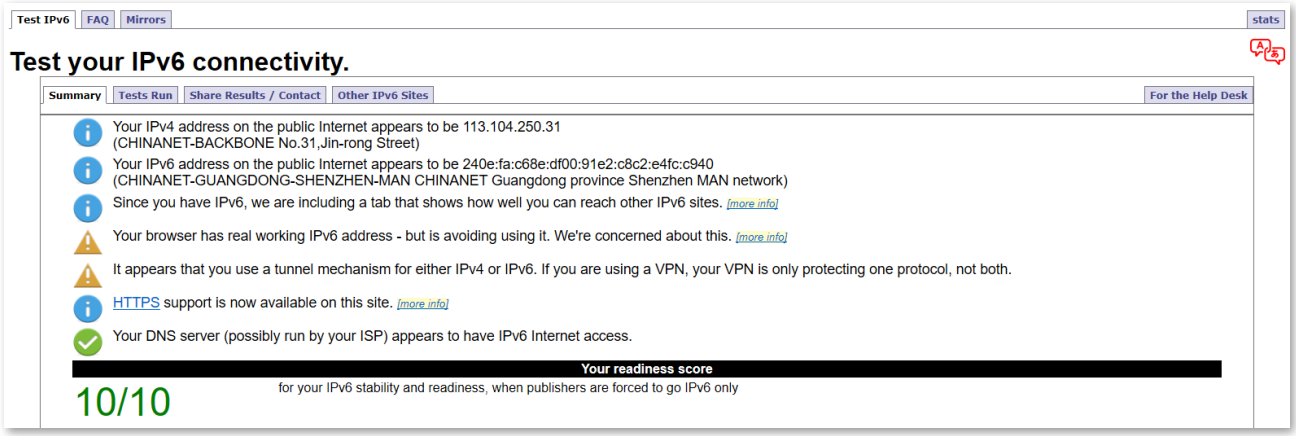


---End

IPv6 network test:

Start a web browser on a phone or a computer that is connected to the Mesh device, 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 succeeds and you can access IPv6 services.

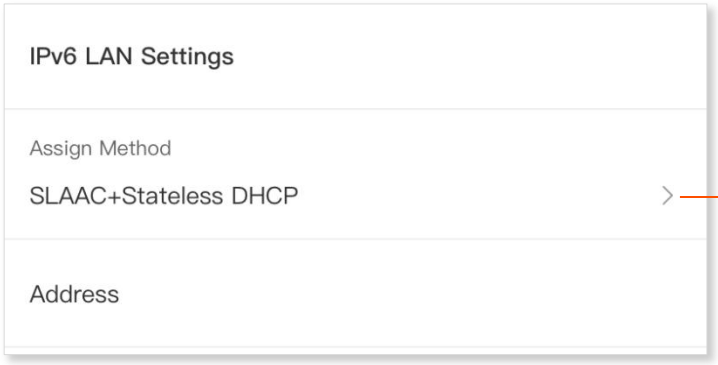


If the IPv6 network test fails, try the following solutions:

- Ensure that devices connected to Mesh device obtain their IPv6 address through DHCP.
- Consult your ISP for help.

IPv6 LAN settings

You can change the IPv6 LAN settings here.



Tap to select method that the router assigns IPv6 address to its clients.

Three assignment methods of IPv6 LAN are as follows:

- **DHCPv6:** Dynamic Host Configuration Protocol for IPv6 (DHCPv6) indicates that a client obtains the complete IPv6 address information from the DHCPv6 server, including the DNS server address. The gateway address is obtained through Router Advertisement (RA).
- **SLAAC + Stateless DHCP:** It indicates that a client obtains the IPv6 prefix and gateway address through RA, and DNS server address from the DHCPv6 server. And the client generates its unique IPv6 address using the IPv6 prefix contained in the RA and interface ID which is generated using the EUI-64 method or generated randomly by the client.
- **SLAAC+RDNSS:** It indicates that a client obtains an IPv6 prefix and gateway address through RA and DNS server address from the RDNSS option. And the client generates its unique IPv6 address using the IPv6 prefix contained in the RA and interface ID which is generated using the EUI-64 method or generated randomly by the client.

3.7.9 LAN settings

The DHCP Server of the Mesh device can assign IP address, subnet mask, default gateway and DNS server address to clients within the LAN.

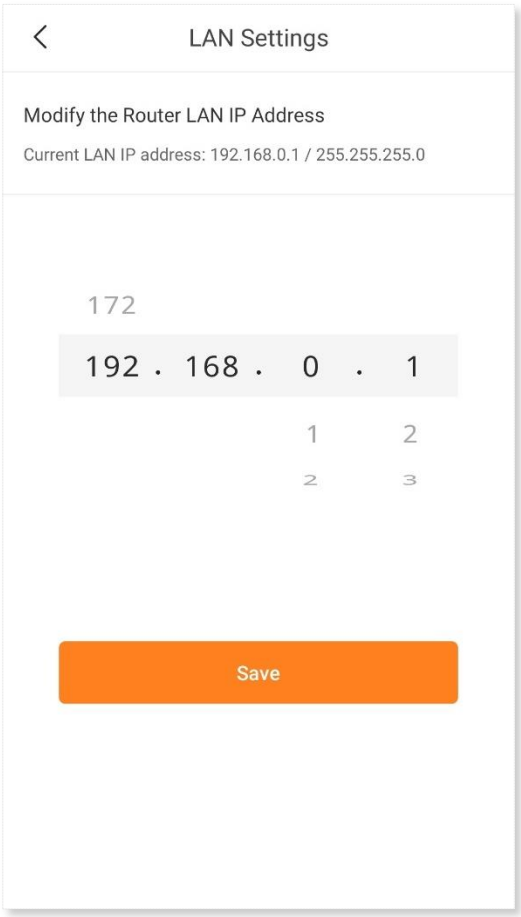
Generally, you are not required to change the settings for the DHCP server of the Mesh device, unless an IP address conflict occurs; for example, if the WAN IP address obtained by the Mesh device is at the same network segment as its LAN IP address, or the IP address of the client of the Mesh device is 192.168.5.1.

Procedure:

Step 1 Run the Tenda WiFi App, and choose **Settings** > **LAN Settings**.

Step 2 Select a LAN IP address for the Mesh device.

Step 3 Tap **Save**.



---End

After the setting completes, clients within the LAN are assigned with IP addresses based on the new LAN IP address of the Mesh device when they request new IP addresses.

3.7.10 DHCP server

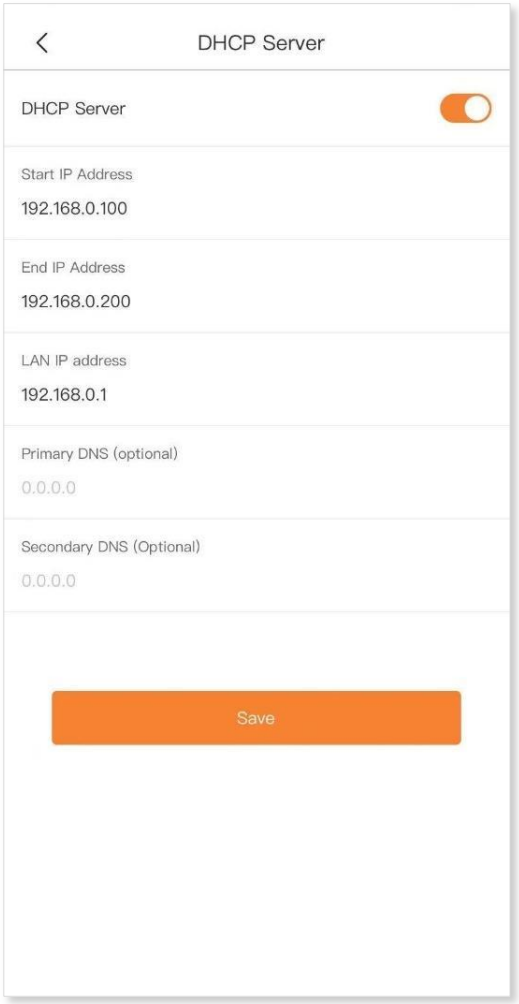
The Dynamic Host Configuration Protocol (DHCP) is an automatic configuration protocol used on IP networks. If you enable the built-in DHCP server on this device, the TCP/IP protocol settings will be automatically configured for all PCs in the LAN, including IP address, subnet mask, gateway, and DNS.

Procedure:

Step 1 Run the Tenda WiFi App, and choose **Settings** > **Advanced** > **DHCP Server**.

Step 2 Specify the **Start IP Address**, **End IP Address**, **LAN IP Address**, **Primary DNS (Optional)** and **Secondary DNS (Optional)**.

Step 3 Tap **Save**.



---End

3.7.11 Static IP reservation

Through the Static IP Reservation function, specified clients can always obtain the same IP address when connecting to the Mesh device, ensuring that the port forwarding or port mapping, DDNS, DMZ host and other functions are normal. This function takes effect only when the DHCP server function of the Mesh device is enabled.

Assign static IP addresses to LAN clients:

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

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

Solution: You can configure the DHCP reservation function to reach the goal. Assume that:

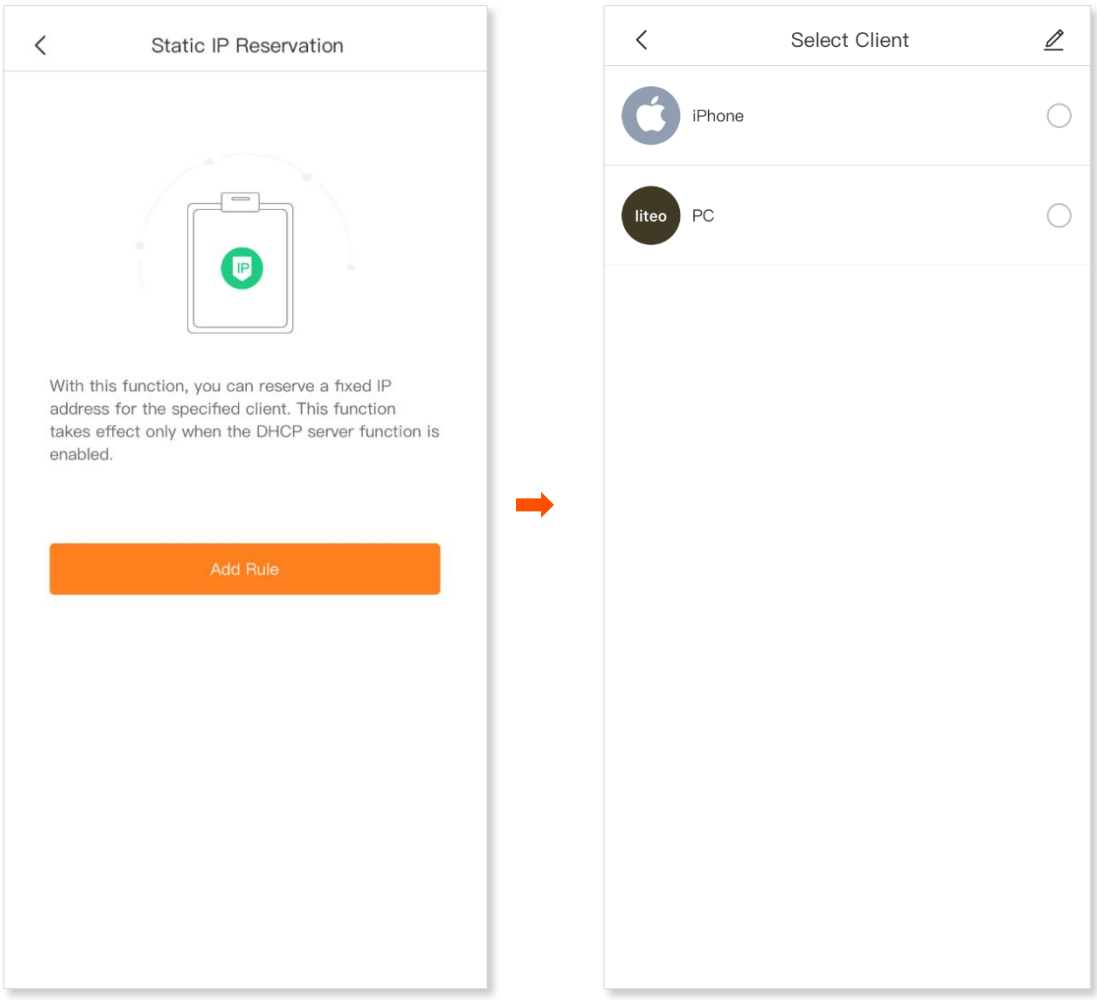
- Fixed IP address for the server: 192.168.0.143
- MAC address of the FTP server host: C0:9A:D0:5B:28:70

Procedure:

Step 1 Run the Tenda WiFi App, and choose **Settings** > **Advanced** > **Static IP Reservation**.

Step 2 Tap **Add Rule**.

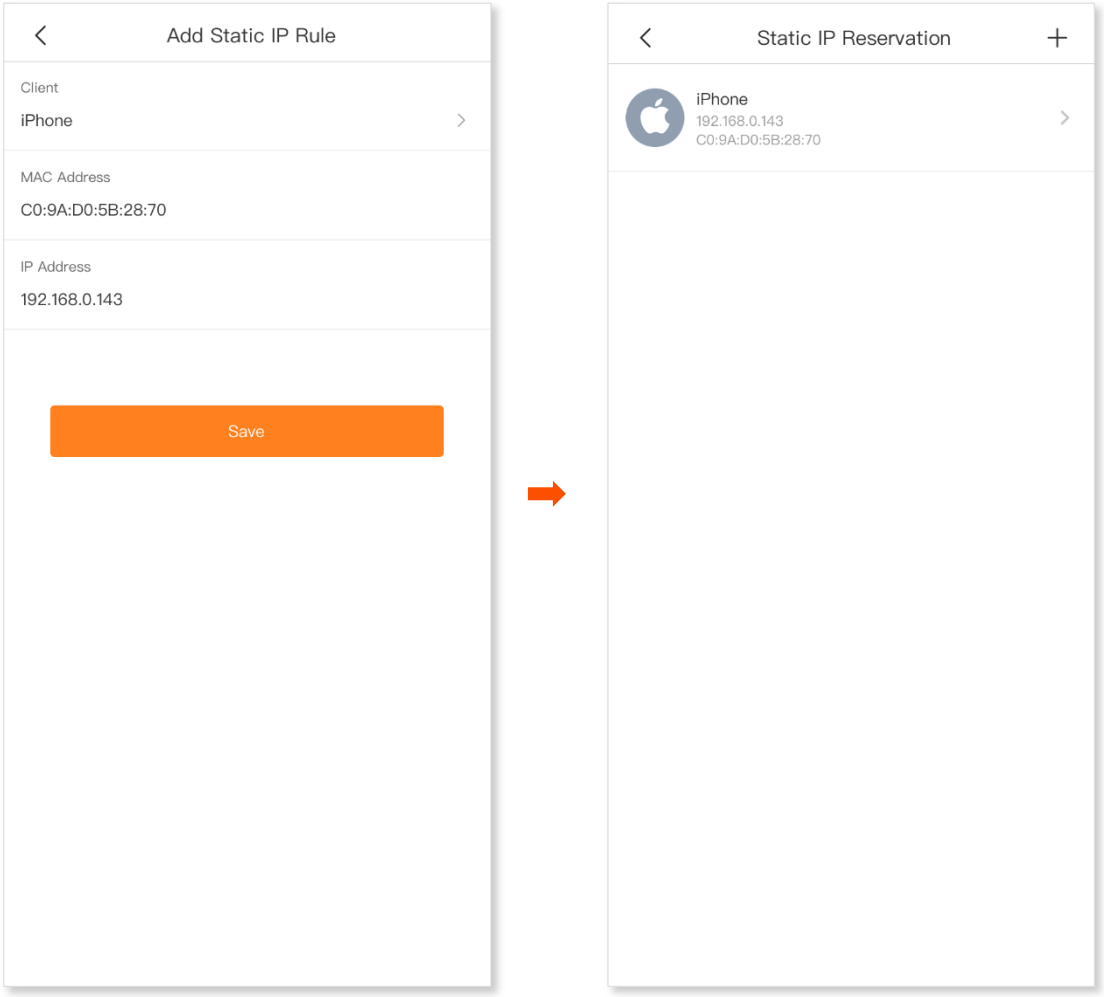
Step 3 Select the device to which the rule applies, which is **iPhone** in this example.



Step 4 Set up a port forwarding rule.

IP Address: IP address reserved for the client, which is **192.168.0.143** in this example

Step 5 Tap **Save**.



---End

After the settings complete, the FTP server host always gets the same IP address when connecting to the Mesh device.

3.7.12 DNS

If clients connected to the WiFi network cannot access the websites using the domain names whereas the IP address works, a DNS resolution problem may exist. You can try changing the DNS settings to solve the problem.

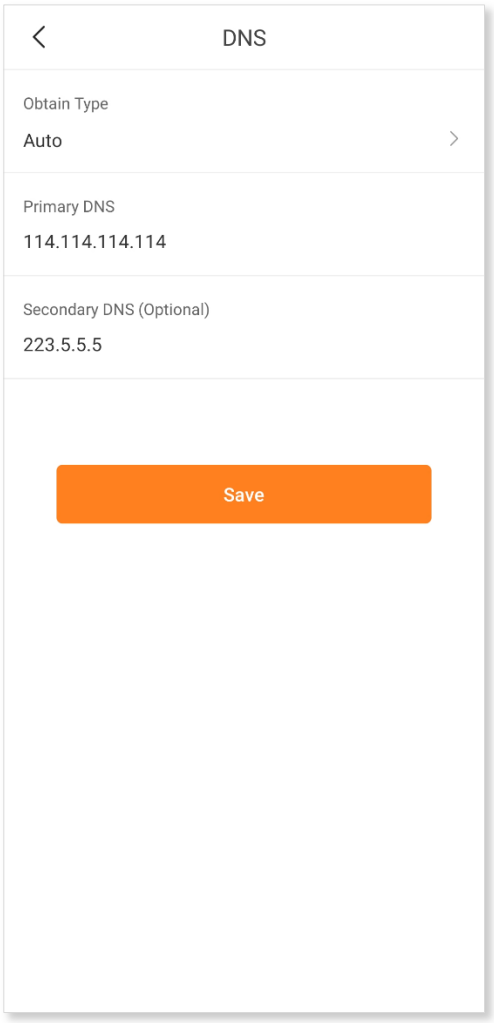
Procedure:

Step 1 Run the Tenda WiFi App, and choose **Settings** > **Advanced** > **DNS**.

Step 2 Tap **Obtain Type**, and select **Auto** or **Manual**.

If you select **Manual**, enter the correct DNS IP address in **Primary DNS**. If you have another DNS server IP address, enter it in **Secondary DNS (Optional)**.

Step 3 Tap **Save**.



---End

3.7.13 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.

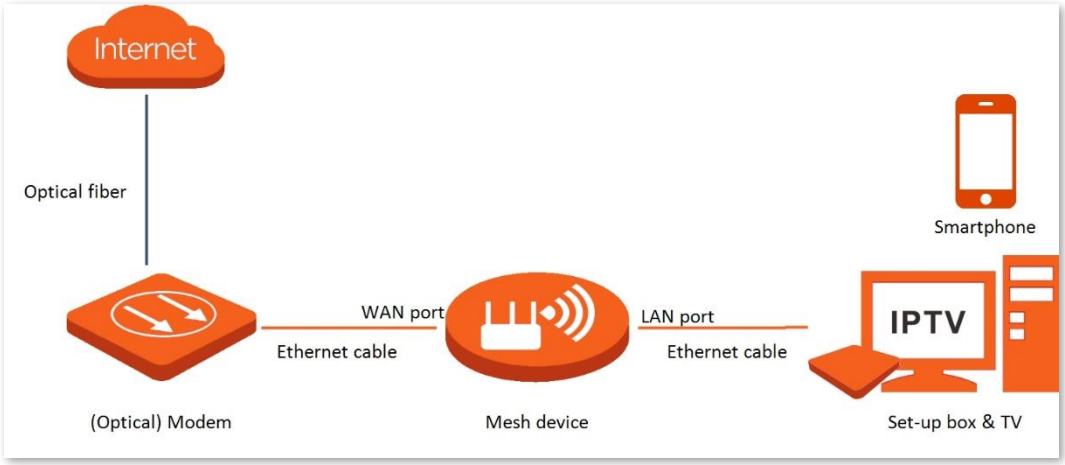
- **Multicast**: If you want to watch multicast videos from the WAN side of the Mesh device on your computer, you can enable the multicast function of the Mesh device.
- **STB** (set-top box): If the IPTV service is included in your broadband service, you can enjoy both internet access through the Mesh device and rich IPTV contents with a set-top box when it is enabled.

Watch IPTV programs through the Mesh device

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 Mesh device.

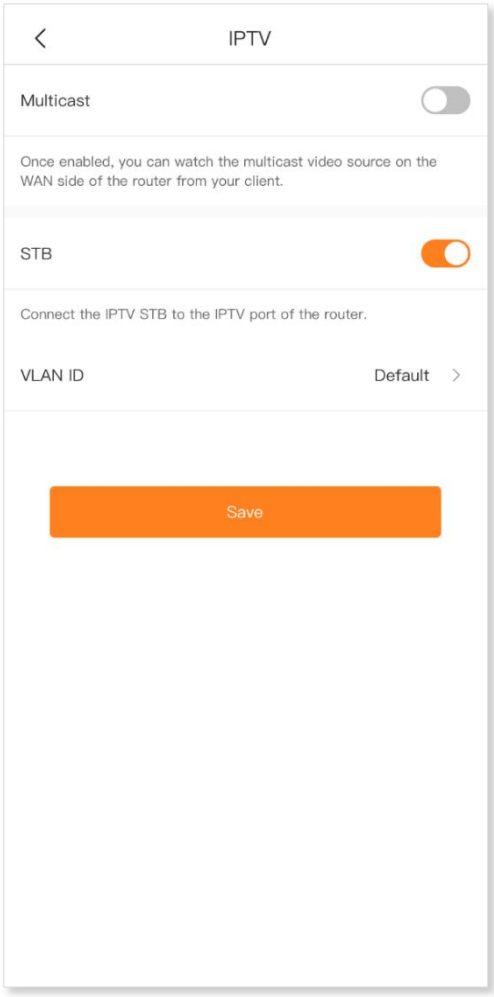
Solution: You can configure the IPTV function to reach the goal.



Procedure:

Step 1 Set your Mesh device.

1. Run the Tenda WiFi App, and choose **Settings** > **Advanced** > **IPTV**.
2. Enable the **STB** function.
3. Tap **Save**.



Step 2 Configure the set top box.

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

---End

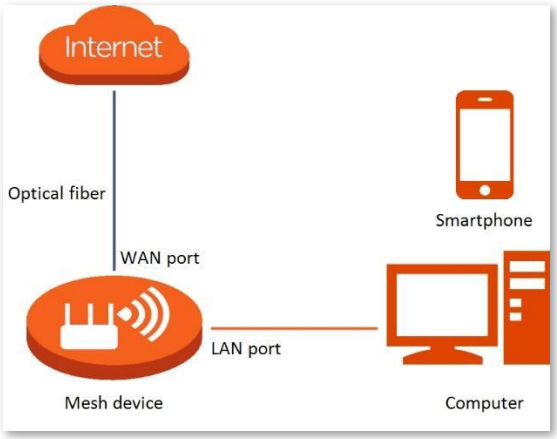
After the setting completes, you can watch IPTV programs on your TV.

Watch multicast videos through the Mesh device

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.

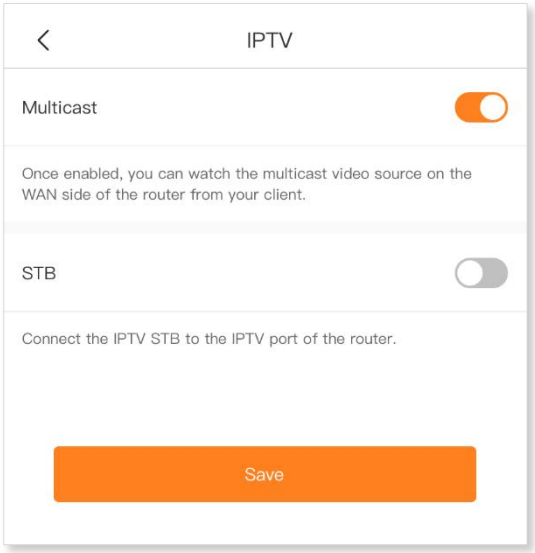


Procedure:

Step 1 Run the Tenda WiFi App, and choose **Settings** > **Advanced** > **IPTV**.

Step 2 Enable the **Multicast** function.

Step 3 Tap **Save**.



---End

After the setting completes, you can watch multicast videos on your computer.

3.7.14 MESH button

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

TIP

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

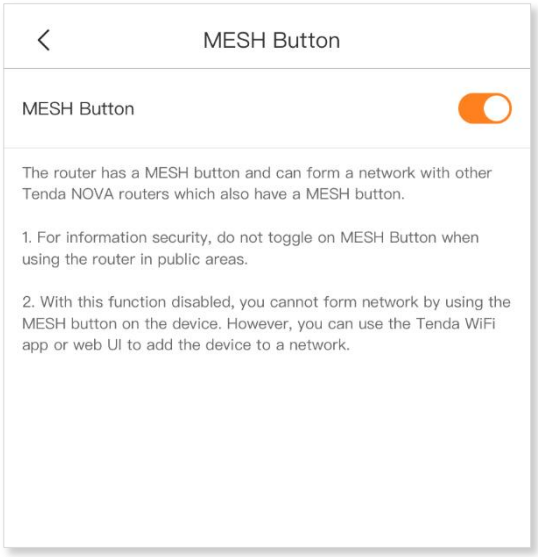
The Mesh device supports three methods for mesh networking:

- Method 1: Press the **MESH** button for about 1 to 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** button of another device for 1 to 3 seconds to negotiate with this device.
- Method 2: Run the **Tenda WiFi** App and manage the network, tap + on **My WiFi** page, and follow the on-screen instructions.
- Method 3: Log in to web UI of the node, click  on **Network Status** page, and follow the on-screen instructions.

Procedure:

Step 1 Run the Tenda WiFi App, and choose **Settings** > **Advanced** > **MESH Button**.

Step 2 Enable or disable the **MESH Button** function as required.



---End

3.7.15 WPS

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

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.

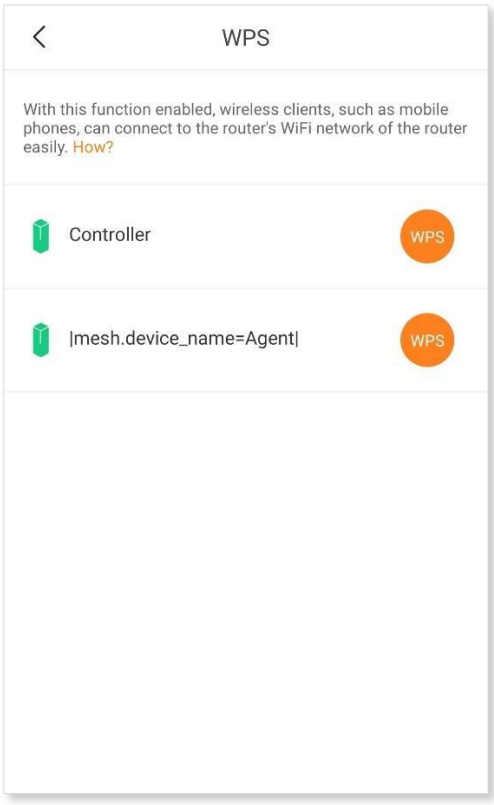
Procedure:

Step 1 Run the Tenda WiFi App, and choose **Settings** > **Advanced** > **WPS**.

Step 2 Tap the WPS button on the row where the target node resides.

The LED indicator on the Mesh device blinks as the WPS function is enabled.

Step 3 Enable the WPS function on the WPS-supported device within 2 minutes to start WPS negotiation.



---End

3.7.16 Port mapping

The Port Forwarding function enables you to access your LAN resources, such as resources on a web server or an FTP server, through the internet.

TIP

- Before the configuration, ensure that the Mesh device obtains a public IP address. Otherwise, this function will not work properly. Common IPv4 addresses are categorized 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.
- ISPs may block unreported web services from being accessed with the default port number 80. Therefore, when the default WAN port number is 80, please change it to an uncommon port number (1024 to 65535), such as 9999.
- The internal port number can be different from the external port number.

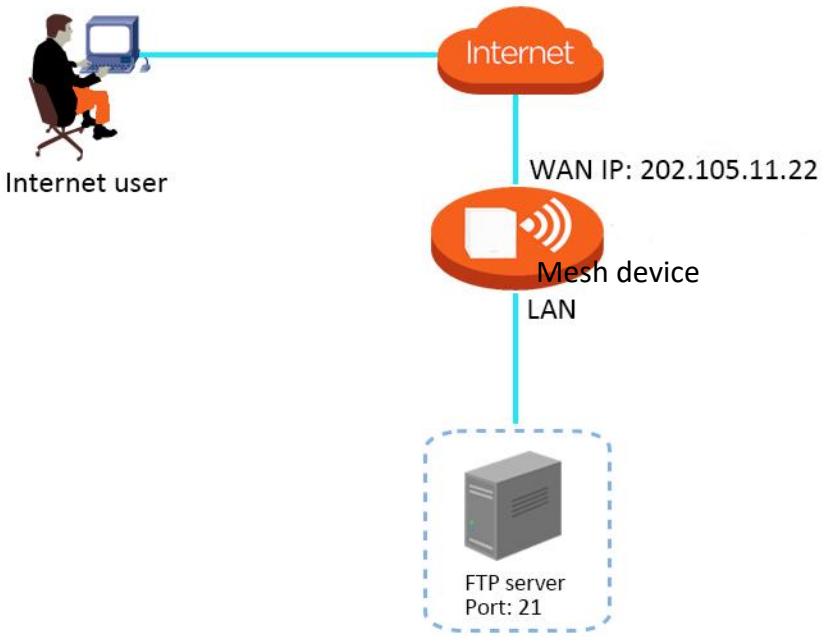
An example of configuring the port forwarding function:

Scenario: You have an FTP server within the LAN.

Goal: Open the FTP server to internet users and enable family members to access the resources of the FTP server when they are not at home.

Solution: You can configure the port forwarding function to reach the goal. Assume that:

- WAN IP address of the Mesh device: 202.105.11.22
- Service port of the FTP server: 21



Procedure:

Step 1 Run the Tenda WiFi App, and choose **Settings** > **Advanced** > **Port Forwarding**.

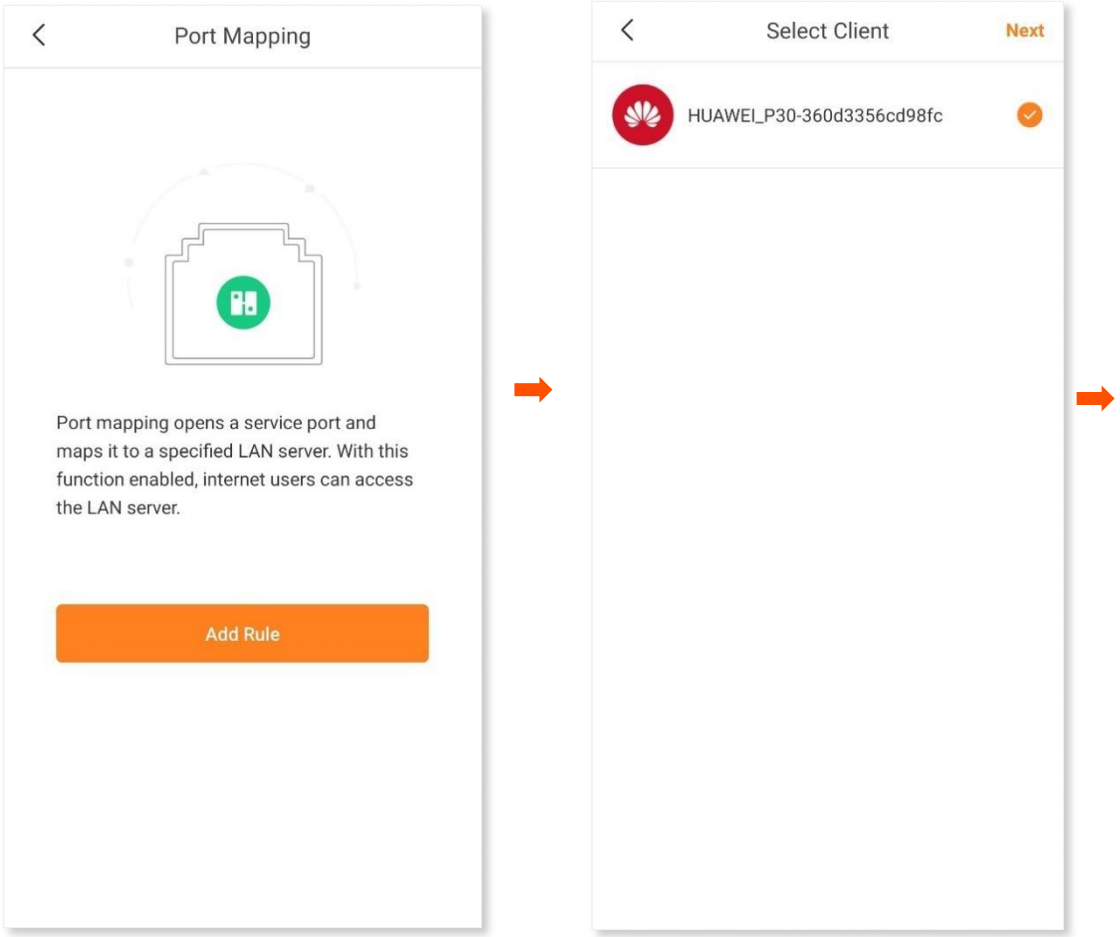
Step 2 Tap **Add Rule**.

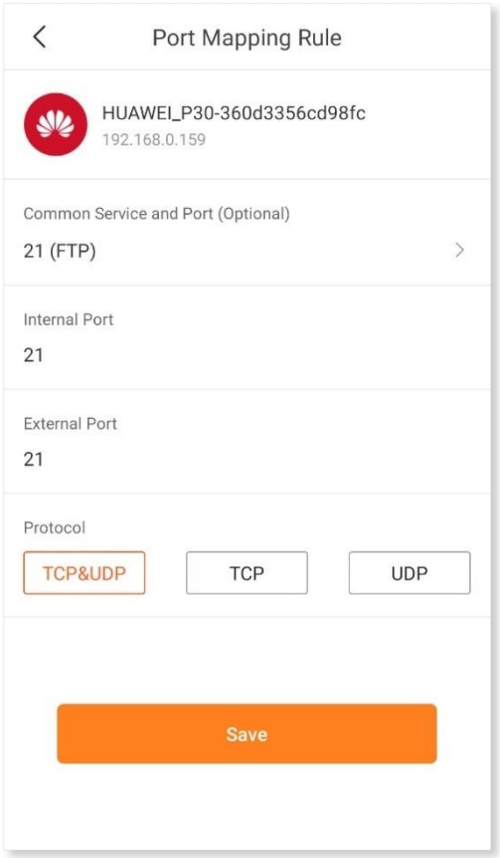
Step 3 Select the device to which the rule applies, and tap **Next**.

Step 4 Set up a port forwarding rule.

- **Common Protocol and Port (Optional)**: Optional. The App presets some common protocols and their port numbers, such as FTP and TELNET. You can select one as required, and the **Internet Port** and **External Port** are automatically populated. **FTP** is selected in this example.
- **Internal Port**: The service port of the server on the LAN, which is **21** in this example.
- **External Port**: The port opened for internet users, which is **21** in this example.
- **Protocol**: The protocol of the service. If you are not sure about it, you can select **TCP&UDP**.

Step 5 Tap **Save**.





---End

After the setting completes, internet users can visit "**Protocol name://WAN port IP address of the Mesh device**" to access LAN resources on the FTP server. If the internal port number is not kept the default, internet users need to visit "**Protocol name://WAN port IP address of the Mesh device: External port number**" to access the resources on the FTP server.

The address in this example is **ftp:// 202.105.11.22**. You can find the WAN port IP address of the Mesh device on the internet connection page.

NOTE

If you cannot access the FTP server after the setting completes, try the following solutions:

- Ensure that the WAN IP address of the Mesh device is a public IP address, and the internal port number you entered is correct.
- Security software, antivirus software, and the built-in OS firewall of the server may cause port forwarding function failures. Disable them when using this function.
- Manually set an IP address for the web server to avoid the service disconnection caused by the dynamic IP address.

3.7.17 UPnP

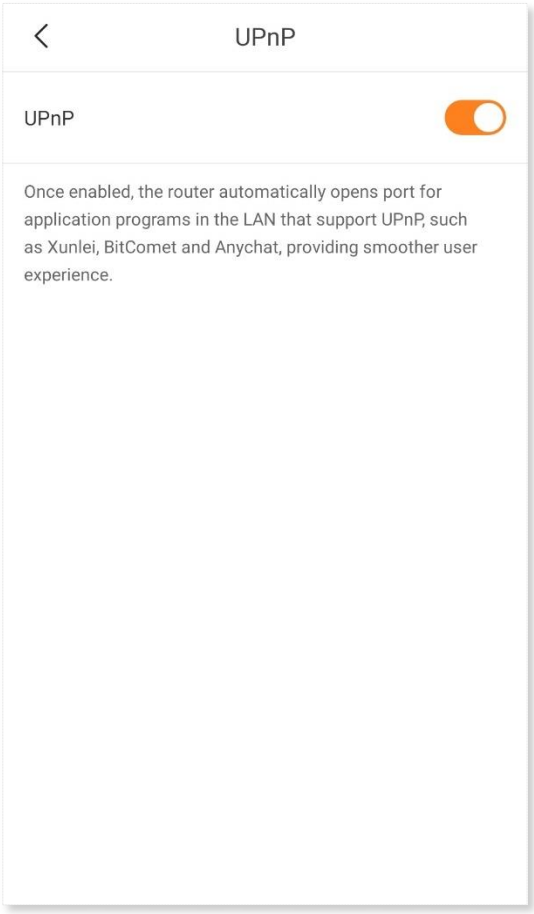
UPnP is short for Universal Plug and Play. This function enables the Mesh device to open port automatically for UPnP-based programs. It is generally used for P2P programs, such as BitComet and AnyChat, and helps increase the download speed.

This function is enabled by default.

Procedure:

Step 1 Run the Tenda WiFi App, and choose **Settings** > **Advanced** > **UPnP**.

Step 2 Enable or disable the **UPnP** function as required.



---End

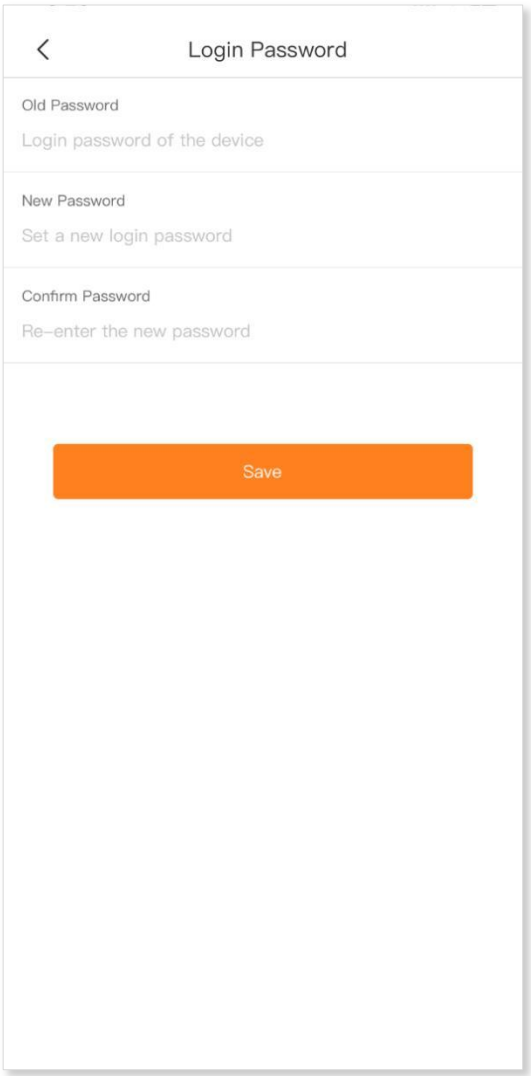
3.8 System Settings

3.8.1 Login password

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

Run the Tenda WiFi App, and choose **Settings** > **Login Password**.

If you have already set a login password, you can change the password on this page and the old password is required.



3.8.2 Auto system maintenance

This function reboots the Mesh devices regularly to keep them in the best working condition. You can set up the auto system maintenance function here:

Procedure:

Step 1 Run the Tenda WiFi App, and choose **Settings** > **Auto System Maintenance**.

Step 2 Enable **Auto System Maintenance**.

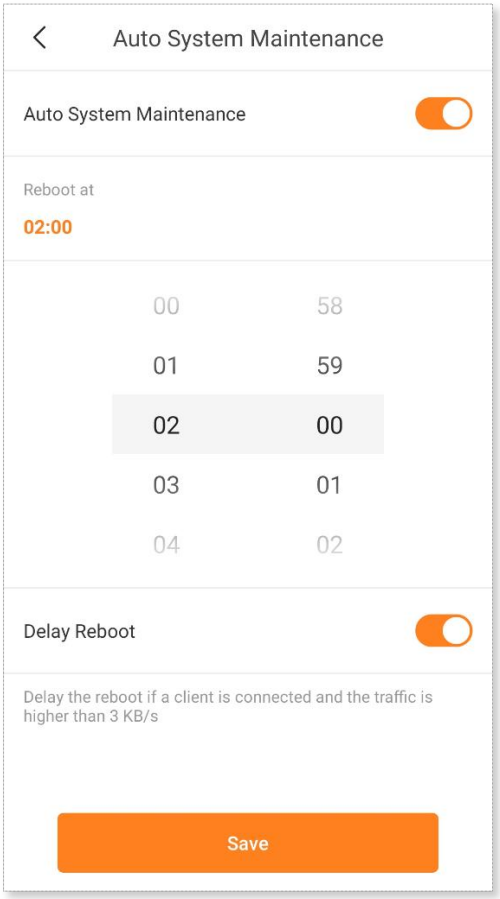
Step 3 Select a reboot time for **Reboot at**.

You are recommended to set a time when your network is idle. **02:00** is used as an example.

Step 4 Select the days on which the rule takes effect.

Step 5 Enable or disable the **Delay Reboot** function as required.

Step 6 Tap **Save**.



TIP

If the devices are exchanging data and the traffic is greater than 3 KB/s, the devices will not reboot at the specified time even when the **Delay Reboot** function is disabled. Within 2 hours after the specified reboot time, the devices keep detecting the traffic, and reboot once when the traffic is lower than 3 KB/s. Otherwise, the devices will reboot the next day at the specified reboot time.

---End

3.8.3 Firmware upgrade

Tenda is dedicated to improving its products to let users enjoy better performance. Please update the firmware when the App notifies that a new firmware version is available.

NOTE

Do not remove the power supply of the Mesh devices during the upgrade.

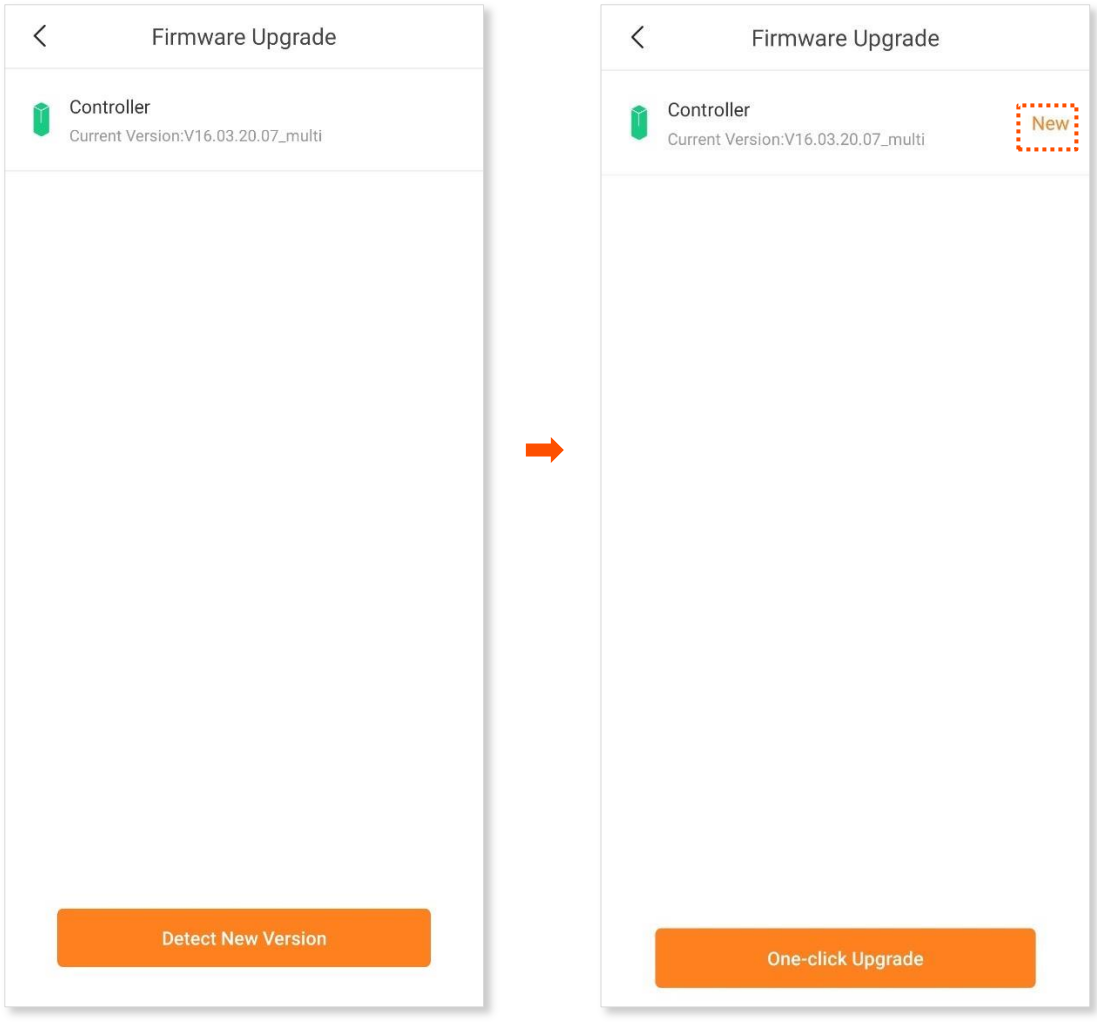
Procedure:

Step 1 Run the Tenda WiFi App, and choose **Settings** > **Firmware Upgrade**.

Step 2 Tap **Detect New Version**.

New appears if a new firmware version is detected.

Step 3 Tap **One-click Upgrade** to upgrade.



---End

4 FAQ

4.1 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 node.
  - 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 primary node 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 Mesh device to factory settings.

4.2 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 Mesh device.
- Ensure that the Ethernet cable is not damaged and well-connected, and the modem is powered on.
- If the problem persists, please contact your ISP.

4.3 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 Mesh devices.

4.4 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:
  - If you used the default password and forgot it, find it on the bottom label.

  - If you have changed the 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 used different passwords for Wi-Fi login and web UI login:
  - The default Wi-Fi password can be found on the bottom label. If you have changed the password, log in to the web UI, and navigate to Wi-Fi settings to find the password.
  - If you also 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.

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 Mesh device.
	Wi-Fi password	
IPv6		Disabled
Unify 2.4 GHz & 5 GHz		Enabled
Guest Wi-Fi		Disabled
MESH button		Enabled
VPN		Disabled
IPTV		Disabled
App remote management		Enabled
MAC address filter		Disabled
DMZ host		Disabled

Parameter	Default value
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
RA	Router Advertisement

Acronym or Abbreviation	Full Spelling
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
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