

Tenda

User Guide

Whole Home Mesh Wi-Fi System



Copyright Statement

© 2023 Shenzhen Tenda Technology Co., Ltd. All rights reserved.

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

Disclaimer

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

Preface

Thank you for choosing Tenda!

This user guide walks you through all functions on the Whole Home Mesh Wi-Fi System, which can be managed on both the web UIs (for computers and mobile clients) and App. All the screenshots and product figures herein, unless otherwise specified, are taken from MX15 Pro.





- The web UI of different models may differ. The web UI actually displayed shall prevail.
- The Whole Home Mesh Wi-Fi 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: <i>XX:XX:XX:XX:XX:XX</i>
UI control	Bold	On the Policy page, click the OK button.
Message	“ ”	The “Success” message appears.

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

Symbol	Meaning
	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configuration, loss of data or damage to device.
	This format is used to highlight a procedure that will save time or resources.

For more documents

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

The related documents are listed as below.

Document	Description
Datasheet	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.



<https://www.tendacn.com/>

Website



support.nova@tenda.com.cn

Email

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 user guide was introduced.

Version	Date	Description
V1.1	2023-2-24	<p>Added function description about 6 GHz WiFi network for MX21 Pro/EX21 Pro/Mesh21XEP in the following sections:</p> <p>Web UI operations (computer)</p> <ul style="list-style-type: none">- 2.5 Wi-Fi settings- 2.8.2 Guest Wi-Fi- 2.8.8 Advanced Wi-Fi settings <p>App operations</p> <ul style="list-style-type: none">- 3.6.2 WiFi settings- 3.6.3 Guest network <p>Web UI operations (mobile client)</p> <ul style="list-style-type: none">- 4.6 Wi-Fi settings- 4.9.1 Guest Wi-Fi
V1.0	2023-1-18	Original publication.

Contents

1	Get to know your device	1
1.1	Product overview	2
1.2	Appearance	3
1.2.1	LED indicator	3
1.2.2	Buttons and Ports	5
1.2.3	Label	8
2	Web UI operations (computer).....	9
2.1	Quick setup	10
2.1.1	Connect your primary node	10
2.1.2	Connect your primary node to the internet.....	11
2.1.3	Extend your network	17
2.2	Web UI (computer)	18
2.2.1	Log in to the web UI (computer)	18
2.2.2	Log out of the web UI (computer).....	19
2.2.3	Change the language	19
2.3	Network status	20
2.3.1	Network status	20
2.3.2	Network topology.....	21
2.4	Internet settings.....	30
2.4.1	Overview	30
2.4.2	Access the internet with a PPPoE account	33
2.4.3	Access the internet through a dynamic IP address	34
2.4.4	Access the internet with a set of static IP address information.....	35

2.4.5 Set up dual access connection	36
2.5 Wi-Fi settings	38
2.5.1 Basic settings	38
2.5.2 Separate the Wi-Fi networks	41
2.5.3 Unify the Wi-Fi networks.....	42
2.5.4 Disable or Enable the WiFi networks	43
2.6 Client management.....	45
2.6.1 View client information	45
2.6.2 Change a client name	47
2.6.3 Add a client to the blacklist	47
2.6.4 Remove a client from the blacklist.....	48
2.6.5 Delete an offline client	49
2.7 Parental control.....	50
2.7.1 Create a parental control rule	50
2.7.2 Other operations on the parental control rules.....	54
2.8 More.....	55
2.8.1 Router information.....	55
2.8.2 Guest Wi-Fi.....	59
2.8.3 Working mode	62
2.8.4 IPv6.....	67
2.8.5 Network diagnosis	73
2.8.6 TR069.....	74
2.8.7 Smart power saving.....	77
2.8.8 Advanced Wi-Fi settings.....	79
2.8.9 Network settings	85
2.8.10 Advanced	101
2.8.11 System settings.....	122

3 App operations..... 133

3.1 App download and installation	134
3.2 Registration and binding	135
3.2.1 Register a Tenda account.....	135
3.2.2 Log in to Tenda WiFi App.....	138
3.2.3 Bind the administrator account	140
3.3 Quick setup	141
3.3.1 Connect your primary node to the internet.....	141
3.3.2 Extend your network.....	143
3.4 Management type.....	145
3.4.1 Local management	145
3.4.2 Remote management.....	145
3.5 My WiFi	146
3.5.1 View managed nodes	147
3.5.2 View internet status	148
3.5.3 Add a node	150
3.5.4 Manage nodes	154
3.5.5 Manage connected clients	156
3.6 Common settings	158
3.6.1 Internet settings	159
3.6.2 WiFi settings	164
3.6.3 Guest network.....	166
3.6.4 Bandwidth test	167
3.6.5 Parental control	169
3.6.6 Blacklist.....	177
3.6.7 LED indicator	179
3.6.8 Experience monthly report	181
3.6.9 Working mode	182
3.6.10 IPv6.....	185

3.6.11 LAN settings.....	192
3.6.12 DHCP server.....	194
3.6.13 Static IP reservation.....	195
3.6.14 DNS.....	198
3.6.15 IPTV.....	199
3.6.16 MESH button	202
3.6.17 WPS	203
3.6.18 Port mapping.....	204
3.6.19 UPnP.....	207
3.7 System settings	208
3.7.1 Login password.....	208
3.7.2 Auto system maintenance.....	209
3.7.3 Firmware upgrade	210
3.7.4 Account authorization	211
3.8 My profile.....	214
4 Web UI operations (mobile client).....	215
4.1 Quick setup	216
4.1.1 Connect your primary node to the internet.....	216
4.1.2 Extend your network.....	218
4.2 Login.....	219
4.3 Router information	221
4.4 Network overview.....	225
4.4.1 Network status	225
4.4.2 Network topology.....	226
4.5 Internet settings.....	242
4.5.1 Overview	242
4.5.2 Access the internet with a PPPoE account.....	245
4.5.3 Access the internet through a dynamic IP address.....	246

4.5.4	Access the internet with a set of static IP address information	247
4.5.5	Set up dual access connection	248
4.6	Wi-Fi settings	250
4.6.1	Basic settings	250
4.6.2	Separate the Wi-Fi networks	253
4.6.3	Unify the Wi-Fi networks.....	255
4.7	Client management.....	257
4.7.1	View client information	257
4.7.2	Change a client name	259
4.7.3	Set speed limit.....	260
4.7.4	Add a client to the blacklist	262
4.7.5	Remove a client from the blacklist.....	264
4.7.6	Delete an offline client	264
4.8	Parental control.....	267
4.8.1	Create a parental control rule	267
4.8.2	Disable a parental control rule	273
4.8.3	Delete a parental control rule	273
4.9	More.....	275
4.9.1	Guest Wi-Fi.....	275
4.9.2	Smart power saving.....	277
4.9.3	Login password.....	278
4.9.4	IPv6.....	279
4.9.5	Reset a node.....	285
4.9.6	Reboot a node	286
4.9.7	Firmware upgrade	288
5	FAQ	290
5.1	Failed to access the web UI.....	290
5.2	Internet detection failed upon the first setup	291

5.3 Failed to find or connect my wireless network.....	292
5.4 Forgot my password.....	293
Appendixes	294
A.1 Factory settings.....	294
A.2 Acronyms and Abbreviations.....	296

1

Get to know your device

This chapter introduces the product in the following sections:

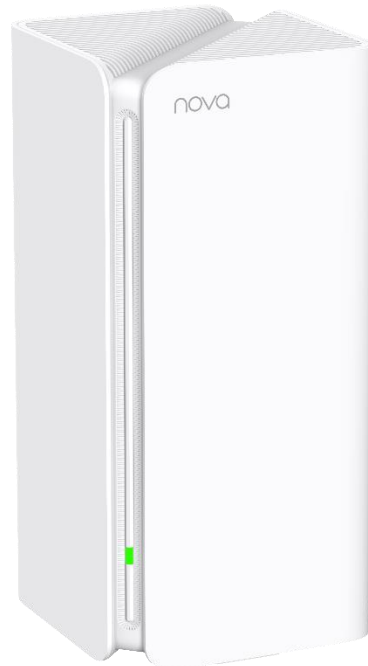
- [Product overview](#)
- [Appearance](#)

1.1 Product overview

The Whole Home Mesh Wi-Fi 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 UIs (for computers and mobile clients) and App. EasyMesh is also supported for the product to interwork with devices of other brands.


1.2 Appearance

1.2.1 LED indicator



(MX15 Pro used for example)

This product has only one LED 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 <ul style="list-style-type: none"> - 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

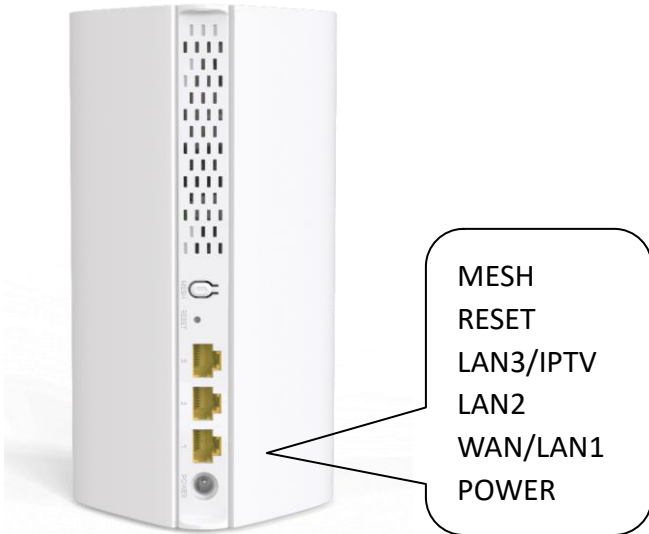
MX3&EX3




MESH, WAN/LAN, LAN, PWR
RST

Jack/Port/Button	Description
MESH	<p>Mesh button.</p> <ul style="list-style-type: none"> 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. <p> TIP</p> <p>Do not hold down the MESH button for 8 seconds unless necessary.</p>
RST	<p>Reset button.</p> <p>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.</p>
WAN/LAN	<p>WAN/LAN multiplexing port, WAN port by default.</p> <ul style="list-style-type: none"> 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.
LAN	<p>LAN/IPTV multiplexing port, LAN port by default.</p> <p>When the IPTV function is enabled, this port is used as the IPTV port only.</p>
PWR	Power jack.

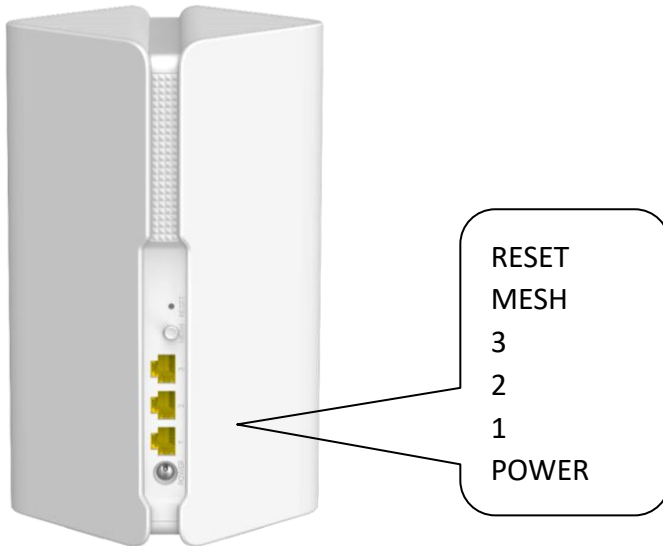
MX6&EX6&MX12&EX12



Jack/Port/Button	Description
MESH	<p>Mesh button.</p> <ul style="list-style-type: none"> - 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. <p> TIP</p> <p>Do not hold down the MESH button for 8 seconds unless necessary.</p>
RESET	<p>Reset button.</p> <p>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.</p>
LAN3/IPTV	<p>LAN/IPTV multiplexing port, LAN port by default.</p> <p>When the IPTV function is enabled, this port is used as the IPTV port only.</p>
LAN2	<p>LAN port.</p>
WAN/LAN1	<p>WAN/LAN multiplexing port, WAN port by default.</p> <ul style="list-style-type: none"> - 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.

Jack/Port/Button	Description
POWER	Power jack.

MX15 Pro&EX15 Pro&MX21 Pro&EX21 Pro



Jack/Port/Button	Description
RESET	<p>Reset button.</p> <p>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.</p>


Mesh button.

MESH

- 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.

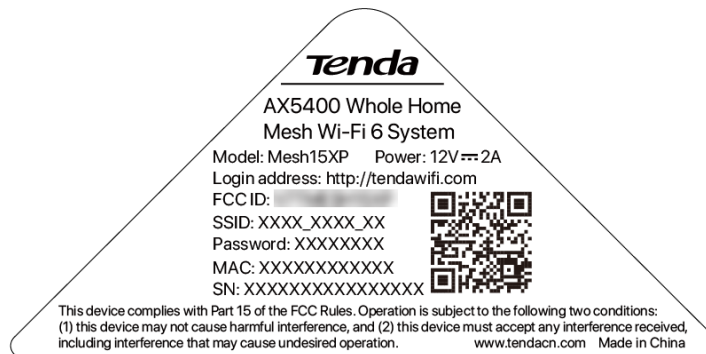


Do not hold down the **MESH** button for 8 seconds unless necessary.

Jack/Port/Button	Description
1/2/3	<p>WAN/LAN auto-adaptive port.</p> <p>You can connect to any port and the Mesh device will automatically determine how the port is used.</p> <p> NOTE</p> <p>When the IPTV function is enabled, you need to configure the IPTV port in IPTV.</p>
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 figure shows the label of MX15 Pro as an example:



Model: Specifies the device model.

Power: Specifies the power of the device.

Login Address/IP 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.

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

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

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

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

2

Web UI operations (computer)

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

- [Quick setup](#)
- [Brief introduction to the Web UI](#)
- [Network status](#)
- [Internet settings](#)
- [Wi-Fi settings](#)
- [Client management](#)
- [Parental control](#)
- [More advanced settings](#)

Some functions and operations are also available on the Tenda WiFi App and web UI (mobile client). For details, see [App operations](#) and [Web UI operations \(mobile client\)](#).

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:

- [Connect your primary node](#)
- [Connect your primary node to the internet](#)
- [Extend your network](#)

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 port of the primary node to your modem.



The WAN port of the primary node may vary with models.

- For MX3/EX3, connect to the **WAN/LAN** port.
 - For MX6/EX6/MX12/EX12, connect to the **WAN/LAN1** port.
 - For MX15 Pro/EX15 Pro/MX21 Pro/EX21 Pro, connect to any of **1, 2** and **3** ports.
-

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 port of the primary node to the LAN port of the Ethernet device.



The WAN port of the primary node may vary with models.

- For MX3/EX3, connect to the **WAN/LAN** port.
 - For MX6/EX6/MX12/EX12, connect to the **WAN/LAN1** port.
 - For MX15 Pro/EX15 Pro/MX21 Pro/EX21 Pro, connect to any of **1, 2** and **3** ports.
-

- 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:

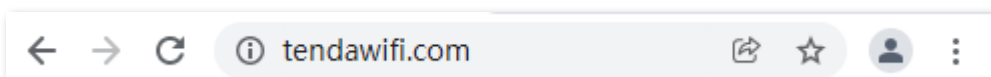
- Step 1** Use an Ethernet cable to connect your computer to the LAN port of the primary node.

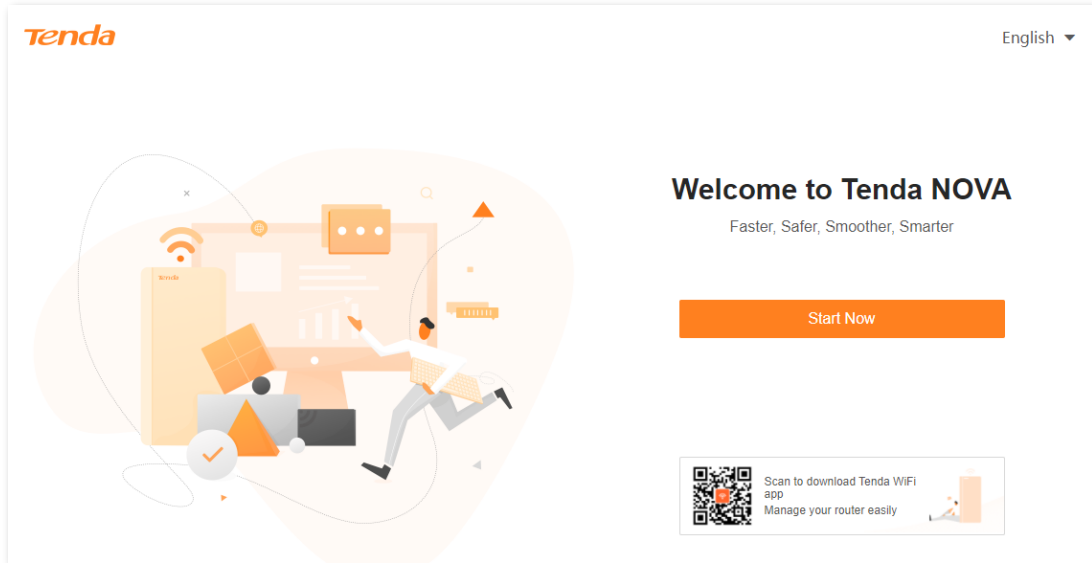


The LAN port of the primary node may vary with models.

- For MX3/EX3, connect to the **LAN** port.
 - For MX6/EX6/MX12/EX12, connect to the **LAN2** or **LAN3/IPTV** port.
 - For MX15 Pro/EX15 Pro/MX21 Pro/EX21 Pro, connect to any of **1, 2** and **3** ports.
-

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

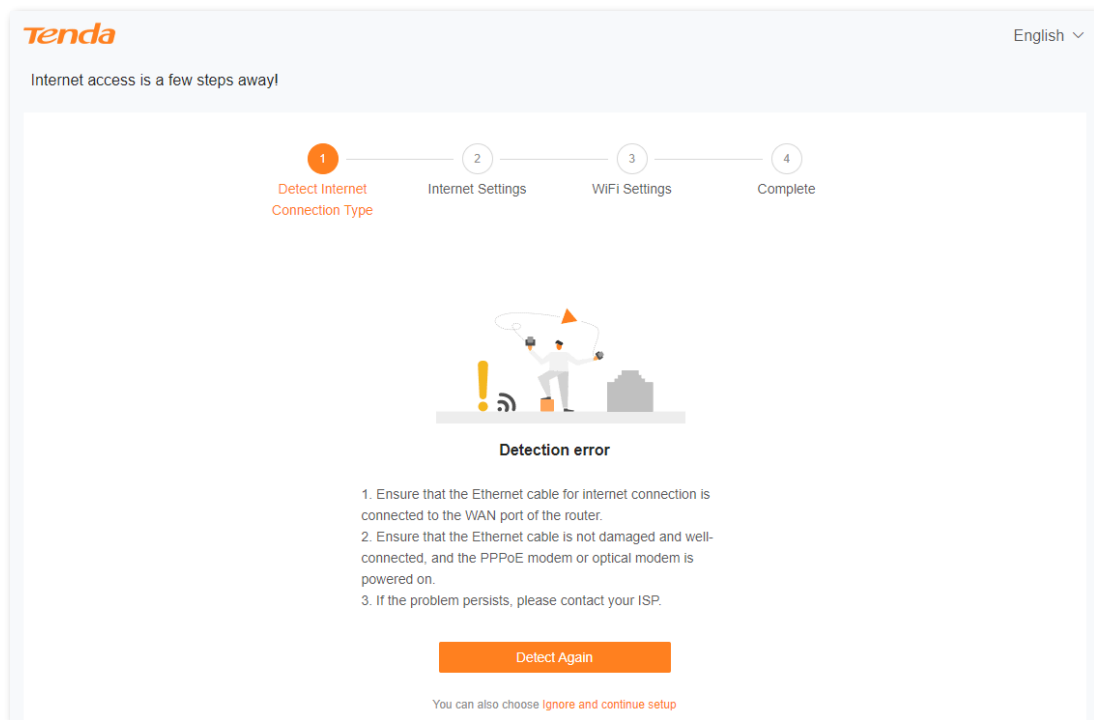


Step 3 Click **Start Now**.

The system will automatically detect your internet connection type.

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

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

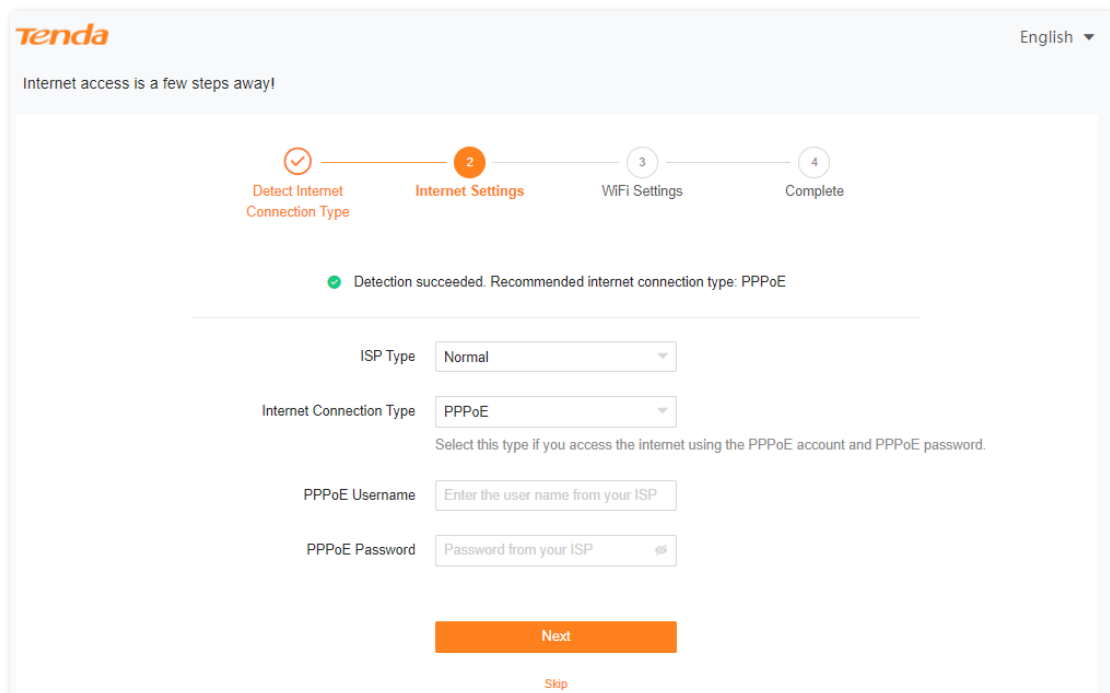


Step 4 Set **ISP Type**, **Internet Connection Type** and other parameters as required. Then, click **Next**.





TIP


For MX3/EX3/Mesh3X, you can click **Import PPPoE user name and password from your original router** to see how to import PPPoE user name and password from your original router. After you import your PPPoE user name and password into the router, **ISP Type**, **Internet Connection Type**, **PPPoE Username** and **PPPoE Password** will be set automatically.



The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
ISP Type	<p>Specifies the type of your ISP, such as Normal, Russia, Unifi, Maxis, Celcom, Digi and Manual. Parameters required for each option may differ.</p> <p> TIP</p> <p>The available options may vary with models. Refer to the product that you purchased.</p> <p>Refer to the following to choose your connection type:</p> <ul style="list-style-type: none"> - Normal, Unifi, Maxis, Celcom and Digi: Select these options when your ISP provides no setup information, except for the PPPoE user name and password, or static IP address information. - Russia: Select this option when your ISP provides dual access information, such as PPTP, L2TP connection information. - Manual: Select this option when your ISP provides VLAN ID information, besides the PPPoE user name and account, or static IP address. <p>If you are still not sure, contact your ISP for reference.</p>
Internet Connection Type	<p>Specifies how your Mesh device connects to the internet, including:</p> <ul style="list-style-type: none"> - 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	When the internet connection type is PPPoE, you need to enter the user name and password provided by your ISP to access the internet.
PPPoE Password	
IP Address	
Subnet Mask	When the internet connection type is static IP, you need to enter the fixed IP address information provided by your ISP.
Default Gateway	 TIP
Primary DNS	If your ISP provides only one DNS server, you can leave Secondary DNS blank.
Secondary DNS	
Address Type/DHCP	<p>When you set ISP Type to Russia, this parameter is required.</p> <p>It specifies the method for obtaining IP address information to access the “local” network, where the internal resources of the ISP are located.</p>

Parameter	Description
DNS Settings	<p>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.</p> <ul style="list-style-type: none"> - 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.
Server IP Address/Domain Name	<p>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.</p>
User Name	
Password	
Area	<p>When you set ISP Type to Maxis, Celcom or Digi, this parameter is required.</p> <p>It specifies the ISP area, including:</p> <ul style="list-style-type: none"> - Maxis: Maxis and Maxis-Special - Celcom: Celcom West(BIZ), Celcom West(HOME), Celcom East(BIZ) and Celcom East(HOME) - Digi: Digi-TM, Digi, Digi-CT Sabah and Digi-TNB
Internet VLAN ID	<p>When you select Manual for ISP Type, you can configure these parameters.</p>
IPTV VLAN ID	<p> TIP</p> <p>Internet VLAN ID is required, while IPTV VLAN ID is optional. Blank VLAN ID indicates that the IPTV function is disabled.</p>

Step 5 Set the Wi-Fi name, Wi-Fi password and login password as required, and click **Next**.



- 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.
- If you do not want to use a password, select **Not encrypted**. In this case, any client can access the network without a password. Selecting this option is not recommended as it leads to low network security. This option is only available for some models. Refer to the product that you purchased.

Tenda English ▾

Internet access is a few steps away!

Detect Internet Connection Type
 Internet Settings
 3 WiFi Settings
 4 Complete

WiFi Name:

WiFi Password:

Set WiFi password to router login password ⓘ

Login Password:

Confirm Password:

Next

[Previous](#)

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

Tenda English ▾

Internet access is a few steps away!

Detect Internet Connection Type
 Internet Settings
 WiFi Settings
 4 Complete

Configuration completes. You can access the internet now
 Current WiFi network is cut off. Please connect to the new WiFi network

WiFi Name:

WiFi Password:

Login Password:

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 information instructing how to extend the network with secondary nodes in the same kit is displayed. 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.

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 (computer)

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

- [Log in to the web UI](#)
- [Log out of the web UI](#)
- [Change the language](#)

2.2.1 Log in to the web UI (computer)

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

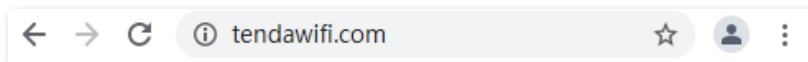
Step 1 Use an Ethernet cable to connect your computer to the LAN port of the primary node.



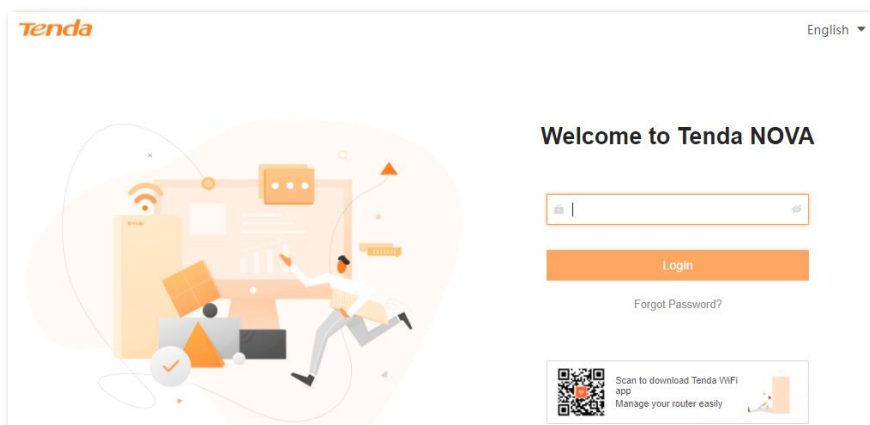
The LAN port of the primary node may vary with models.

- For MX3/EX3, connect to the **LAN** port.
- For MX6/EX6/MX12/EX12, connect to the **LAN2** or **LAN3/IPTV** port.
- For MX15 Pro/EX15 Pro/MX21 Pro/EX21 Pro, connect to any of **1, 2** and **3** ports.

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 login password, and click **Login**.



- If this is your first login and internet access is not configured, go to [Connect your primary node to the internet](#).
- The login password is the one that you specified in [Step 5](#) in [Connect your primary node to the internet](#). It is case-sensitive. If you forgot the login password, go to [Forgot my password](#).

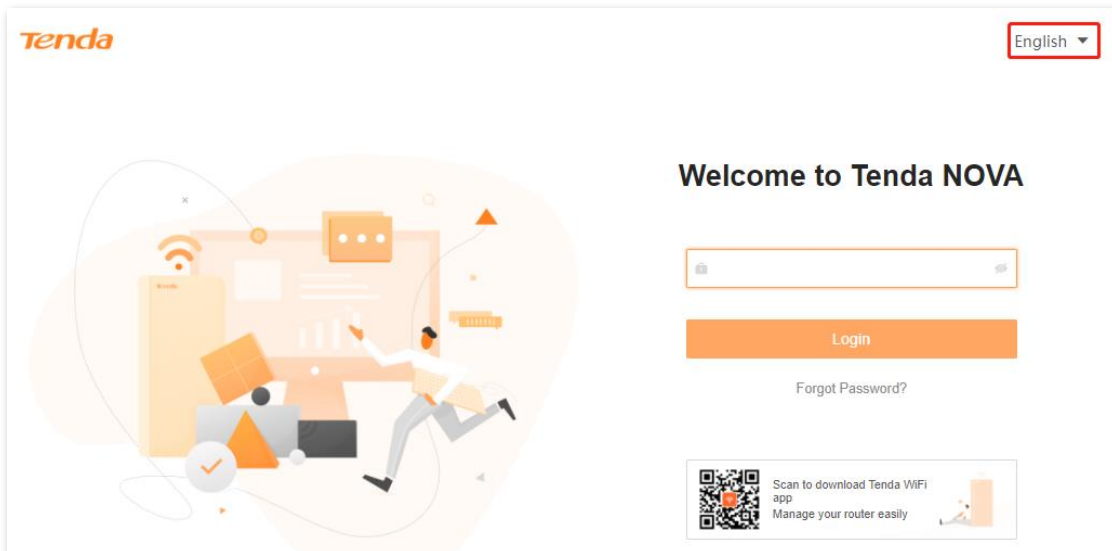
---End

2.2.2 Log out of the web UI (computer)

If you log in to the web UI (computer) 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.



2.3 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:

- [Network status](#)
- [Network topology](#)

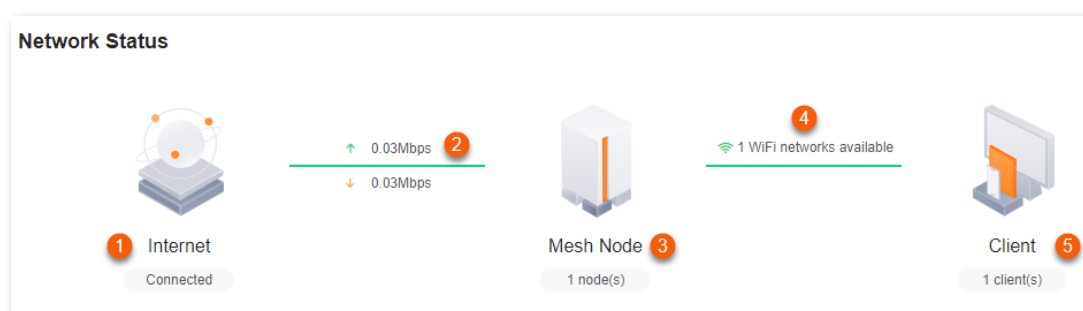
2.3.1 Network status

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	<p>Indicates the internet connection status.</p> <ul style="list-style-type: none"> - Connected: The primary node is connected to the internet successfully. - Disconnected: The primary node is disconnected from the internet.
2	<p>The information here varies depending on the internet connection status.</p> <ul style="list-style-type: none"> - 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.

No.	Description
3	Indicates the number of available Wi-Fi networks.
4	Indicates the Wi-Fi name and frequency band.
5	Indicates the number of clients connected in the network, including secondary Mesh nodes.

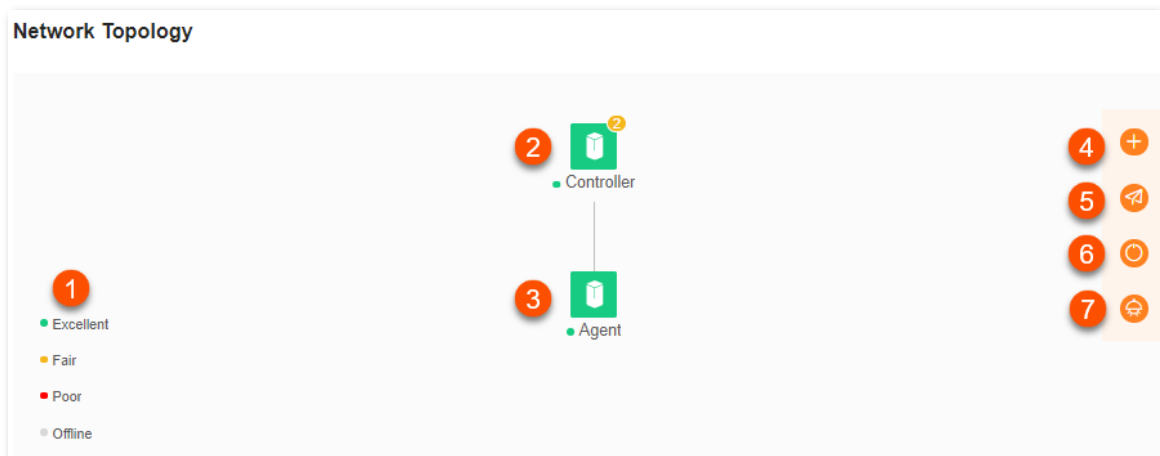
2.3.2 Network topology

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. <ul style="list-style-type: none"> - 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	Form a network topology. For details, see Controller information and Agent information .
3	
4	Used to Add a node .
5	Used for One-click optimization .

No.	Description
6	Used to Reboot all nodes .
7	Used to Turn on/off all indicators .

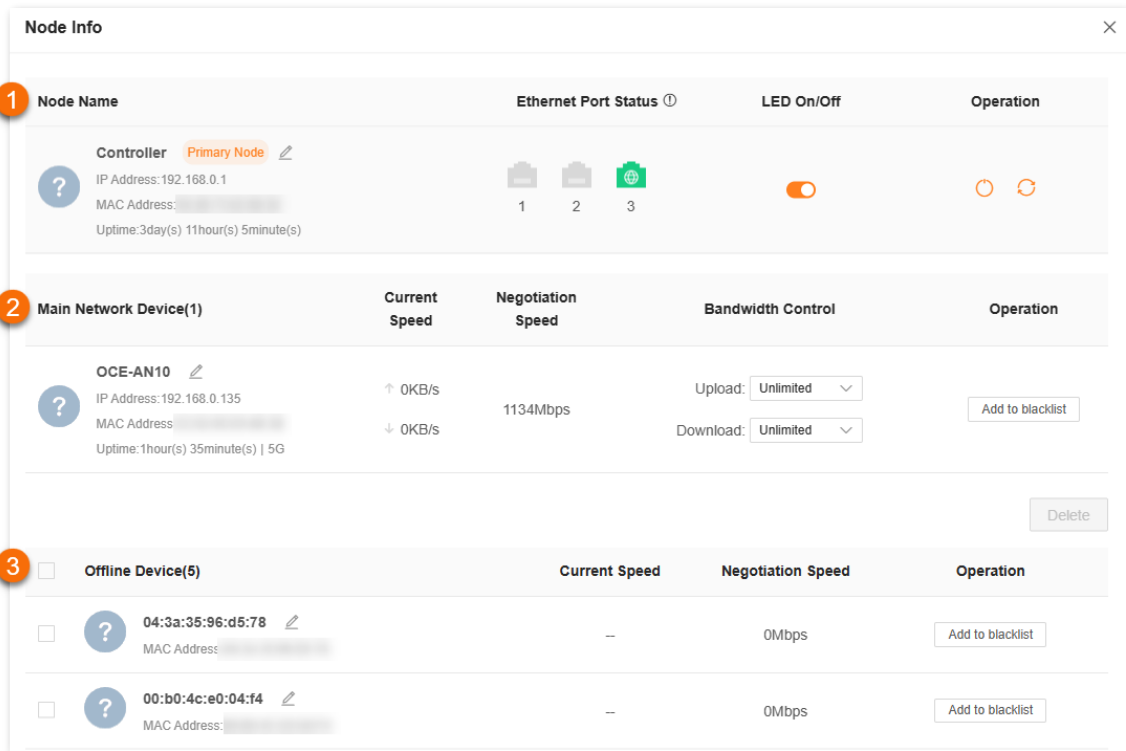
Controller information

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.



The screenshot shows a 'Node Info' dialog box with the following sections:










- 1 Node Name:**
 - Controller (Primary Node):** IP Address: 192.168.0.1, MAC Address: [redacted], Uptime: 3day(s) 11hour(s) 5minute(s). Ethernet Port Status shows 3 ports (1, 2, 3). LED On/Off is turned on. Operation icons include a power button and a refresh button.
- 2 Main Network Device(1):**
 - OCE-AN10:** IP Address: 192.168.0.135, MAC Address: [redacted], Uptime: 1hour(s) 35minute(s) | 5G. Current Speed: ↑ 0KB/s, ↓ 0KB/s. Negotiation Speed: 1134Mbps. Bandwidth Control: Upload: Unlimited, Download: Unlimited. Operation: Add to blacklist.
- 3 Offline Device(5):**
 - MAC Address: 04:3a:35:96:d5:78, Negotiation Speed: 0Mbps. Operation: Add to blacklist.
 - MAC Address: 00:b0:4c:e0:04:f4, Negotiation Speed: 0Mbps. Operation: Add to blacklist.

---End

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

No.	Description
-----	-------------

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.
- **Ethernet Port Status:** Indicates the status of the Ethernet ports of the primary node. Currently, this parameter is only available for Mesh15XP, MX15 Pro, EX15 Pro, Mesh21XEP, MX21 Pro and EX21 Pro.
 - : Indicates that the port is connected and used as a WAN port.
 - : Indicates that the port is connected and used as a LAN port.
 - : Indicates that the port is connected and used as an IPTV port.
 - : Indicates that the port is not connected.
- **Connection Quality:** Shows the connection signal strength with the primary node. You can hover your mouse over  to see the strength value. This parameter is only available for some models. Refer to the product that you purchased.
- **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.


1




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

No.	Description
-----	-------------

This area displays the information and operation shortcuts of main network clients, including:

- 2
- 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.

This area displays the information and operation shortcuts of offline clients, including:

- 3
- 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.




A maximum of 30 offline clients can be displayed here. A client will be automatically deleted from the list if it is offline for 3 days. A client is displayed under **Offline Device** after it is disconnected from the network for 90 seconds (wired client)/60 seconds (wireless client).

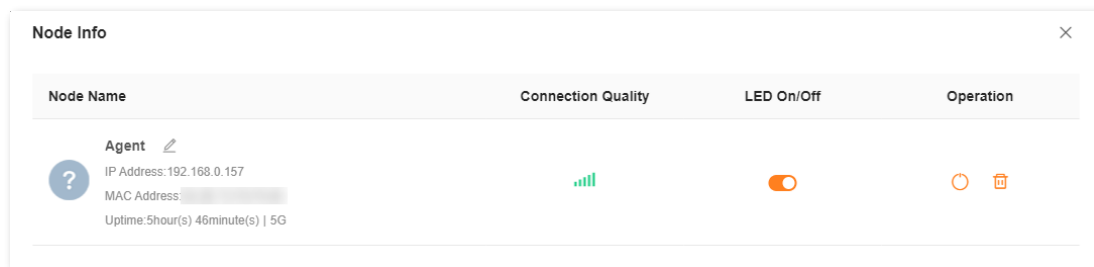
Agent information

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  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 .
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



- 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](#).

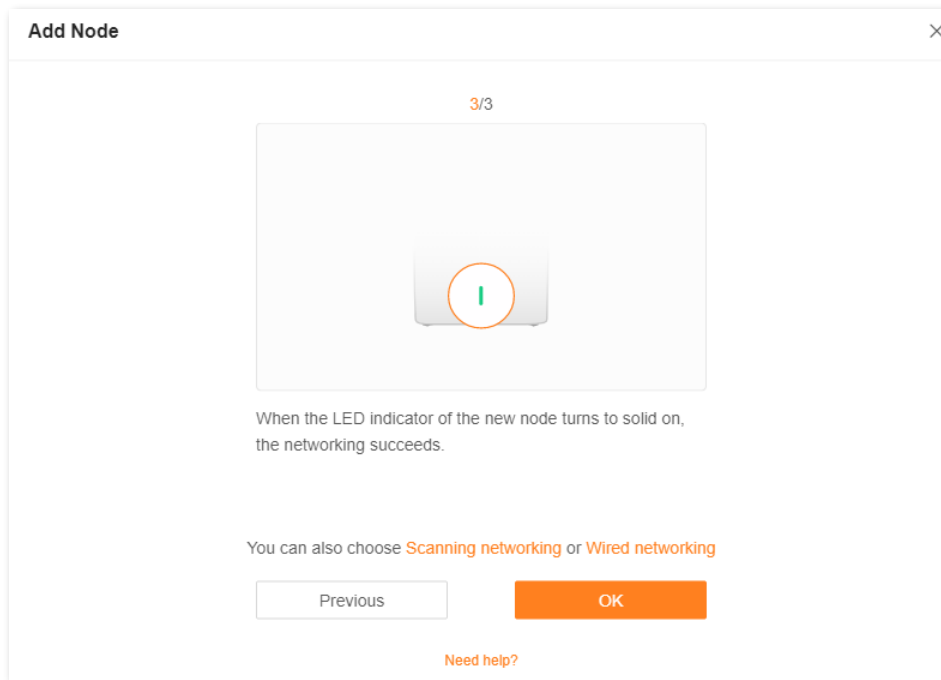
Step 2 Choose **Network Status**. Then, click  under **Network Topology**.

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.

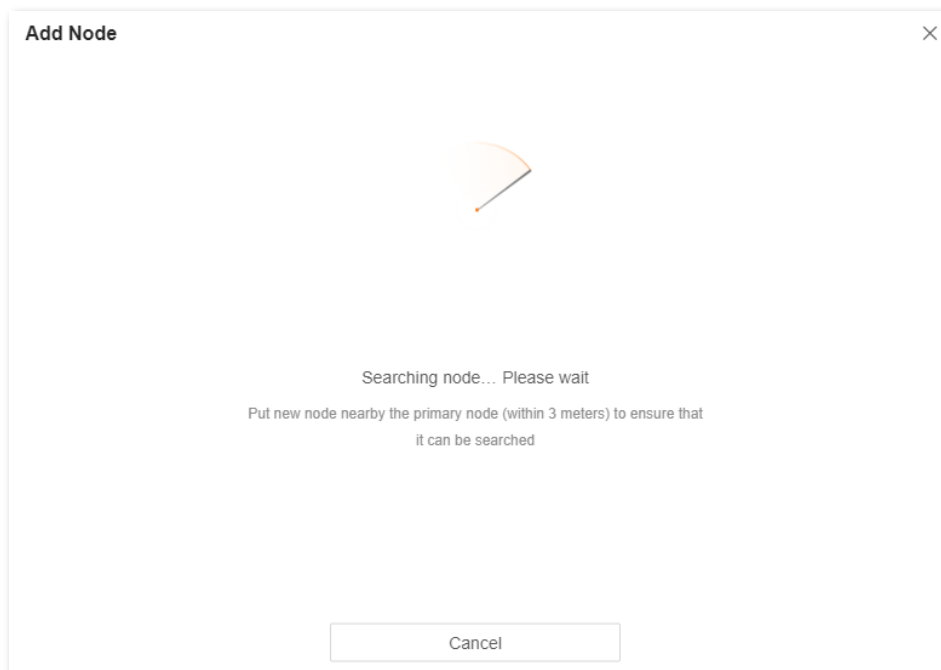
---End

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 following figure:

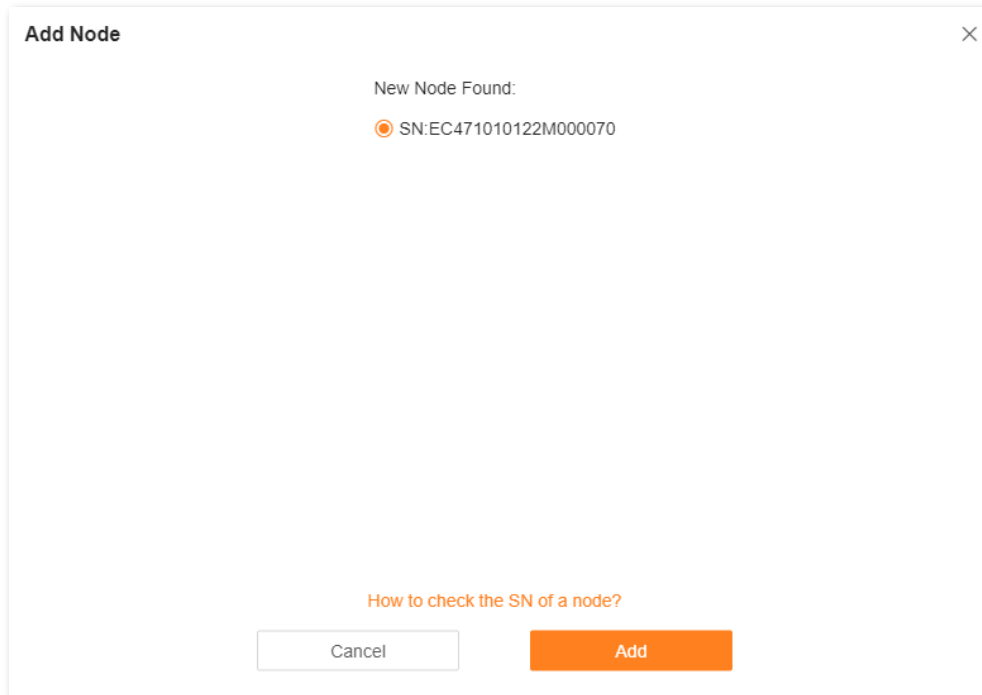


■ **To scan a new node:**

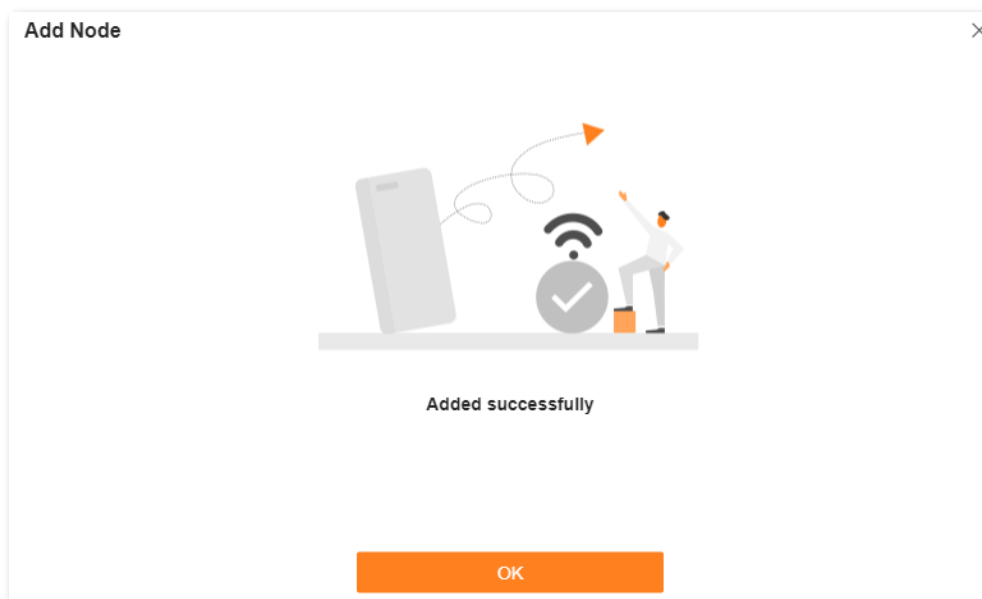
Step 1 Click **Scanning networking**.



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.

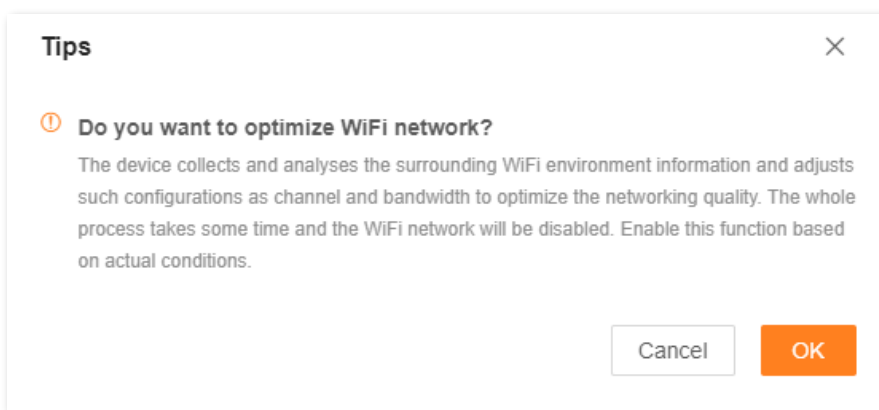
One-click optimization

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

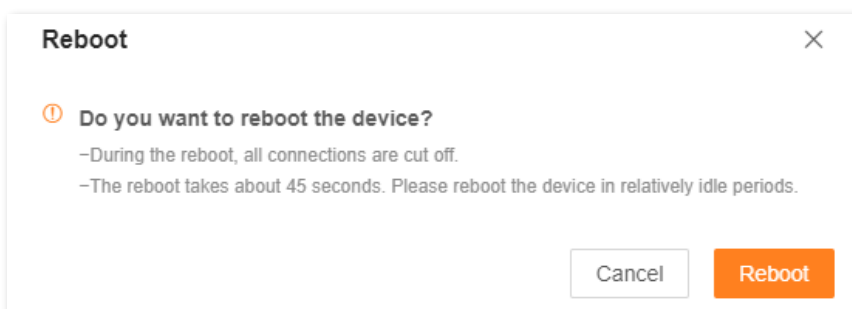
Reboot all nodes

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



This operation prevails to LED indicator operations for each node and [Smart power saving](#).

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

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

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

The indicators turn on/off immediately.

---End

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:

- [Overview](#)
- [Access the internet with a PPPoE account](#)
- [Access the internet through a dynamic IP address](#)
- [Access the internet with a set of static IP address information](#)
- [Set up dual access connection](#)

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.

Internet Settings

Network Status Connected

Uptime 5hour(s) 47minute(s)

ISP Type

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

PPPoE Username

PPPoE Password

Advanced ^

Server Name

Service Name

MTU


MAC Address Clone
Default MAC Address: 50:2B:73:F8:F9:81

DNS Settings

The following table describes the parameters displayed on this page.

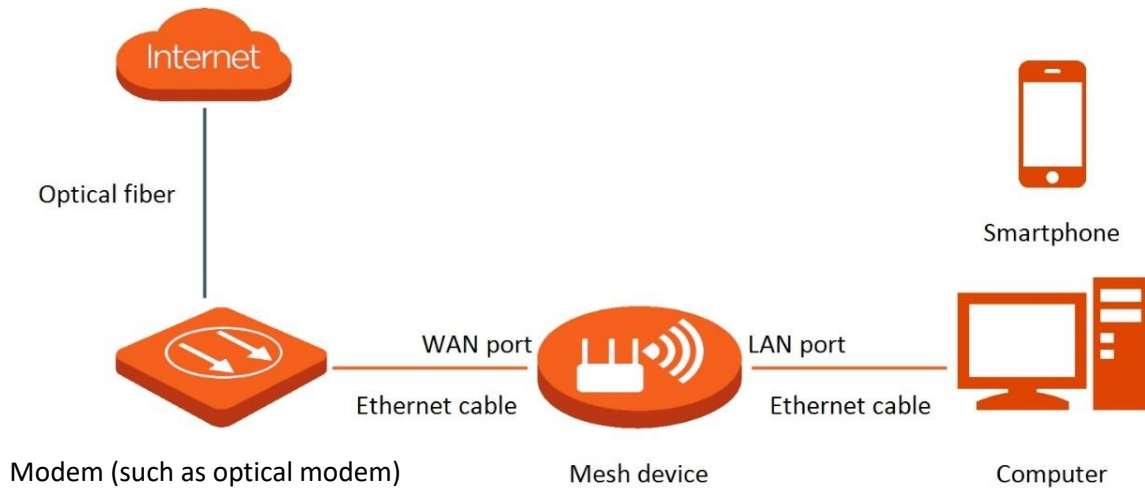
Parameter description

Parameter	Description
Network Status	<p>Indicates the internet connection status.</p> <ul style="list-style-type: none"> - 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/Connected time	Indicates the network connection time of the Mesh device.
ISP Type	
Internet Connection Type	
PPPoE Username	
PPPoE Password	
IP Address	
Subnet Mask	
Gateway	
Primary DNS	
Secondary DNS	See Parameter description in Connect your primary node to the internet .
Address Type	
DNS Settings	
Server IP Address/Domain Name	
User Name	
Password	
Area	
Internet VLAN ID	

Parameter	Description
IPTV VLAN ID	
Server Name	Displayed after you click Advanced if the connection type is PPPoE. They specify the PPPoE server name and PPPoE service name of the broadband service that you purchased.
Service Name	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	<p>Displayed after you click Advanced.</p> <p>It specifies the largest data packet transmitted by a network device. Do not change the value unless:</p> <ul style="list-style-type: none"> - 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. <p> TIP</p> <p>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.</p> <p>The MTU value range is as follows:</p> <ul style="list-style-type: none"> - When the internet connection type is PPPoE, the default value is 1480. Its allowed range is 1280 to 1492. - When the internet connection type is dynamic IP or static IP, the default value is 1500. Its allowed range is 1280 to 1500. - When the internet connection type is PPTP/L2TP, the default value is 1400. Its allowed range is 1280 to 1460.
MAC Address Clone	<p>Used to clone and change the MAC address of the WAN port of primary node.</p> <p>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.</p> <ul style="list-style-type: none"> - 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**.



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**.

Internet Settings

Network Status: Disconnected

ISP Type:

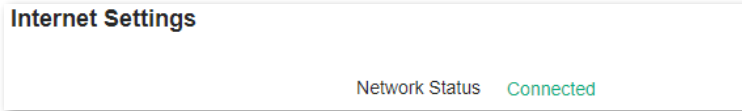
Internet Connection Type:
Select this type if you access the internet using the PPPoE account and PPPoE password.

PPPoE Username:

PPPoE Password:

Advanced ▼

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



---End



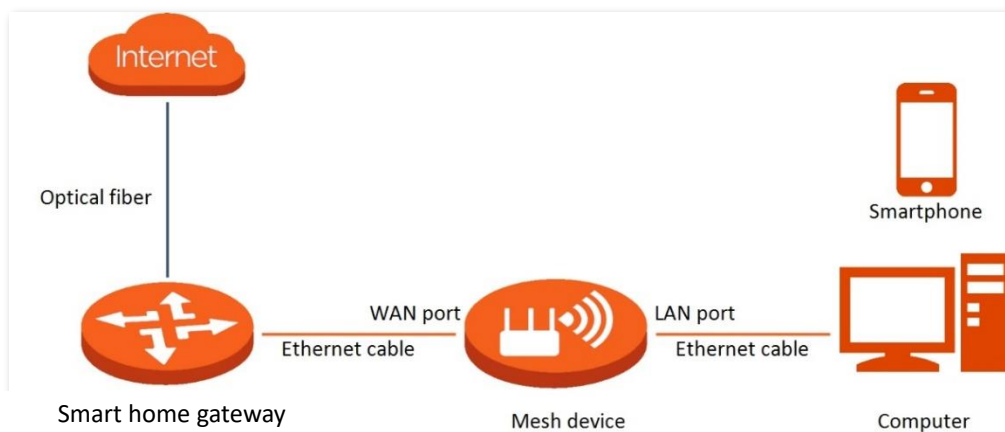
If there is no response from the remote server, troubleshoot as prompted under **Network Status** on the **Internet Settings** page.

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**.



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**.

Internet Settings

Network Status Disconnected

ISP Type Normal

Internet Connection Type Dynamic IP

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

Advanced

Connect

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

Internet Settings

Network Status Connected

---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**.



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**.

Internet Settings

Network Status Disconnected

ISP Type Normal

Internet Connection Type Static IP

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

IP Address . . .

Subnet Mask . . .

Gateway . . .

Primary DNS . . .

Secondary DNS . . .

Advanced ▼

Connect

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

Internet Settings

Network Status Connected

---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.

ISP Type

Internet Connection Type

If you select Russia PPTP or Russia L2TP, the VPN function will be disabled

Server IP Address/Domain Name

User Name

Password

Address Type Dynamic IP Address Static IP Address

DNS Settings

Advanced

Connect

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.

Internet Settings

Network Status **Connected**

---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 and unifying the 2.4 GHz, 5 GHz and 6 GHz networks.



The 6 GHz WiFi network is only supported by MX21 Pro/EX21 Pro/Mesh21XEP.

This section includes the following parts:

- [Basic settings](#)
- [Separate the Wi-Fi networks](#)
- [Unify the Wi-Fi networks](#)
- [Disable or Enable the WiFi 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.

WiFi Settings

Unify 2.4 GHz & 5 GHz

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

WiFi Name: NOVA



Security: WPA2-PSK (Recommended)



WiFi Password:

Save

The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
Unify 2.4 GHz & 5 GHz	<p>Used to enable or disable the Unify 2.4 GHz & 5 GHz function.</p> <p>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 Wi-Fi networks and Unify the Wi-Fi networks.</p> <p> TIP</p> <p>If any device that supports 2.4 GHz network only needs to connect to the Wi-Fi network, do not enable this function.</p>
Unify 2.4 GHz & 5 GHz & 6 GHz	<p>Used to enable or disable the Unify 2.4 GHz & 5 GHz & 6 GHz function. It is available only for MX21 Pro/EX21 Pro/Mesh21XEP.</p> <p>When this function is enabled, the 2.4 GHz, 5 GHz and 6 GHz Wi-Fi networks share the same SSID and password. WiFi-enabled clients connected to it will use the frequency with better connection quality. For its operations, see Separate the Wi-Fi networks and Unify the Wi-Fi networks for reference.</p> <p> TIP</p> <p>If any device that supports 2.4 GHz network only needs to connect to the Wi-Fi network, do not enable this function.</p>
WiFi Enable/2.4 GHz WiFi/5 GHz WiFi/6 GHz WiFi	<p>Used to enable or disable the Wi-Fi networks.</p> <ul style="list-style-type: none"> - WiFi Enable is displayed when Unify 2.4 GHz & 5 GHz or Unify 2.4 GHz & 5 GHz & 6 GHz is enabled. - 2.4 GHz WiFi, 5 GHz WiFi or 6 GHz WiFi is displayed when Unify 2.4 GHz & 5 GHz or Unify 2.4 GHz & 5 GHz & 6 GHz is disabled.
WiFi Name	Specifies the Wi-Fi network name (SSID) of the corresponding Wi-Fi network.

Parameter	Description
Security	<p>Specifies the encryption mode supported by the Mesh device, including:</p> <ul style="list-style-type: none"> - 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. It is available for the 2.4 GHz and 5 GHz Wi-Fi networks. - WPA2-PSK (Recommended): The network is encrypted with WPA2-PSK/AES. It is available for the 2.4 GHz and 5 GHz Wi-Fi networks. - WPA3-SAE/WPA2-PSK: The network is encrypted with both WPA3-SAE and WPA2-PSK, improving both security and compatibility. This option is only available for some models. Refer to the product you purchased. - WPA3-SAE: The network is encrypted with WPA3-SAE. It is available for only the 6 GHz Wi-Fi network. - OWE: The network is encrypted with the Opportunistic Wireless Encryption (OWE) mode. It is available for only the 6 GHz Wi-Fi network. With this option selected, clients can access the 6 GHz WiFi network without the WiFi password while the data exchanged will still be encrypted. <p> TIP</p> <p>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).</p>
WiFi Password	<p>Specifies the password for connecting to the Wi-Fi network. You are strongly recommended to set a Wi-Fi password for security.</p> <p> TIP</p> <p>It is recommended to use the combination of numbers, uppercase letters, lowercase letters and special symbols in the password to enhance the security of the Wi-Fi network.</p>

2.5.2 Separate the Wi-Fi networks

The Mesh device supports 2.4 GHz, 5 GHz and 6 GHz Wi-Fi networks, which are unified and only one Wi-Fi name is displayed by default.



The 6 GHz WiFi network is only supported by MX21 Pro/EX21 Pro/Mesh21XEP.

To separate the Wi-Fi names of the networks:

Step 1 [Log in to the web UI](#), and choose **WiFi Settings**.

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



For MX21 Pro/EX21 Pro/Mesh21XEP:

- To separate the Wi-Fi names of the three networks, disable **Unify 2.4 GHz & 5 GHz & 6 GHz**.
- To separate only the 6 GHz Wi-Fi name, enable **Unify 2.4 GHz & 5 GHz** but disable **Unify 2.4 GHz & 5 GHz & 6 GHz**.

Step 3 (Optional) Enable **WiFi Enable** or **2.4 GHz WiFi**, **5 GHz WiFi** and **6 GHz WiFi** as required.



This step is only required for MX21 Pro/EX21 Pro/Mesh21XEP.

Step 4 Set **WiFi Name**, **Security** and **WiFi Password** of each WiFi network.

MX15 Pro is used for example here. In this example, the 2.4 GHz Wi-Fi network is named **NOVA_9JK3_A3**, the 5 GHz Wi-Fi network is named **NOVA_9JK3_A3_5G**, and **WPA2-PSK (Recommended)** is selected for **Security**.

Step 5 Click **Save**.

WiFi Settings

Unify 2.4 GHz & 5 GHz

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

2.4 GHz WiFi

WiFi Name

Security

WiFi Password ⓘ

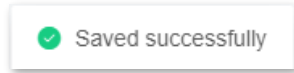
5 GHz WiFi

WiFi Name

Security

WiFi Password ⓘ

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.

2.5.3 Unify the Wi-Fi networks

The Mesh device supports 2.4 GHz, 5 GHz and 6 GHz Wi-Fi networks. You can unify their Wi-Fi names and passwords as required.



The 6 GHz WiFi network is only supported by MX21 Pro/EX21 Pro/Mesh21XEP. To unify the Wi-Fi names of the networks:

Step 1 [Log in to the web UI](#), and choose **WiFi Settings**.

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



For MX21 Pro/EX21 Pro/Mesh21XEP:

- To unify the Wi-Fi names of the three networks, enable **Unify 2.4 GHz & 5 GHz & 6 GHz**.
- To unify only the 2.4 GHz and 5 GHz Wi-Fi name, enable **Unify 2.4 GHz & 5 GHz** but disable **Unify 2.4 GHz & 5 GHz & 6 GHz**.

Step 3 (Optional) Enable **WiFi Enable** and **6 GHz WiFi** as required.



This step is only required for MX21 Pro/EX21 Pro/Mesh21XEP.

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

MX15 Pro is used for example here. In this example, the Wi-Fi networks are named **NOVA_KF7R_A1** and **WPA2-PSK (Recommended)** is selected for **Security**.

Step 5 Click **Save**.

WiFi Settings

Unify 2.4 GHz & 5 GHz


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

WiFi Name

Security

WiFi Password ⓘ

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

 Saved successfully

---End

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

2.5.4 Disable or Enable the WiFi networks

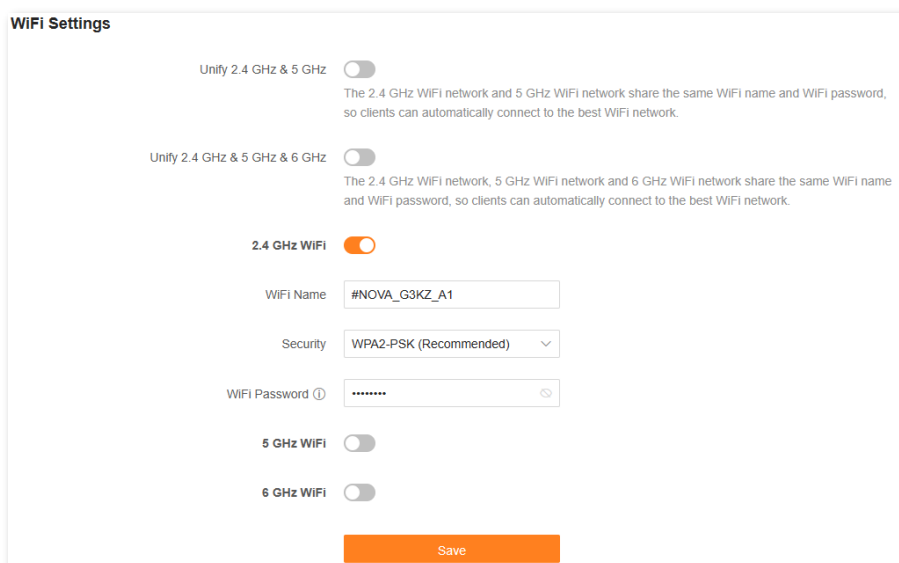


This function is only available for MX21 Pro/EX21 Pro/Mesh21XEP.

■ To disable some Wi-Fi networks:

- Step 1** [Log in to the web UI](#), and choose **WiFi Settings**.
- Step 2** Enable or disable **Unify 2.4 GHz & 5 GHz** or **Unify 2.4 GHz & 5 GHz & 6 GHz** as required.
- Step 3** Disable **WiFi Enable** or **2.4 GHz WiFi**, **5 GHz WiFi** and **6 GHz WiFi** as required.
- Step 4** Click **Save**.

In this example, all Wi-Fi networks are separated and 5 GHz and 6 GHz Wi-Fi networks are disabled.



WiFi Settings

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

Unify 2.4 GHz & 5 GHz & 6 GHz The 2.4 GHz WiFi network, 5 GHz WiFi network and 6 GHz WiFi network share the same WiFi name and WiFi password, so clients can automatically connect to the best WiFi network.

2.4 GHz WiFi

WiFi Name

Security

WiFi Password

5 GHz WiFi

6 GHz WiFi

---End

When the configuration is completed, the corresponding WiFi networks are disabled.

■ To enable some Wi-Fi networks:

- Step 1** [Log in to the web UI](#), and choose **WiFi Settings**.
- Step 2** Enable or disable **Unify 2.4 GHz & 5 GHz** or **Unify 2.4 GHz & 5 GHz & 6 GHz** as required.
- Step 3** Enable **WiFi Enable** or **2.4 GHz WiFi**, **5 GHz WiFi** and **6 GHz WiFi** as required.
- Step 4** Set **WiFi Name**, **Security**, and **WiFi Password**.
- Step 5** Click **Save**.

In this example, all Wi-Fi networks are separated enabled.

WiFi Settings

Unify 2.4 GHz & 5 GHz

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

Unify 2.4 GHz & 5 GHz & 6 GHz

The 2.4 GHz WiFi network, 5 GHz WiFi network and 6 GHz WiFi network share the same WiFi name and WiFi password, so clients can automatically connect to the best WiFi network.

2.4 GHz WiFi

WiFi Name

Security

This requires that the clients support the WPA3-SAE/WPA2-PSK mode as well. If any connection issues arise in the process, switch back to WPA2-PSK.

WiFi Password ⓘ

5 GHz WiFi

WiFi Name

Security

This requires that the clients support the WPA3-SAE/WPA2-PSK mode as well. If any connection issues arise in the process, switch back to WPA2-PSK.

WiFi Password ⓘ

6 GHz WiFi

WiFi Name

Security

WiFi Password ⓘ

---End

When the configuration is completed, the corresponding WiFi networks are enabled.

2.6 Client management

This section describes how to manage your clients, including:

- [View client information](#)
- [Change a client name](#)
- [Add a client to the blacklist](#)
- [Remove a client from the blacklist](#)
- [Delete an offline client](#)

2.6.1 View client information

To view information of clients:

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





Step 2 Choose **Client Management**.



TIP



- The information of all clients is displayed by default.
- To view information of only the clients connected to the controller (primary node), select the controller from the drop-down list box under **Client Management**. The controller name is **Controller** by default. You can change it in [Controller information](#).
- To view information of only clients connected to an agent, select the agent from the drop-down list box on the right. You can change the agent names in [Agent information](#).

The following page is displayed.

Client Management					
Main Network Device(2)		Guest Device(0)	Offline Device(0)	Blacklist(0)	All Nodes ▼
Main Network Device(2)	Current Speed	Negotiation Speed	Bandwidth Control	Operation	
 DESKTOP-RGGBS4D  IP Address: 192.168.0.145 MAC Address: XXXXXXXXXX Uptime: 1hour(s) 30minute(s) Wired	↑ 0KB/s	100Mbps	Upload: <input type="text" value="Unlimited"/> ▼ Download: <input type="text" value="Unlimited"/> ▼	Local Host	
 HUAWEI_P30-360d3356c...  IP Address: 192.168.0.159 MAC Address: XXXXXXXXXX Uptime: 1hour(s) 30minute(s) 5G	↑ 0KB/s	867Mbps	Upload: <input type="text" value="Unlimited"/> ▼ Download: <input type="text" value="Unlimited"/> ▼	<input type="button" value="Add to blacklist"/>	

---End

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


Item	Description
Main Network Device	<p>Displays the information and operation shortcuts of main network clients, including:</p> <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> ✦ 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: <ul style="list-style-type: none"> ✦ 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.
Guest Device	<p>Displays the information and operation shortcuts of clients connected to the guest network, including:</p> <ul style="list-style-type: none"> - 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.
Offline Device	<p>Displays the information and operation shortcuts of offline clients, including:</p> <ul style="list-style-type: none"> - 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. <p>A maximum of 30 offline clients can be displayed here. A client is displayed under Offline Device after it is disconnected from the network for 90 seconds (wired client)/60 seconds (wireless client). A client will be automatically deleted from this list if it is offline for 3 days.</p>
Blacklist	<p>Displays the information and operation shortcut of blacklisted clients, including:</p> <ul style="list-style-type: none"> - Device Name: Indicates the name of the blacklisted client. - MAC Address: Indicates the MAC address of the blacklisted client. - Operation: Provides a Remove from the blacklist button for removing clients from the blacklist.

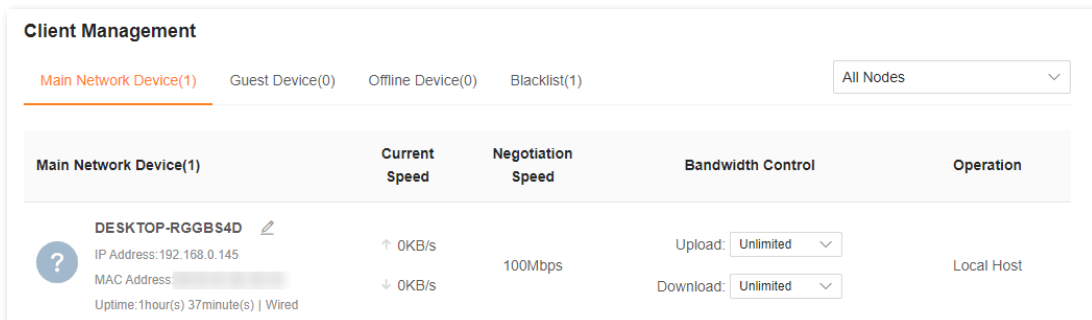
2.6.2 Change a client name

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:

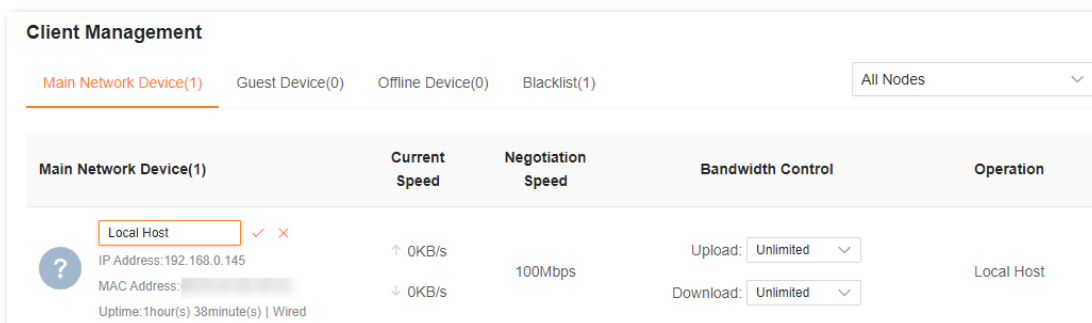
Step 1 [Log in to the web UI](#), and choose **Client Management**.

Step 2 Click  beside the client name.



The screenshot shows the 'Client Management' interface. At the top, there are tabs for 'Main Network Device(1)', 'Guest Device(0)', 'Offline Device(0)', and 'Blacklist(1)'. A dropdown menu is set to 'All Nodes'. Below this is a table with columns: 'Main Network Device(1)', 'Current Speed', 'Negotiation Speed', 'Bandwidth Control', and 'Operation'. The first row shows a client named 'DESKTOP-RGGBS4D' with an edit icon (pencil) next to its name. The client details include IP Address: 192.168.0.145, MAC Address: [redacted], Uptime: 1hour(s) 37minute(s) | Wired, Current Speed: 0KB/s, Negotiation Speed: 100Mbps, and Bandwidth Control: Upload: Unlimited, Download: Unlimited. The Operation column shows 'Local Host'.

Step 3 Enter a new name and click .



The screenshot shows the 'Client Management' interface after the name change. The client name is now 'Local Host' and is highlighted with a red border and a checkmark icon. The rest of the interface, including the tabs, dropdown menu, and table columns, remains the same as in the previous screenshot.

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.

Client Management

Main Network Device(2) Guest Device(0) Offline Device(0) Blacklist(0) All Nodes

Main Network Device(2)	Current Speed	Negotiation Speed	Bandwidth Control	Operation
DESKTOP-RGGBS4D IP Address: 192.168.0.145 MAC Address: [REDACTED] Uptime: 1minute(s) Wired	↑ 0KB/s ↓ 0KB/s	100Mbps	Upload: Unlimited Download: Unlimited	Local Host
HUAWEI_P30-360d3356c... IP Address: 192.168.0.159 MAC Address: [REDACTED] Uptime: 0minute(s) 5G	↑ 0KB/s ↓ 2KB/s	867Mbps	Upload: Unlimited Download: Unlimited	Add to blacklist

Step 3 Click **OK**.

Confirm Operation

Once blacklisted, the client cannot access the internet through this router. Continue?

Cancel **OK**

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

Client Management

Main Network Device(1) Guest Device(0) Offline Device(0) **Blacklist(1)**

Device Name	MAC Address	Operation
HUAWEI_P30-360d3356cd98fc	[REDACTED]	Remove from the blacklist



- 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.
- The blacklist rule prevails when conflicting with the parent control rule.

---End

2.6.4 Remove a client from the blacklist

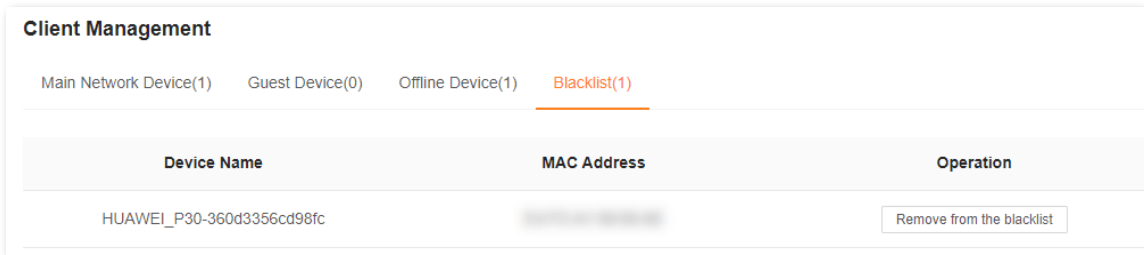
If you blacklist a client by mistake, you can remove it from the blacklist.

To remove a client from the blacklist:

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

Step 2 Choose **Blacklist**.

- 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 **Main Network Device**, **Guest Device** or **Offline Device** now. It can access the network upon the next connection.

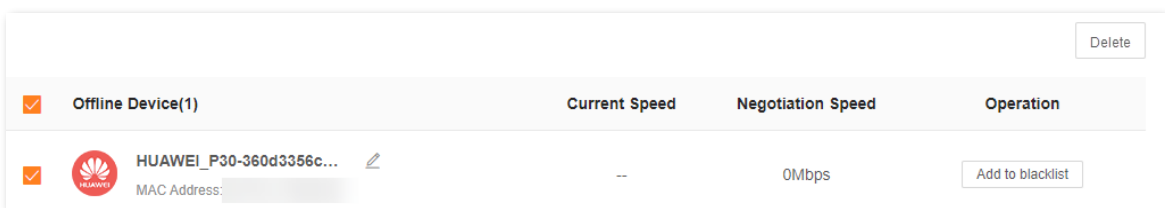
---End

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.



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

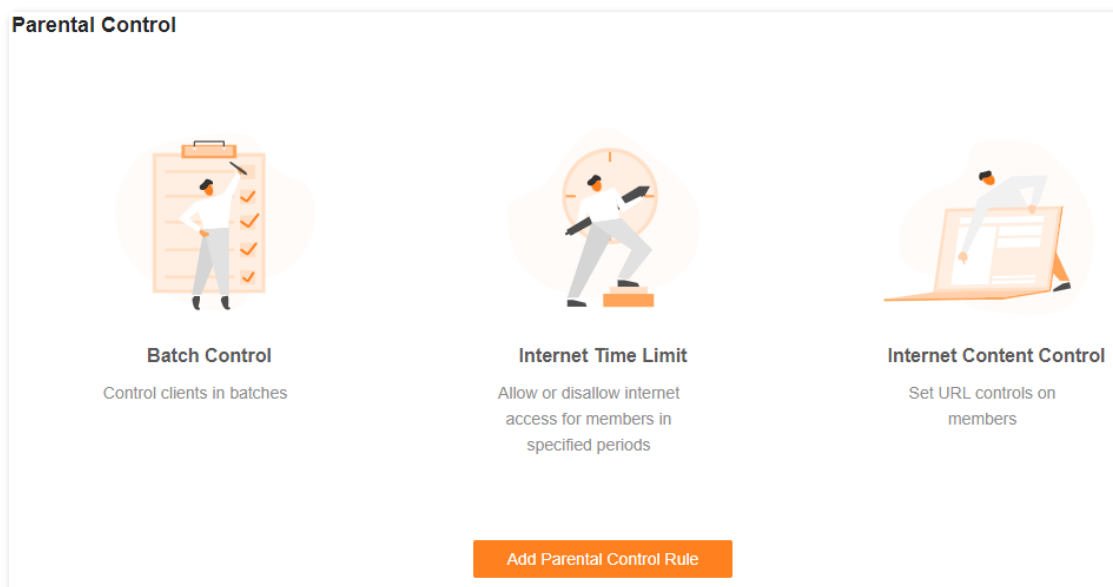


- The blacklist rule prevails when conflicting with the parent control rule.
- A maximum of 10 rules can be added.
- A maximum of 30 clients can be controlled.

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.

Parental Control Add				
Group Name	Control Period	URL Filter	Parental Control	Operation
Parental control rule 1	08:00-22:00 Sat., Sun.	Disallowed Facebook, Twitter, YouTube, Instagram	<input checked="" type="checkbox"/>	

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

Step 3 Set the parameters as required.



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

Add Parental Control Rule ×

Client

Group Name

Selected clients +

Control Period

Time 1

→ 🕒 Mon. × Tues. × +5 ▾

Add control period

URL Filter

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

URL

Add URL

Cancel
Save

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.
Time <i>n</i>	Specifies whether the parental control rule takes effect in the specified period.
Add control period	Available when Control Period is enabled. If you want to set multiple periods, click this button.
URL Filter	<p>Specifies whether the URL filter rule is applied.</p> <ul style="list-style-type: none"> When it is enabled, Filter mode and URL must be set. The parental control rule takes effect on specific websites. When it is disabled, the URL filter rule is not applied.
Filter mode	<p>Required when URL Filter is enabled. Two modes are available here.</p> <ul style="list-style-type: none"> 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 enabled. 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:

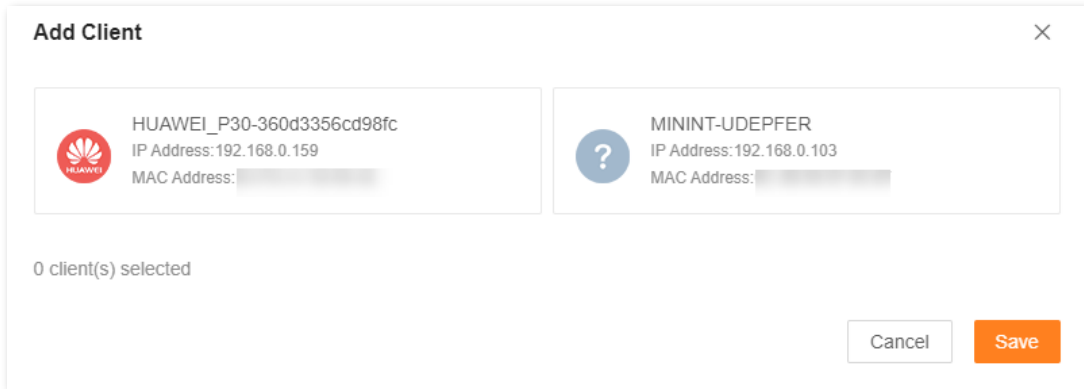
Step 1 [Log in to the web UI](#), and choose **Parental Control**.

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

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

Step 4 Click  beside **Selected clients**.

The following dialog box is displayed.

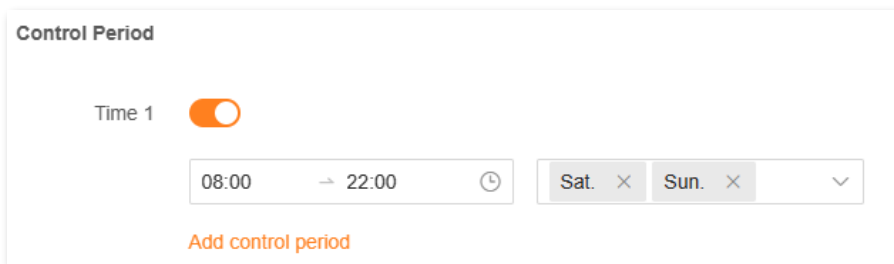


Step 5 Select the clients to which this parental control rule is applied, and click **Save**.

Step 6 Enable **Time 1**.

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

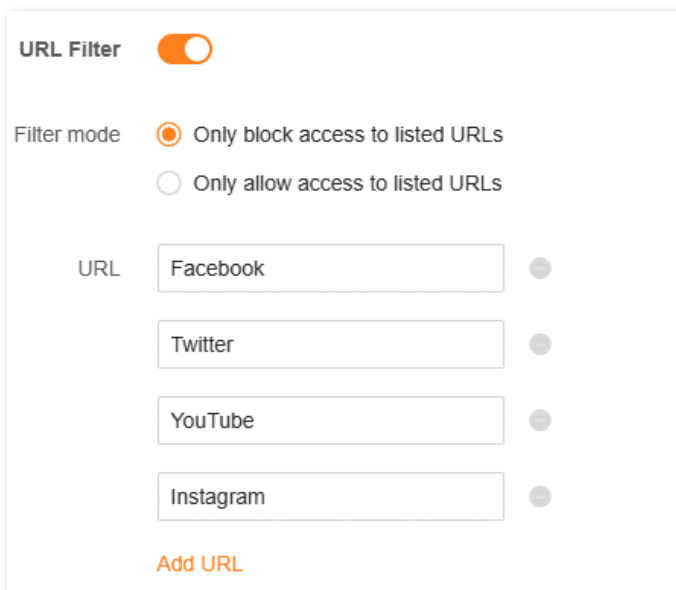
1. Click the left field to set **Start Time** to **08:00** and **End Time** to **22:00**.
2. Select **Sat.** and **Sun.** from the right drop-down list box.



Step 8 Enable **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.

Parental Control Add				
Group Name	Control Period	URL Filter	Parental Control	Operation
Parental control rule 1	08:00-22:00 Sat., Sun.	Disallowed Facebook, Twitter, YouTube, Instagram	<input checked="" type="checkbox"/>	

---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**.

Parental Control Add				
Group Name	Control Period	URL Filter	Parental Control	Operation
Parental control rule 1	08:00-22:00 Sat., Sun.	Disallowed Facebook, Twitter, YouTube, Instagram	<input checked="" type="checkbox"/>	

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](#)
- [Network diagnosis](#)
- [TR069](#)
- [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.

Router Info

You can check the information of the router here.

Basic Info

Product Model	[REDACTED]
System Time	2022-12-02 11:05:28
Runtime	1hour(s) 13minute(s)
Firmware Version	V16.03.31.03_multi
Hardware Version	V1.0

WAN Port Info

Internet Connection Status	Connected
Internet Connection Type	PPPoE
Connected time	1hour(s) 12minute(s)
IP Address	172.16.200.93
Subnet Mask	255.255.255.255
Default gateway	172.16.200.1
Primary DNS	202.96.134.133
Secondary DNS	202.96.128.166
MAC Address	[REDACTED]

LAN Info

IP Address	192.168.0.1
Subnet Mask	255.255.255.0
MAC Address	[REDACTED]

2.4 GHz WiFi

Status	Visible
Wi-Fi Name	NOVA_RAN9_A1
Security	WPA2-PSK (Recommended)
Channel	4
Bandwidth	20
MAC Address	[REDACTED]

5 GHz WiFi

Status	Visible
Wi-Fi Name	NOVA_RAN9_A1
Security	WPA2-PSK (Recommended)
Channel	48
Bandwidth	80
MAC Address	[REDACTED]

---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.
System Time	Specifies the current system time.
Runtime	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.
Connected time	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.
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	
MAC Address	Specifies the WAN MAC address of the primary node.

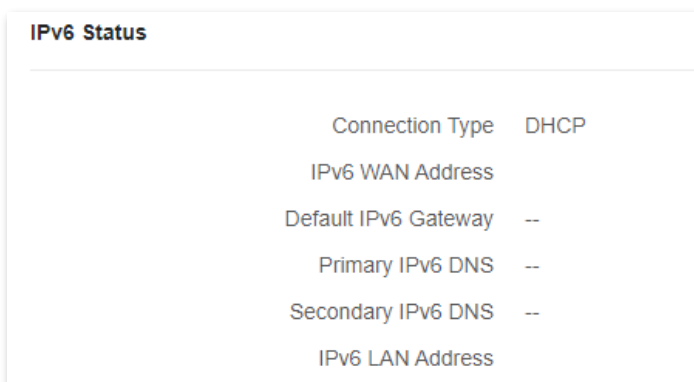
LAN information

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.
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.
Wi-Fi Name	Specifies the Wi-Fi name of the respective Wi-Fi network.
Security	Specifies the security mode of the respective Wi-Fi network.
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.

IPv6 status



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

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

Parameter	Description
Connection Type	Specifies the IPv6 connection type of the primary node.

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

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 **More > Guest WiFi**. This function is disabled by default. The following figure shows the **Guest WiFi** page with the **Guest WiFi** function enabled.

Guest WiFi

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

Guest WiFi

2.4 GHz WiFi Name

5 GHz WiFi Name

WiFi Password 🔒

Validity ▼

Shared Bandwidth ▼

Parameter description

Parameter	Description
Guest WiFi	Used to enable or disable the guest network function.
2.4 GHz WiFi Name	Specify the Wi-Fi name of the Mesh system's guest network.
5 GHz WiFi Name	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.
6 GHz WiFi Name	6 GHz WiFi Name is only available for MX21 Pro/EX21 Pro/Mesh21XEP.
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:

- MX15 Pro used
- 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**
- 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**.


Guest WiFi


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


Guest WiFi

2.4 GHz WiFi Name

5 GHz WiFi Name

WiFi Password 

Validity 

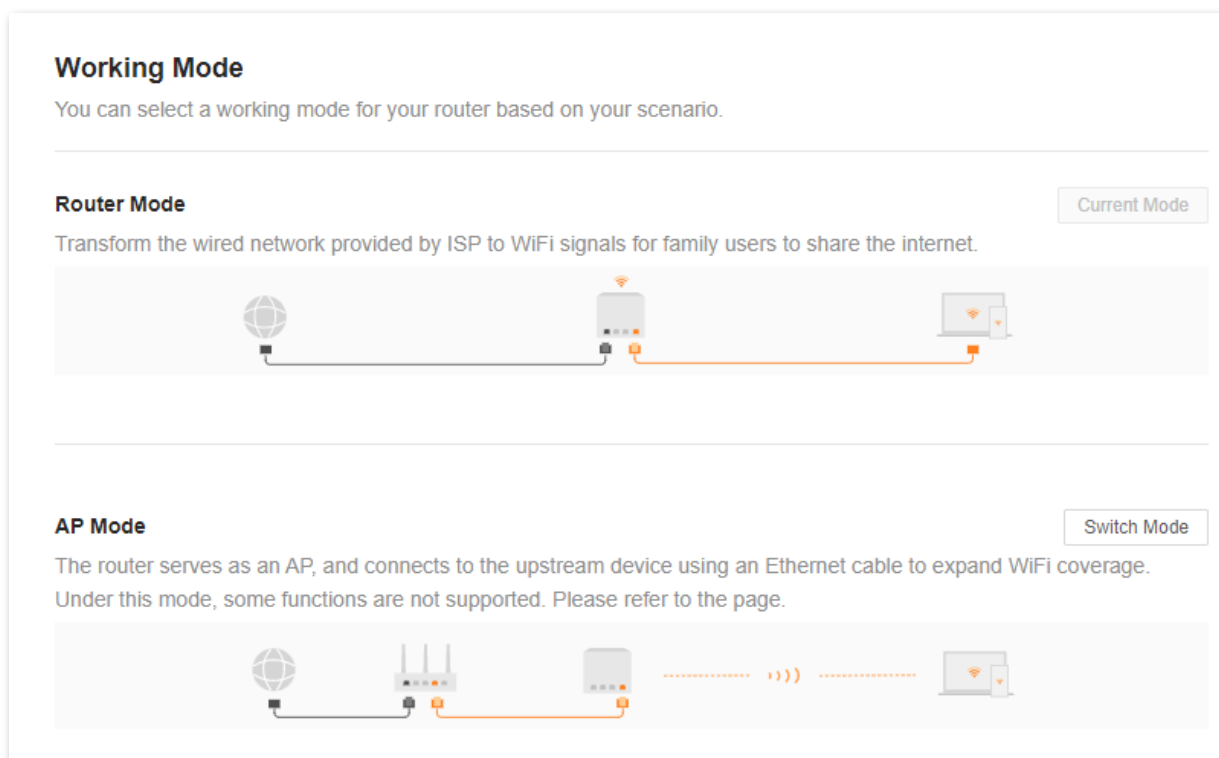
Shared Bandwidth 

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**.

Working Mode

You can select a working mode for your router based on your scenario.

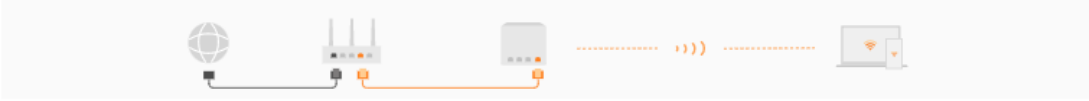
Router Mode Switch Mode

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.



Step 4 Click **OK**.

Tips

✕

ⓘ **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 can connect to the WAN port of the device, and clients can access the internet either by connecting to other Ethernet ports or WiFi network.

Cancel
OK

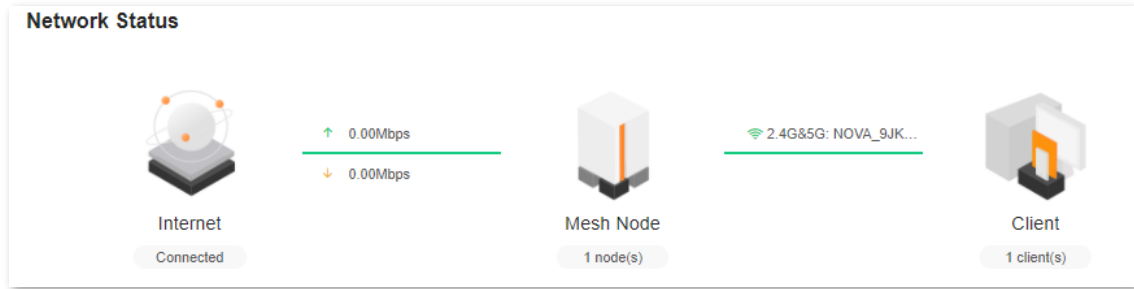
Step 5 Wait until the devices are restarted.

Rebooting... Please wait about 1 minute

5%

You will be redirected to the login page when the reboot completes

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**.

Working Mode

You can select a working mode for your router based on your scenario.


Router Mode Current Mode

Transform the wired network provided by ISP to WiFi signals for family users to share the internet.



AP Mode Switch 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.



Step 4 Click **OK**.

Tips ✕

ⓘ Do you want to switch to AP mode?

1. After the AP mode is enabled, the device will reboot, and the configuration takes effect after the device is rebooted.
2. Under the AP mode, some functions are unavailable, such as Internet Settings, Parental Control, VPN, and Port Mapping.
3. Under the AP mode, all Ethernet ports are LAN ports, and you can connect the device to the upstream device using any Ethernet port.
4. Under the AP mode, please visit tendawifi.com to log in to the web UI.

Cancel
OK

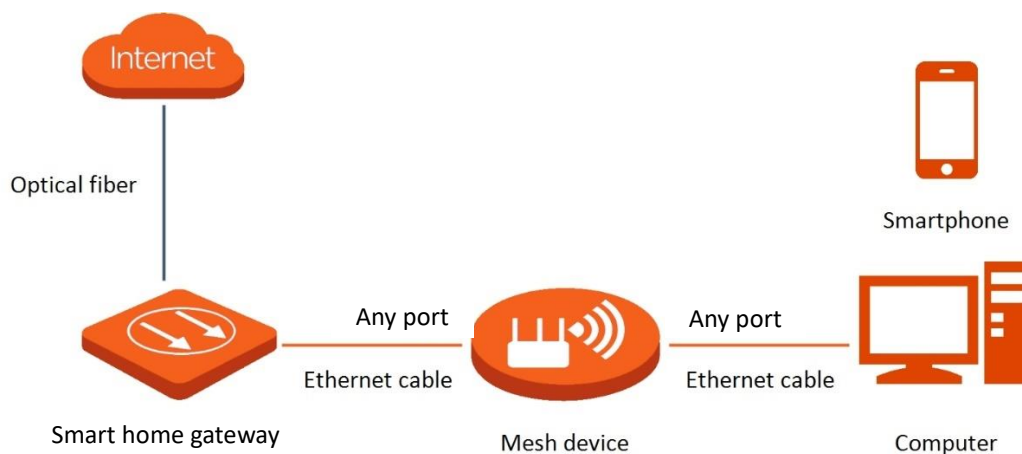
Step 5 Wait until the devices are restarted.

Rebooting... Please wait about 1 minute

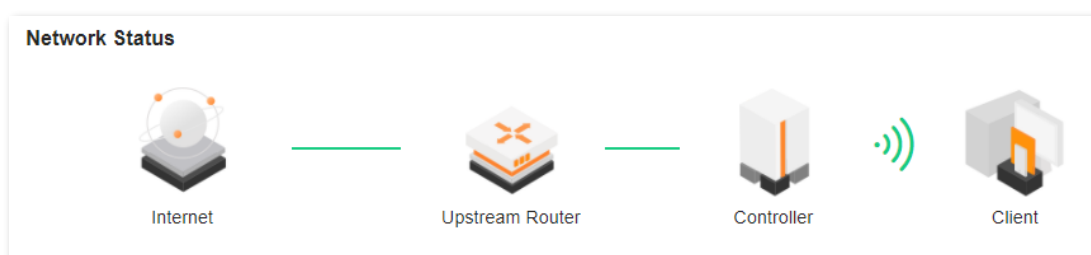
5%

You will be redirected to the login page when the reboot completes

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.



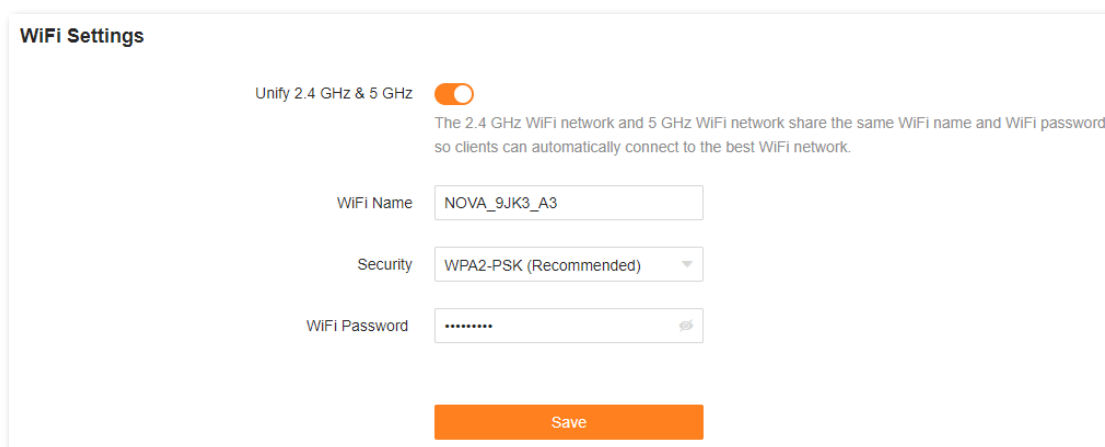
---End

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.





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



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

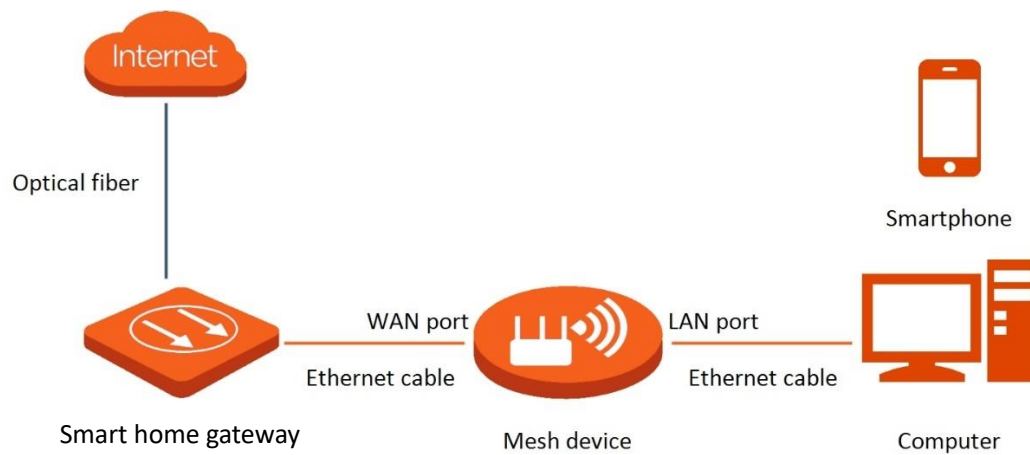


Before configuring the IPv6 function, ensure that you are within the coverage of the IPv6 network and already subscribe to the IPv6 internet service. Contact your ISP for any doubt about it.

DHCPv6

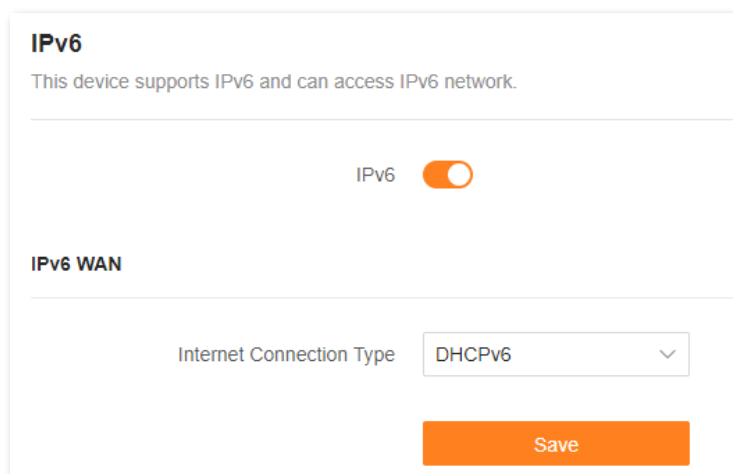
DHCPv6 enables the Mesh device to obtain an IPv6 address from the DHCPv6 server to access the internet. It is applicable in the following scenarios:

- 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.

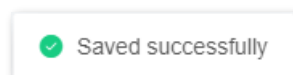


Configuration procedure:

- 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 **DHCPv6**.
- Step 5** Click **Save**.



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



---End

Verification:

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

- Step 1** On a computer connected to the Mesh device, press **Windows + R** to open the **Run** dialog box.
- Step 2** Type **cmd** and then click **OK** to open a regular Command Prompt.

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

---End

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

```
C:\Users\user>ping 240c::6666
Pinging 240c::6666 with 32 bytes of data:
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Reply from 240c::6666 bytes=32 time<1ms TTL=128

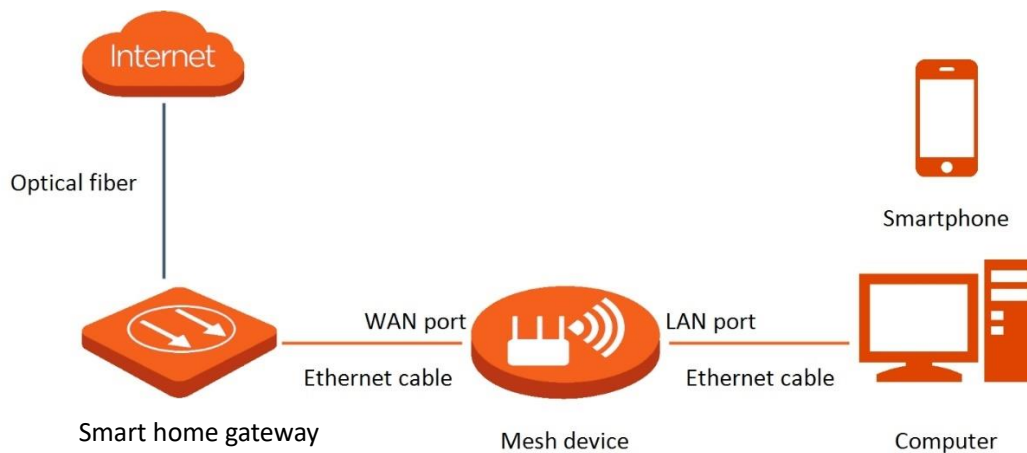
Ping statistics for 240c::6666:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

If the IPv6 network fails, try the following solutions:

- Ensure that clients connected to the Mesh device obtain their IPv6 address through DHCP.
- 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** provided by your ISP, and click **Save**.

IPv6

This device supports IPv6 and can access IPv6 network.

IPv6

IPv6 WAN

Internet Connection Type

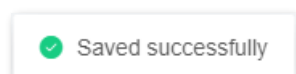
PPPoE Username

PPPoE Password

Parameter description

Parameter	Description
PPPoE Username	Specify the PPPoE user name and password provided by your ISP.
PPPoE Password	<div style="display: flex; align-items: center;"> TIP IPv4 and IPv6 services share the same PPPoE account. </div>

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



---End

Verification:

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

- Step 1** On a computer connected to the Mesh device, press **Windows + R** to open the **Run** dialog box.
- Step 2** Type **cmd** and then click **OK** to open a regular Command Prompt.
- Step 3** Enter **ping 240c::6666** and press **Enter**.

---End

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

```

C:\Users\user>ping 240c::6666
Pinging 240c::6666 with 32 bytes of data:
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Ping statistics for 240c::6666 :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss):
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

If the IPv6 network fails, try the following solutions:

- Ensure that clients connected to the Mesh device obtain their IPv6 address through DHCP.
- 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**.

IPv6 WAN

Internet Connection Type Static IPv6 Address ▼

IPv6 Address /


Default IPv6 Gateway

Primary IPv6 DNS

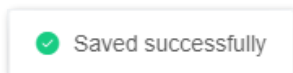
Secondary IPv6 DNS

Parameter description

Parameter	Description
IPv6 Address	Specify the fixed IPv6 address information provided by your ISP.

Parameter	Description
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

Verification:

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

- Step 1** On a computer connected to the Mesh device, press **Windows + R** to open the **Run** dialog box.
- Step 2** Type **cmd** and then click **OK** to open a regular Command Prompt.
- Step 3** Enter **ping 240c::6666** and press **Enter**.

---End

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

```
C:\Users\user>ping 240c::6666
Pinging 240c::6666 with 32 bytes of data:
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Reply from 240c::6666 bytes=32 time<1ms TTL=128
Ping statistics for 240c::6666 :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss):
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

If the IPv6 network 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 DHCP.
- Consult your ISP for help.

2.8.5 Network diagnosis




This function is available only for some models. If it is not displayed on your web UI, it is unavailable for the product that you purchased.

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

To perform troubleshooting:

- Step 1** [Log in to the web UI.](#)
- Step 2** Choose **More > Network Diagnosis**.
- Step 3** Click **Diagnose**.

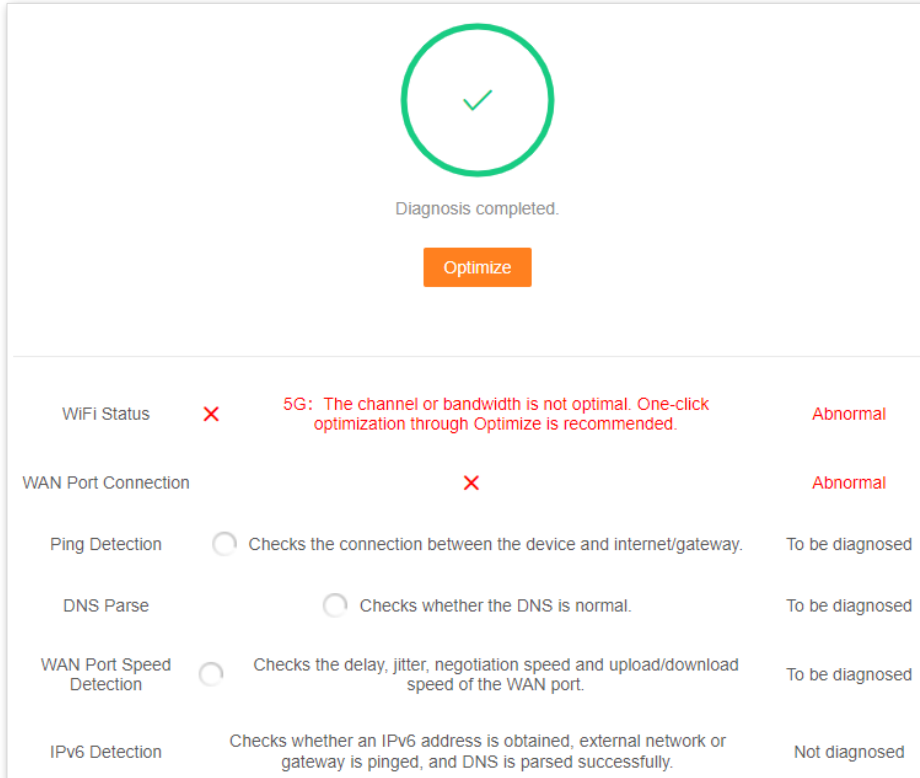


If the internet access failed or the internet lag is severe, network diagnosis is recommended.

[Diagnose](#)

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

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



Diagnosis completed.

Optimize

WiFi Status	×	5G: The channel or bandwidth is not optimal. One-click optimization through Optimize is recommended.	Abnormal
WAN Port Connection	×		Abnormal
Ping Detection	○	Checks the connection between the device and internet/gateway.	To be diagnosed
DNS Parse	○	Checks whether the DNS is normal.	To be diagnosed
WAN Port Speed Detection	○	Checks the delay, jitter, negotiation speed and upload/download speed of the WAN port.	To be diagnosed
IPv6 Detection		Checks whether an IPv6 address is obtained, external network or gateway is pinged, and DNS is parsed successfully.	Not diagnosed

---End

2.8.6 TR069



This function is available only for some models. If it is not displayed on your web UI, it is unavailable for the product that you purchased.

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

To access the configuration page, [Log in to the web UI](#) of the router and choose **More > TR069**.

TR069

TR069

ACS

URL

ACS Username

ACS Password

Periodic Notification

Notification Interval

Connection Request

Connection Request Username

Connection Request Password

Port

STUN Connection

STUN

The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description	
TR069	Used to enable or disable the Technical Report 069 (TR-069) function.	
ACS	URL	Specifies the domain name of the ACS.
	ACS Username	Specifies the user name used to authenticate the Mesh device when the Mesh device connects to the ACS using the CPE WAN management protocol.

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

2.8.7 Smart power saving

WiFi schedule



This function is available only for some models. If it is not displayed on your web UI, it is unavailable for the product that you purchased.

Overview

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

To access the configuration page, [log in to the web UI](#) of the Mesh device, and choose **More > Smart Power Saving > WiFi Schedule**. The following figure displays the page when the WiFi Schedule function is enabled.


WiFi Schedule

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

WiFi Schedule

Turn Off at: → ⓘ The Schedule Disable time takes effect based on the system time

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



Scan to download app

How to connect to the WiFi network during WiFi-disabling period?

Method 1: Use the Tenda WiFi app with your account and enable/disable the WiFi network anytime, anywhere.

Method 2: Use an Ethernet cable to connect your computer to the router, visit tendawifi.com to log in to the web UI, and enable the WiFi network manually.



To make the WiFi schedule work properly, ensure that the system time is synchronized with the internet time. Refer to [System time](#) for configuration.

The following table describes the parameters displayed on this page.

Parameter description

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

Set a WiFi schedule

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

Configuration procedure:

- Step 1** [Log in to the web UI.](#)
- Step 2** Choose **More > Smart Power Saving > WiFi Schedule.**
- Step 3** Enable **WiFi Schedule.**
- Step 4** Set a period for the Wi-Fi networks to be disabled, which is **22:00 – 07:00** in this example.
- Step 5** Set the days when the function works, which is **Every Day** in this example.
- Step 6** Click **Save.**

WiFi Schedule

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

WiFi Schedule

Turn Off at → ⓘ The Schedule Disable time takes effect based on the system time

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

---End

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

LED indicator

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



[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**.

LED Indicator

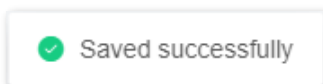
You can enable/disable LED indicators of all modes here.

LED Indicator Schedule Disable

Turn Off at 00:00 - 07:00

Save

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



---End

2.8.8 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**.



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

Channel & Bandwidth

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

2.4 GHz WiFi

Network Mode

Channel
Current Channel:1

Bandwidth
Current Bandwidth:20

5 GHz WiFi


Network Mode



Channel
Current Channel:48

Bandwidth
Current Bandwidth:80

The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
	<p>Specifies various protocols used for wireless transmission.</p> <p> TIP</p> <p>The network modes vary with models. Refer to the product you purchased.</p> <p>2.4 GHz Wi-Fi network supports the following modes:</p> <ul style="list-style-type: none"> - 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/ac: 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 802.11 ac protocol 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. - 802.11b/g/n/ac/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, IEEE 802.11ac or IEEE 802.11ax protocol can connect to the 2.4 GHz WiFi network of the Mesh device. <p>5 GHz WiFi network supports the following modes:</p> <ul style="list-style-type: none"> - 802.11a/n: Indicates that devices compliant with the IEEE 802.11a protocol, and devices working at 5 GHz and compliant with the IEEE 802.11n can connect to the 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. <p>6 GHz Wi-Fi network supports the 802.11ax mode.</p> <ul style="list-style-type: none"> - 802.11ax: Indicates that devices working at 6 GHz and compliant with the IEEE 802.11ax can connect to the router.
Network Mode	
Channel	<p>Specifies the channel in which the Wi-Fi network works.</p> <p>By default, the wireless channel is Auto, which indicates that the 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.</p>

Parameter	Description
Bandwidth	<p>Specifies the bandwidth of the wireless channel of a Wi-Fi network. Please change the default settings only when necessary.</p> <p> TIP</p> <p>The bandwidth varies with models. Refer to the product you purchased.</p> <ul style="list-style-type: none"> - 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 at 5 GHz and 6 GHz. - 160MHz: Indicates that the channel bandwidth used by the Mesh device is 160 MHz. This option is available at 5 GHz and 6 GHz. - 20/40/80MHz: Specifies that a Mesh device can switch its channel bandwidth among 20 MHz, 40 MHz and 80 MHz based on the ambient environment. This option is available only at 5 GHz. - 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 at 5 GHz and 6 GHz.
Enable PSC	<p>Specifies whether the Preferred Scanning Channel (PSC) function is enabled. When it is enabled, the success rate and stability of Wi-Fi 6E wireless terminals connecting to the router's 6 GHz network will be improved. It is enabled by default.</p> <p> TIP</p> <p>This option is only available for MX21 Pro/EX21 Pro/Mesh21XEP.</p>

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 **More > WiFi Settings > WPS**.



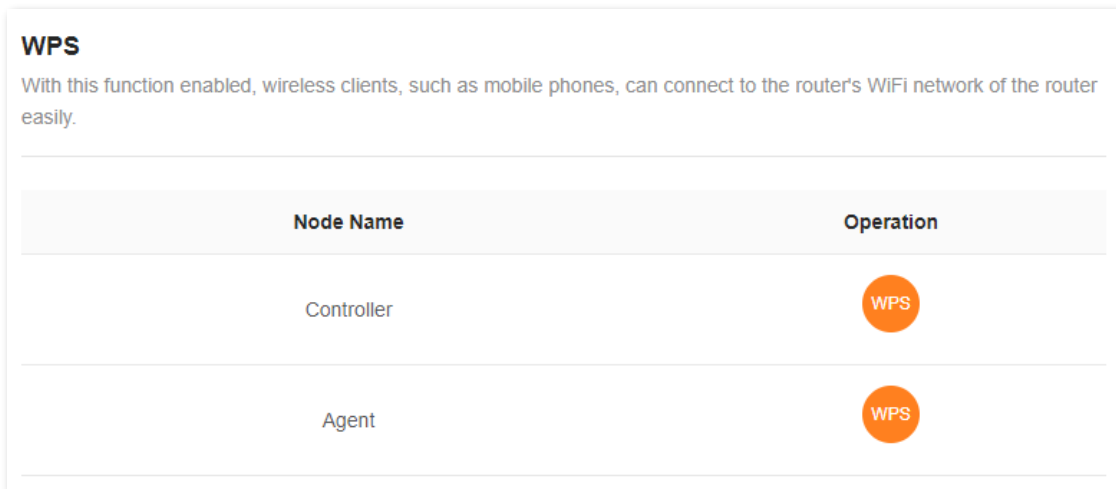
- This function only applies to WPS-enabled Wi-Fi devices. It is enabled by default and cannot be disabled.
- Wi-Fi networks encrypted with WPA3 cannot be connected through WPS.
- The WPS negotiation times out in 120 seconds. The **WPS** button is disabled during WPS negotiation.

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


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

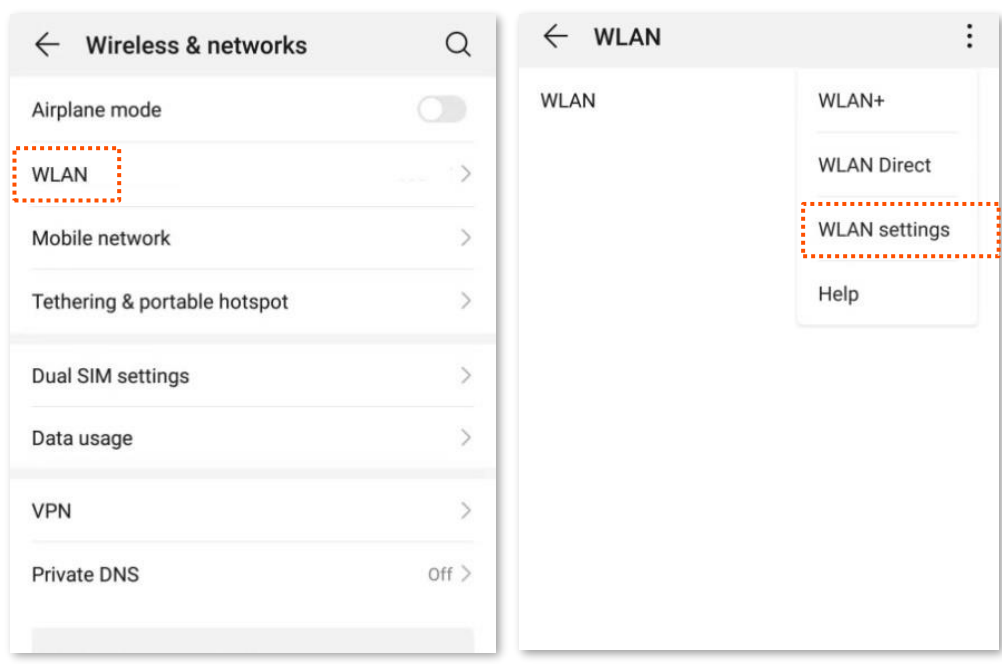
Step 2 Choose **More > WiFi Settings > WPS**.

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

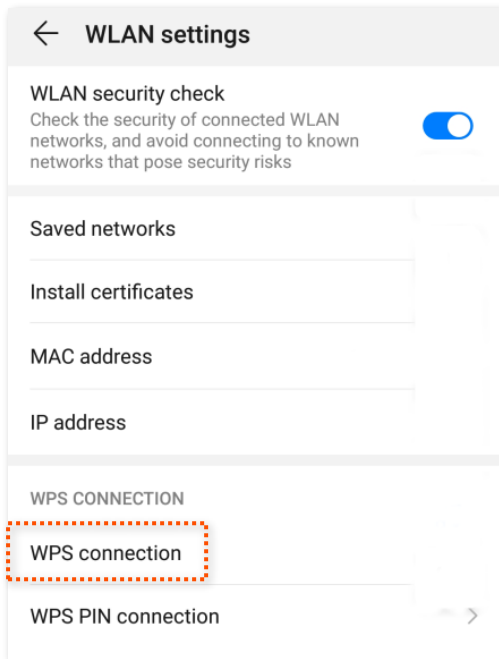


Step 4 Configure the WPS function on your WiFi-enabled devices within 2 minutes. Configuration on various devices may differ (Example: HUAWEI P10).

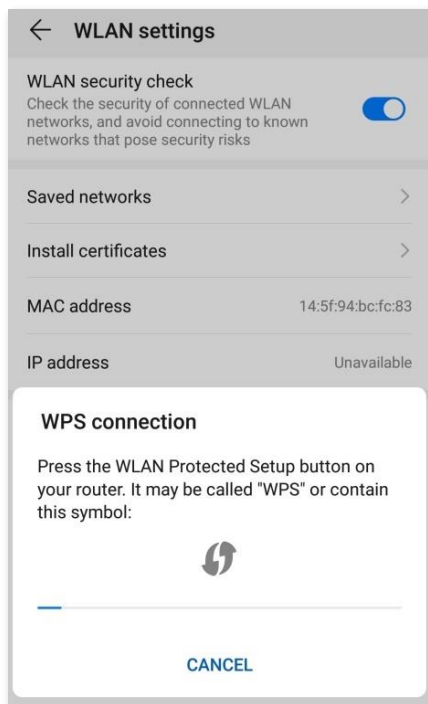
1. Find **WLAN** settings on your phone.
2. Tap , and choose **WLAN settings**.



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.



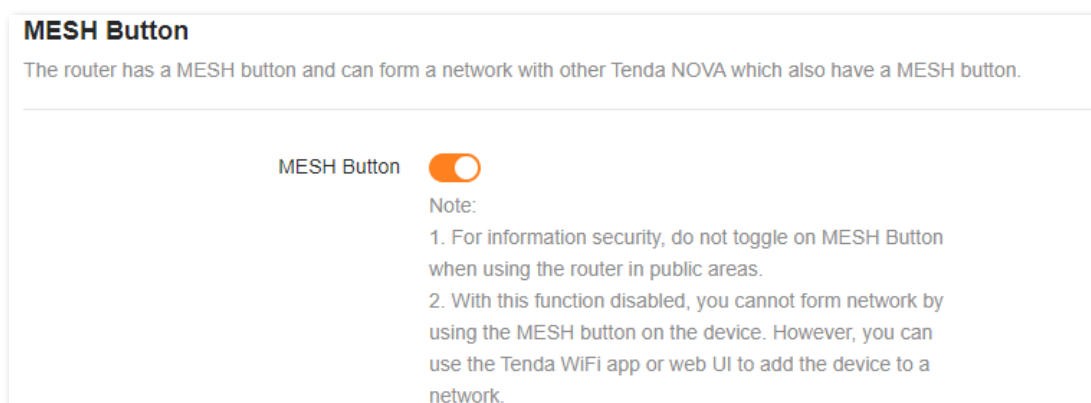
- For information security, do not enable **MESH Button** when using the Mesh device in public areas.
- With this function disabled, you cannot form a network by using the **MESH** button on the device. However, you can use the Tenda WiFi App or web UI to add the device to a network.

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

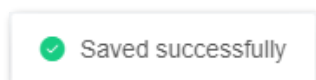
Step 1 [Log in to the web UI](#).

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

Step 3 Enable or disable **MESH Button**.



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



---End

2.8.9 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.

LAN Settings

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

LAN IP Address

Subnet Mask

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

Address Pool Range -

Lease Time ⓘ

DNS

Primary DNS

Secondary DNS





Static IP Reservation List

Device Name	IP Address	MAC Address	Operation
123	192.168.0.143	XXXXXXXXXX	✎ 🗑

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	<p>Specifies the valid duration of the IP address that is assigned to a client.</p> <p>When the lease time reaches half, the client will send a DHCP Request to the DHCP server for renewal. If the renewal succeeds, the lease is renewed based on the time of the renewal application. If the renewal fails, the renewal process is repeated at 7/8 of the lease period. If it succeeds, the lease is renewed based on the time of the renewal application. If it still fails, the client needs to reapply for IP address information after the lease expires.</p> <p>It is recommended to keep the default value.</p>
DNS	<p>Specifies whether to allocate another DNS address to the client. 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.</p> <p> TIP</p> <p>This Mesh device has the DNS proxy function.</p>
Primary DNS	<p>Specifies the primary DNS address allocated to the client by the Mesh device.</p> <p> TIP</p> <p>Make sure that the primary DNS server is the IP address of the correct DNS server or DNS proxy. Otherwise, you may fail to access the internet.</p>
Secondary DNS	<p>Specifies the secondary DNS server address of the Mesh device used to assign to the clients. It is optional.</p>
Static IP Reservation List	<p>Device Name Specifies the name of the client.</p>
	<p>IP Address Specifies the IP address reserved for the client.</p>
	<p>MAC Address Specifies the MAC address of the client.</p>
	<p>Operation</p> <p> : Used to edit a static IP address reservation rule.</p> <p> : Used to delete a static IP address reservation rule.</p>

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 **Add** in **Static IP Reservation List**.

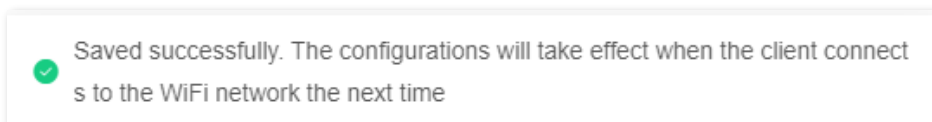
Step 4 Set **Select Device**.

- 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.

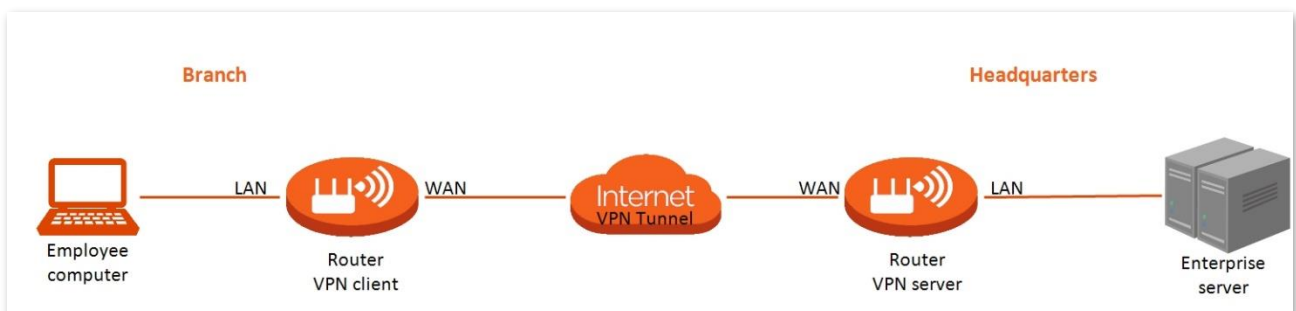


---End

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 Mesh devices 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.

VPN

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

PPTP Server
PPTP/L2TP Client

PPTP Server

Address Pool Range - 10.0.0.

MPPE Encryption

Save

PPTP Account Add

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





Online PPTP User

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

The following table describes the parameters displayed on this page.

Parameter description

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

• 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**.

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

The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
User Name	Specifies the VPN user name, which the VPN user uses when making PPTP dial-ups (VPN connection).
Dial-In IP Address	Specifies the IP address of the PPTP client. If the client is a 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**.



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**.

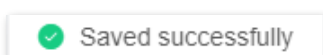
Step 3 Enable **PPTP Server**.

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

Step 5 Click **Add**. 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.



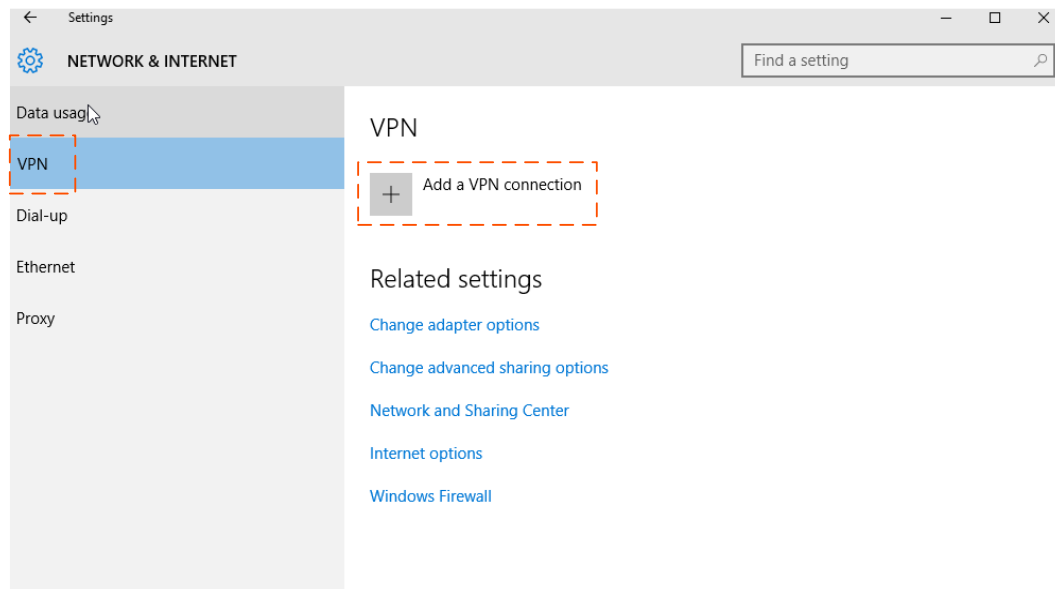
---End

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**.

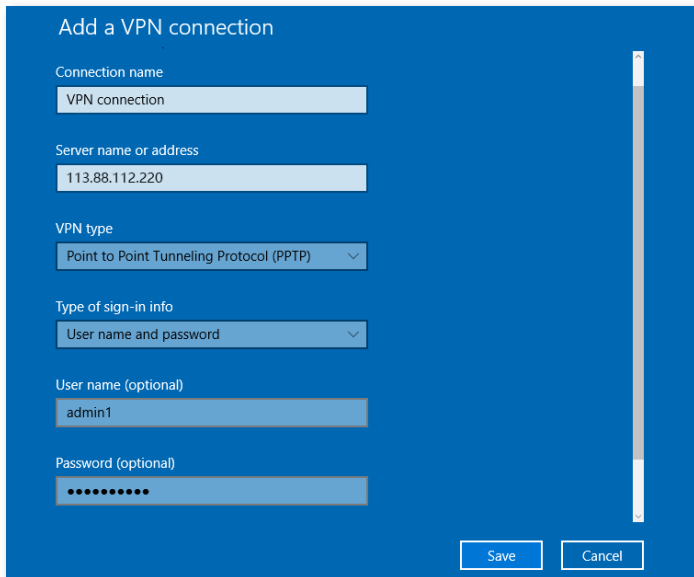


- Step 2** Choose **VPN** on the left side, and click **Add a VPN connection**.

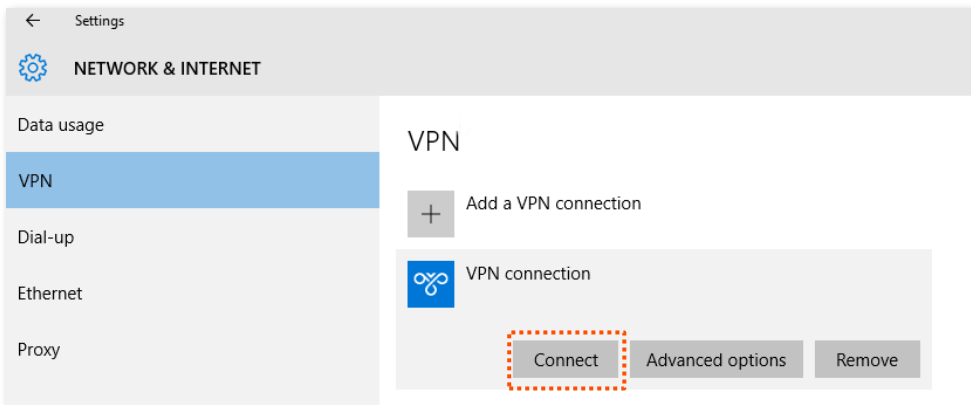



- Step 3** Configure the VPN parameters.

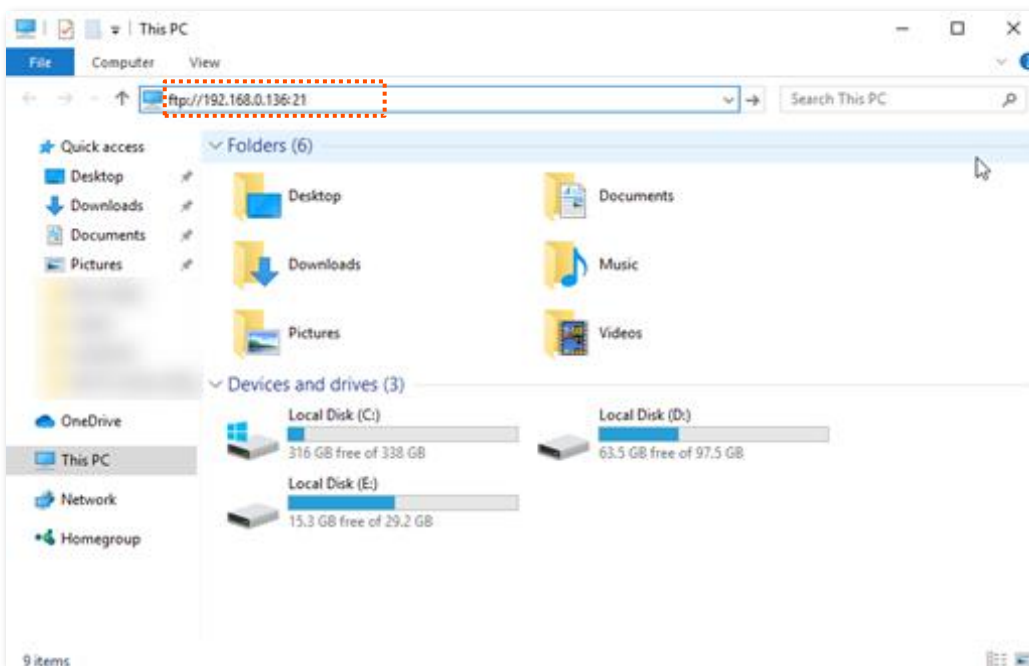
1. Enter a connection name, such as **VPN connection**.
2. Enter the server address, which is **113.88.112.220** in this example.
3. Select a VPN type, which is **Point to Point Tunneling Protocol (PPTP)** in this example.
4. Select a type of sign-in info, which is **User name and password** in this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

Log On As

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

FTP server: 192.168.0.136

User name:

Password:

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

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

Log on anonymously Save password

Log On Cancel

---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.

VPN

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

PPTP Server **PPTP/L2TP Client**

PPTP/L2TP Client

Client Type: PPTP

Server IP/Domain Name:

User Name:

Password:

Status: Disconnected

Save

Parameter description

Parameter	Description
PPTP/L2TP Client	Used to enable or disable the PPTP/L2TP client function.
Client Type	<p>Specifies the client type that the Mesh device serves as, either PPTP or L2TP.</p> <ul style="list-style-type: none"> - 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/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	Specify the user name and password that the PPTP/L2TP server assigns to the PPTP/L2TP clients.
Password	
Status	Specifies the connection status of the VPN connection.

- **Access VPN resources with the 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/Domain Name**, which is **113.88.112.220** in this example.

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

Step 7 Click **Save**.

VPN

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

PPTP Server **PPTP/L2TP Client**

PPTP/L2TP Client

Client Type

Server IP/Domain Name

User Name

Password

Status Disconnected

---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 set-top box (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:** 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.

IPTV

You can configure multicast and IPTV function here.

Multicast

STB

VLAN

Ethernet Port Selection

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

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

Default

Ethernet Port 3

Save

The following table describes the parameters displayed on this page.

Parameter description

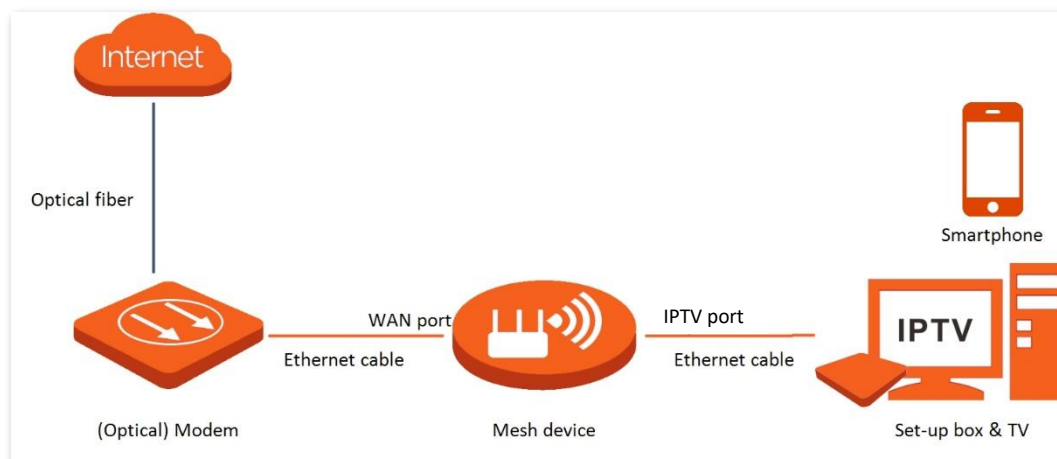
Parameter	Description
Multicast	Used to enable or disable the multicast function.
STB	Used to enable or disable the IPTV function of the Mesh device. When this function is enabled, the port LAN3/IPTV (MX6/EX6/MX12/EX12) or LAN (MX3/EX3) can be used only as an IPTV port and be connected to an IPTV set-top box.
VLAN	Specifies the VLAN ID of your IPTV service. It is required when STB is enabled. <ul style="list-style-type: none"> - If your ISP does not provide any VLAN ID information when the IPTV service is available, keep Default. - If you have obtained the VLAN ID from your ISP when the IPTV service is available, choose Custom VLAN and enter the VLAN value.
Ethernet Port Selection	Specifies the IPTV port. It is required when STB is enabled. <div style="margin-top: 5px;"> TIP This parameter is available only for MX15 Pro/EX15 Pro/Mesh15XP/MX21 Pro/EX21 Pro/Mesh21XEP. </div>

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. Select the IPTV port for **Ethernet Port Selection.**

Ethernet Port 2 is used as an example here.



This substep is required only for MX15 Pro/EX15 Pro/Mesh15XP/MX21 Pro/EX21 Pro/Mesh21XEP.

5. Click **Save.**

IPTV

You can configure multicast and IPTV function here.

Multicast

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

STB

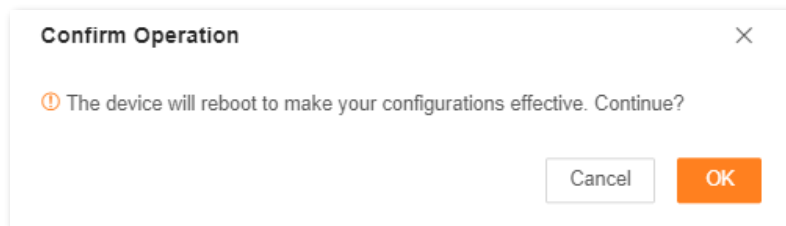
Connect the IPTV STB to the IPTV port of the router.

VLAN

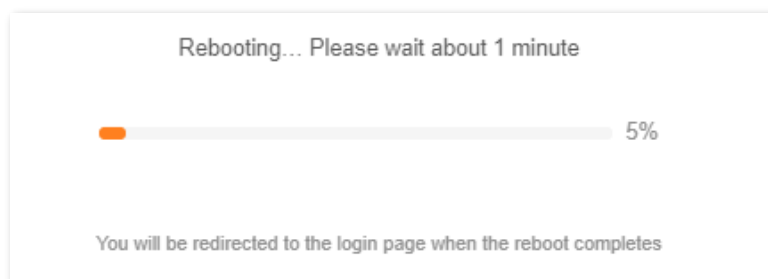
Ethernet Port Selection

Save

6. 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

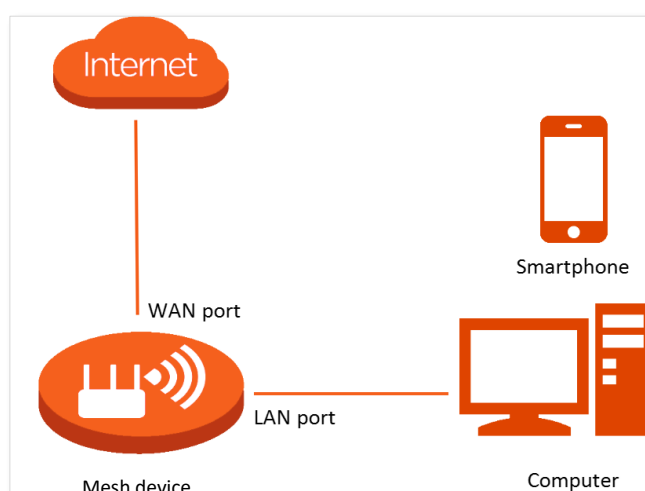
After completing the configuration, you can watch IPTV programs on your TV.

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**.

IPTV
You can configure multicast and IPTV functions here.

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

STB

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 a prompt indicating that 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**.

WAN Parameters

Speed
Current: 1000 Mbps full duplex

Save

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.

Speed	Application
100 Mbps full duplex	Indicates that the WAN port is working at the speed of 100 Mbps, and the port can receive and send data packets at the same time.
100 Mbps half duplex	Indicates that the WAN port is working at the speed of 100 Mbps, but the port can only receive or send data packets alternately.
10 Mbps full duplex	Indicates that the WAN port is working at the speed of 10 Mbps, and the port can receive and send data packets at the same time.
10 Mbps half duplex	Indicates that the WAN port is working at the speed of 10 Mbps, but the port can only receive or send data packets alternately.

2.8.10 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**.

APP Remote Management
Manage the router anytime, anywhere

APP Remote Management

Once enabled, you can remotely manage the router by Tenda WiFi app

ID

Cloud Account

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.

Parameter	Description
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.



- 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.	
Blacklist Device	Device Name	Specifies the name of the blacklisted client.
	MAC Address	Specifies the MAC address of the blacklisted client.
	Operation	: Used to remove a client from the blacklist.

Only prohibit specified clients from accessing the internet

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

Goal: Only prohibit your kid's phone from accessing the internet.

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

Assume that:

Client	MAC address	Status
Your kid's phone	8C:EC:4B:B3:04:92	Connected

Configuration procedure:

- Step 1** [Log in to the web UI.](#)
- Step 2** Choose **More > Advanced > MAC Address Filter.**
- Step 3** Enable **MAC Address Filter.**
- Step 4** Click **Add.**

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

MAC Address Filter

Blacklist Device (Only block internet access from client with listed MAC address) [Add](#)

Device Name	MAC Address	Operation
No Data		

[Save](#)

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

Add Blacklist ×

Select Device

Device Name

MAC Address

Step 6 Click **OK**.

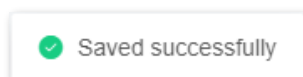
The blacklisted client is displayed under **Blacklist Device**.

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

Device Name	MAC Address	Operation
Kid's phone	8C:EC:4B:B3:04:92	

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**.

Firewall

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

ICMP Flood Attack Defense

TCP Flood Attack Defense

UDP Flood Attack Defense

Block Ping from WAN

Save

The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
ICMP Flood Attack Defense	Used to enable or disable the ICMP flood attack defense. The ICMP flood attack means that, to implement attacks on the target host, the attacker sends a large number of ICMP Echo messages to the target host, which causes the target host to spend a lot of time and resources on processing ICMP Echo messages, but cannot process normal requests or responses.
TCP Flood Attack Defense	Used to enable or disable the TCP flood attack defense. The TCP flood attack means that, to implement attacks on the target host, the attacker quickly initiates a large number of TCP connection requests in a short period, and then suspends in a semi-connected state, thereby occupying a large number of server resources until the server denies any services.
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.



- 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**.

DMZ Host

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

DMZ Host

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

DMZ Host IP Address

192.168.0.100

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.

Parameter	Description
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**

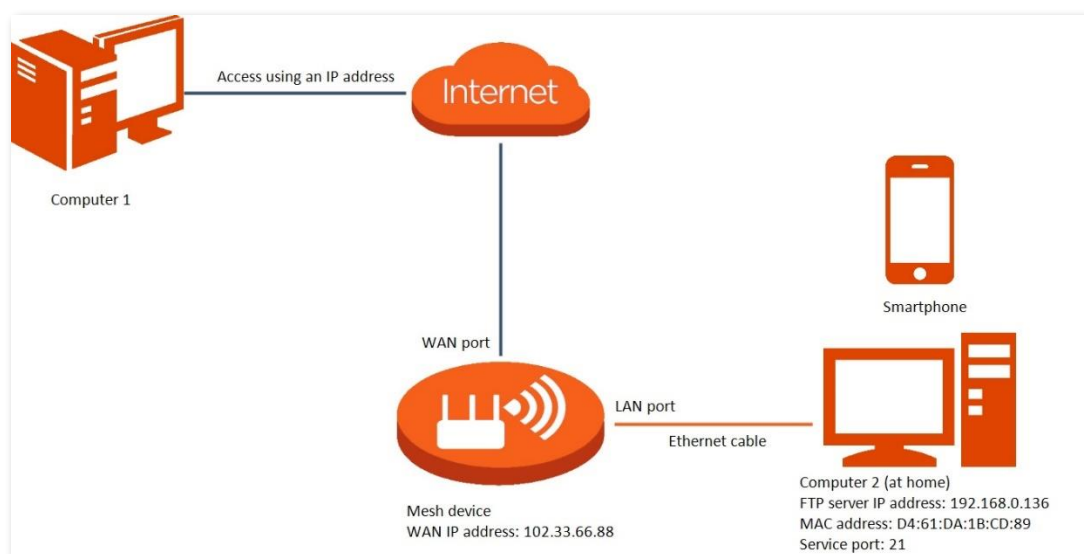
MAC address: **D4:61:DA:1B:CD:89**

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**.

DMZ Host

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

DMZ Host

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

DMZ Host IP Address

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

1. Choose **More > Network Settings > LAN Settings**.
2. Click **Add**.
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**.

Static IP Reservation List <input type="button" value="Add"/>			
Device Name	IP Address	MAC Address	Operation
FTP server	192.168.0.136	d4:61:da:1b:cd:89	<input type="button" value="✎"/> <input type="button" value="🗑️"/>

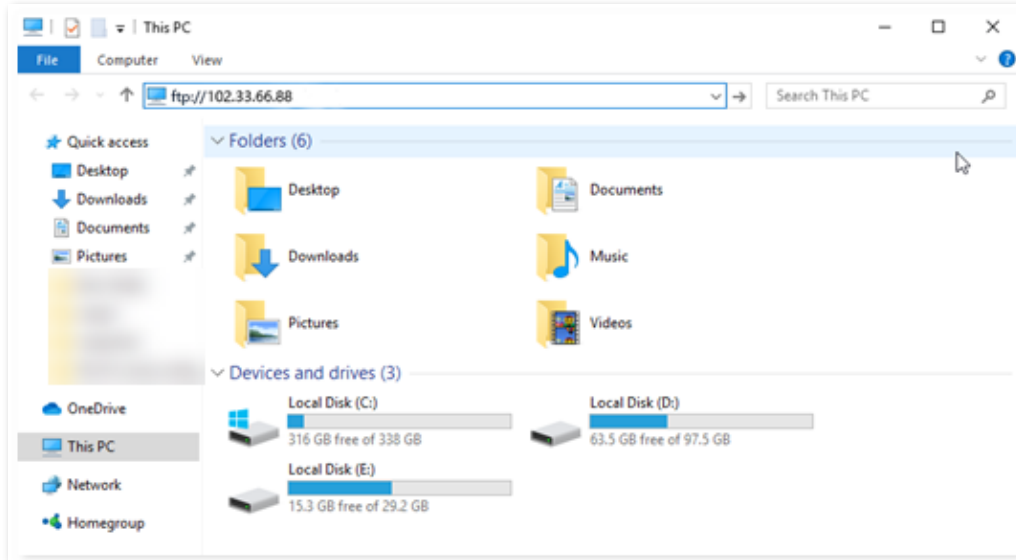
-----End

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"*.

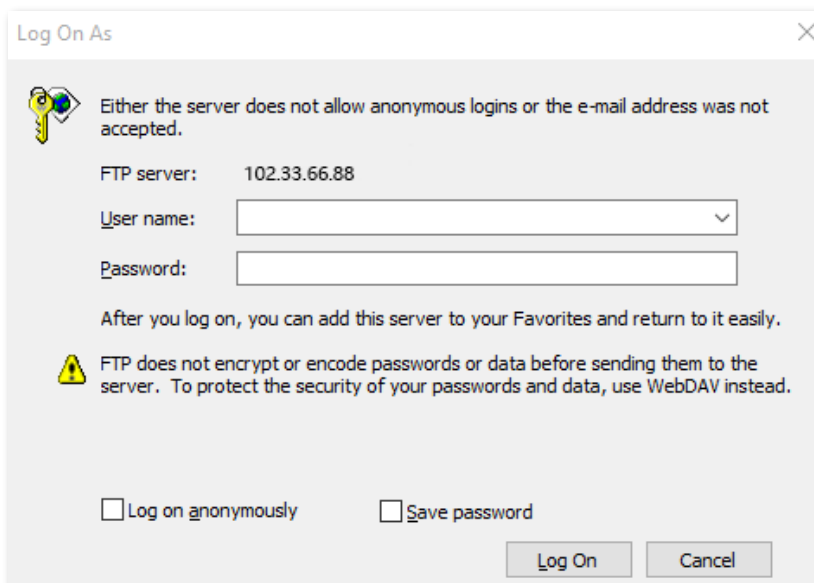
In this example, the address is “<ftp://102.33.66.88>”. You can find the WAN IP address of the Mesh device in [WAN port information](#).



If the default intranet service port number is 80, change the service port number to an uncommon one (1025–65535), such as 9999.



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



If you want to access the server within a LAN using a domain name, refer to the solution [DMZ + DDNS](#).



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

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.

Remote Web Management

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

Remote Web Management


Remote IP Address

Port

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	<p>Specifies the IP address of the host which can access the web UI of the Mesh device remotely.</p> <ul style="list-style-type: none"> - Any IP Address: Indicates that hosts with any IP address from the internet can access the web UI of the 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	<p>Specifies the port number of the Mesh device which is opened for remote management. You can change it as required.</p> <p> TIP</p> <ul style="list-style-type: none"> The port numbers from 1 to 1024 have 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.

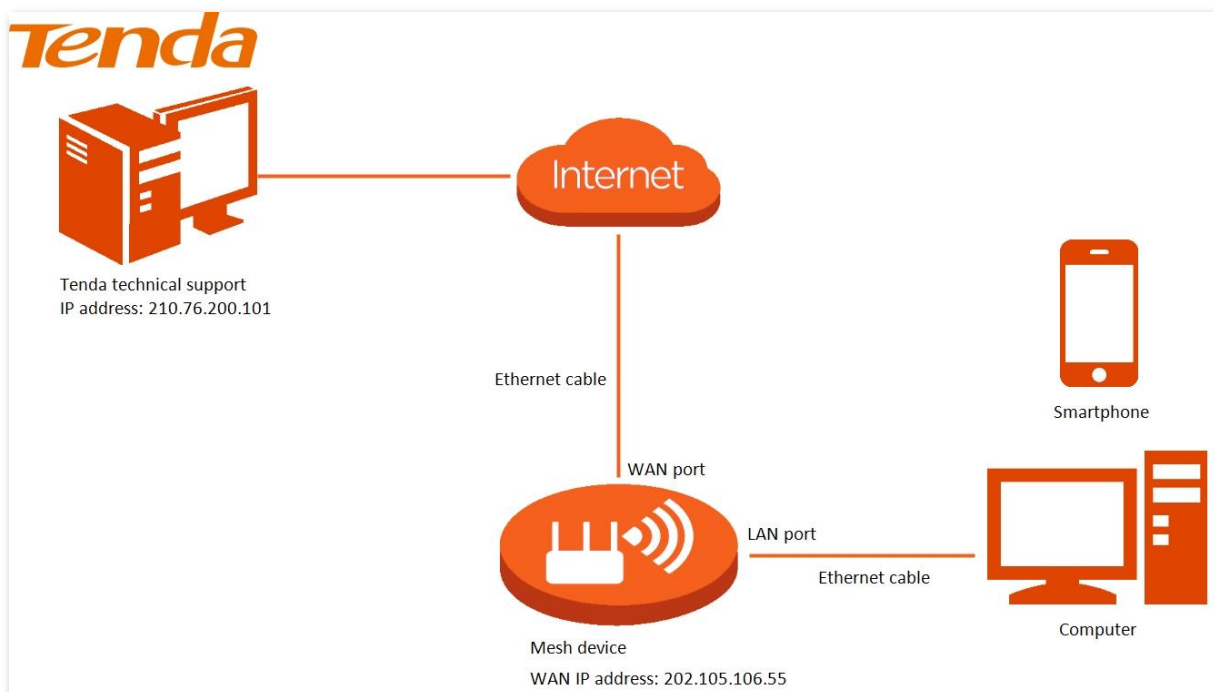
Goal: Ask the Tenda technical support to help you configure the Mesh device remotely.

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

Remote Web Management

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

Remote Web Management

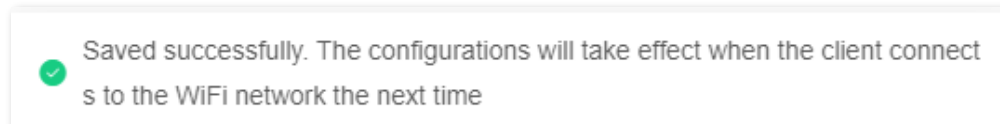
Remote IP Address Specified IP Address

Specified IP Address 210.76.200.101

Port 8888

Save

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**.

Static Routing




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

Routing Table Add

Destination Network	Subnet Mask	Gateway	WAN	Operation
0.0.0.0	0.0.0.0	172.16.200.1	WAN1	System
172.16.200.1	255.255.255.255	0.0.0.0	WAN1	System
192.168.0.0	255.255.255.0	0.0.0.0	br0	System
224.0.0.0	240.0.0.0	0.0.0.0	br0	System
239.0.0.0	255.0.0.0	0.0.0.0	br0	System

The following table describes the parameters displayed on this page.

Parameter description

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

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.

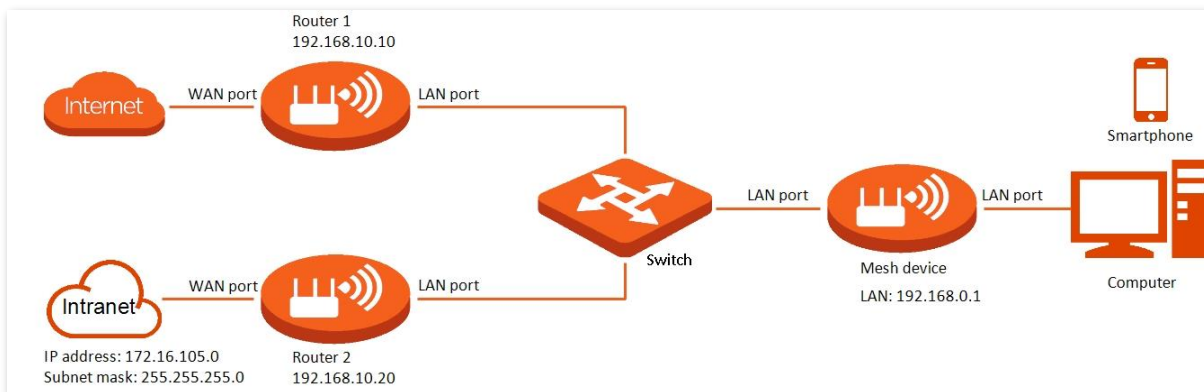
Solution: You can configure the static routing function to reach the goal.

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 the Mesh device.

Internet Settings

Network Status Connected

Connected time 2hour(s) 57minute(s)

ISP Type

Internet Connection Type

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

Advanced v

Step 3 Add a static routing rule on the Mesh device.

1. Choose **More > Advanced > Static Routing**.
2. Click **Add**.
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**.

Static Routing

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

Routing Table **Add**

Destination Network	Subnet Mask	Gateway	WAN	Operation
172.16.105.0	255.255.255.0	192.168.10.20	WAN1	

---End

After completing the configuration, you can access both the internet and intranet through the Mesh device 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**.

DDNS

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

DDNS

ISP Please select Register Now

User Name

Password

Domain Name

Connection Status Disconnected

Save

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 ISP is set, 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.

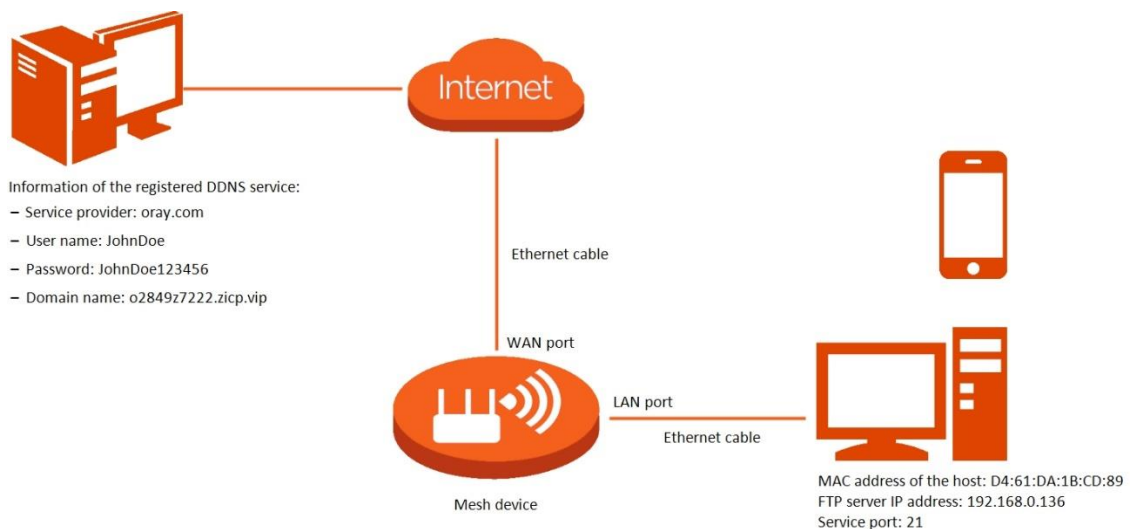
Solution: You can configure the DDNS plus port mapping functions to reach the goal.

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



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**.

DDNS

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

DDNS

ISP [Register Now](#)

User Name

Password

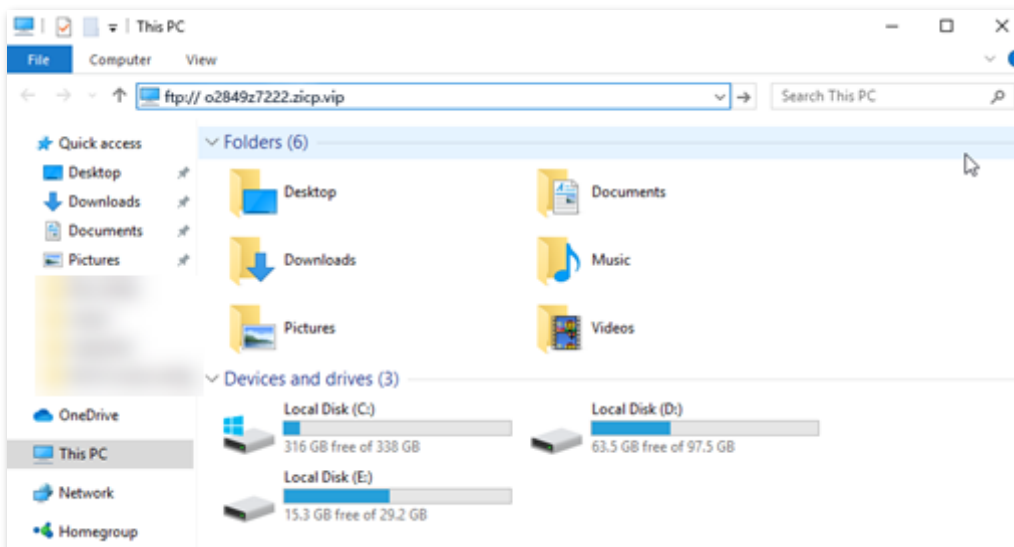
Connection Status Disconnected

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

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

---End

When completing the configuration, users from the internet can access the FTP server by visiting “*Intranet service application layer protocol name://Domain name*”. If the WAN port number is not the same as the default intranet service port number, the visiting address should be: “*Intranet service application layer protocol name://Domain name:WAN port number*”. In this example, the address is **ftp://o2849z7222.zicp.vip**.



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

Log On As

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

FTP server: o2849z7222.zicp.vip

User name:

Password:

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

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

Log on anonymously Save password



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.

UPnP

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

UPnP

UPnP List

Remote Host	External Port	Internal Host	Internal Port	Protocol
anywhere	64476	192.168.0.103	64476	UDP

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**.

Port Mapping

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



Port Mapping List Add

Internal IP Address	Internal Port	External Port	Protocol	Operation
192.168.0.145	21	21	TCP&UDP	✎ ✖

The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
Internal IP Address	Specifies the IP address of the intranet server.
Internal Port	Specifies the service port of the intranet server.
External Port	Specifies the external port for the internal port to map with.

Parameter	Description
Protocol	Specifies the mapping protocol.
Operation	<p>The available options include:</p> <p> : Used to edit a port mapping rule.</p> <p> : Used to delete a port mapping rule.</p>

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 **Add**.

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.

2.8.11 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	



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**.

System Time

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

System Time 2021-09-14 14:37:00

Sync Status Synced

Sync Mode

Time Zone

DST

Start 2021

End 2021

Status DST not use

The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
System Time	Specifies the current system time.
Sync Status	Specifies whether the system is synced.
Sync Mode	Specifies the sync mode of the system time. <ul style="list-style-type: none"> - Sync with internet time: Indicates that the system time is synced with the internet time. Time Zone must be set when this option is selected. - Sync with local time: Indicates that the system time is automatically synced with the local time on your host, and you do not need to select a time zone.
Time Zone	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.

Firmware Upgrade
Through firmware upgrades, the router can get new functions or more stable performance

Device Name	Current Firmware Version	Operation
Controller Primary Node New Version Available: V16.03.16.12(11225) Details	V16.03.16.11_multi	<input type="button" value="Online Upgrade"/> <input type="button" value="Local Upgrade"/>
Agent New Version Available: V16.03.16.12(11225) Details	V16.03.16.11_multi	<input type="button" value="Online Upgrade"/> <input type="button" value="Local Upgrade"/>

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

Firmware Upgrade
Through firmware upgrades, the router can get new functions or more stable performance

Device Name	Current Firmware Version	Operation
Controller Primary Node	V16.03.16.11_multi	<input type="button" value="Detect New Version"/> <input type="button" value="Local Upgrade"/>
Agent	V16.03.16.11_multi	<input type="button" value="Detect New Version"/> <input type="button" value="Local Upgrade"/>

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.**

Firmware Upgrade

Through firmware upgrades, the router can get new functions or more stable performance

Device Name	Current Firmware Version	Operation
Controller Primary Node <small>New Version Available: V16.03.16.12(11225) Details</small>	V16.03.16.11_multi	<div style="text-align: right;"> 92% </div> <div style="text-align: center;"> <input type="button" value="Local Upgrade"/> </div>
Agent <small>New Version Available: V16.03.16.12(11225) Details</small>	V16.03.16.11_multi	<div style="text-align: right;"> 90% </div> <div style="text-align: center;"> <input type="button" value="Local Upgrade"/> </div>

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



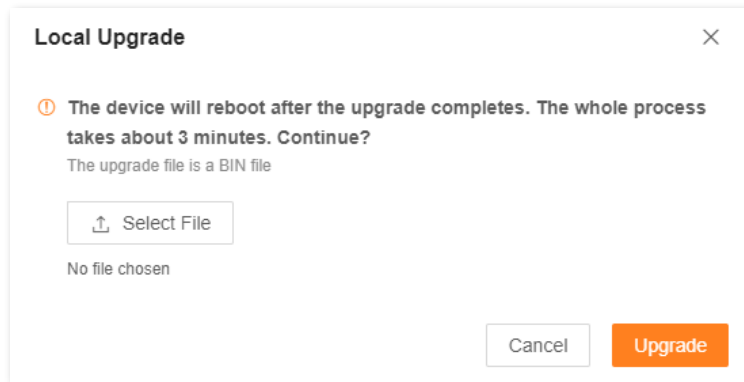
TIP
For better performance of the new firmware of the Mesh device, you are recommended to reset the Mesh device to factory settings and re-configure the Mesh device after the upgrade completes.

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**.

Backup & Restore

Backup
Save the current configuration to local host

Restore
Restore to the previous configurations you backed up (the backup file is a CFG file).

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

Device Name	Operation
Controller	<input type="button" value="Reset"/>

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.**

Backup & Restore

Backup
Save the current configuration to local host

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

---End

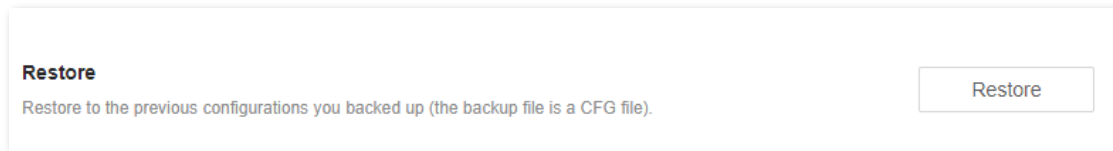
Restore the previous configuration of the Mesh device

To restore the previous configuration of the Mesh device:

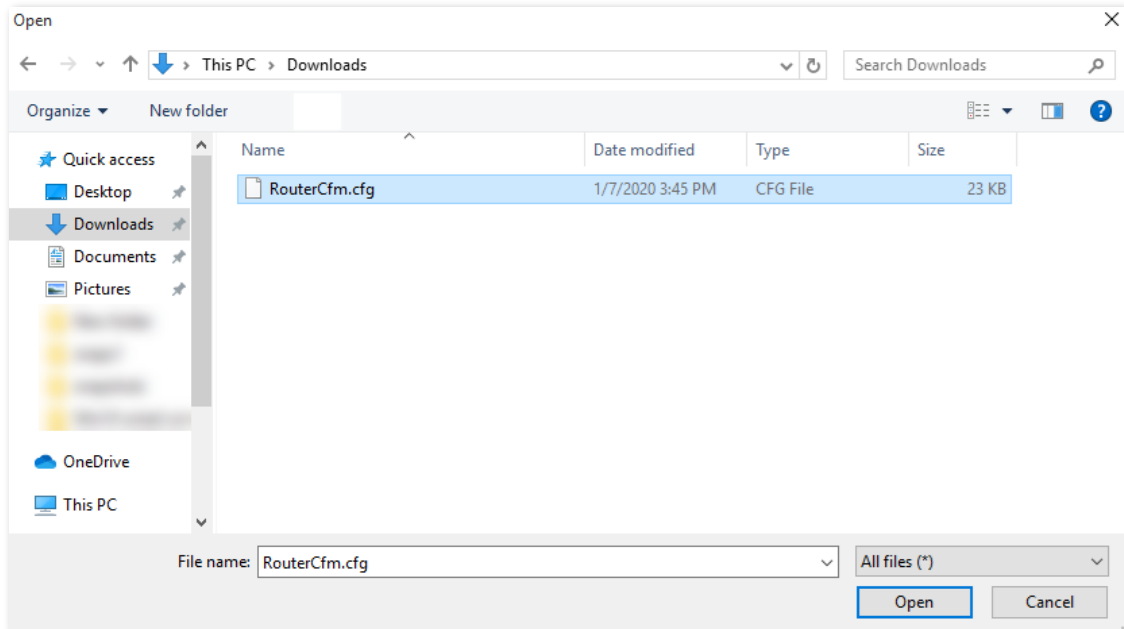
Step 1 [Log in to the web UI.](#)

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



- 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:

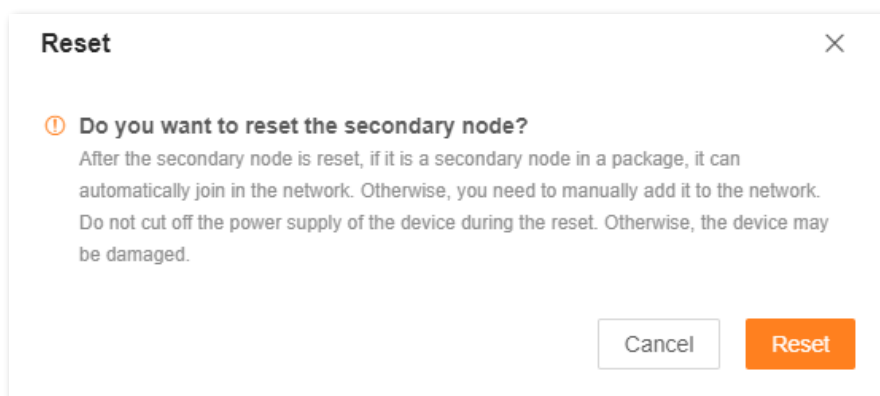
Step 1 [Log in to the web UI](#).

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

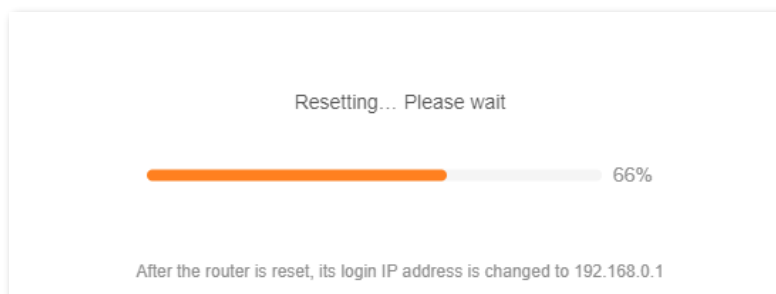
Step 3 Click **Reset** in the line of the node to be reset.

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

Step 4 Click **Reset** 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**.

Auto System Maintenance

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

Auto System Maintenance

Reboot at ⌚ ⓘ The auto system maintenance time takes effect based on the system time

Delay Reboot

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

The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
Auto System Maintenance	Used to enable or disable the auto system maintenance function.
Reboot at	Specifies the time when the Mesh device reboots automatically every day.
Delay Reboot	<p>Used to enable or disable the reboot delay function.</p> <ul style="list-style-type: none"> - Ticked: The function is enabled. When the time for rebooting approaches, if there is any user connected to the 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**.

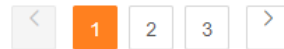
System Log

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

Export to Local

No.	Time	Type	Log Content
1	2022-12-05 08:54:54	system	LAN1 up
2	2022-12-05 08:54:42	system	Sync time success!
3	2000-01-01 00:00:33	system	wan1 up
4	2000-01-01 00:00:31	wan	Get ip success
5	2000-01-01 00:00:31	wan	PPPoE Recv PADS
6	2000-01-01 00:00:31	wan	PPPoE Wait for PADS
7	2000-01-01 00:00:31	wan	PPPoE Send PADR
8	2000-01-01 00:00:31	wan	PPPoE Recv PADO
9	2000-01-01 00:00:31	wan	PPPoE Wait PADO
10	2000-01-01 00:00:31	wan	PPPoE Send PADI

22 items in total



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 (v3.5.14 used for example), including:

- [App download and installation](#)
- [Registration and binding](#)
- [Quick setup](#)
- [Management type](#)
- [My WiFi](#)
- [Common settings](#)
- [System settings](#)
- [My profile](#)

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 \(computer\)](#) and [Web UI operations \(mobile client\)](#).

3.1 App download and installation

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

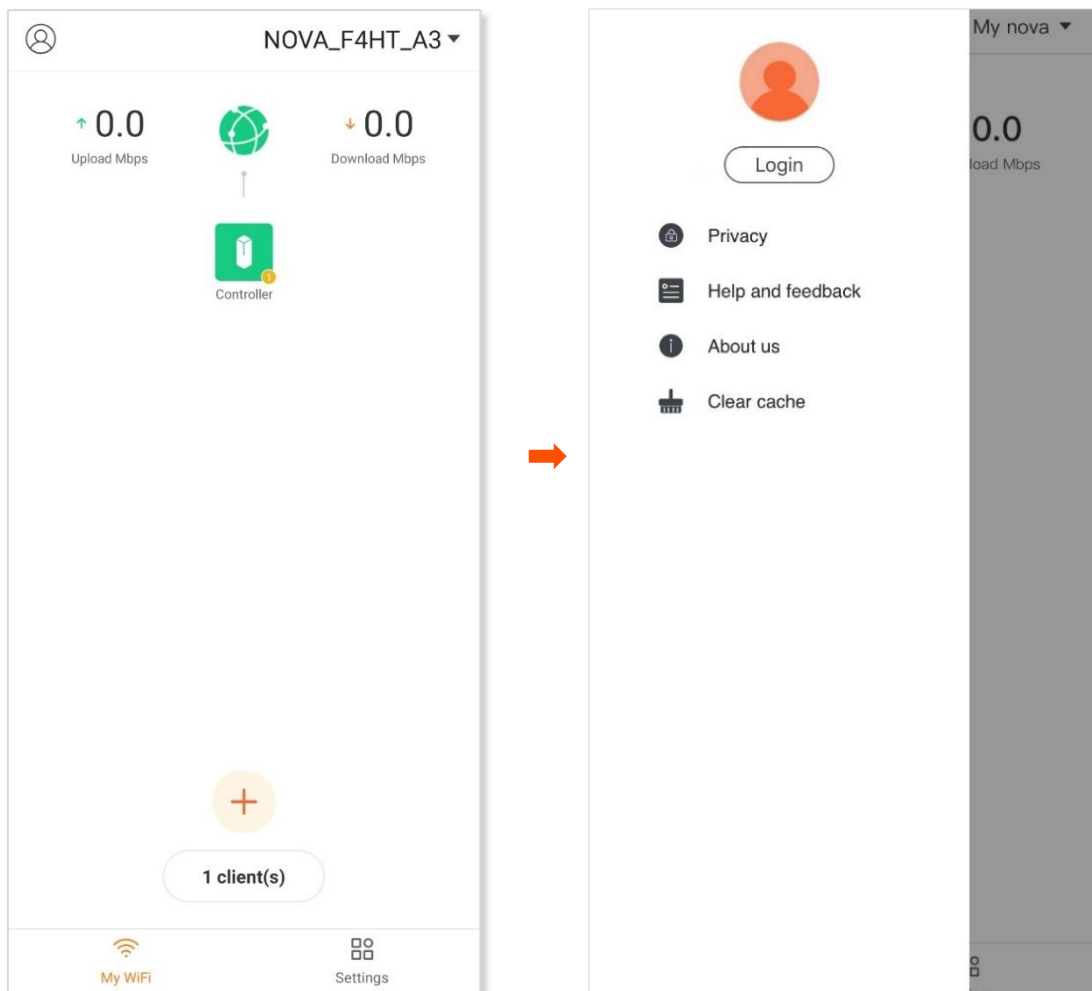


To log in to the Tenda WiFi App using a third-party account without registering a Tenda account, see [Log in to Tenda WiFi App](#).

Configuration procedure:

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

Step 2 Tap **Login**.

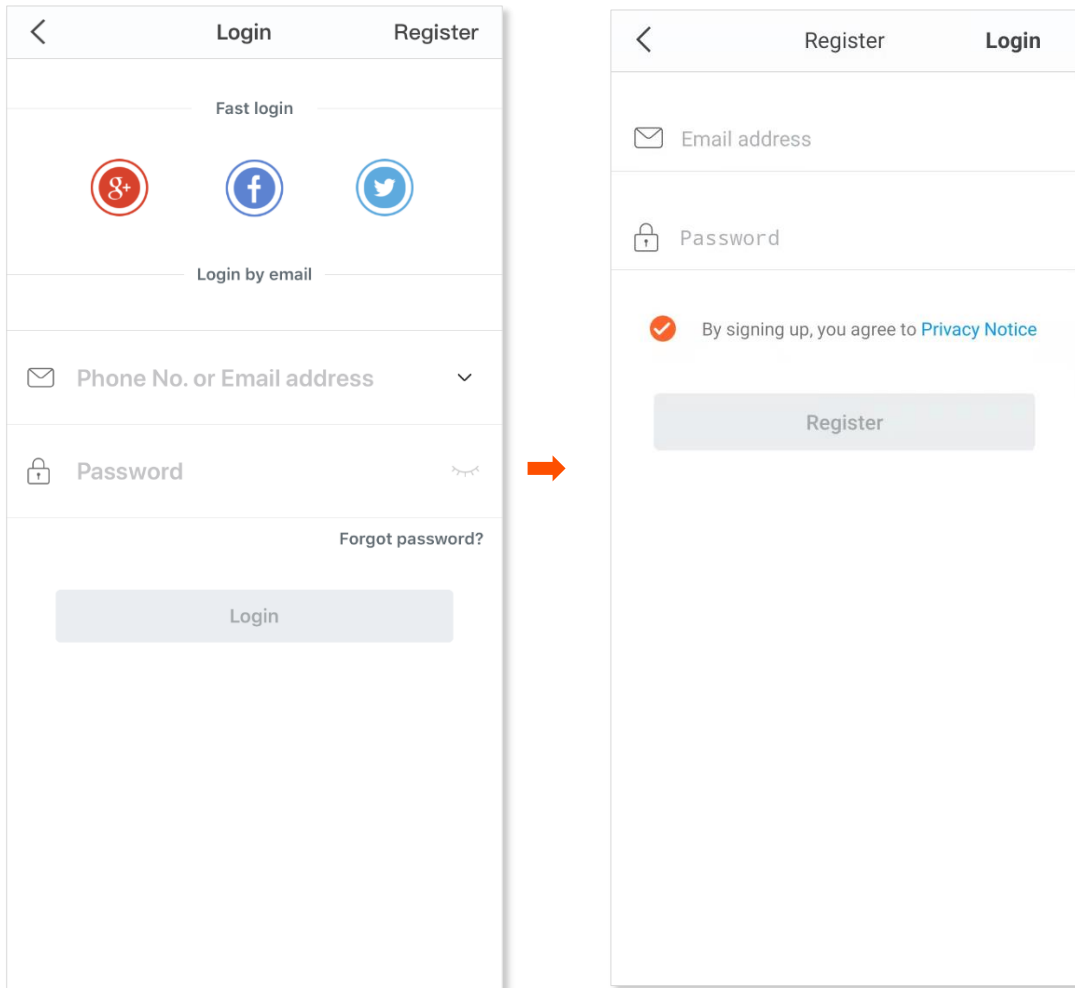


Step 3 Tap **Register** in the upper-right corner.

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**.

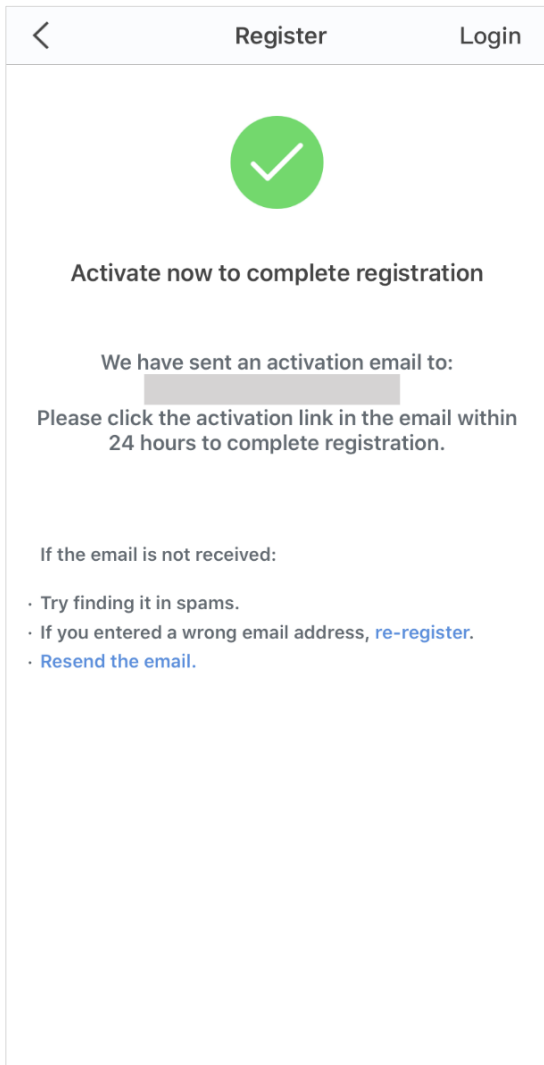
Step 7 Tap **Register**.

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

---End

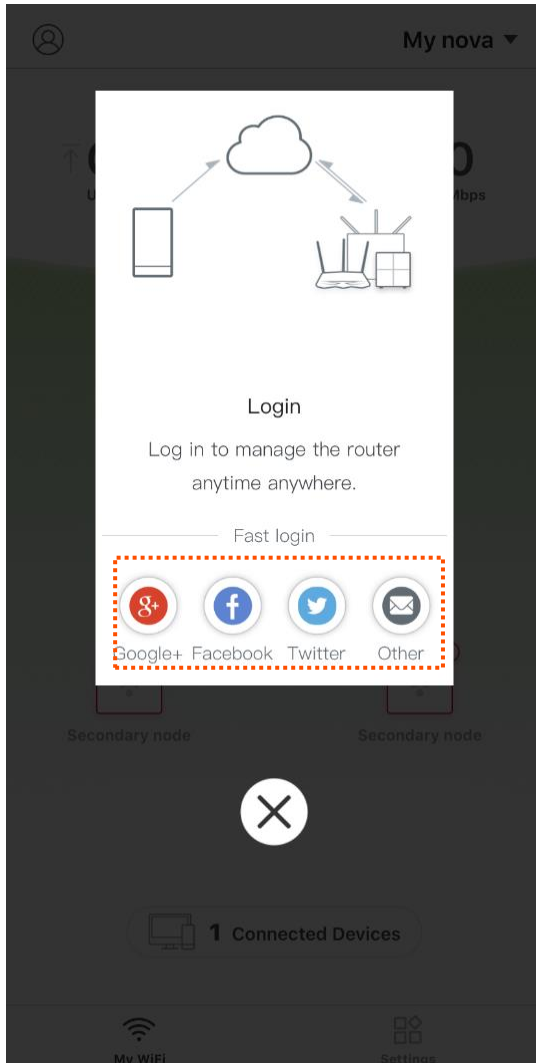
 Registration completes.


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

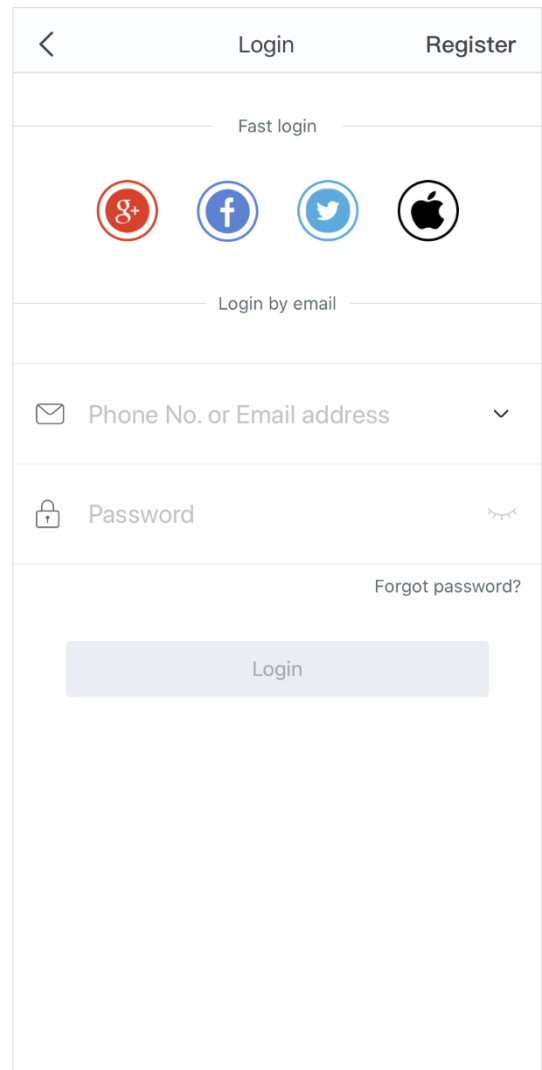
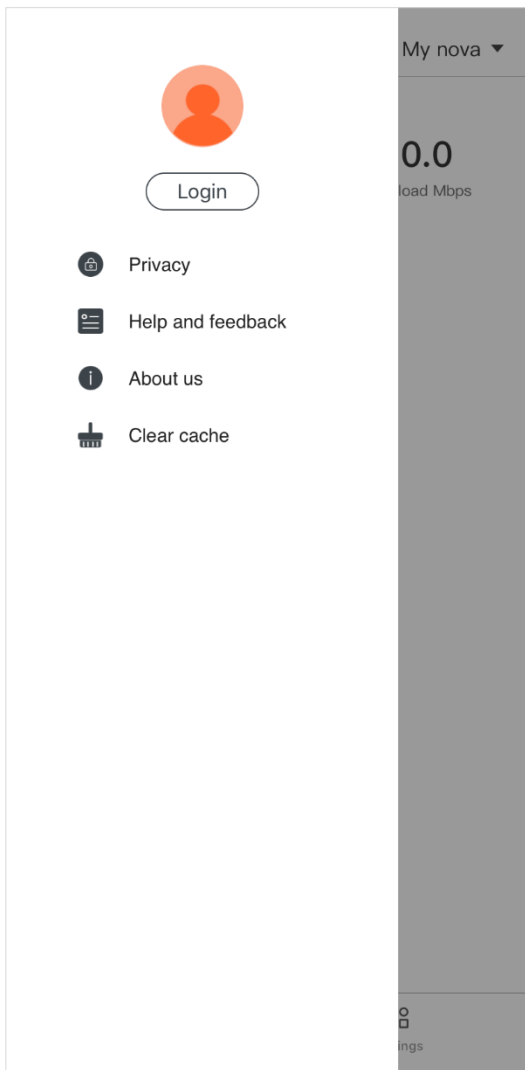


3.2.2 Log in to Tenda WiFi App

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.

Configuration 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



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

The administrator account can be used to authorize accounts. For details, see [Account authorization](#).

3.3 Quick setup

3.3.1 Connect your primary node to the internet

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

Configuration procedure:

Step 1 [Connect your primary node.](#)

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



TIP

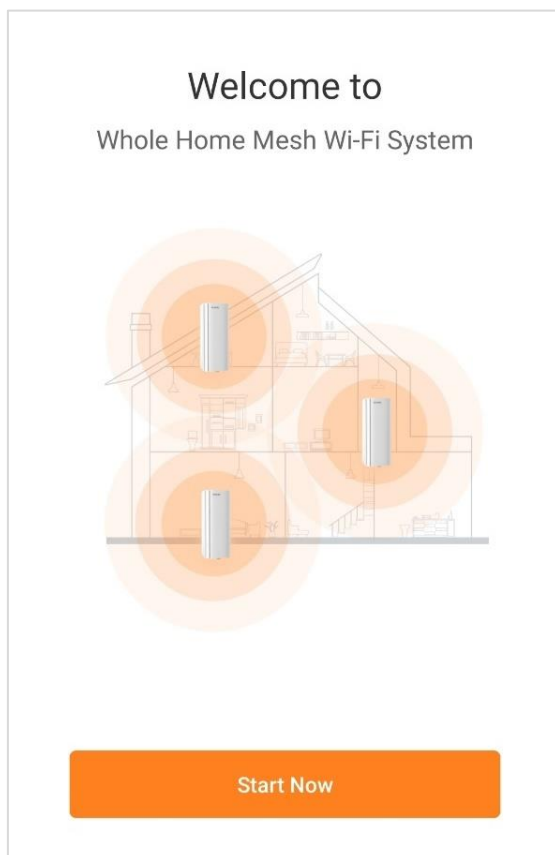
The default Wi-Fi name and password can be found on the bottom label of the device.

Step 3 Run the Tenda WiFi App.

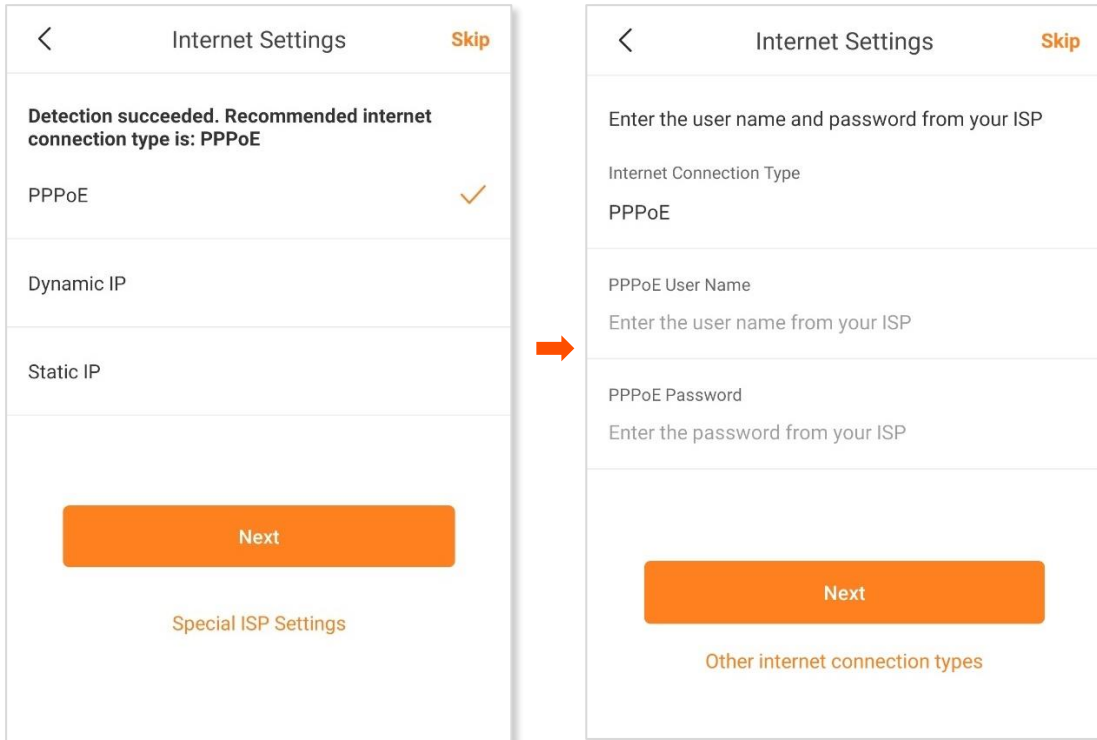


Tenda WiFi

Step 4 Tap **Start Now**.



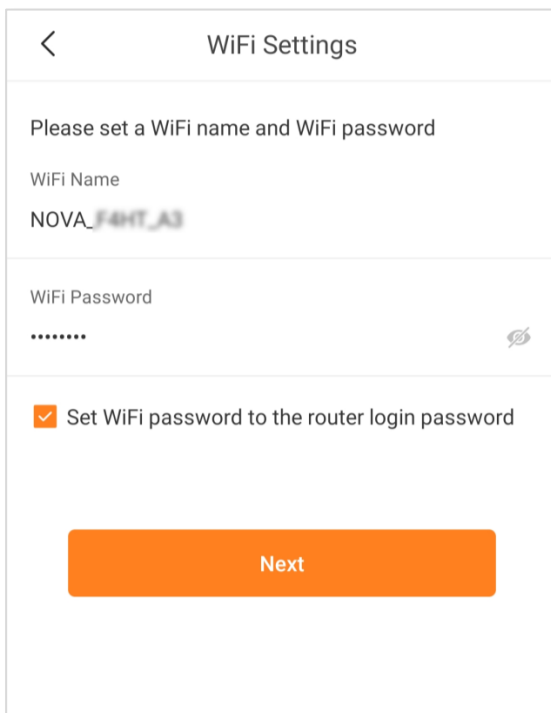
Step 5 Set required parameters (PPPoE is used for illustration here) and tap **Next**.



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.

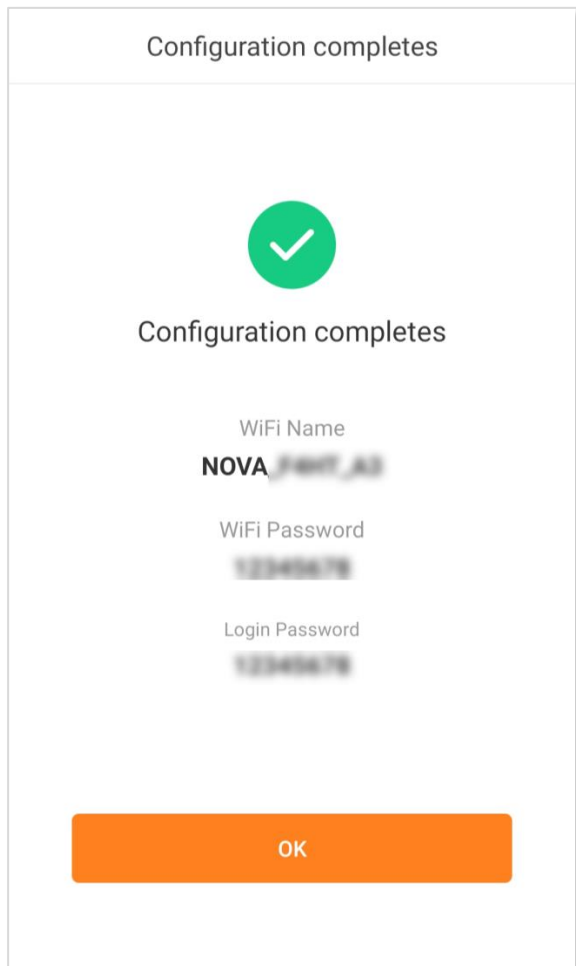
Step 6 Customize the **WiFi Name** and **WiFi Password**.





- 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 **WiFi Name** and **WiFi Password** for Wi-Fi login and **Login Password** for web UI login.

Step 7 Tap **OK**.



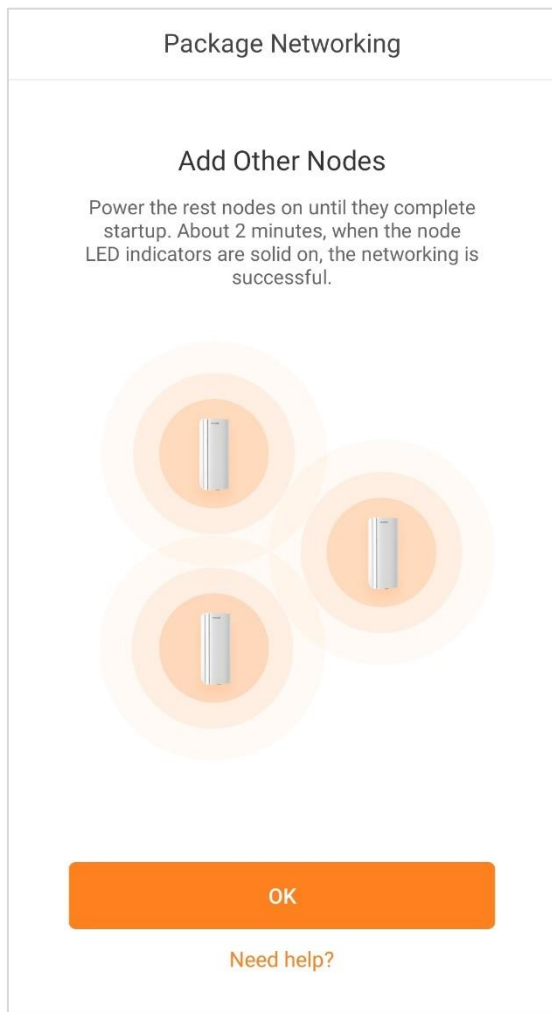
---End

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 \(computer\)](#).

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



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.

Configuration 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.

Configuration 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

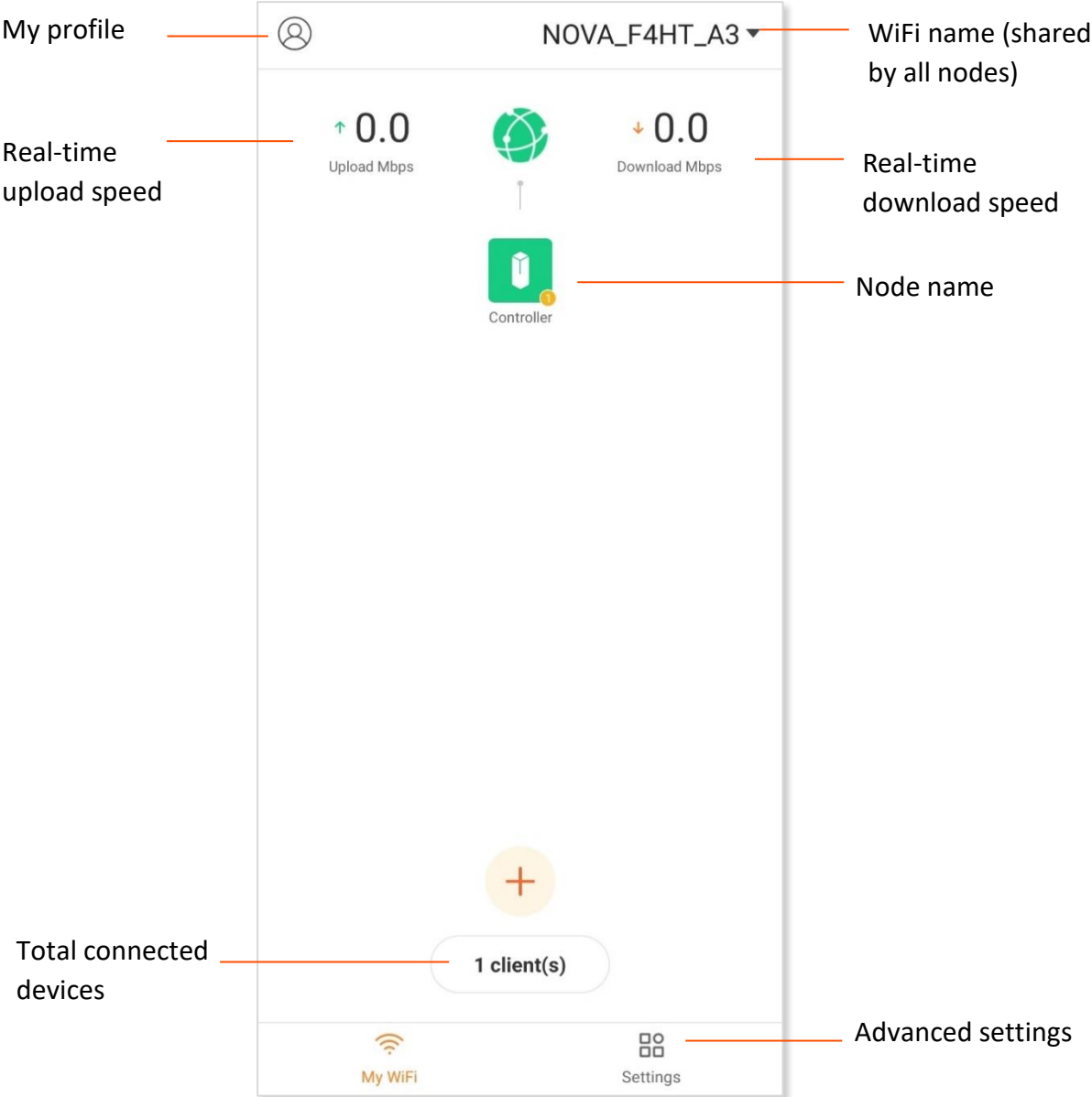
Now, you can manage your Mesh network remotely.

3.5 My WiFi

After completing the quick setup, the following page appears.

You can:

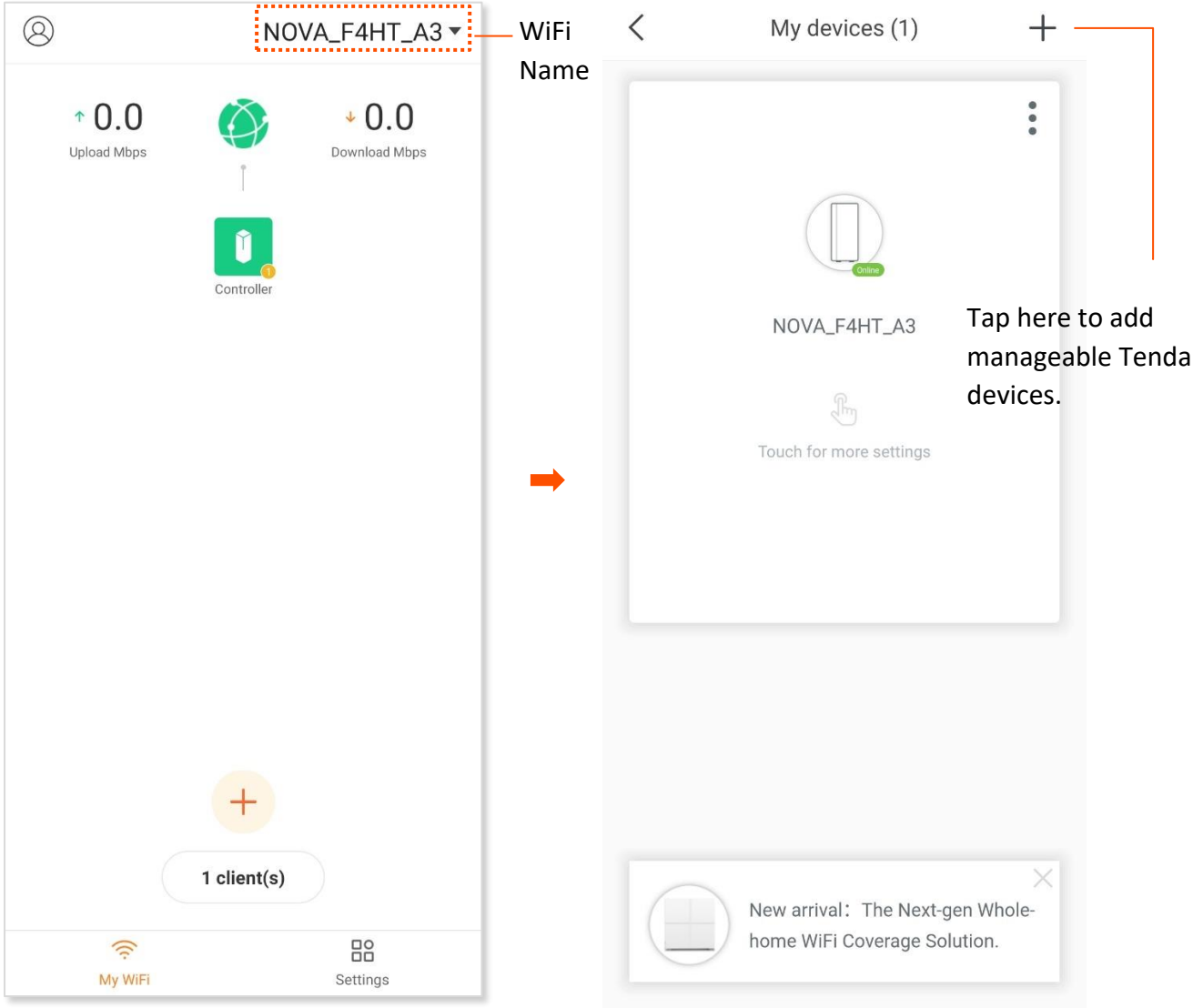
- [View managed nodes](#)
- [View the internet status](#)
- [Add a node](#)
- [Manage nodes](#)
- [Manage connected clients](#)




3.5.1 View managed nodes

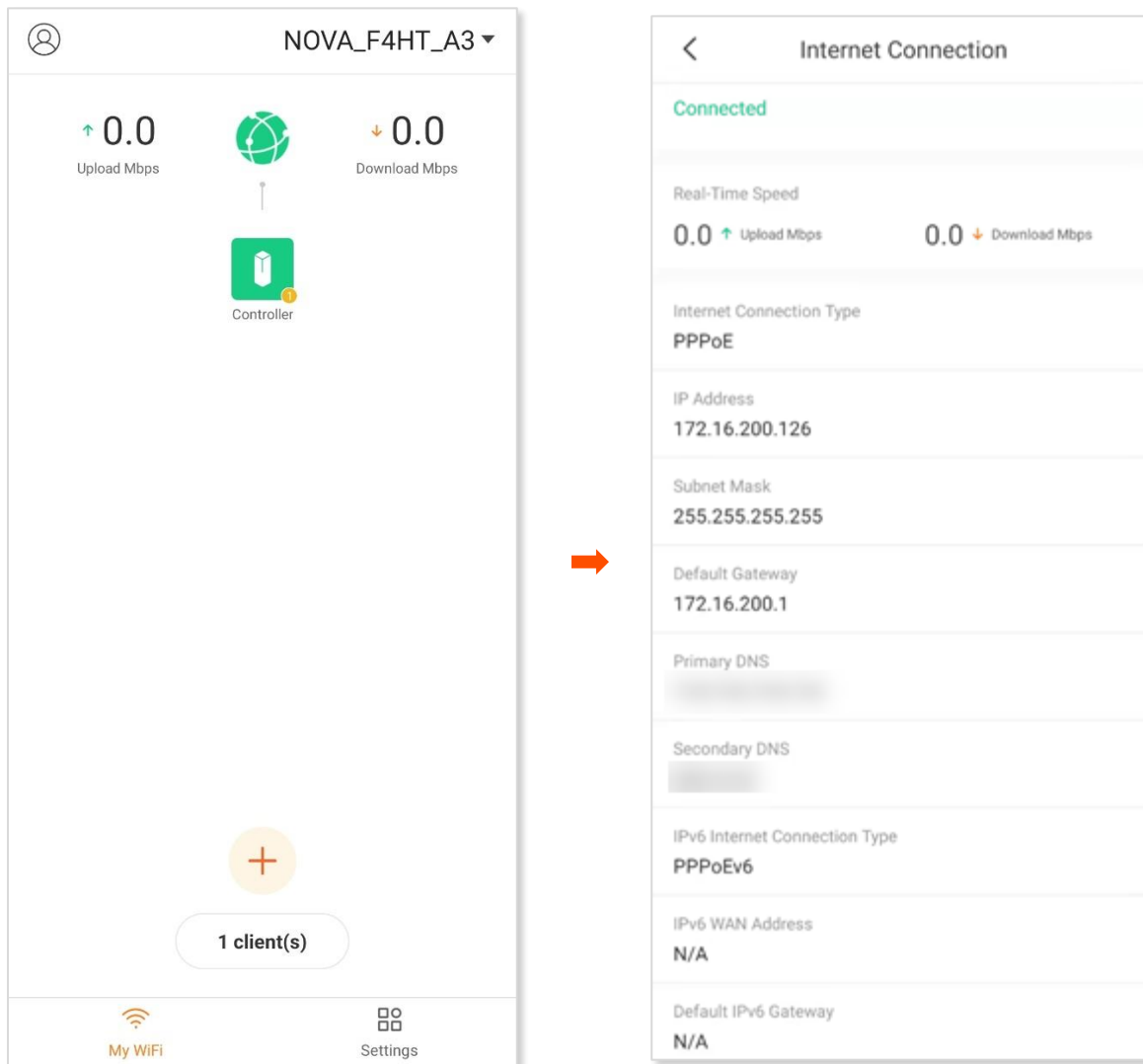
Tap the WiFi name in the upper-right corner of the **My WiFi** page to enter the **My devices** page.

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.




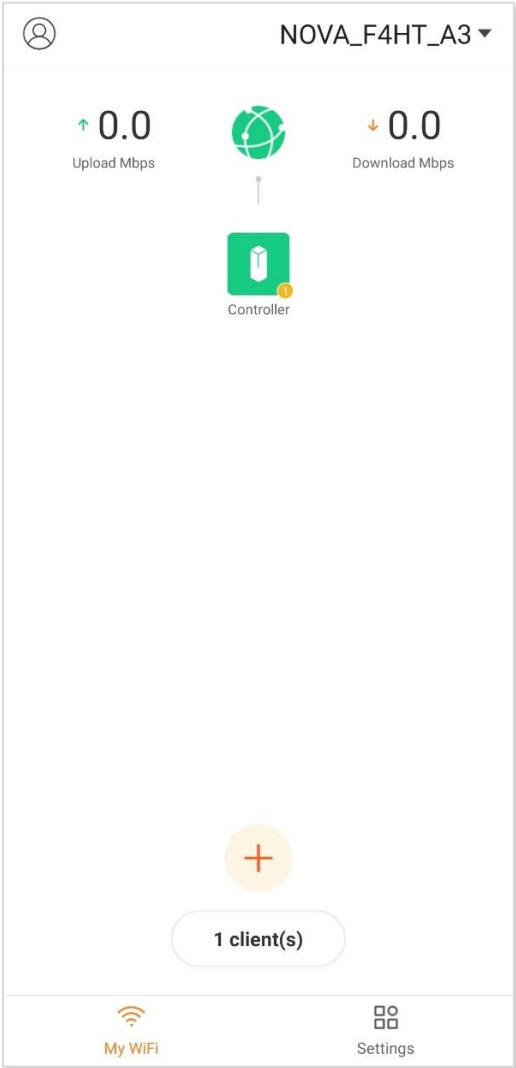
Parameter description

Parameter	Description
Connected/Disconnected	Specifies the internet connection status.
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.

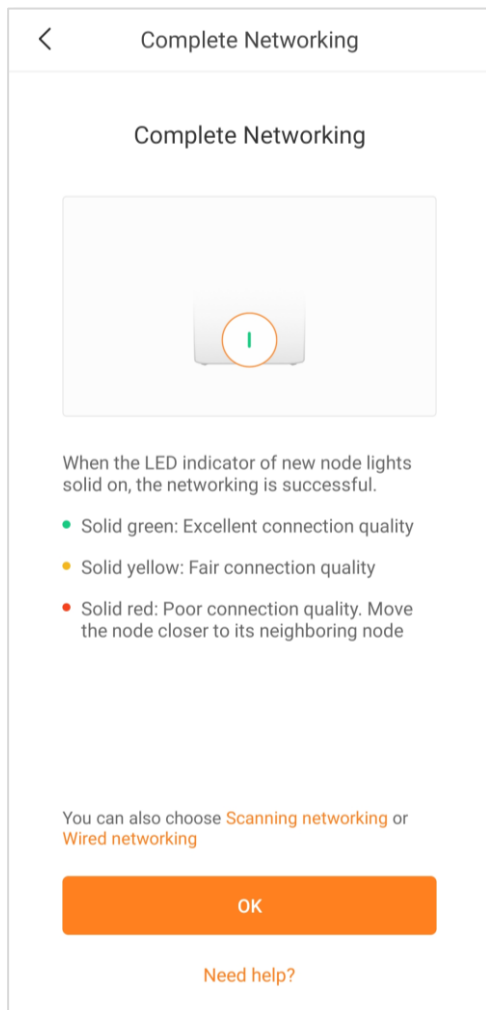
Parameter	Description
Subnet Mask	Specifies the WAN subnet mask of the primary node.
Default Gateway	Specifies the gateway IP address of the primary node.
Primary DNS	Specify the IP address of primary and secondary DNS servers of the primary node.
Secondary DNS	
IPv6 Internet Connection Type	Specifies the IPv6 internet connection type of the primary node. It is displayed only when the IPv6 function is enabled.
IPv6 WAN Address	Specifies the IPv6 WAN address of the primary node. It is displayed only when the IPv6 function is enabled.
Default IPv6 Gateway	Specifies the IPv6 gateway address of the primary node. It is displayed only when the IPv6 function is enabled.
Primary IPv6 DNS	Specify the IPv6 address of primary and secondary DNS servers of the primary node.
Secondary IPv6 DNS	
IPv6 LAN Address	Specifies the IPv6 LAN address of the router. It is displayed only when the IPv6 function is enabled.

3.5.3 Add a node

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

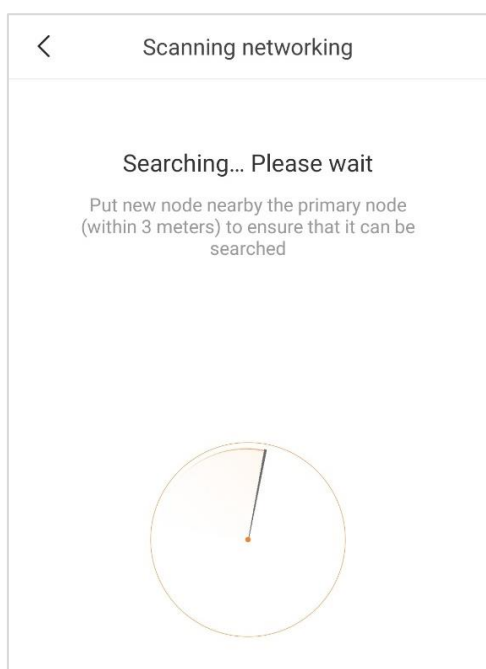


If you cannot add a node by following the instructions, try the following two methods by tapping **Scanning networking** or **Wired networking** shown in the following figure:

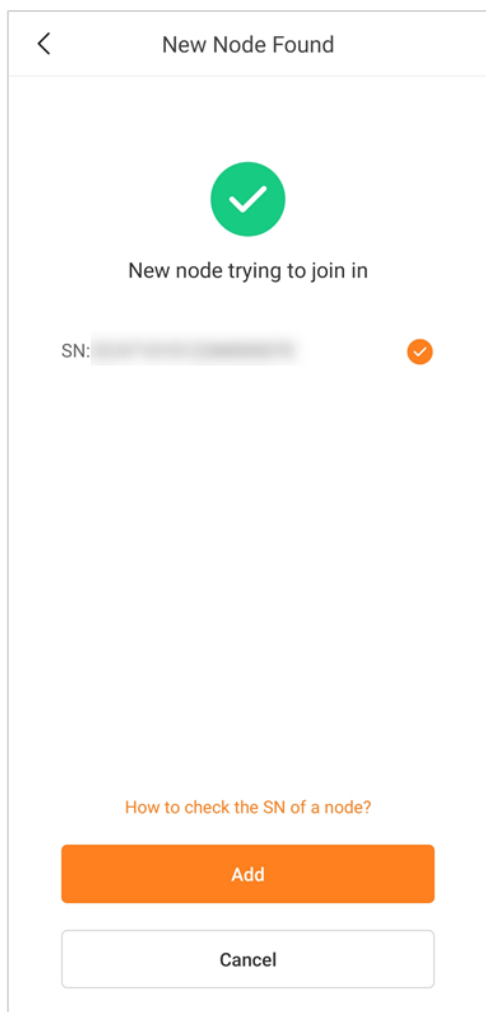


■ **To scan a new node:**

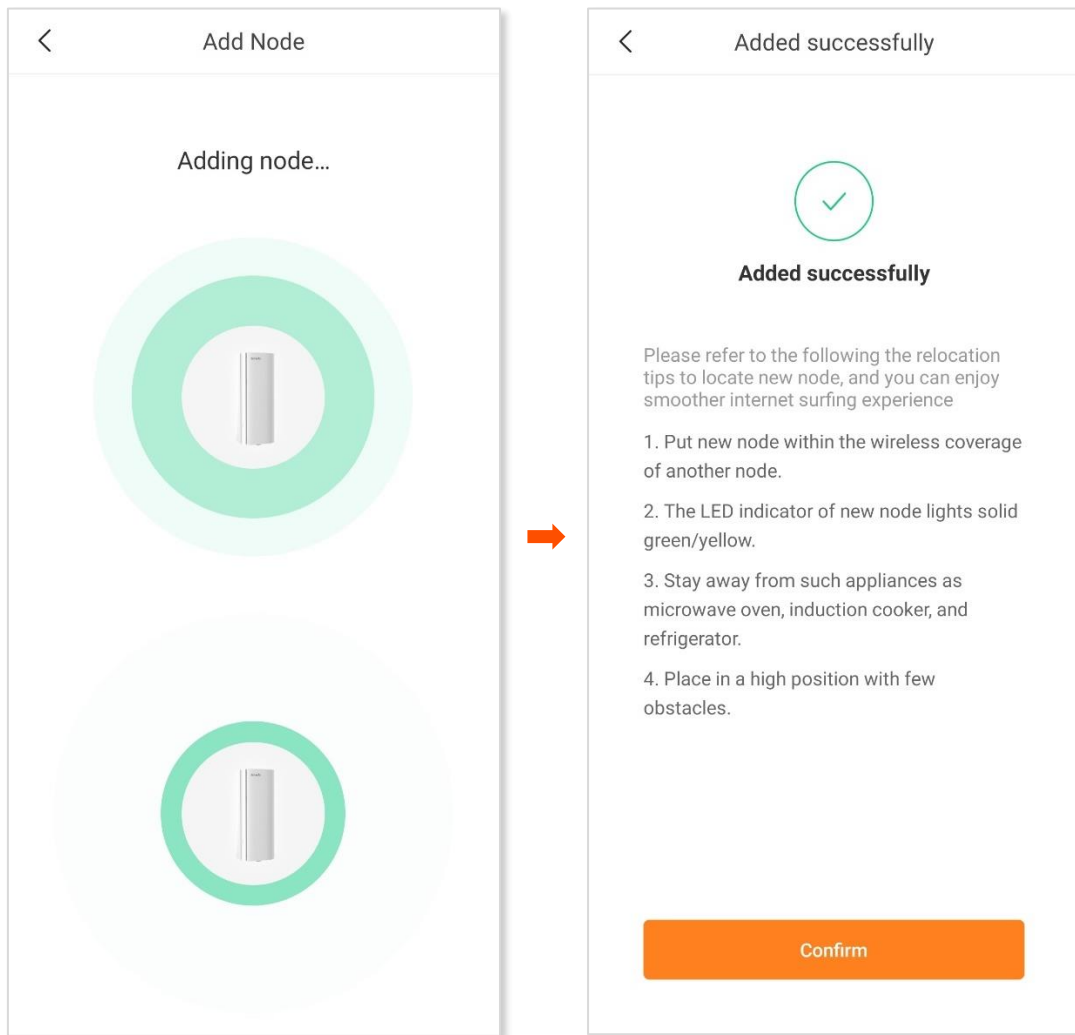
Step 1 Tap **Scanning networking**.



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



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



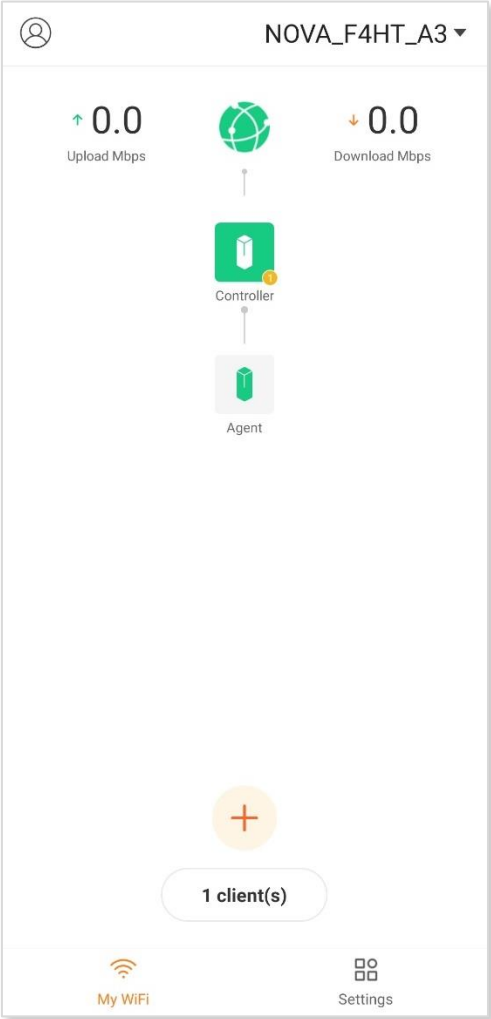
If the LED indicator of new node lights solid on and the new node is displayed in **Network Topology**, the node is added successfully.

---End



■ **To perform wired networking:**

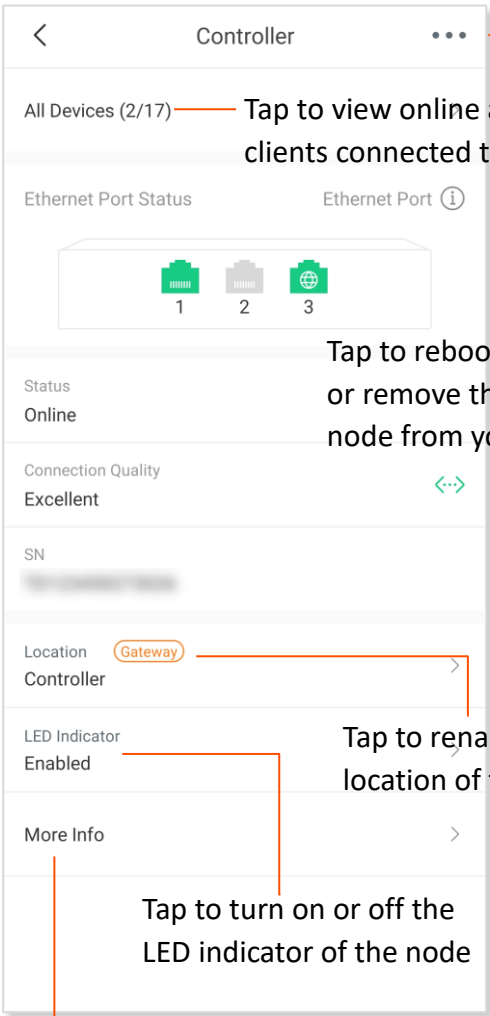
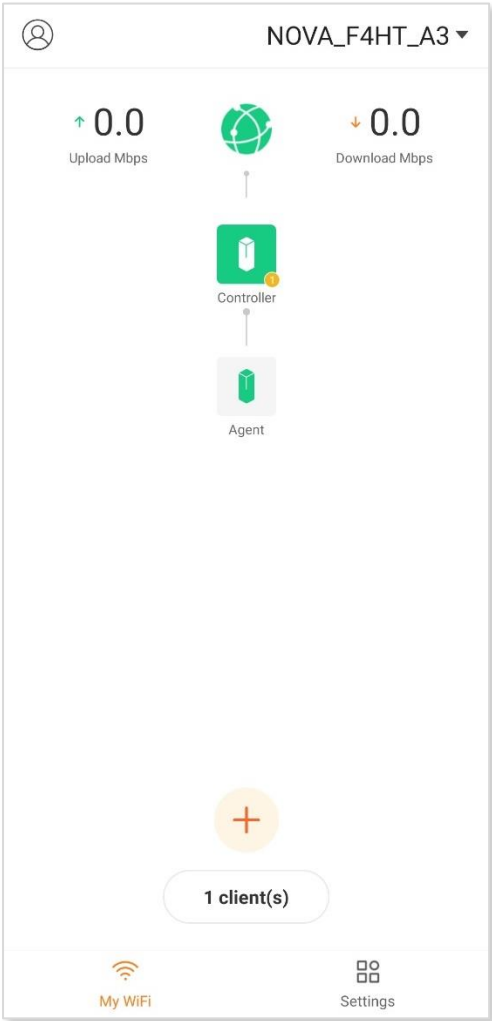
Tap **Wired networking** and follow the instructions displayed.

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.



Tap to view online and offline clients connected to the node

Tap to reboot/reset the node or remove the secondary node from your WiFi network

Tap to rename the location of the node

Tap to turn on or off the LED indicator of the node

Tap to learn more about the node

3.5.5 Manage connected clients

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

Tap to blacklist clients and remove blacklisted clients from the blacklist

Filter the displayed clients according to the connection type

Tap to see and delete offline devices

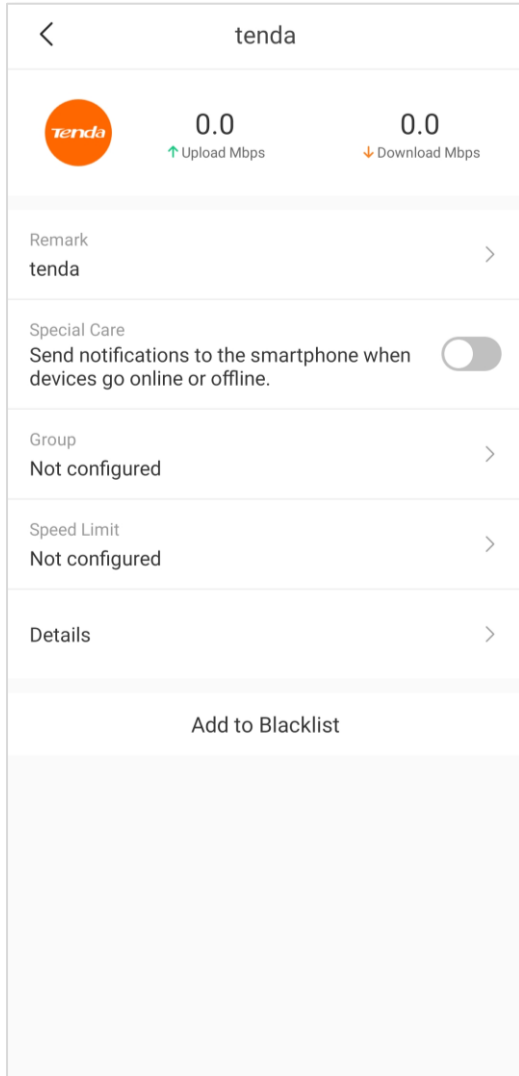
Tap to see clients connecting to the guest network

Frequency band and time point that the client connects

Tap any connected clients and the following page appears.



Special Care is available only for the administrator account on some models. If it is not displayed in your app, it is unavailable for the product that you purchased.

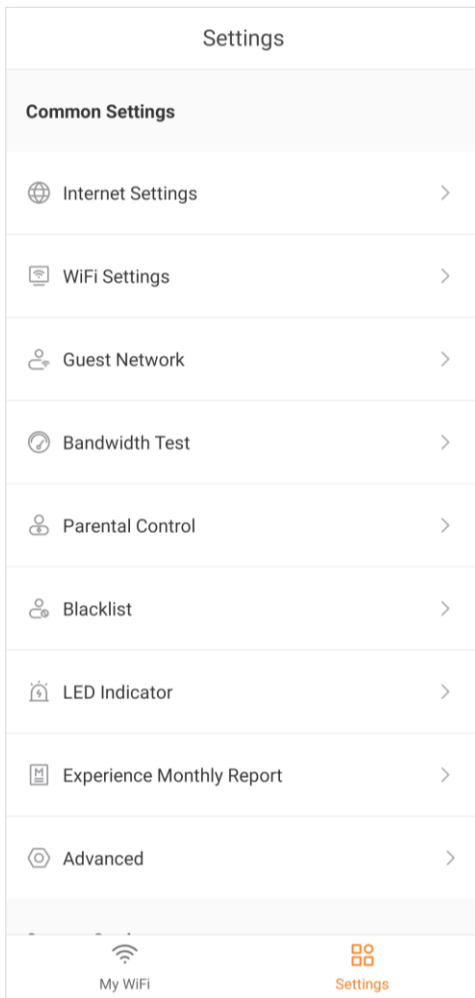


- Tap to rename the client
- Tap to receive notifications on your smartphone when clients get online/offline
- Tap to create a group or add the connected client to a group for the parental control function
- Tap to set upload and download speed of the client
- Tap to check the details of the connected client

3.6 Common settings

You can change common internet settings or set up more parameters here.

Tap **Settings** to enter the page.



3.6.1 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
	PPPoE user name and password	PPPoE
Connect the node to a modem or Ethernet jack using an Ethernet cable.	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.

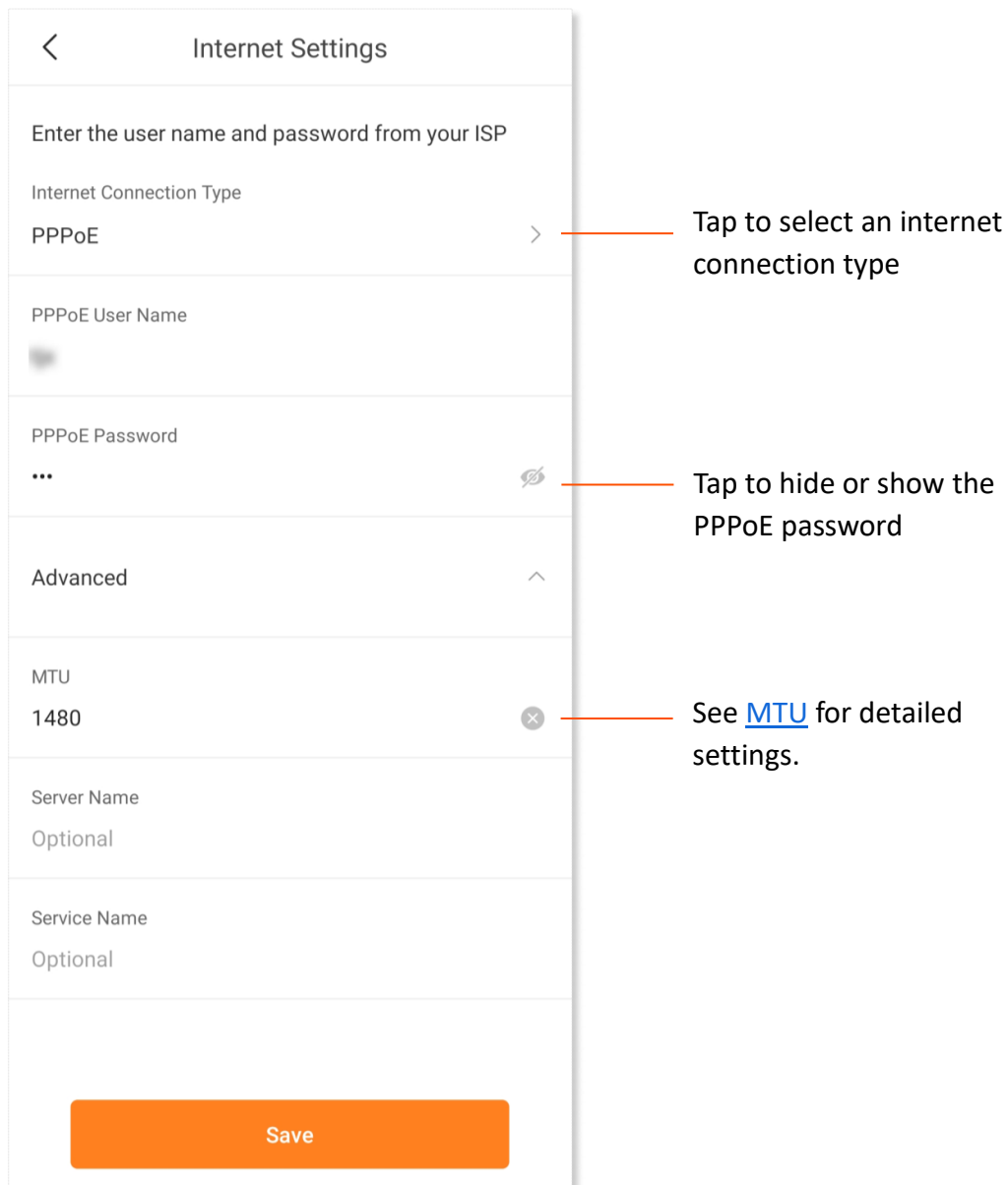
Set up a PPPoE connection

Configuration procedure:

- Step 1** Run the **Tenda WiFi App**, and choose **Settings > Internet Settings**.
- Step 2** Tap **Internet Connection Type**.
- Step 3** Select **PPPoE** and tap **Next**.
- 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**.



The screenshot shows the 'Internet Settings' screen. At the top, there is a back arrow and the title 'Internet Settings'. Below the title, there is a prompt: 'Enter the user name and password from your ISP'. The screen is divided into several sections:

- Internet Connection Type:** Currently set to 'PPPoE'. A right-pointing chevron indicates it can be selected.
- PPPoE User Name:** A text input field with a blurred placeholder.
- PPPoE Password:** A text input field with three dots and a visibility icon (an eye with a slash) to its right.
- Advanced:** A section header with an upward-pointing chevron.
- MTU:** A text input field with the value '1480' and a clear icon (an 'x' in a circle) to its right.
- Server Name:** A text input field with the placeholder 'Optional'.
- Service Name:** A text input field with the placeholder 'Optional'.

At the bottom of the screen is a large orange button labeled 'Save'. Three orange lines with text annotations point to specific elements:

- One line points to the right-pointing chevron next to 'PPPoE' with the text: 'Tap to select an internet connection type'.
- Another line points to the visibility icon next to the password field with the text: 'Tap to hide or show the PPPoE password'.
- A third line points to the clear icon next to the 'MTU' field with the text: 'See [MTU](#) for detailed settings.'

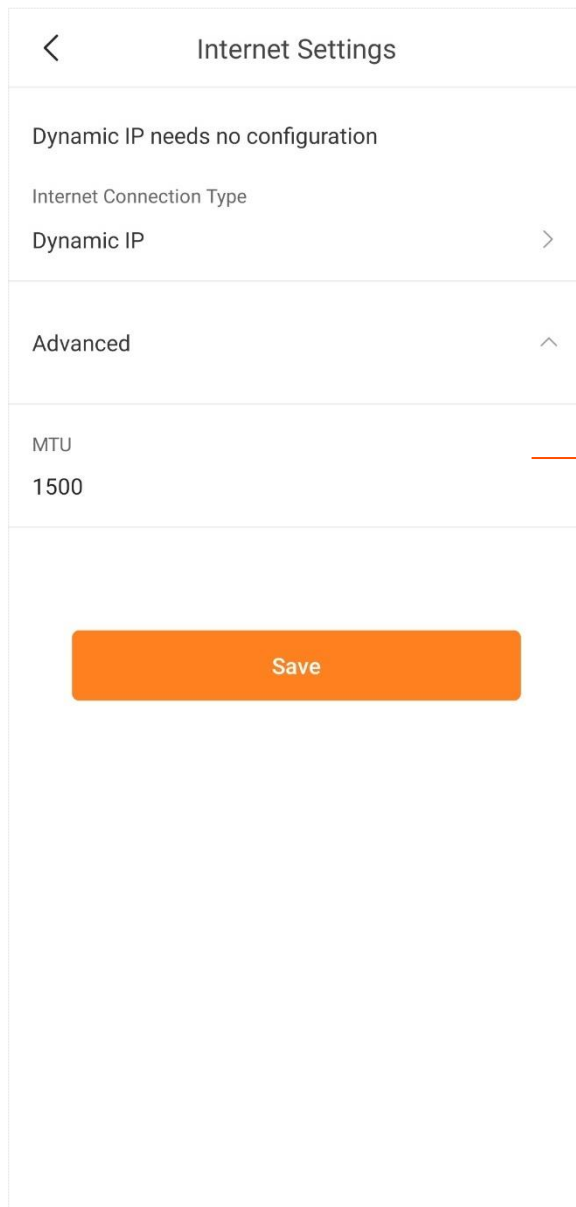
---End

Now you can access the internet.

Set up a dynamic IP address connection

Configuration procedure:

- Step 1** Run the **Tenda WiFi App**, and choose **Settings > Internet Settings**.
- Step 2** Tap **Internet Connection Type**.
- Step 3** Select **Dynamic IP** and tap **Next**.
- Step 4** Tap **Save**.



See [MTU](#) for detailed settings.

---End

Now you can access the internet.

Set up a static IP address connection

Configuration procedure:

- Step 1** Run the **Tenda WiFi App**, and choose **Settings > Internet Settings**.
- Step 2** Tap **Internet Connection Type**.
- Step 3** Select **Static IP** and tap **Next**.
- 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**.

The screenshot shows the 'Internet Settings' screen in the Tenda WiFi app. At the top, there is a back arrow and the title 'Internet Settings'. Below the title, a message reads 'Please enter the fixed IP info for internet access'. The main content area contains several settings:

- Internet Connection Type:** A dropdown menu currently showing 'Static IP' with a right-pointing chevron.
- IP Address:** A text input field containing '0.0.0.0'.
- Subnet Mask:** A text input field containing '0.0.0.0'.
- Default Gateway:** A text input field containing '0.0.0.0'.
- Primary DNS:** A text input field containing '0.0.0.0'.
- Secondary DNS (Optional):** A text input field containing '0.0.0.0'.
- Advanced:** A section header with an upward-pointing chevron.
- MTU:** A text input field containing '1500'.

At the bottom of the screen is a large orange button labeled 'Save'.

See [MTU](#) for detailed settings.

---End

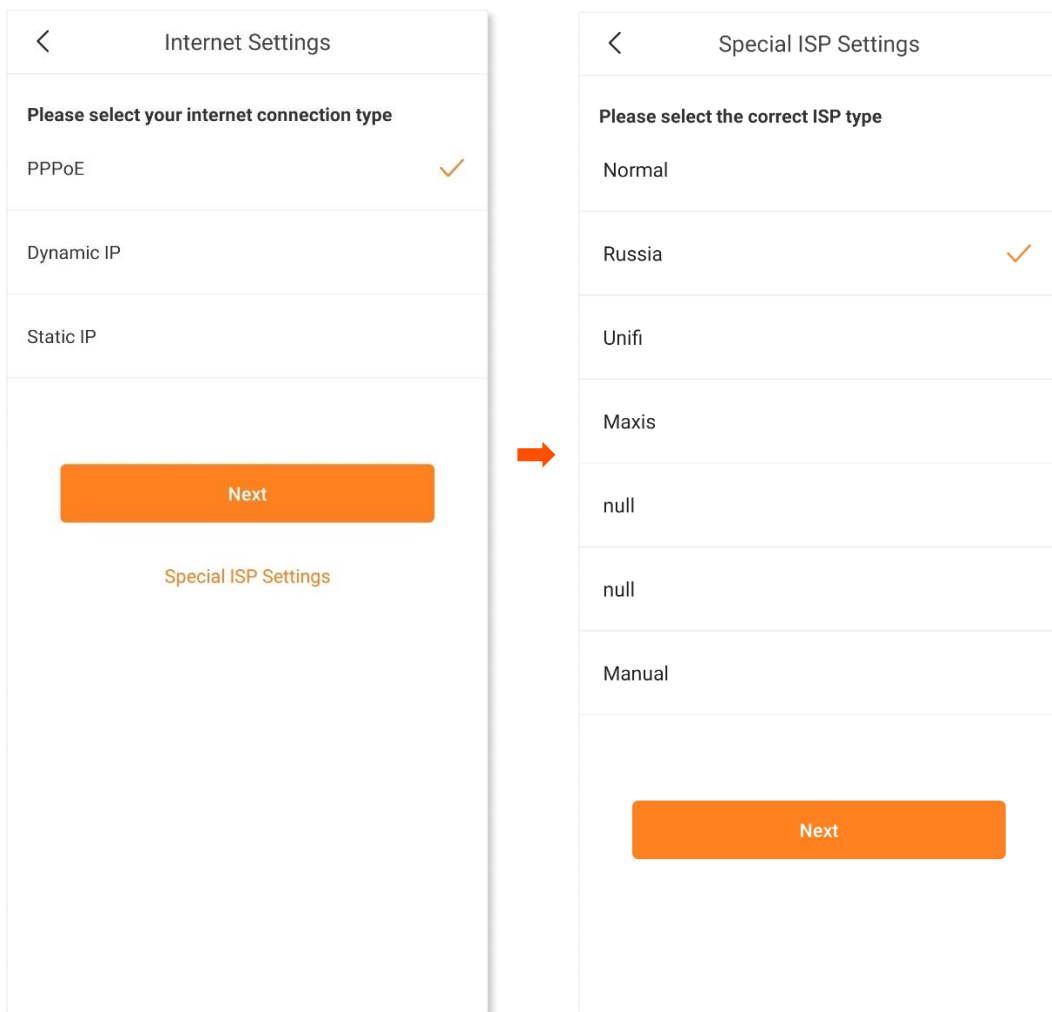
Now you can access the internet.

Set up dual access connection

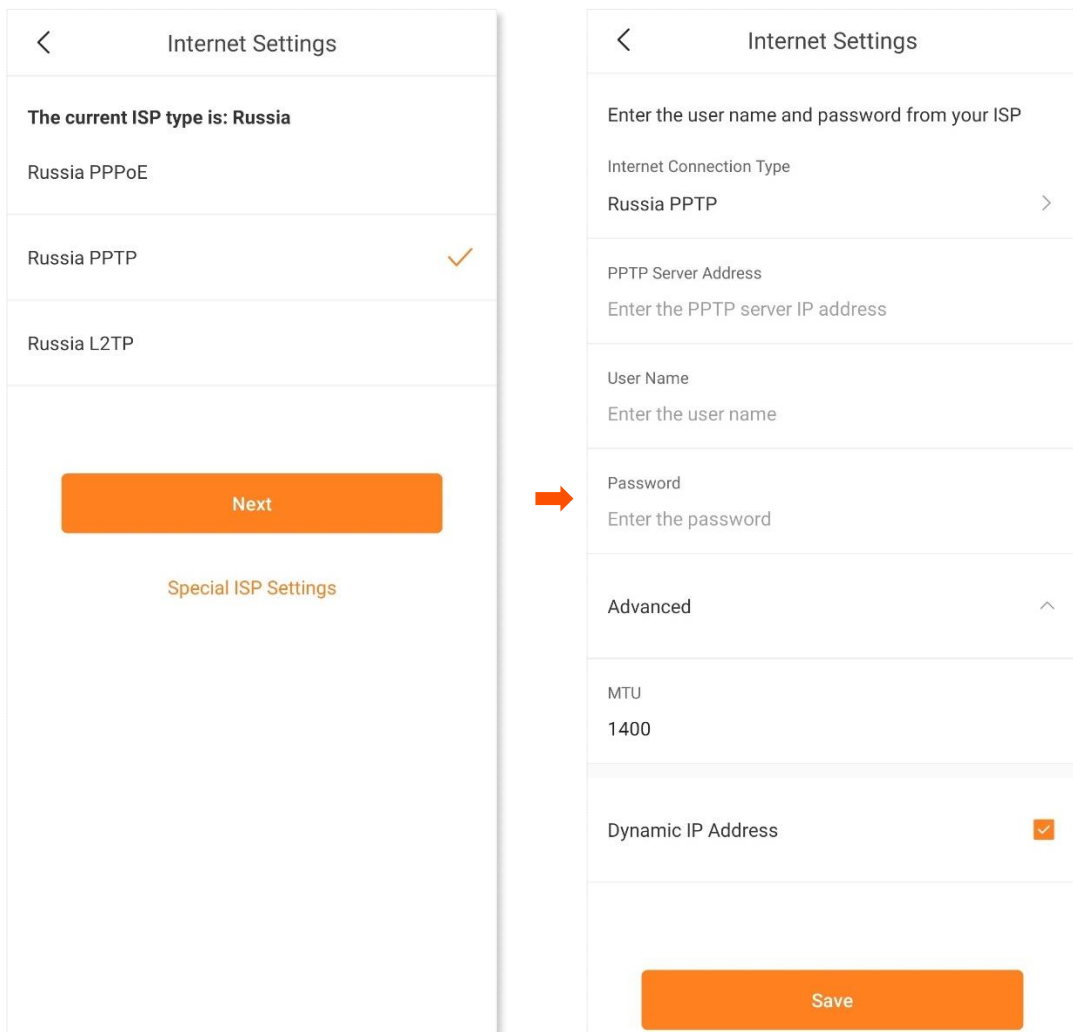
In countries like Russia, the ISP may require you to set up dual access. One is for access to the internet through PPPoE, PPTP or L2TP, and the other is for access to the “local” resources where the ISP is located through DHCP or static IP address. If your ISP provides such connection information, you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

Configuration 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, and tap **Next**. Fill in required parameters, and tap **Save**.



---End

Now you can access the internet.

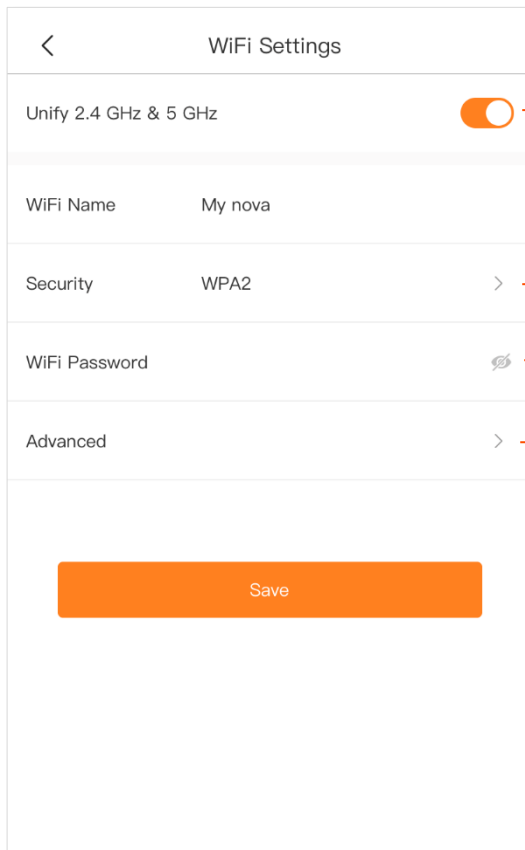
3.6.2 WiFi settings



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

To change the WiFi name and WiFi password of your WiFi network:

- 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.

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

(MX15 Pro for example)



For MX21 Pro/EX21 Pro/Mesh21XEP:

- **Unify 2.4 GHz & 5 GHz & 6 GHz** is available. You can enable it to synchronize the Wi-Fi names and passwords of the 2.4 GHz, 5 GHz and 6 GHz Wi-Fi networks.
- You can enable or disable the Wi-Fi networks by tapping **WiFi Enable** or **2.4 GHz WiFi**, **5 GHz WiFi** and **6 GHz WiFi**. **WiFi Enable** is displayed when **Unify 2.4 GHz & 5 GHz** or **Unify 2.4 GHz & 5 GHz & 6 GHz** is enabled. **2.4 GHz WiFi**, **5 GHz WiFi** or **6 GHz WiFi** is displayed when **Unify 2.4 GHz & 5 GHz** or **Unify 2.4 GHz & 5 GHz & 6 GHz** is disabled.

---End

Now you can connect to the WiFi network using the new WiFi name and password.

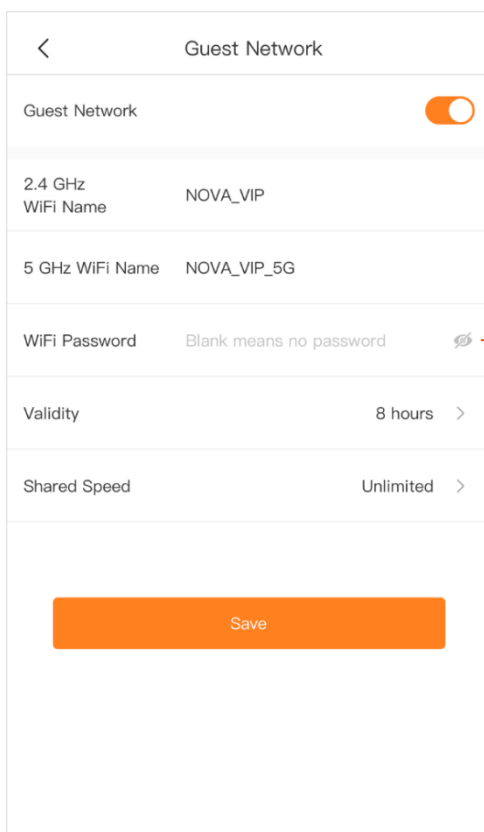
3.6.3 Guest network



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

To configure the guest network:

- Step 1** Run the **Tenda WiFi App**, and choose **Settings > Guest Network**.
- Step 2** Enable the **Guest Network** function.
- Step 3** Customize the WiFi names and password, select a **Validity**, and set a **Shared Speed**.
- Step 4** Tap **Save**.



Tap to hide or show the WiFi password

(MX15 Pro for example)



For MX21 Pro/EX21 Pro/Mesh21XEP, **6 GHz WiFi Name** can be set.

---End

During the specified validity, your guests can connect their WiFi-enabled devices to the internet using the customized WiFi name and password and enjoy the specified shared bandwidth.

3.6.4 Bandwidth test



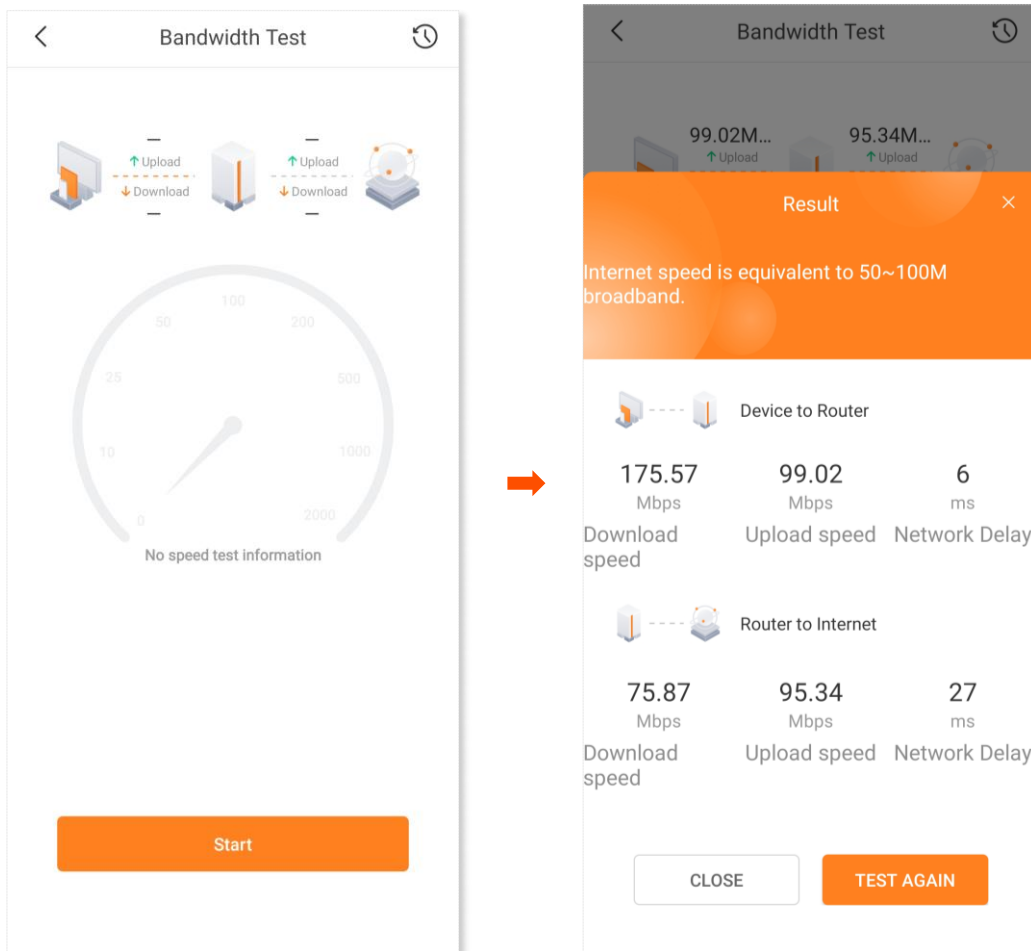
This function is available only for some models. If it is not displayed in your app, it is unavailable for the product that you purchased.

The bandwidth test enables you to check the upload and download speeds and network delay between clients and Mesh device and between Mesh device and the internet.

Perform bandwidth test



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

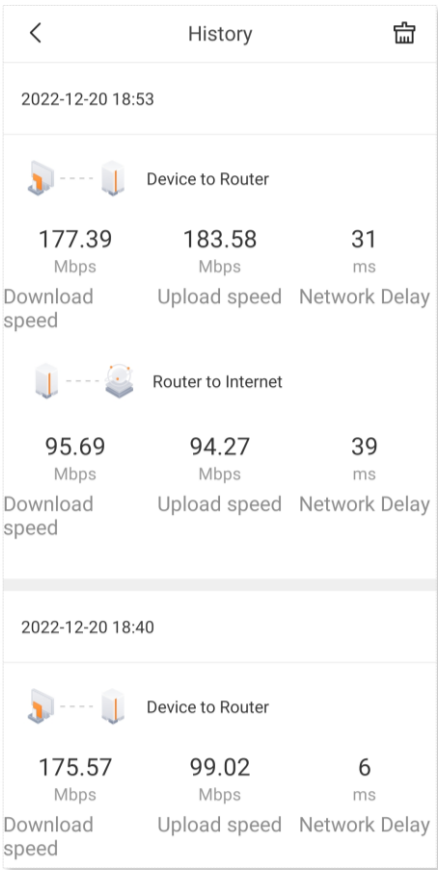
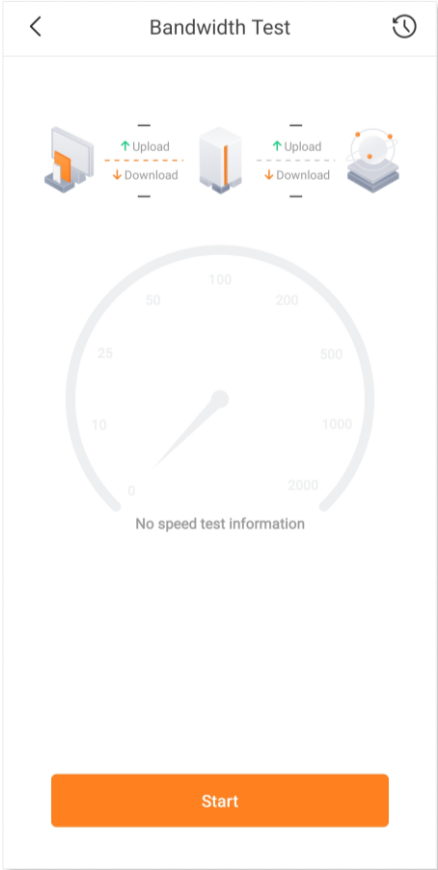
Step 2 Tap **Start**. Wait until the test completes.

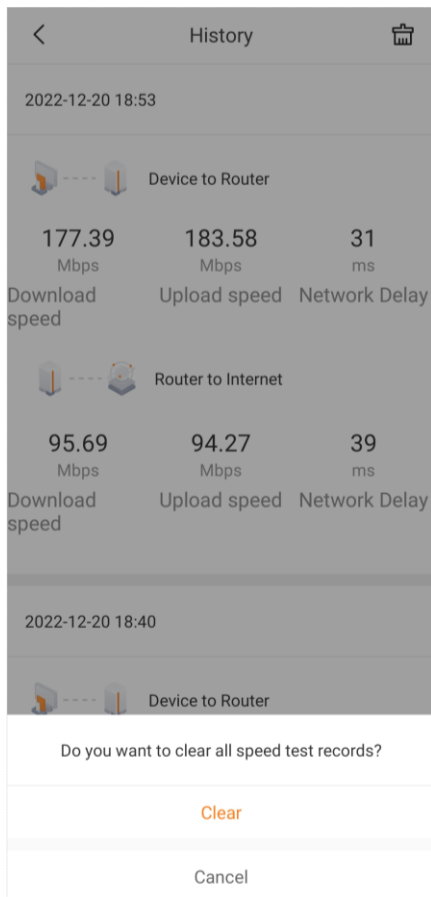


---End

View and clear all bandwidth test results

- Step 1** Run the **Tenda WiFi App**, and choose **Settings > Bandwidth Test**.
- Step 2** Tap  in the upper right corner to view all bandwidth test results.
- Step 3** Tap  in the upper right corner and then tap **Clear** to clear all bandwidth test results.





---End

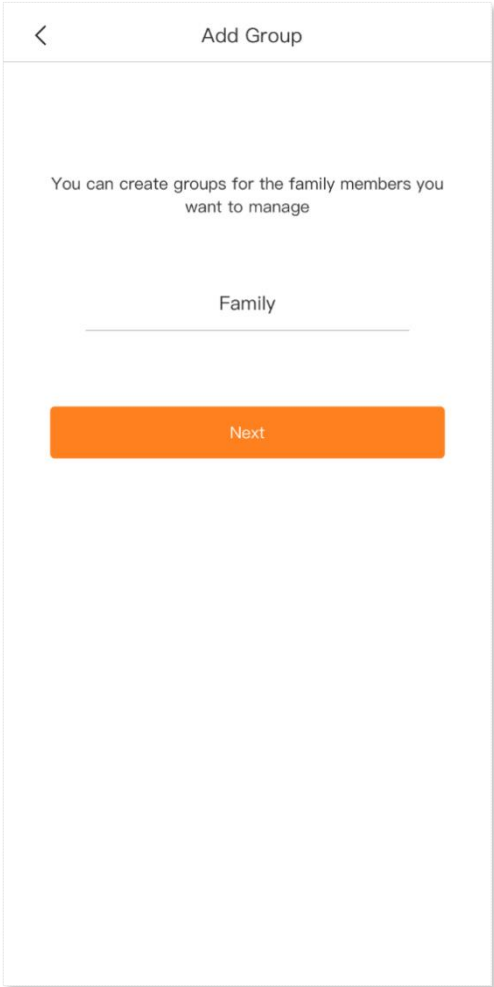
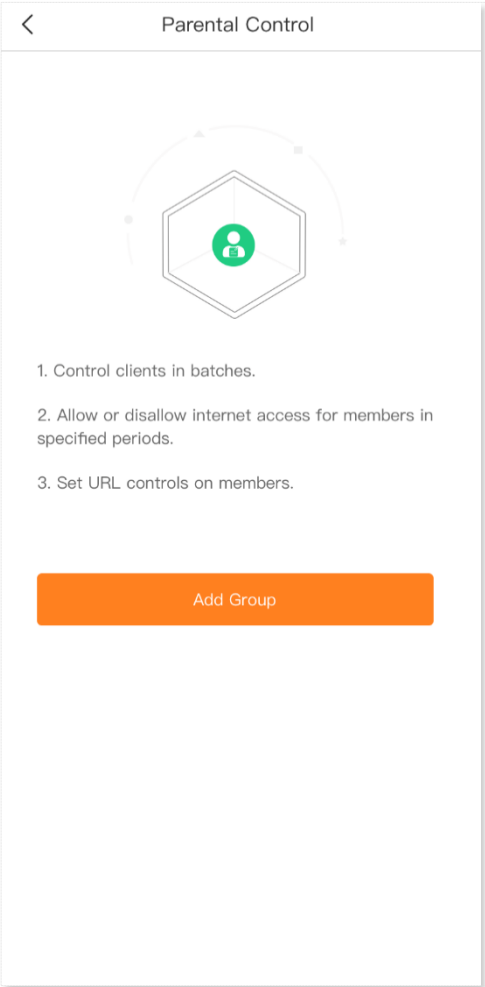
3.6.5 Parental control



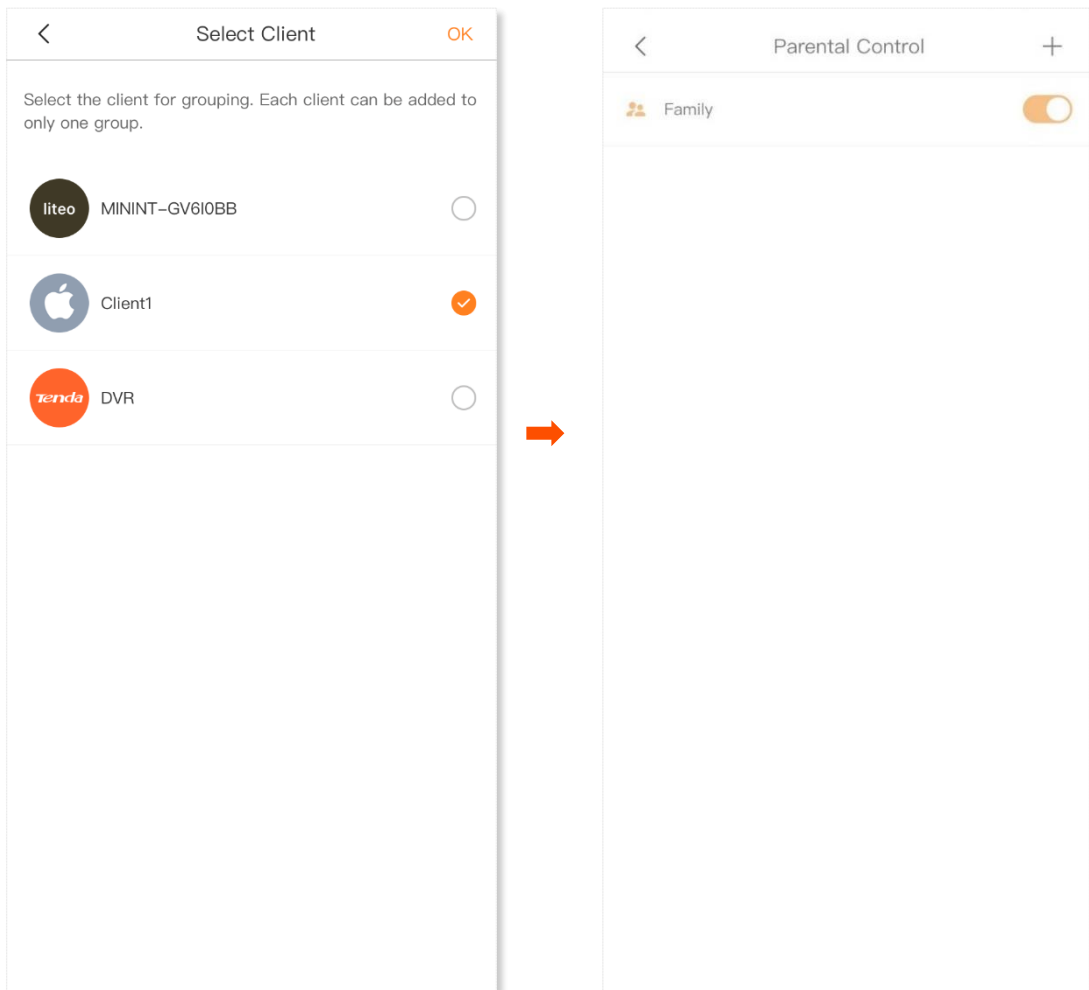
The parental control function enables you to create an appropriate time session for internet access for your family members.





Add a parental control rule

- 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**.



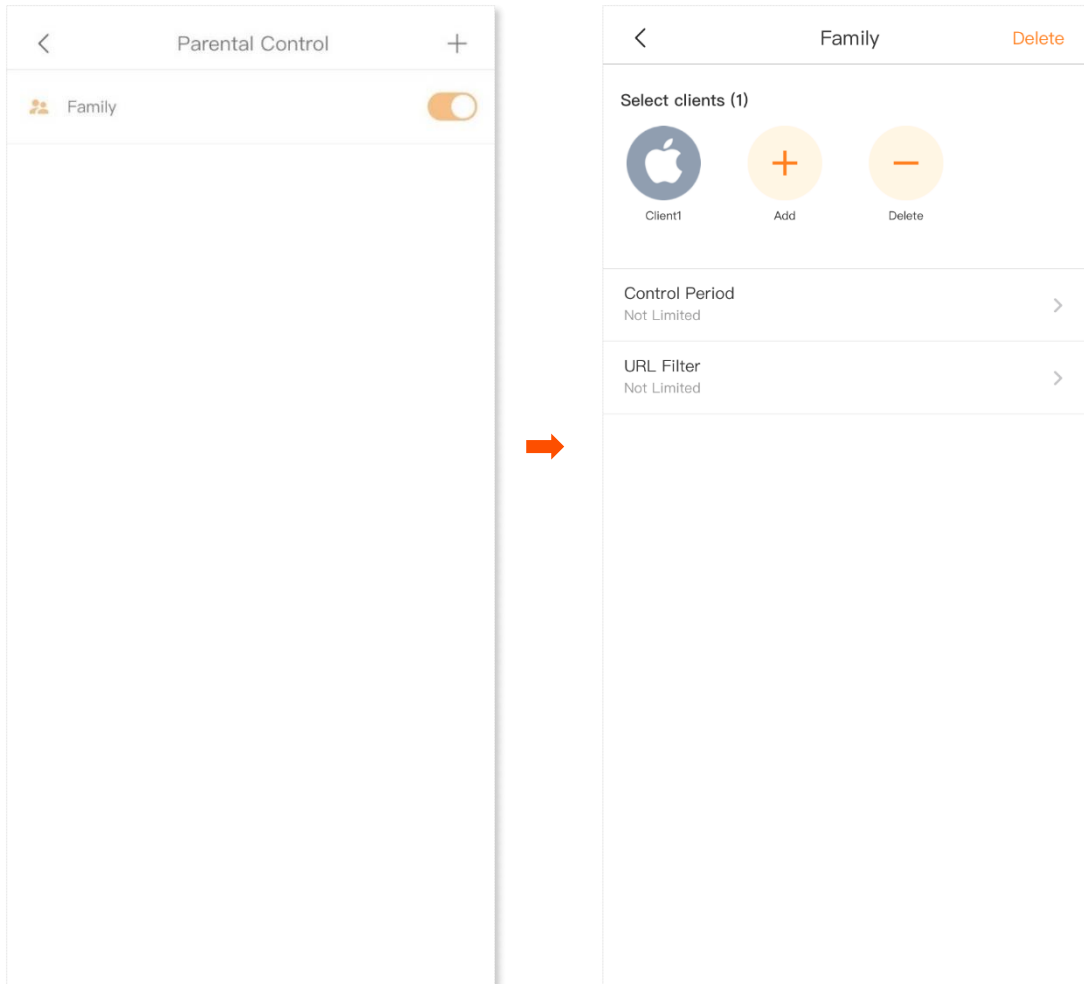
3. Select target clients. **Client1** is used as an example here.
4. Tap **OK** in the upper-right corner.



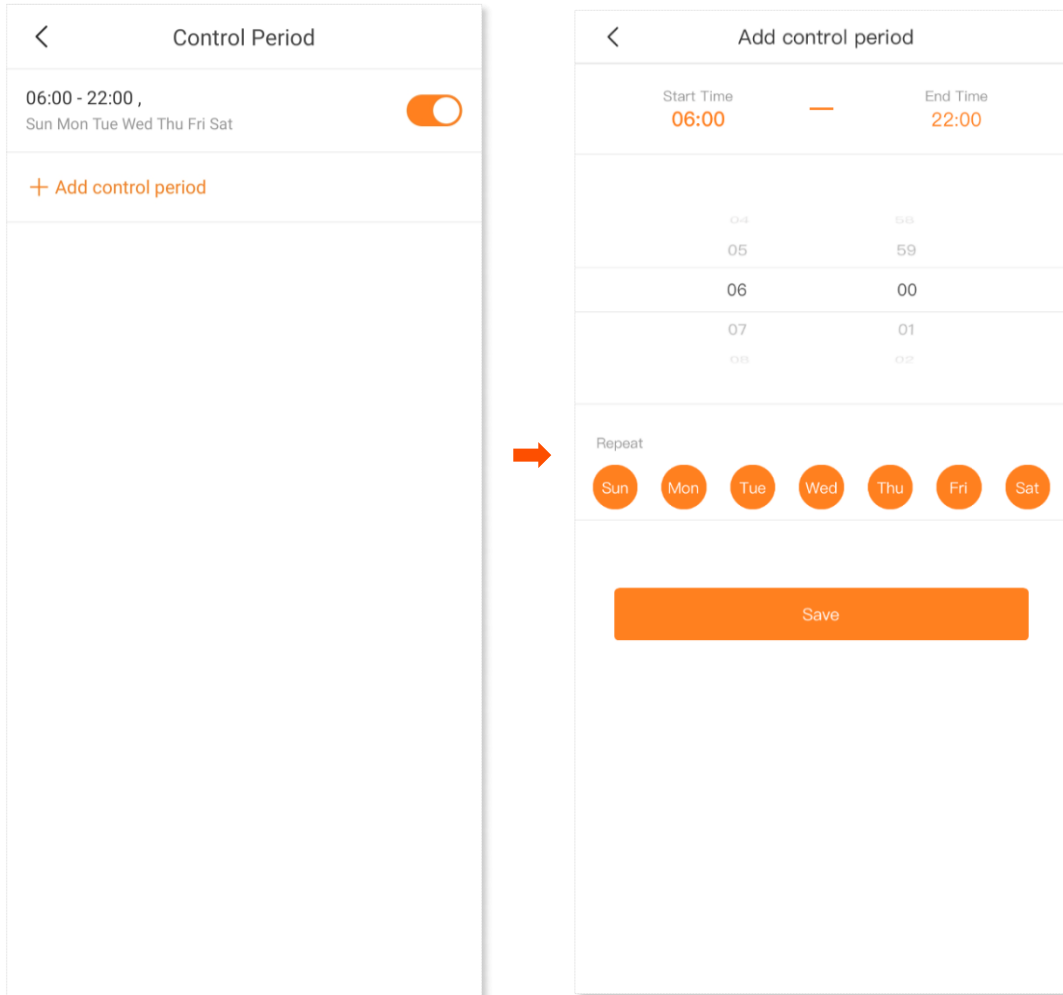
- Step 3** Tap  or  to enable or disable the parental control rule.
-  indicates that the parental control is enabled.
 -  indicates that the parental control is disabled.

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**.



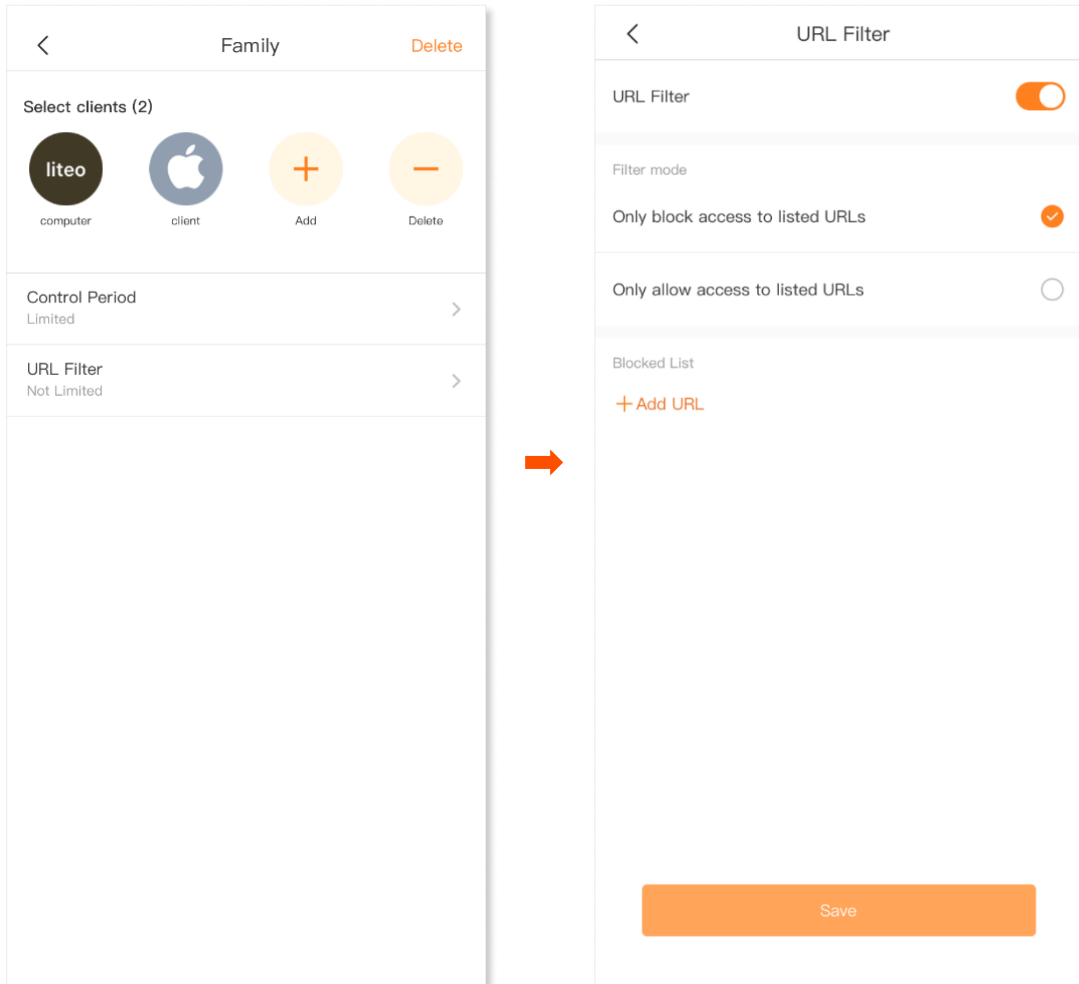
3. Enable the existing control period.
4. Touch the existing period to specify a **Start Time**, **End Time**, and the days on which the rule takes effect. Then, tap **Save**. If you want to add multiple periods, tap **Add control period**.



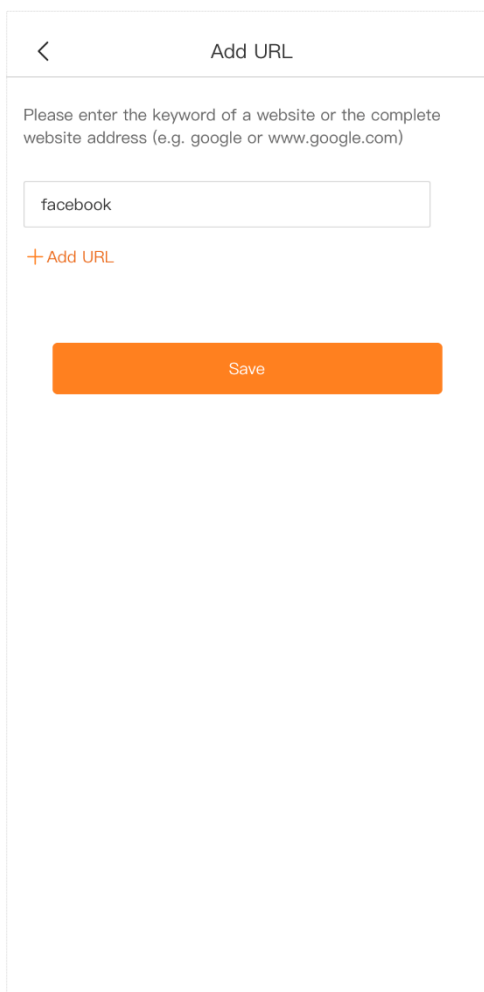
Step 5 Customize the URL filter rule for the group.

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

Only block access to listed URLs is used as an example here.



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



< Add URL

Please enter the keyword of a website or the complete website address (e.g. google or www.google.com)

facebook

+ Add URL

Save



TIP

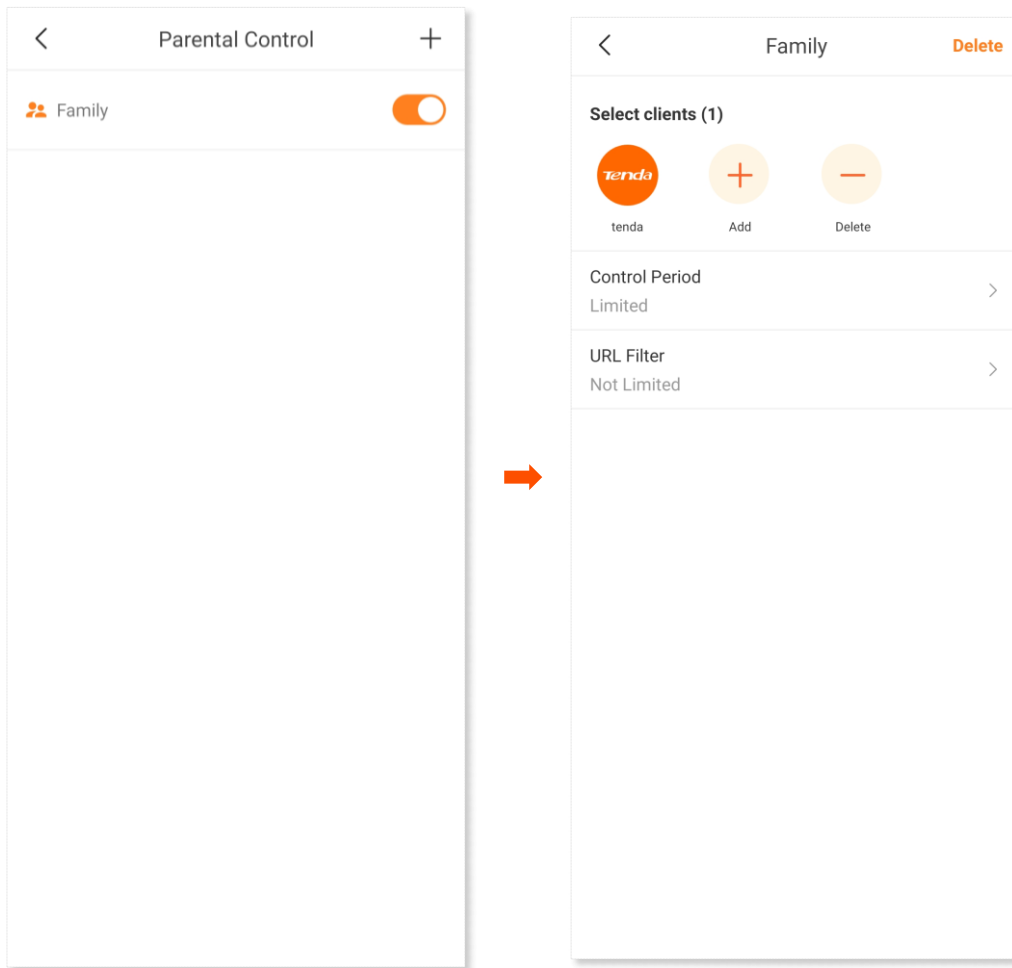
Tap **+Add URL** to add other websites you want to block.

5. Tap **Save**.

---End

Delete a parental control rule

- Step 1** Run the **Tenda WiFi** App, and choose **Settings > Parental Control**.
- Step 2** Tap the parental control rule to be deleted.
- Step 3** Tap **Delete**.



---End

Now clients in the specified group cannot access the specified websites during the specified periods.

3.6.6 Blacklist



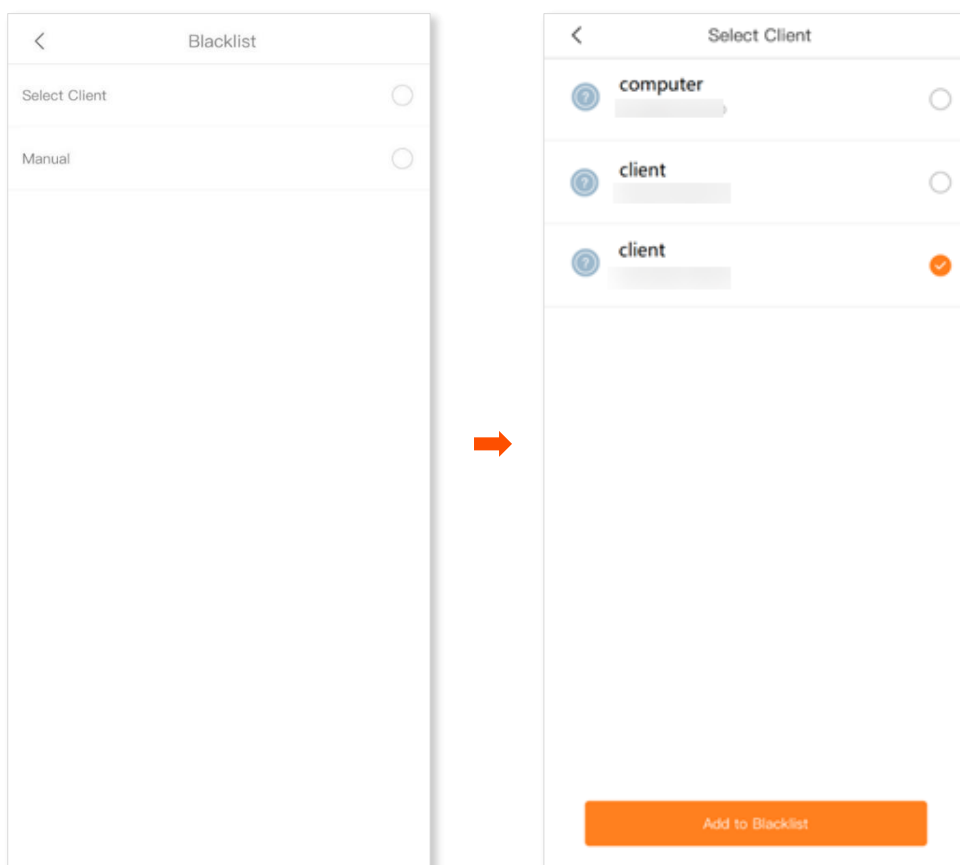
The blacklist function enables you to add a client into the blacklist or remove a client from the blacklist. If you find any unknown client connects to your network and you want to block it from accessing your network, you can blacklist it here. All clients connected to the network can be blacklisted, except the local host.

Add a client to the blacklist

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

Configuration procedure:

- Step 1** Run the **Tenda WiFi App**, and choose **Settings > Blacklist**.
- Step 2** Tap **Add to Blacklist** or **+**, 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

Now the selected client cannot access the internet.

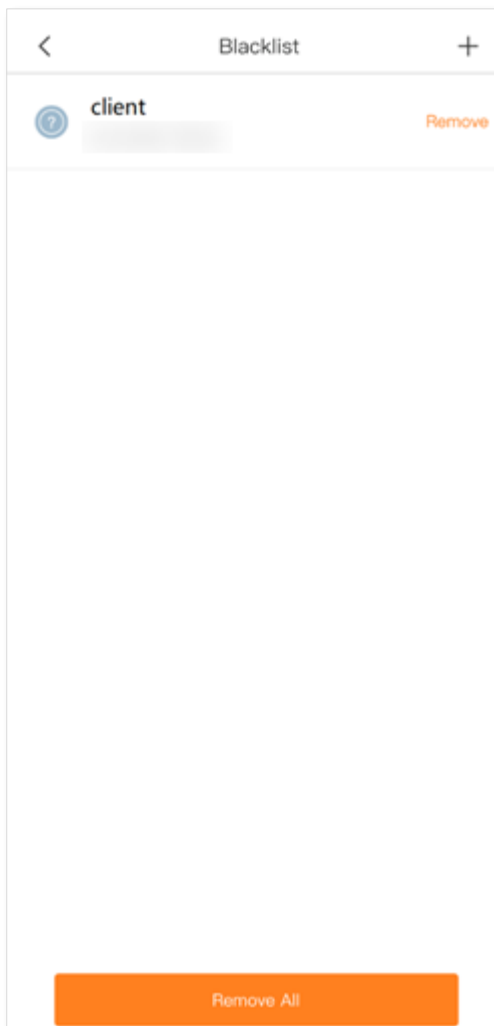
Remove a client from the blacklist

After a client is added into the blacklist, the client cannot access the internet through the Mesh device.

You can remove the client from the blacklist as required.

Configuration procedure:

- Step 1** Run the **Tenda WiFi** App, and choose **Settings > Blacklist**.
- Step 2** Locate the 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.

3.6.7 LED indicator

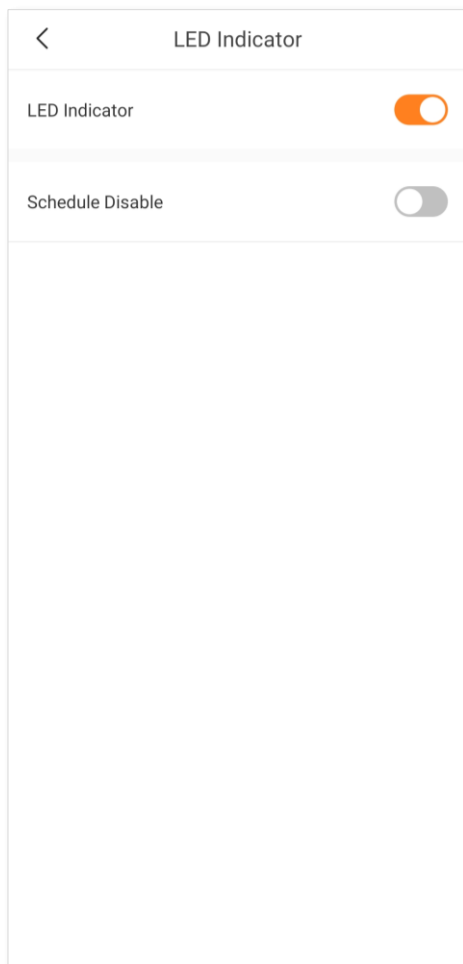


The LED indicator function enables you to turn on or off the LED indicators of the Mesh devices. You can also set a schedule to turn off the LED indicators. By default, the LED indicators are turned on.

Turn on/off all indicators

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

Step 2 Enable/Disable **LED Indicator** to turn on/off all indicators of Mesh devices.

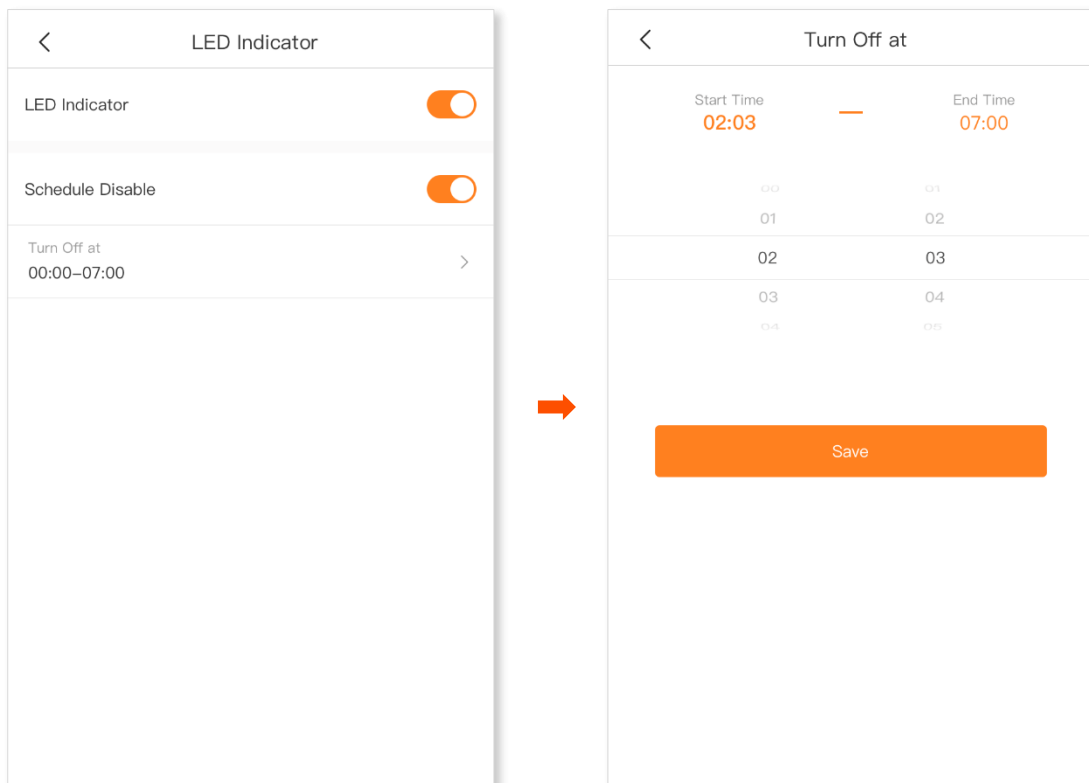


---End

After the setting completes, the LED indicators of the Mesh devices will turn on/off.

Set a schedule to turn off the LED indicators

- 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.

3.6.8 Experience monthly report

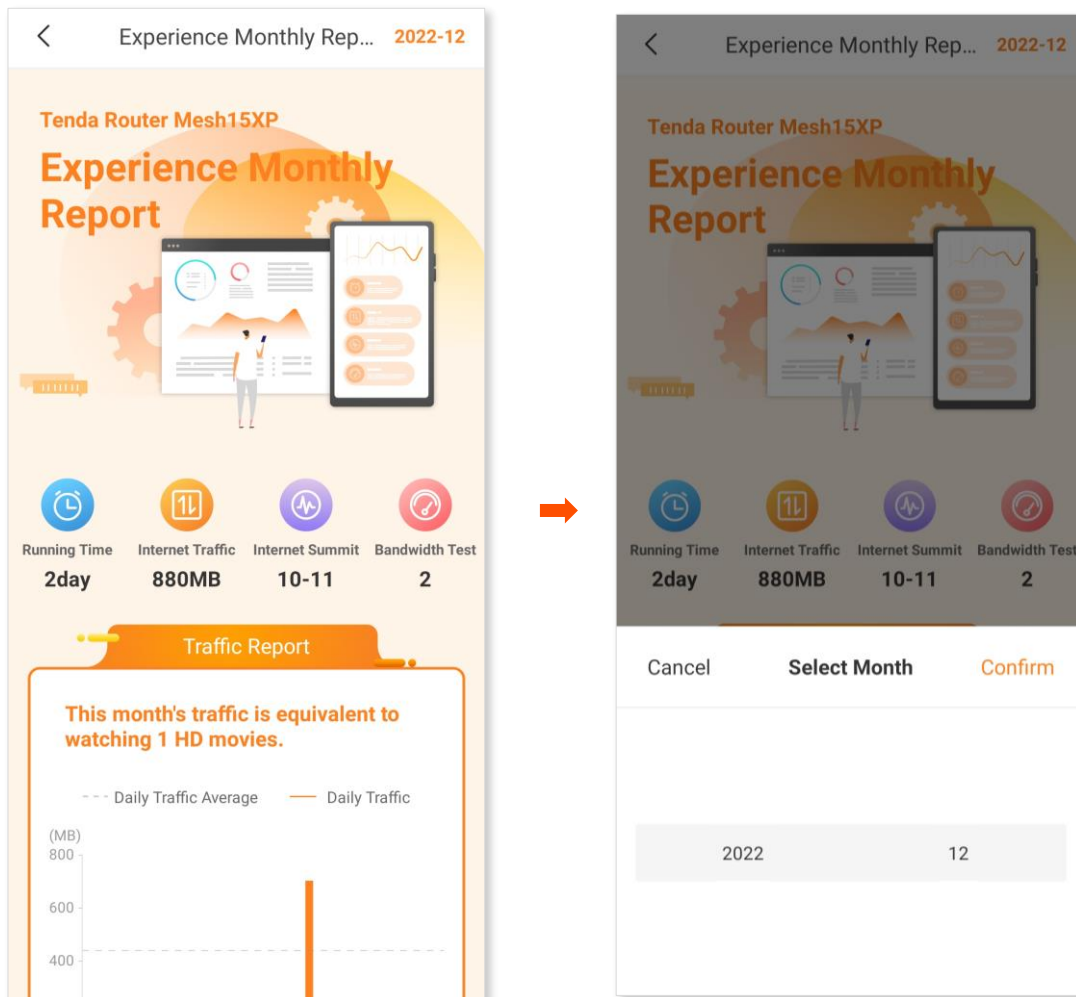


This function is available only for the administrator account for some models. If it is not displayed in your app, it is unavailable for the product that you purchased.

The experience monthly report function enables you to check the performance of Mesh devices by month, including running time, internet traffic, internet summit, bandwidth test results, traffic rank and internet time rank.

To view experience monthly report:

- Step 1** Run the **Tenda WiFi** App, and choose **Settings > Experience Monthly Report**.
- Step 2** Tap the month in the upper right corner to select the month and tap **Confirm**.



---End

Now you can check the experience report of the selected month.

3.6.9 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

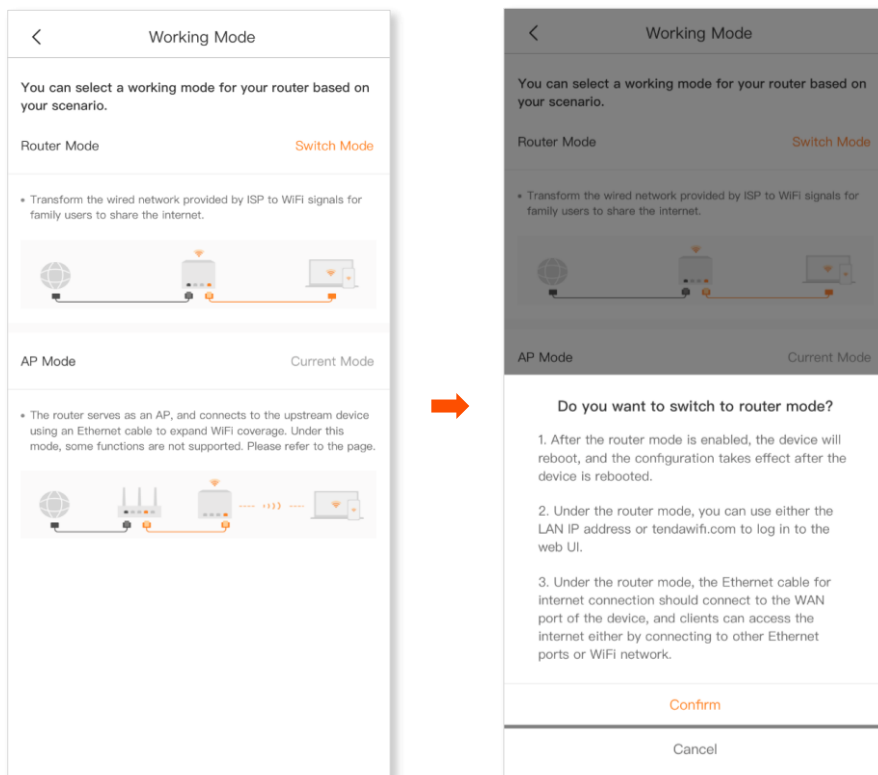
By default, all nodes work in the router mode. All functions are available in this mode. If you want to switch from the router mode to AP mode, see [AP mode](#).

To switch to the router mode:

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.



---End

Now the Mesh device works in the router mode and all functions are available under this mode.

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.

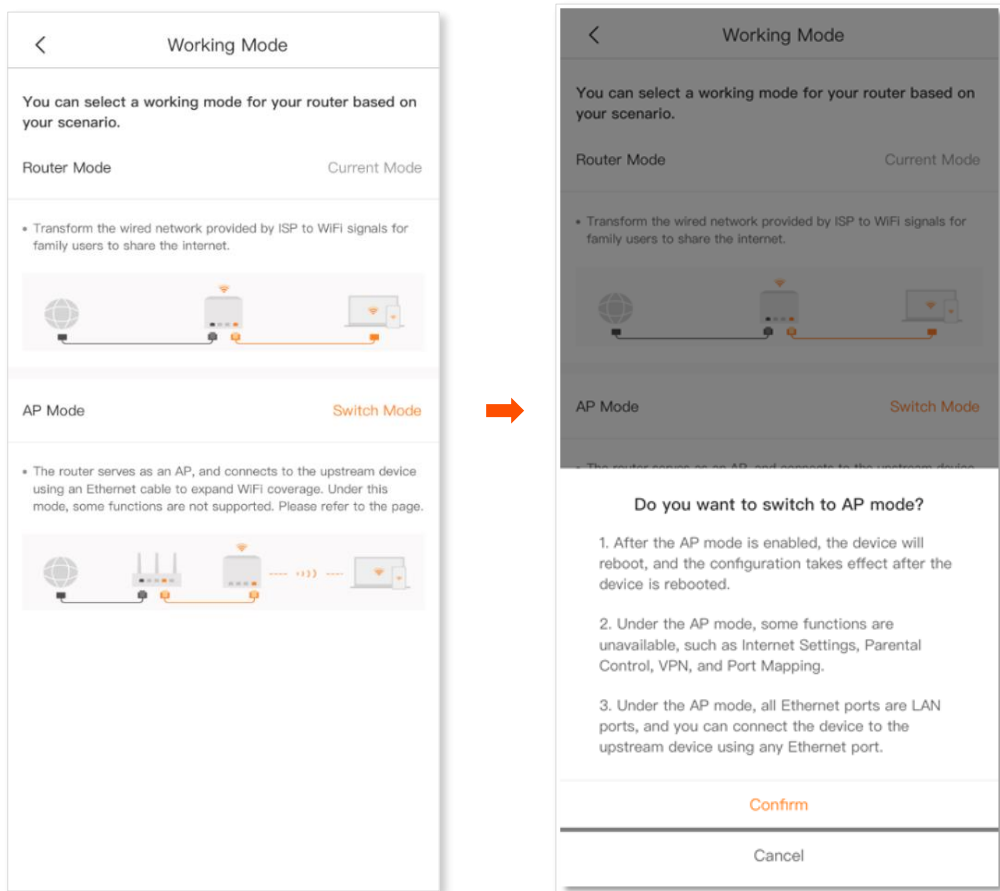


When the Mesh device is set to AP mode:

- 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.

To switch to the AP mode:

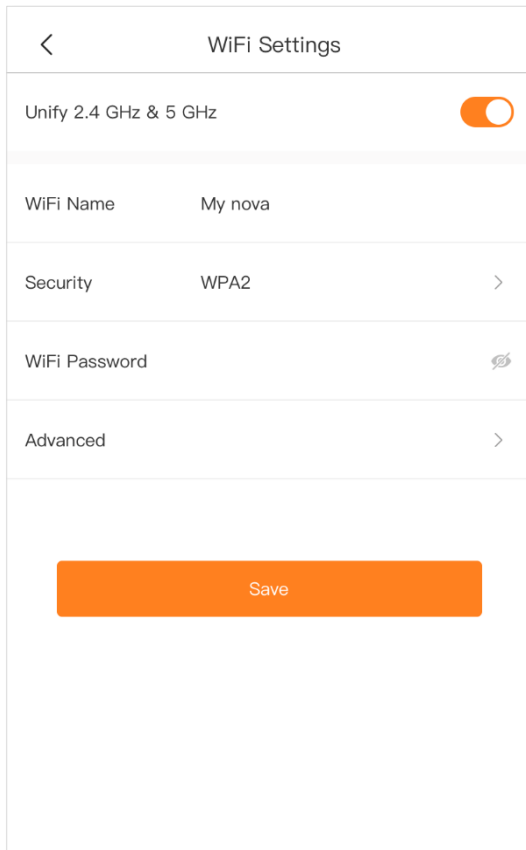
- Step 1** Run the **Tenda WiFi App**, and choose **Settings > Advanced > Working Mode**.
- Step 2** Tap **Switch Mode**.
- Step 3** Tap **Confirm** in the pop-up window.
- Step 4** Use an Ethernet cable to connect the LAN port of your Mesh device to a LAN port of your upstream router (the router has 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.



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

- Ensure that the upstream 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.

3.6.10 IPv6



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

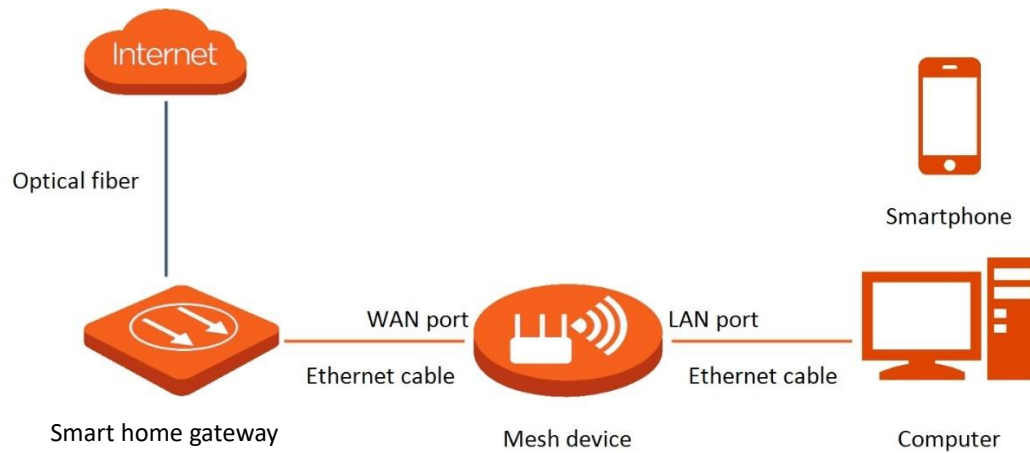


Before configuring the IPv6 function, ensure that you are within the coverage of the IPv6 network and already subscribe to the IPv6 internet service. Contact your ISP for any doubt about it.

DHCPv6

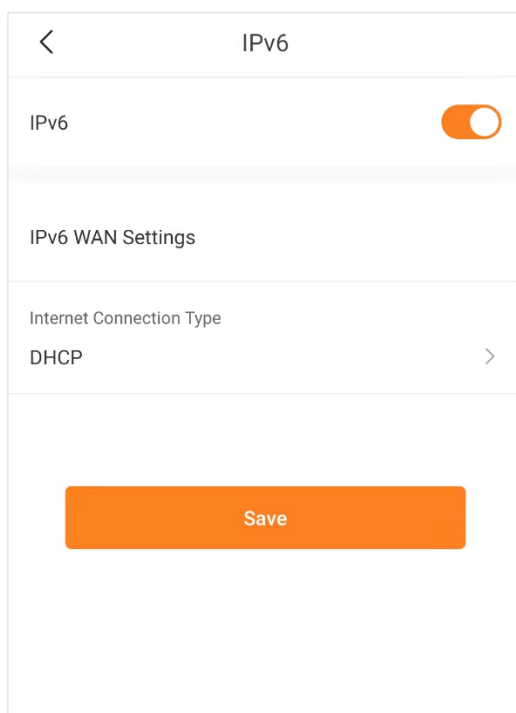
DHCPv6 enables the Mesh device to obtain an IPv6 address from the DHCPv6 server to access the internet. It is applicable in the following scenarios:

- 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.



To access the internet through DHCPv6:

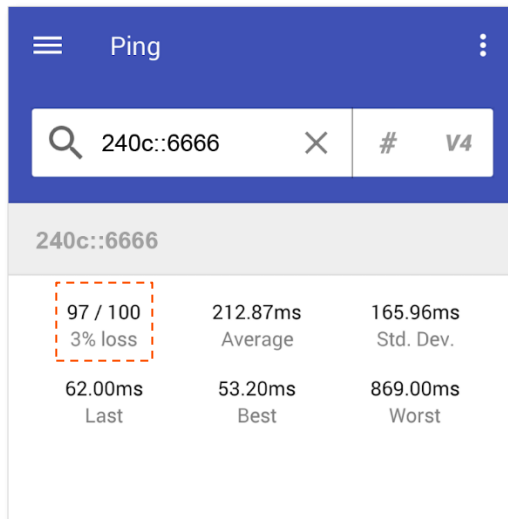
- Step 1** Run the **Tenda WiFi App**, and choose **Settings > Advanced > IPv6**.
- Step 2** Enable the **IPv6** function.
- Step 3** Set the **Internet Connection Type** to **DHCP** or **DHCPv6**.
- Step 4** Tap **Save**.



---End

Verification:

You can download a network diagnosis App (**HE.NET Network Tools** for example here) on your wireless client and ping an IPv6 website (**240c::6666** for example) to check whether the Mesh device accesses the IPv6 network successfully. As shown in the following figure, if the number of packets received is not 0, the Mesh device accesses the IPv6 network successfully.



If the IPv6 network fails, try the following solutions:

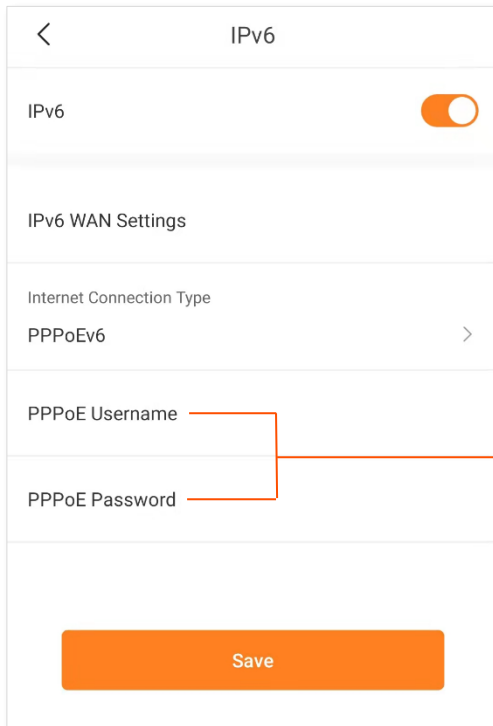
- Ensure that devices connected to Mesh device obtain their IPv6 addresses through DHCP.
- Consult your ISP for help.

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.

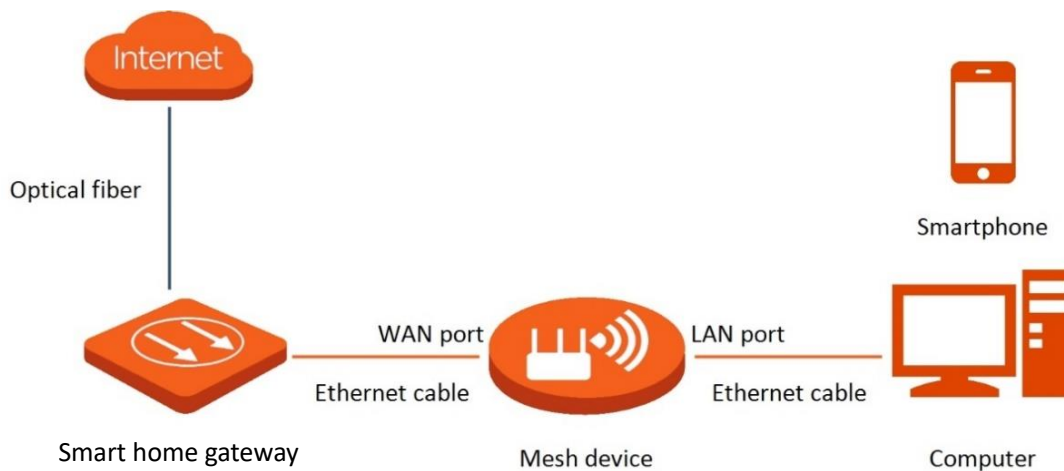
Run the Tenda WiFi App, and choose **Settings > Advanced > IPv6**. When the connection type is set to PPPoEv6, the page is shown as below.



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

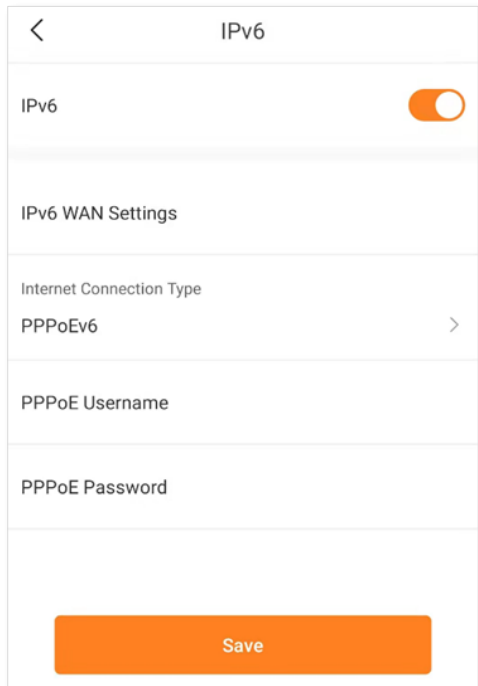
Access the internet through PPPoEv6

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.



Configuration procedure:

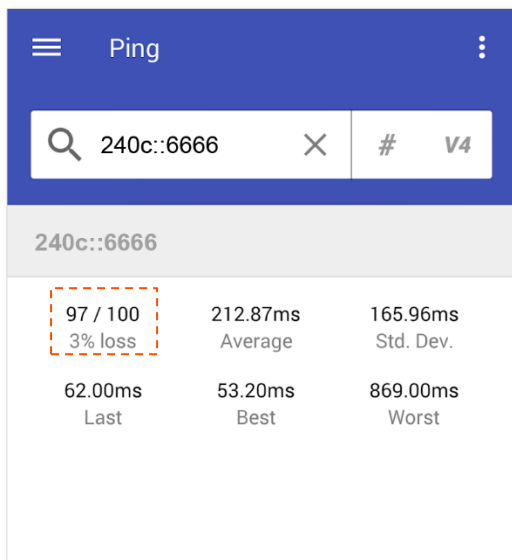
- Step 1** Run the **Tenda WiFi App**, and choose **Settings > Advanced > IPv6**.
- Step 2** Enable the **IPv6** function.
- Step 3** Set the **Internet Connection Type** to **PPPoEv6**.
- Step 4** Enter the **PPPoE Username** and **PPPoE Password** provided by your ISP.
- Step 5** Tap **Save**.



---End

Verification:

You can download a network diagnosis App (**HE.NET Network Tools** for example here) on your wireless client and ping an IPv6 website (**240c::6666** for example) to check whether the Mesh device accesses the IPv6 network successfully. As shown in the following figure, if the number of packets received is not 0, the Mesh device accesses the IPv6 network successfully.



If the IPv6 network fails, try the following solutions:

- Ensure that devices connected to Mesh device obtain their IPv6 addresses 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.

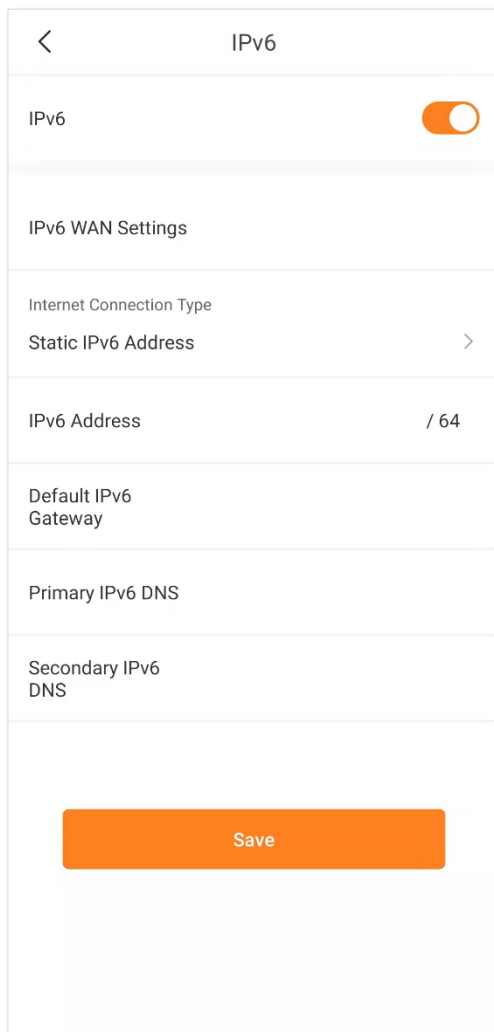
The screenshot shows the IPv6 settings page in the Tenda WiFi App. At the top, there is a back arrow and the title 'IPv6'. Below this is a toggle switch for 'IPv6' which is turned on. Underneath is a section titled 'IPv6 WAN Settings'. The 'Internet Connection Type' is set to 'Static IPv6 Address'. There are four input fields: 'IPv6 Address' (with a '/ 64' suffix), 'Default IPv6 Gateway', 'Primary IPv6 DNS', and 'Secondary IPv6 DNS'. A large orange 'Save' button is at the bottom of the page.

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

Access the internet through static IPv6 address

Configuration procedure:

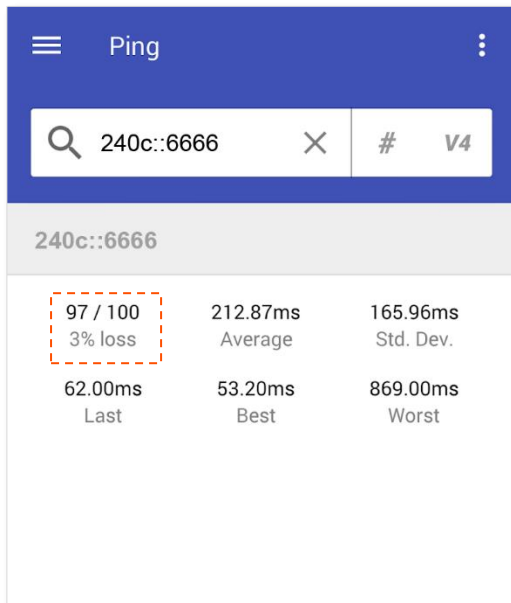
- Step 1** Run the **Tenda WiFi App**, and choose **Settings > Advanced > IPv6**.
- Step 2** Enable the **IPv6** function.
- Step 3** Set **Internet Connection Type** to **Static IPv6 Address**.
- Step 4** Enter the required parameters under **IPv6 WAN Settings**.
- Step 5** Tap **Save**.



---End

Verification:

You can download a network diagnosis App (**HE.NET Network Tools** for example here) on your wireless client and ping an IPv6 website (**240c::6666** for example) to check whether the Mesh device accesses the IPv6 network successfully. As shown in the following figure, if the number of packets received is not 0, the Mesh device accesses the IPv6 network successfully.



If the IPv6 network fails, try the following solutions:

- Ensure that you have entered the correct WAN IPv6 address.
- Ensure that devices connected to Mesh device obtain their IPv6 addresses through DHCP.
- Consult your ISP for help.

3.6.11 LAN settings

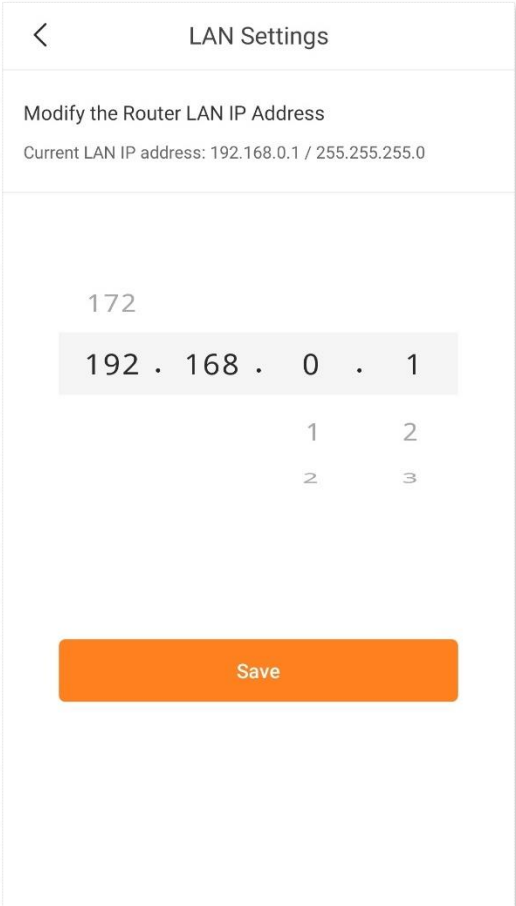


The DHCP server of the Mesh device can assign IP address, subnet mask, default gateway and DNS server address to clients within the LAN.

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.

Configuration 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.

3.6.12 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.

To set up a DHCP server:

- Step 1** Run the **Tenda WiFi App**, and choose **Settings > Advanced > DHCP Server**.
- Step 2** Enable **DHCP Server**.
- Step 3** Specify the **Start IP Address**, **End IP Address**, and **LAN IP address**.
- Step 4** Enable **DNS** as required and set **Primary DNS** and **Secondary DNS (Optional)**.
- Step 5** Tap **Save**.

The screenshot shows the DHCP Server configuration interface. At the top, there is a back arrow and the title "DHCP Server". Below this, the "DHCP Server" toggle is turned on. The "Start IP Address" is set to 192.168.1.100, the "End IP Address" is 192.168.1.200, and the "LAN IP address" is 192.168.1.1. The "DNS" toggle is also turned on. Below it, the "Primary DNS" is set to 0.0.0.0 and the "Secondary DNS (Optional)" is also set to 0.0.0.0. At the bottom of the screen, there is a large orange "Save" button.

---End

Now a DHCP server is established.

3.6.13 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:

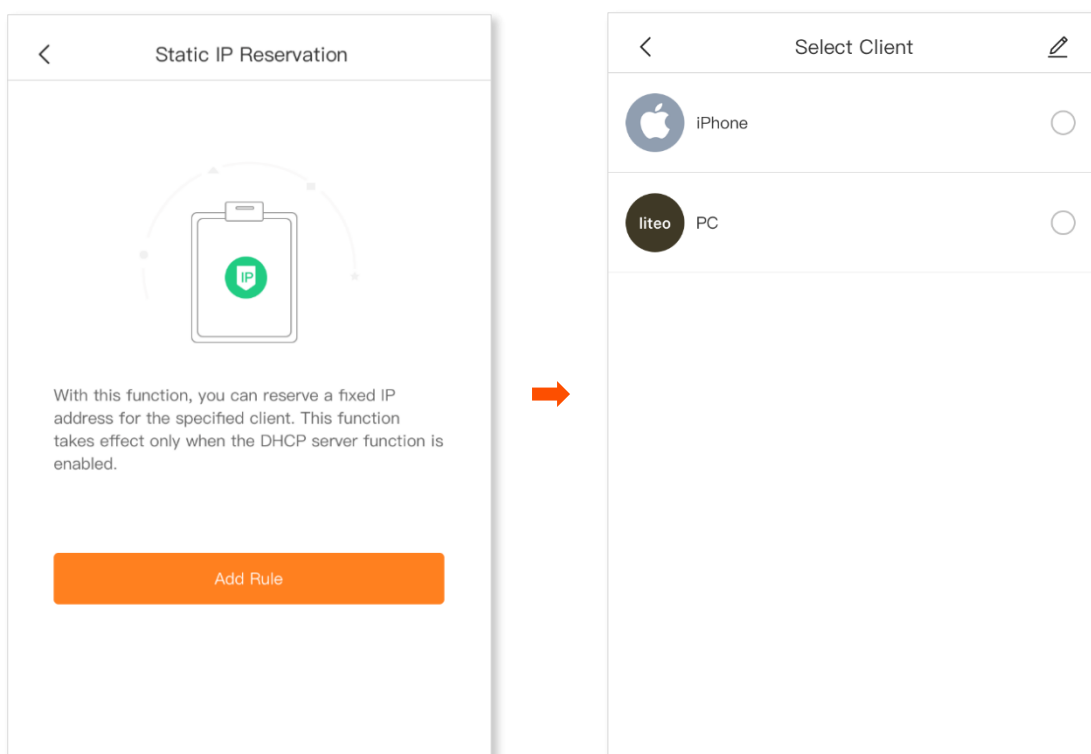
- Fixed IP address for the server: 192.168.0.143
- MAC address of the FTP server host: C0:9A:D0:5B:28:70

Configuration procedure:

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

Step 2 Tap **Add Rule**.

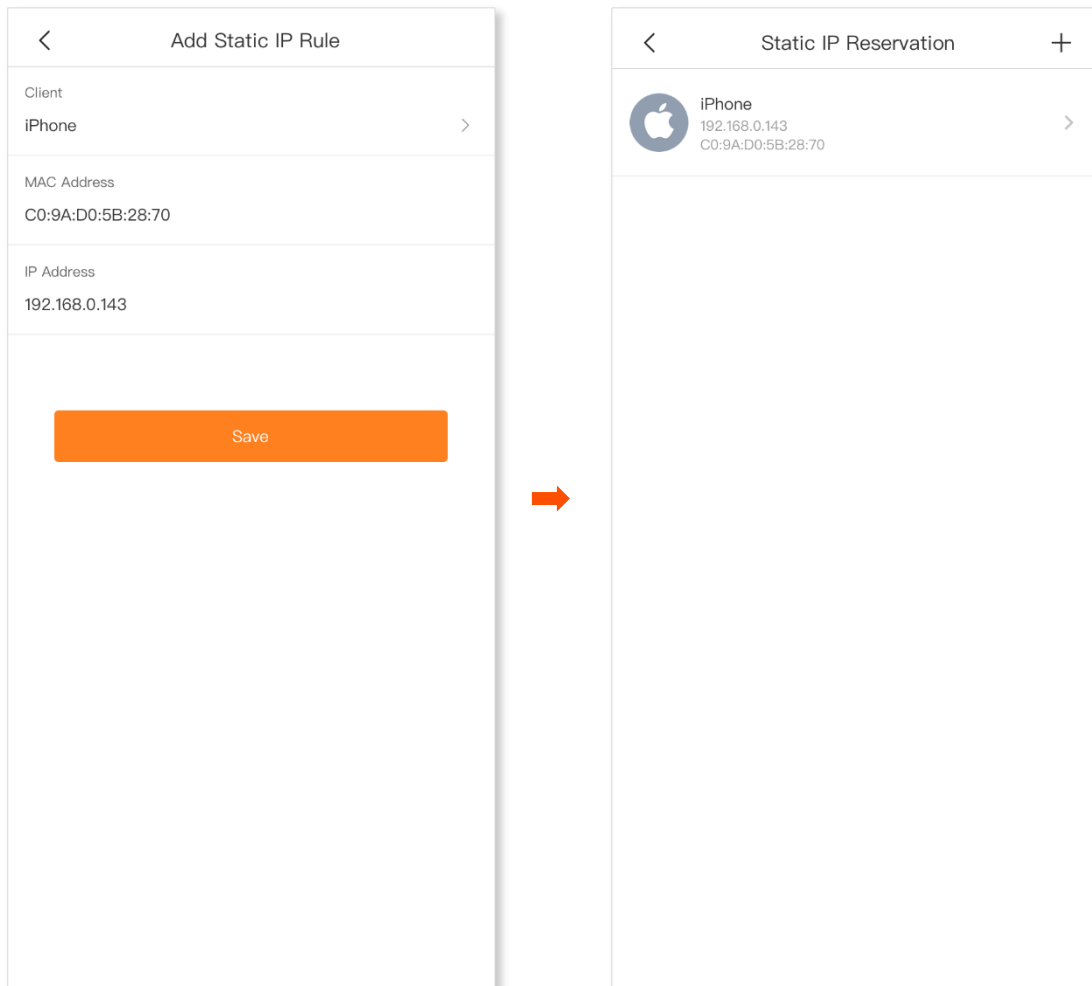
Step 3 Select the device to which the rule applies, which is **iPhone** in this example.



Step 4 Set up a port mapping rule.

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

Step 5 Tap **Save**.



---End

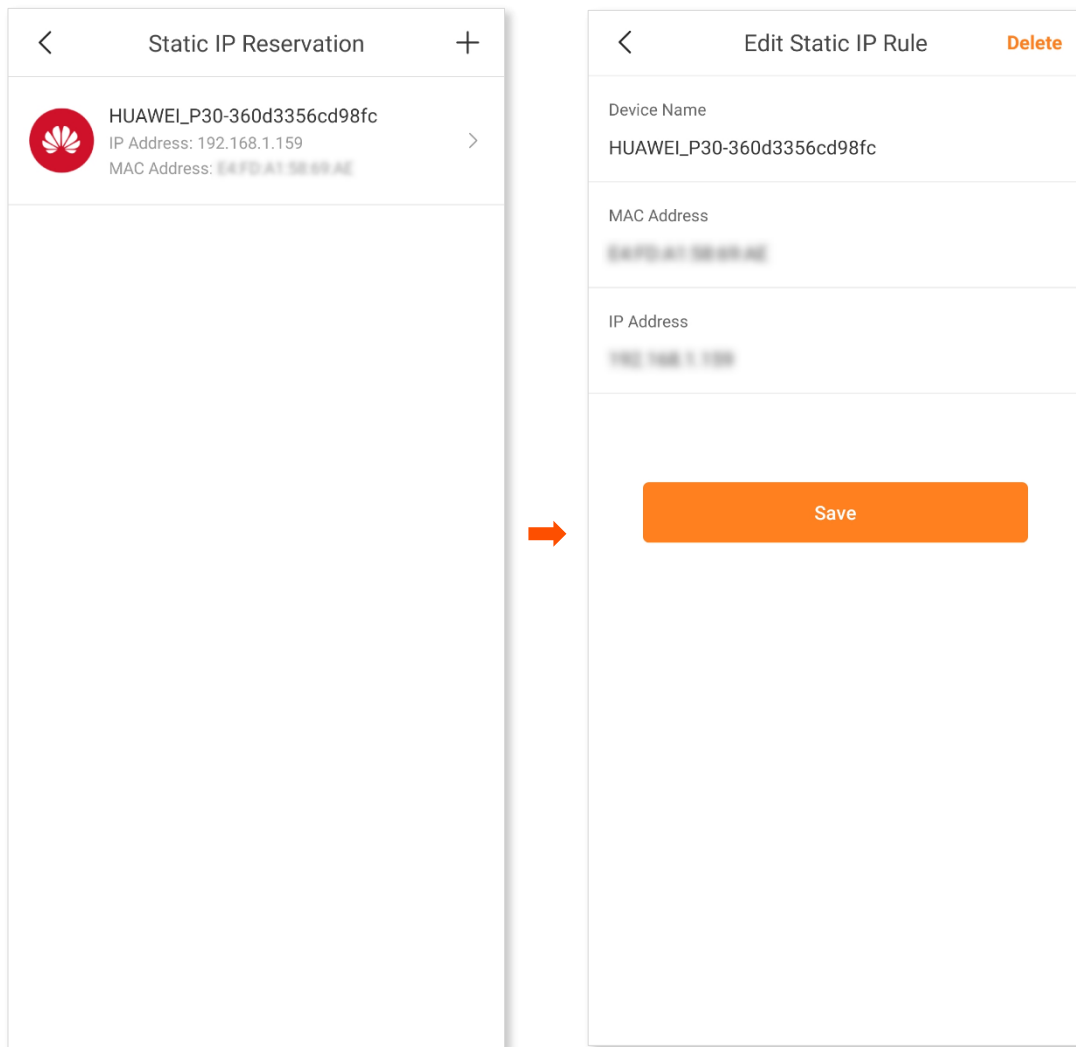
After the settings complete, the FTP server host always gets the same IP address when connecting to the Mesh device.

Delete a static IP reservation rule

Configuration procedure:

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

Step 2 Tap the rule to be deleted, and then tap **Delete**.



---End

When “Saved successfully” is displayed, the static IP reservation rule is deleted successfully.

3.6.14 DNS



Enable this function only when necessary.

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.

To change the DNS settings:

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**.

The screenshot shows the DNS configuration interface. At the top, there is a back arrow and the title 'DNS'. Below this, there are three rows of settings:

- Obtain Type:** Set to 'Auto' with a right-pointing chevron.
- Primary DNS:** Set to '114.114.114.114'.
- Secondary DNS (Optional):** Set to '223.5.5.5'.

At the bottom of the screen, there is a large orange button labeled 'Save'.

---End

3.6.15 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 set-top box (STB) functions here.

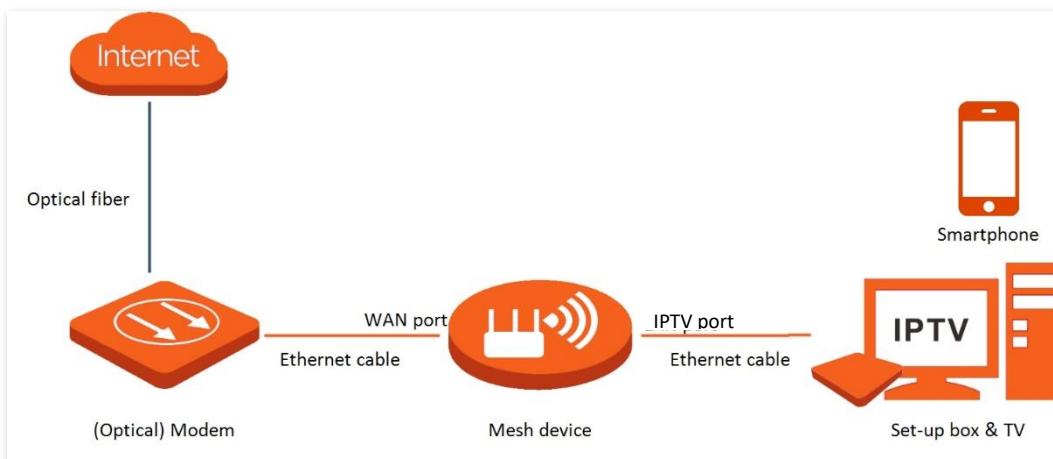
- **Multicast:** If you want to watch multicast videos from the WAN side of the Mesh device on your computer, you can enable the multicast function of the Mesh device.
- **STB:** If the IPTV service is included in your broadband service, you can enjoy both internet access through the Mesh device and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

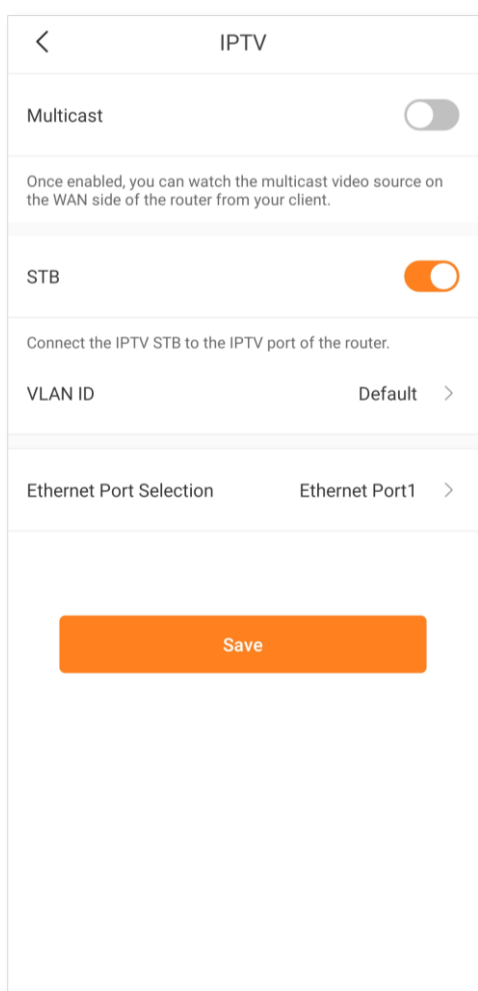


Configuration procedure:**Step 1** Set your Mesh device.

1. Run the **Tenda WiFi App**, and choose **Settings > Advanced > IPTV**.
2. Enable the **STB** function.
3. Set **Ethernet Port Selection** as required.



This substep is required only for some models, such as MX15 Pro/EX15 Pro/Mesh15XP/MX21 Pro/EX21 Pro/Mesh21XEP.

4. 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

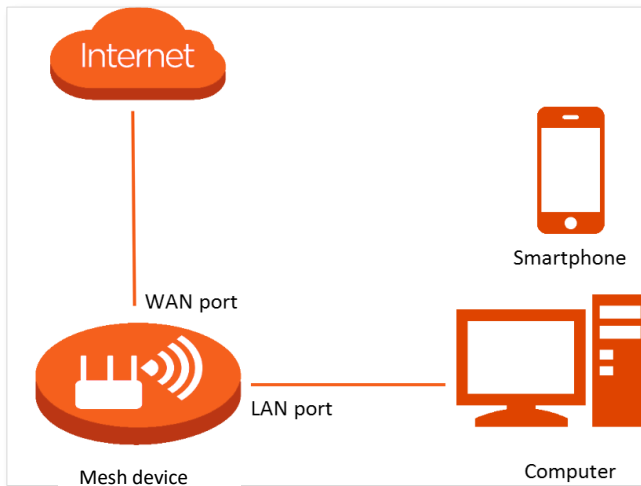
After the setting completes, you can watch IPTV programs on your TV.

Watch multicast videos through the Mesh device

Scenario: You have the address of multicast videos.

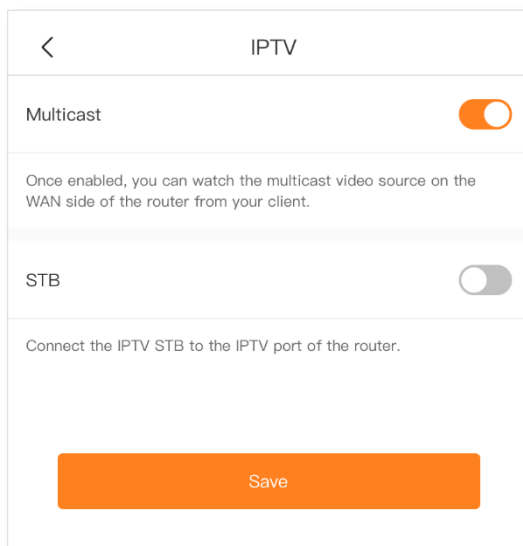
Goal: You can watch multicast videos.

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



Configuration 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.



3.6.16 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.



- For information security, do not enable **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.

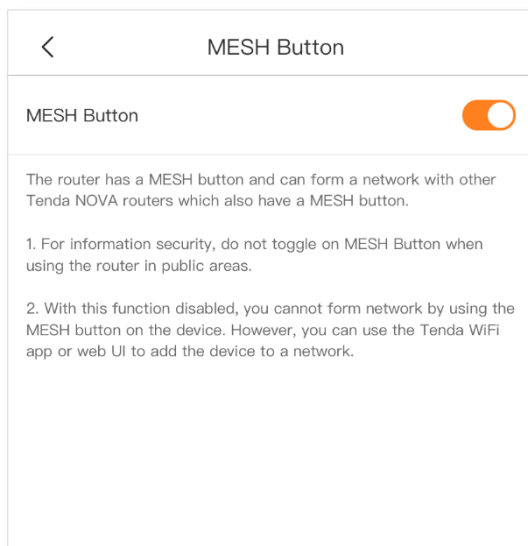
The Mesh device supports three methods for mesh networking:

- 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.

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

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

3.6.17 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.



- 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.

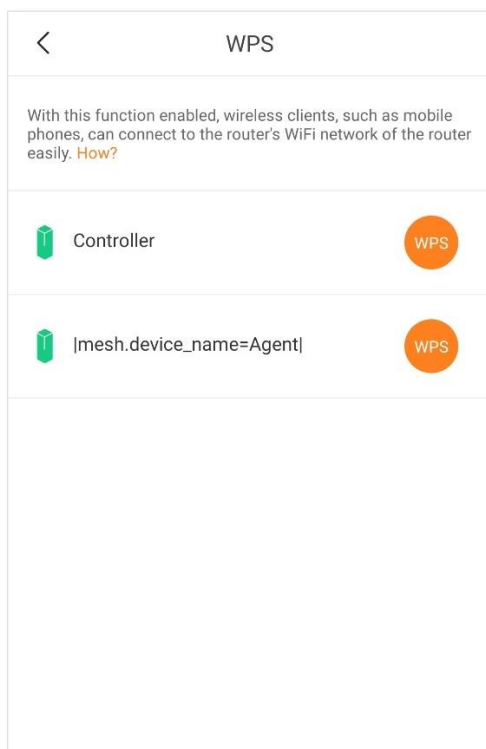
To connect a device to the Wi-Fi network using the WPS function:

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.

Countdown starts when the WPS function is enabled.

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



---End

Now the WPS-supported device is connected to the internet.

3.6.18 Port mapping



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



- 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 (1025 to 65535), such as 9999.
- The internal port number can be different from the external port number.

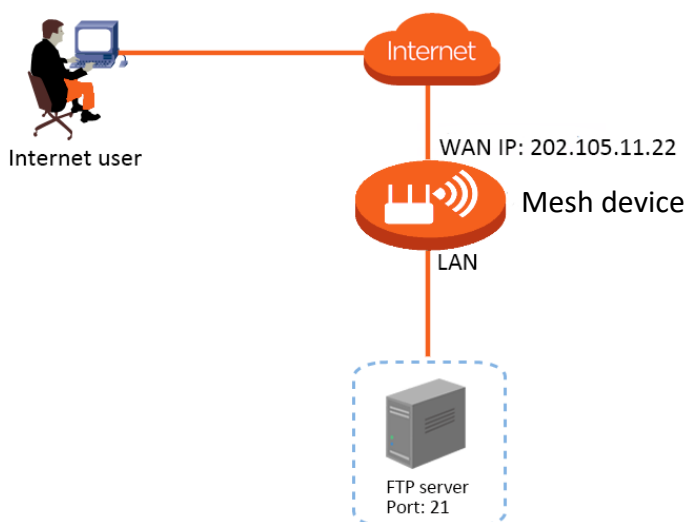
An example of configuring the port mapping function:

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 mapping 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



Configuration procedure:

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

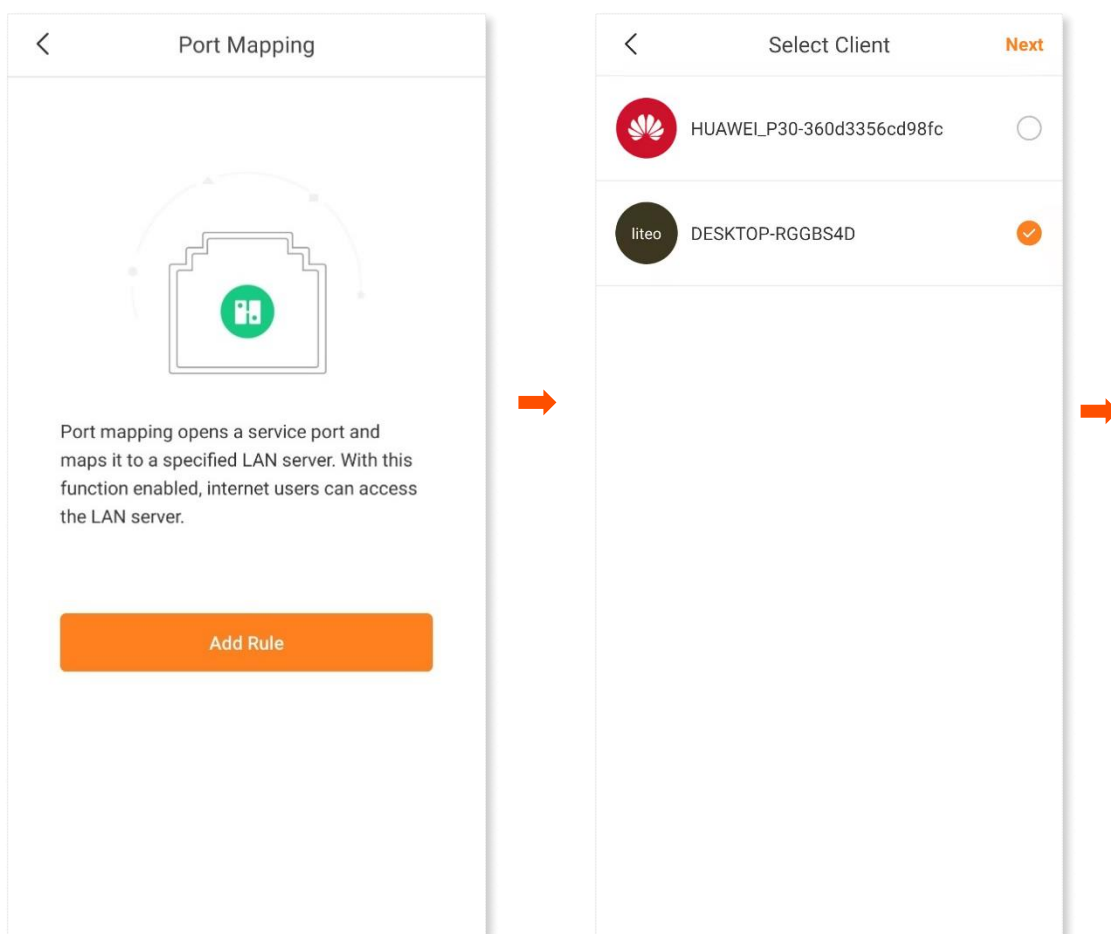
Step 2 Tap **Add Rule**.

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

Step 4 Set up a port mapping 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 **Internal 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 default internal port number is not used, 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 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 mapping function failures. Disable them when using this function.
- Manually set an IP address for the server to avoid the service disconnection caused by the dynamic IP address.

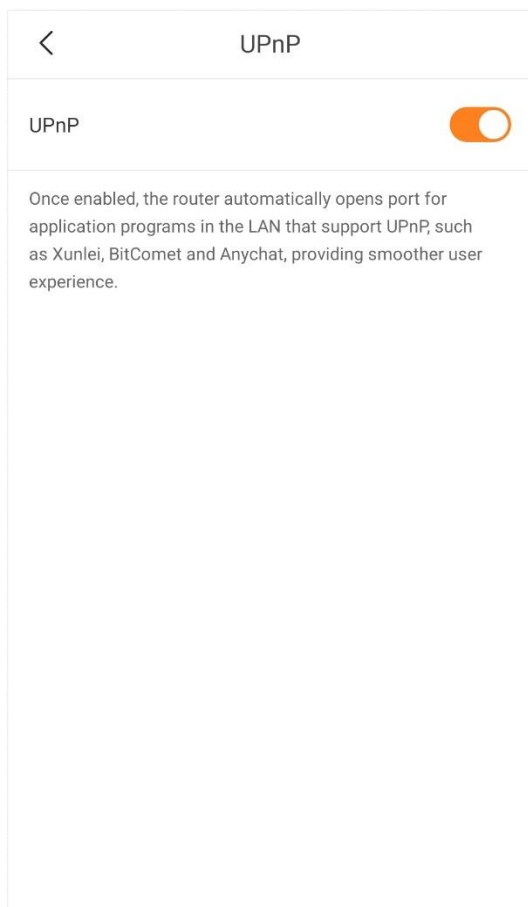
3.6.19 UPnP

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.

To enable or disable the UPnP function:

- Step 1** Run the **Tenda WiFi** App, and choose **Settings > Advanced > UPnP**.
- Step 2** Enable or disable the **UPnP** function as required.



---End

3.7 System settings

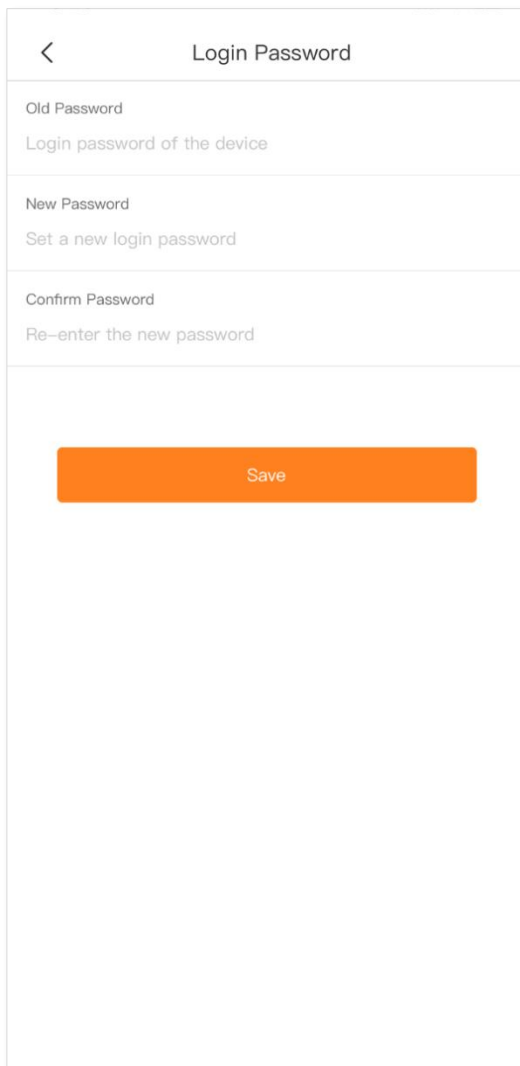
3.7.1 Login password



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.



< Login Password

Old Password
Login password of the device

New Password
Set a new login password

Confirm Password
Re-enter the new password

Save

3.7.2 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:

Configuration procedure:

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

Step 2 Enable **Auto System Maintenance**.

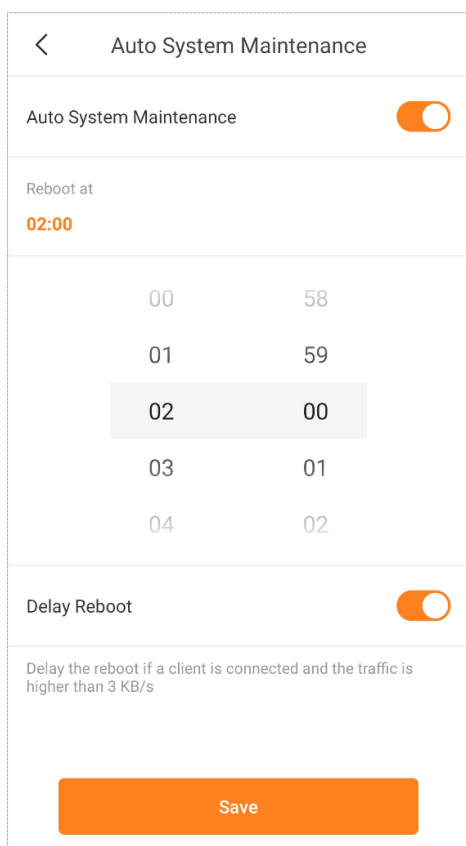
Step 3 Select a reboot time for **Reboot at**.

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**.



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 enabled. 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 for 0.5h. Otherwise, the devices will reboot the next day at the specified reboot time.

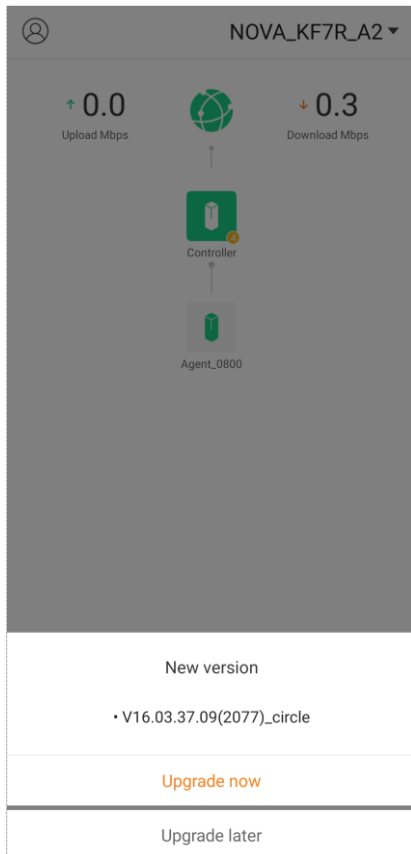
---End

Now the devices will automatically reboot at the specified time.

3.7.3 Firmware upgrade



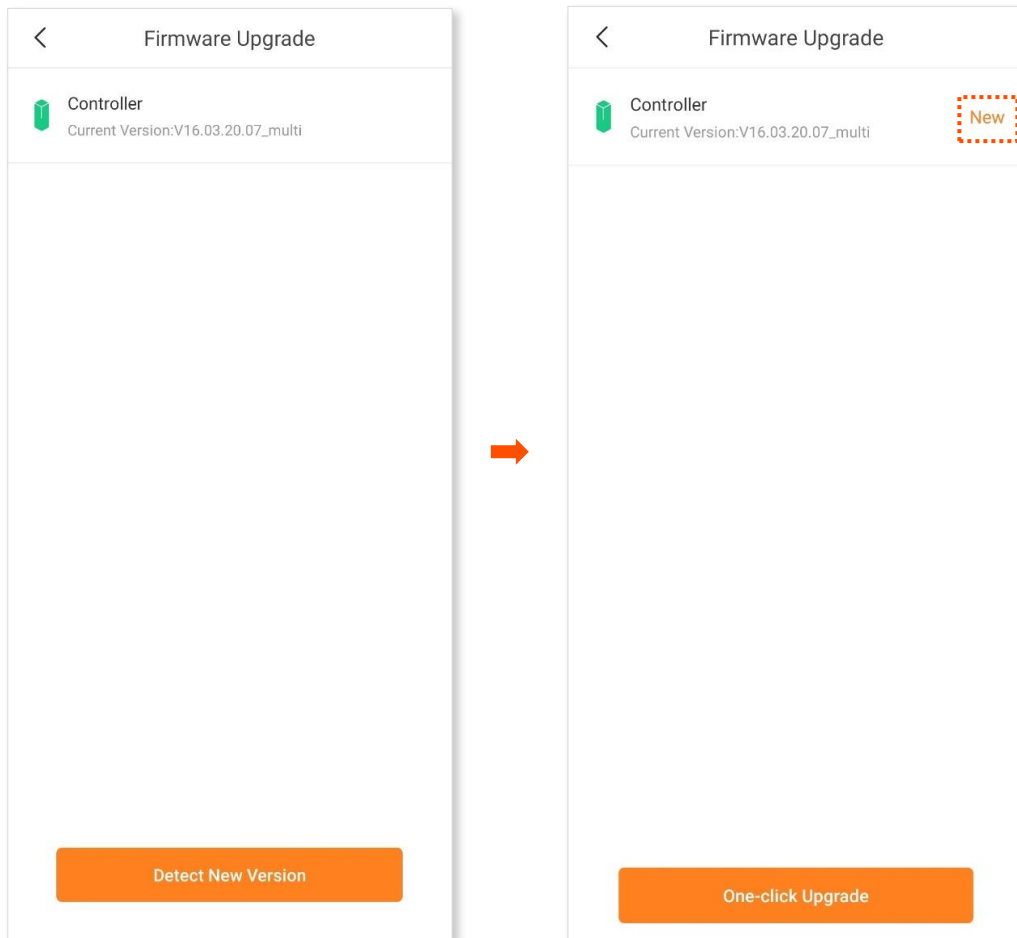
Tenda is dedicated to improving its products to let users enjoy better performance. Please update the firmware when the App notifies that a new firmware version is available.



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

Configuration 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

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

3.7.4 Account authorization

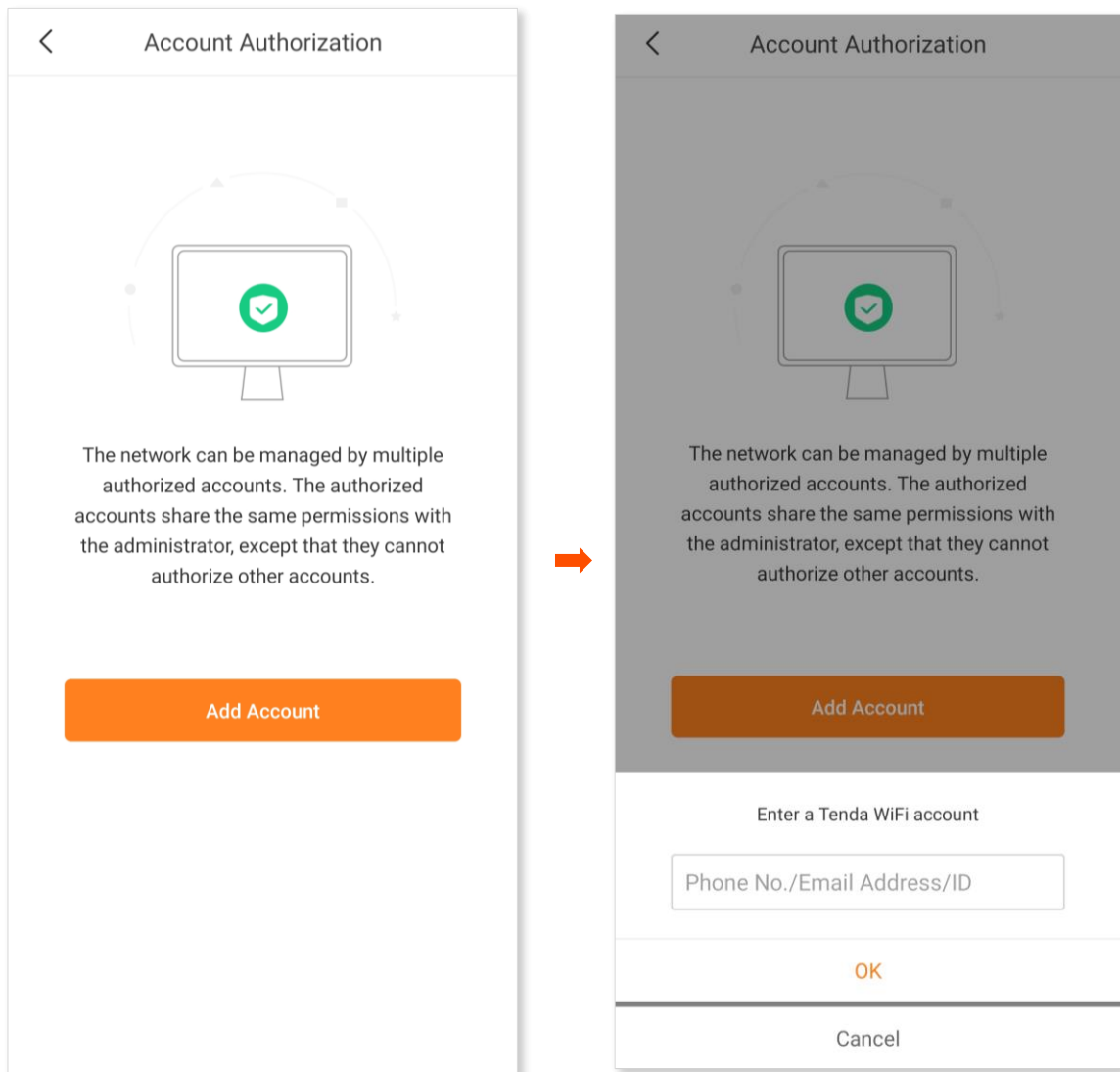


This function is available only for the administrator account for some models. If it is not displayed in your app, it is unavailable for the product that you purchased.

The Mesh device can be managed by multiple authorized accounts, which share the same permissions with the administrator, except that they cannot authorize other accounts.

Authorize an account

- Step 1** Run the **Tenda WiFi App**, and choose **Settings > Account Authorization**.
- Step 2** Tap **Add Account** or **+** in the upper right corner.
- Step 3** Enter an existing account and tap **OK**.




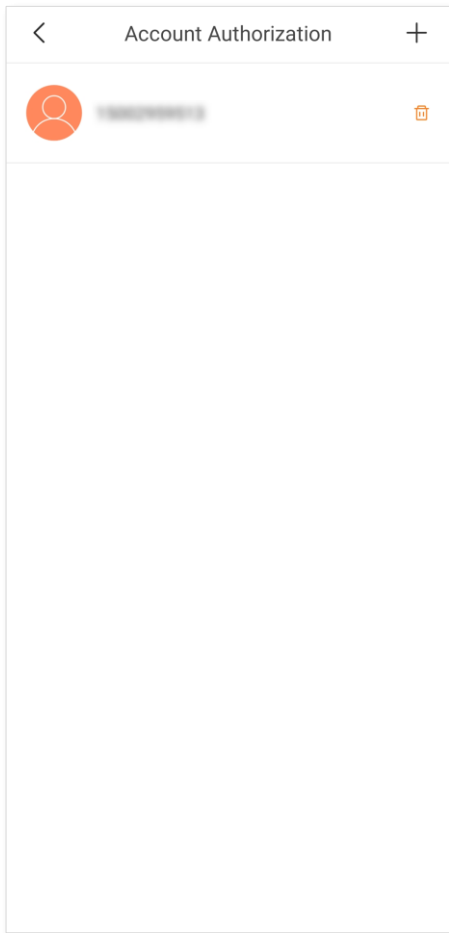
---End

The added account will be displayed in the list, and the added account can be used to manage the Mesh devices.

Delete an authorized account

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


Step 2 Locate the account to be deleted, and tap  after it.

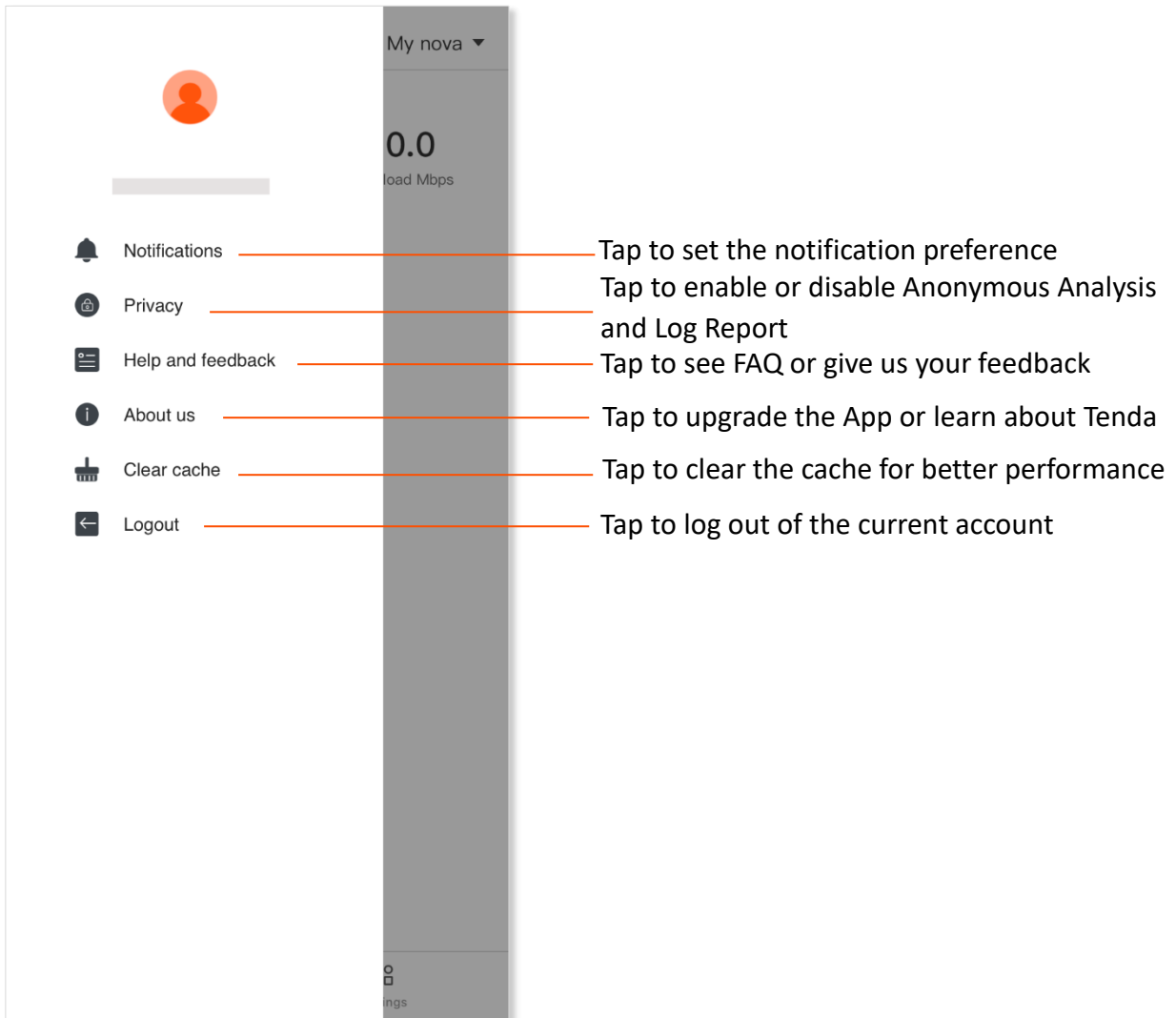


---End

The account will be removed from the list.

3.8 My profile

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



4 Web UI operations (mobile client)

This chapter introduces all functions and operations available on the web UI (mobile client), including:

- [Quick setup](#)
- [Login](#)
- [Router information](#)
- [Network overview](#)
- [Internet settings](#)
- [Wi-Fi settings](#)
- [Client management](#)
- [Parental control](#)
- [More](#)

More functions and operations are available on the web UI (computer) and Tenda WiFi App. For details, see [Web UI operations \(computer\)](#) and [APP operations](#).

4.1 Quick setup

4.1.1 Connect your primary node to the internet

A smartphone is used for illustration here.

Configuration procedure:

Step 1 [Connect your primary node.](#)

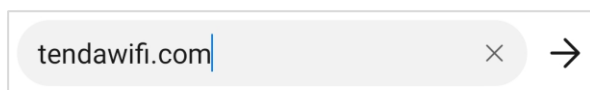
Step 2 Connect your smartphone to the Wi-Fi network of the primary node.



TIP

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

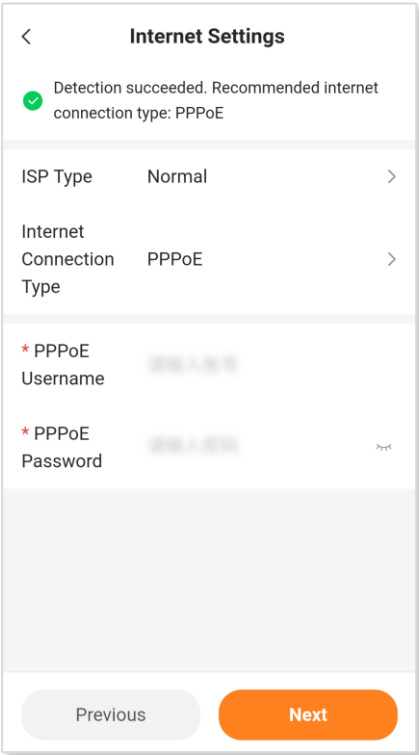
Step 3 Start a browser on your smartphone and enter **tendawifi.com** in the address bar to access the web UI.



Step 4 Tap **Start**.

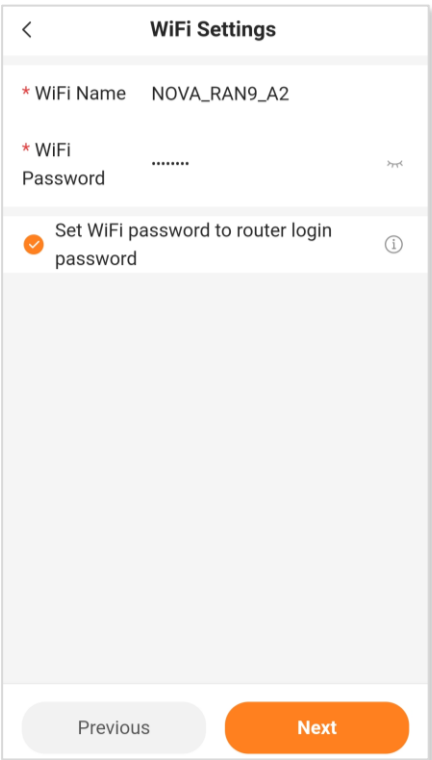


Step 5 Set required parameters (PPPoE is used for illustration here) and tap **Next**.



The connection type of WAN port of the Mesh device will be detected automatically. If the WAN port is not connected properly, follow the instructions on the page to complete the connection.

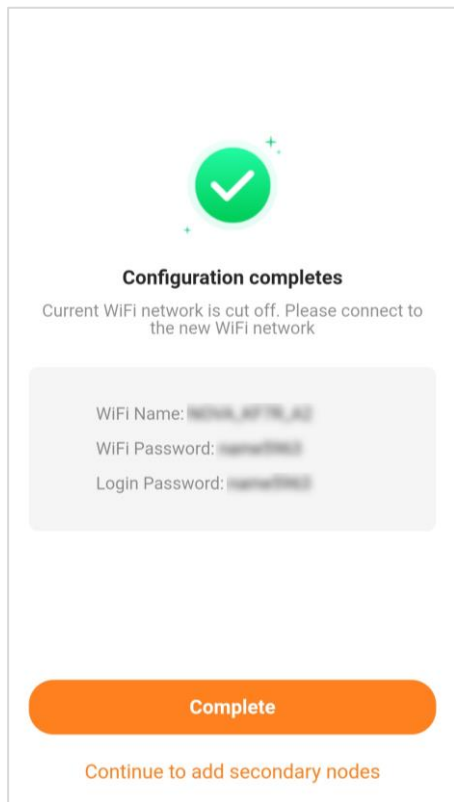
Step 6 Customize the **WiFi Name** and **WiFi Password**, and click **Next**.
NOVA_RAN9_A2 is used for example here.





- 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 **WiFi Name** and **WiFi Password** for Wi-Fi login and **Login Password** for web UI login.

Step 7 Tap **Complete**.



---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, tap **Continue to add secondary nodes** and add new nodes according to the onscreen instructions.

4.1.2 Extend your network

To extend the network with other nodes, see [Add a node](#).

For detailed steps, see [Extend your network](#) in [Web UI operations \(mobile client\)](#).

4.2 Login

**TIP**

A smartphone is used for illustration here.

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

Step 1 Connect your smartphone to the Wi-Fi network of the primary node.

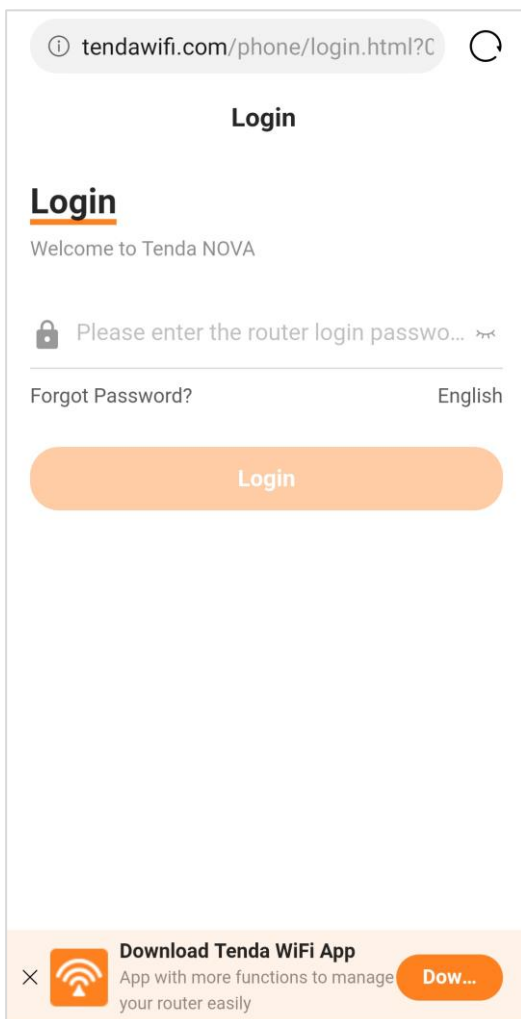
**TIP**

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

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



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





- 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

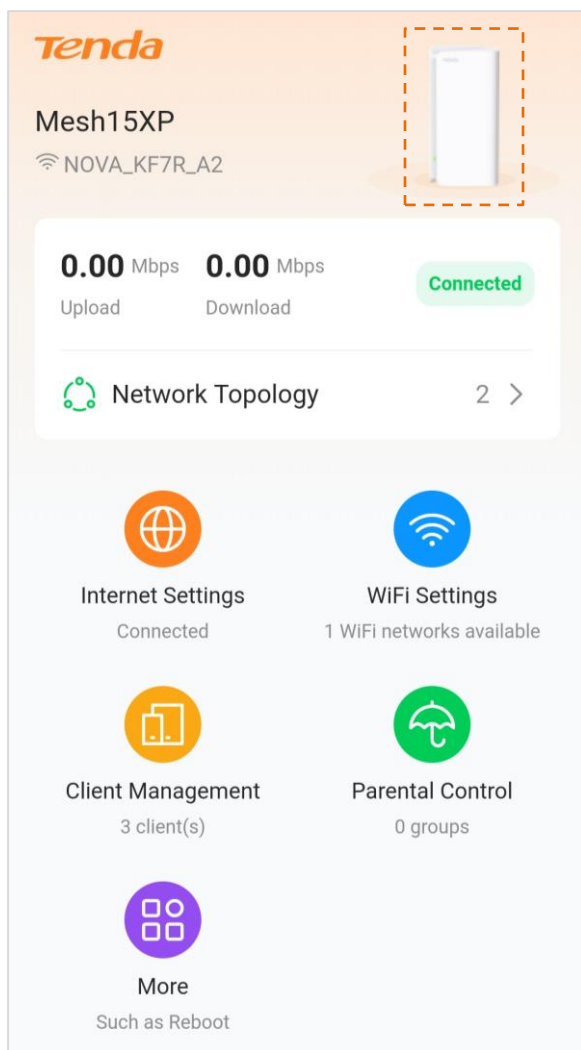
4.3 Router information

On this page, you can view the information of the primary node, including [Basic information](#), [WAN port information](#), [LAN information](#) and [Wi-Fi information](#).

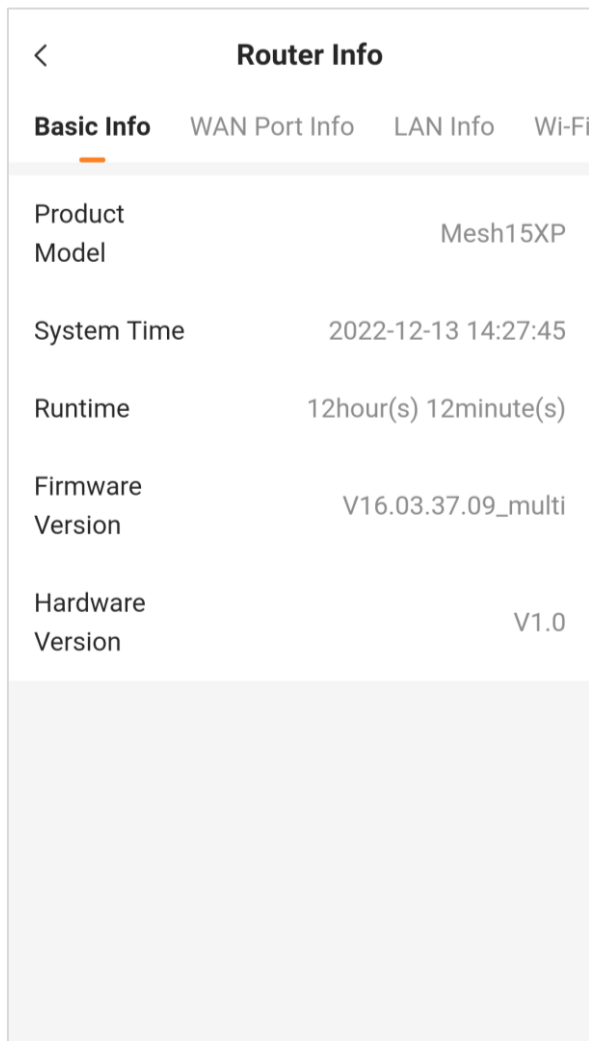
To view the information of the primary node:

Step 1 [Log in to the web UI \(mobile client\)](#).

Step 2 Tap the Mesh device icon.



The following page is displayed.



---End

Basic information

Tap **Basic Info** to view the 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.
System Time	Specifies the current system time.
Runtime	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.

Tap **WAN Port Info** to 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.
Connected time	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.
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	
MAC Address	Specifies the WAN MAC address of the primary node.

LAN information

Tap **LAN Info** to 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.
Subnet Mask	Specifies the LAN subnet mask of the primary node.
MAC Address	Specifies the LAN MAC address of the primary node.

Wi-Fi information

Tap **Wi-Fi Info** to view LAN information of the primary node, as described in the following table.

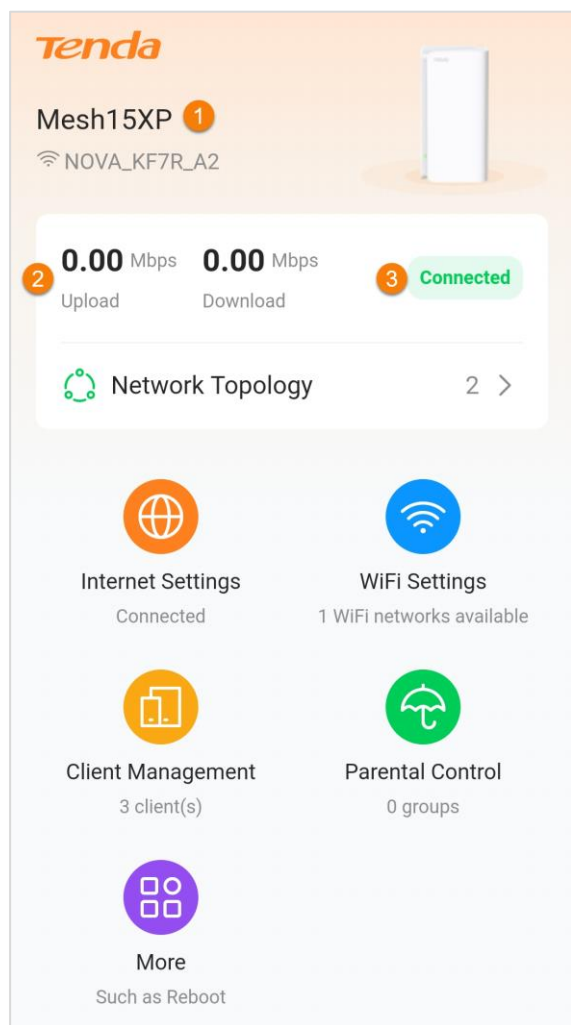
Parameter description

Parameter	Description
Status	Specifies the visibility of the Wi-Fi network.
Wi-Fi Name	Specifies the Wi-Fi name of the respective Wi-Fi network.
Security	Specifies the security mode of the respective Wi-Fi network.
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.

4.4 Network overview

4.4.1 Network status

To view the network status, [log in to the web UI \(mobile client\)](#). The following page is displayed.



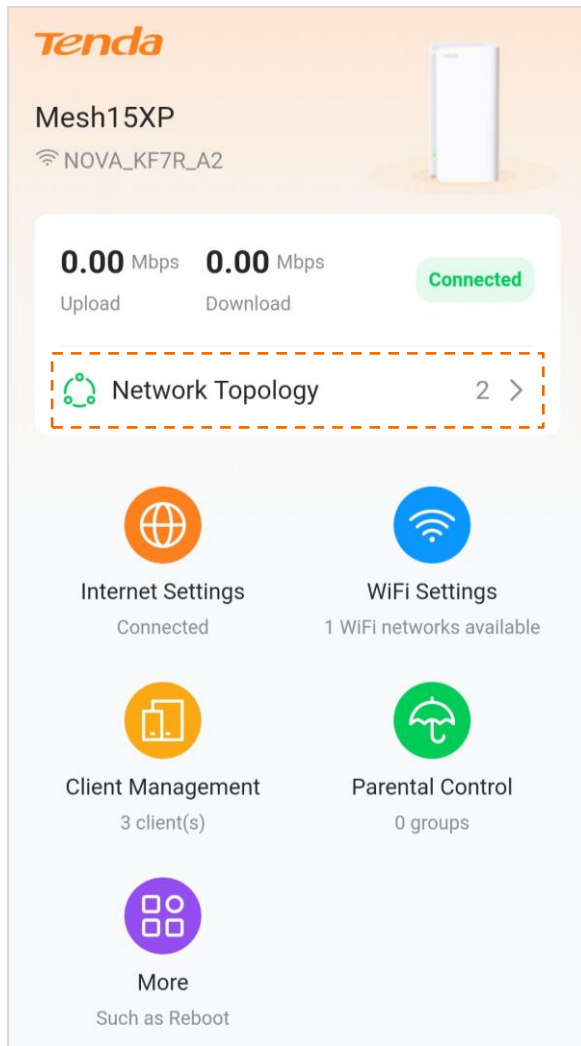
No.	Description
1	Displays the device model and Wi-Fi name.
2	Displays the real-time upload and download speed of the primary node.
3	Displays the internet connection status. <ul style="list-style-type: none"> - Connected: The primary node is connected to the internet successfully. - Disconnected: The primary node is disconnected from the internet.

4.4.2 Network topology

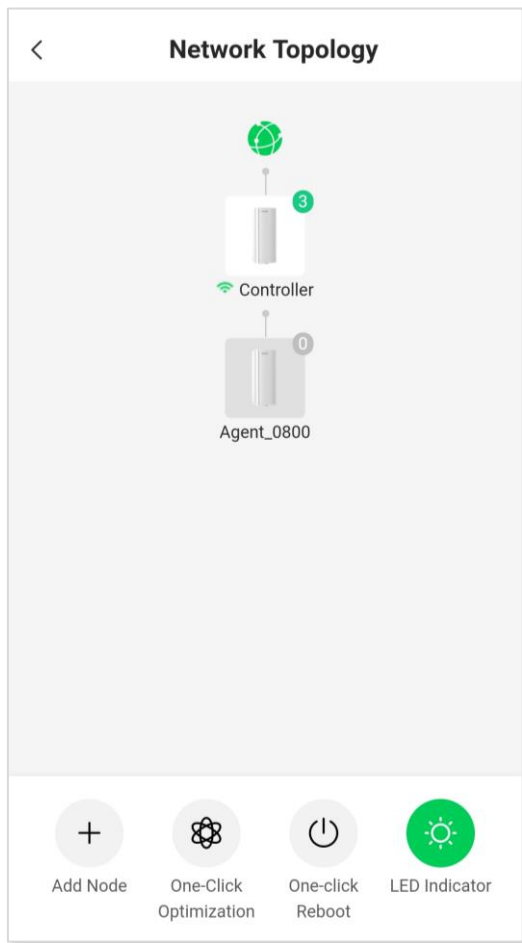
To view the basic information of the network topology and perform quick operations:

Step 1 [Log in to the web UI \(mobile client\)](#).

Step 2 Tap **Network Topology**.



The following page is displayed.



---End

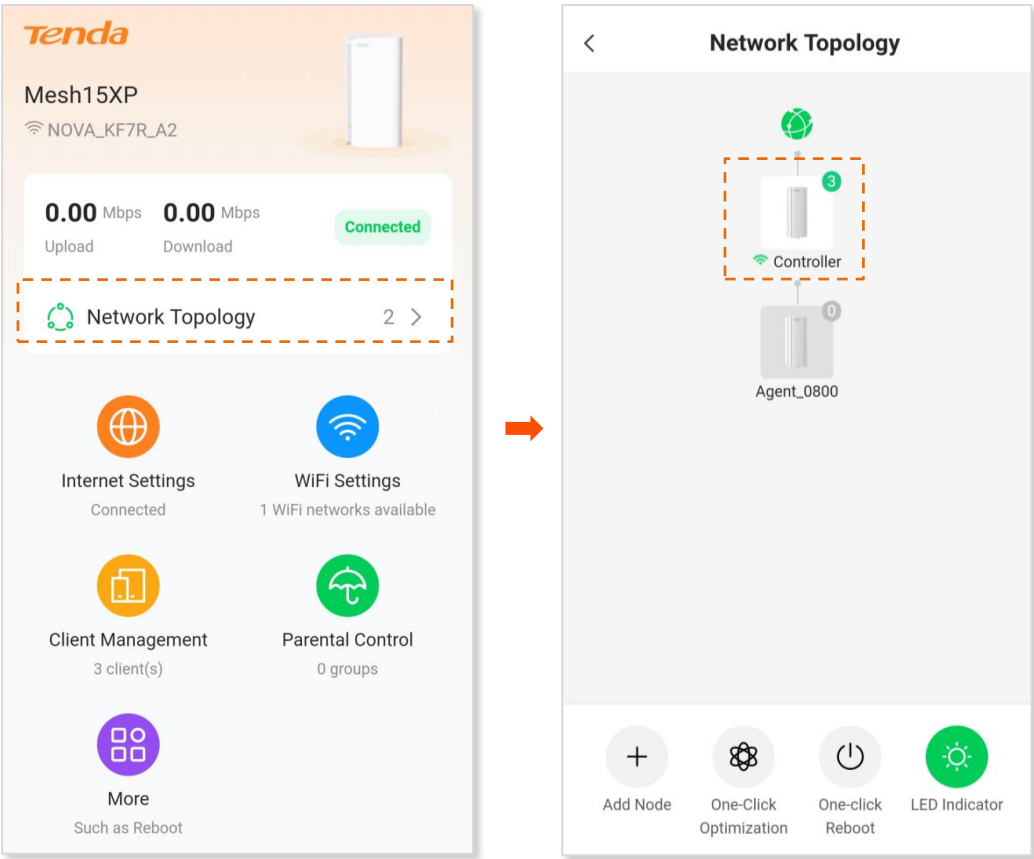
Item	Description
Controller Agent	Form a network topology. For details, see Controller information and Agent information .
Add Node	Used to Add a node .
One-Click Optimization	Used for One-click optimization .
One-click Reboot	Used to Reboot all nodes .
LED Indicator	Used to Turn on/off all indicators .

Controller information

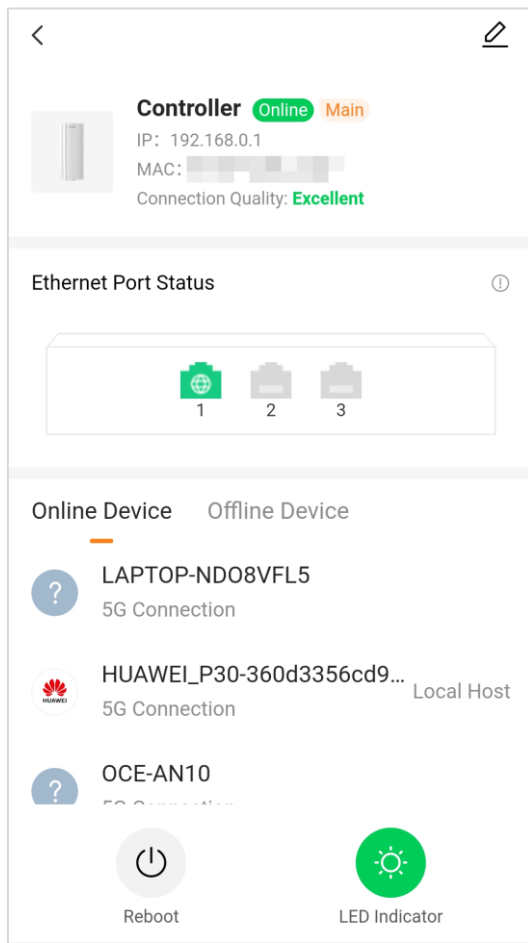
To view the information about and perform quick operations on the controller (primary node) and clients in the network:

Step 1 [Log in to the web UI \(mobile client\)](#).

Step 2 Tap **Network Topology** and then **Controller**.









The following page is displayed.



---End

Parameter/Button	Description
	Used to modify the node name.
IP	Indicates the IP address of the primary node.
MAC	Indicates the MAC address of the primary node.
Connection Quality	Indicates the internet connection quality of the primary node.

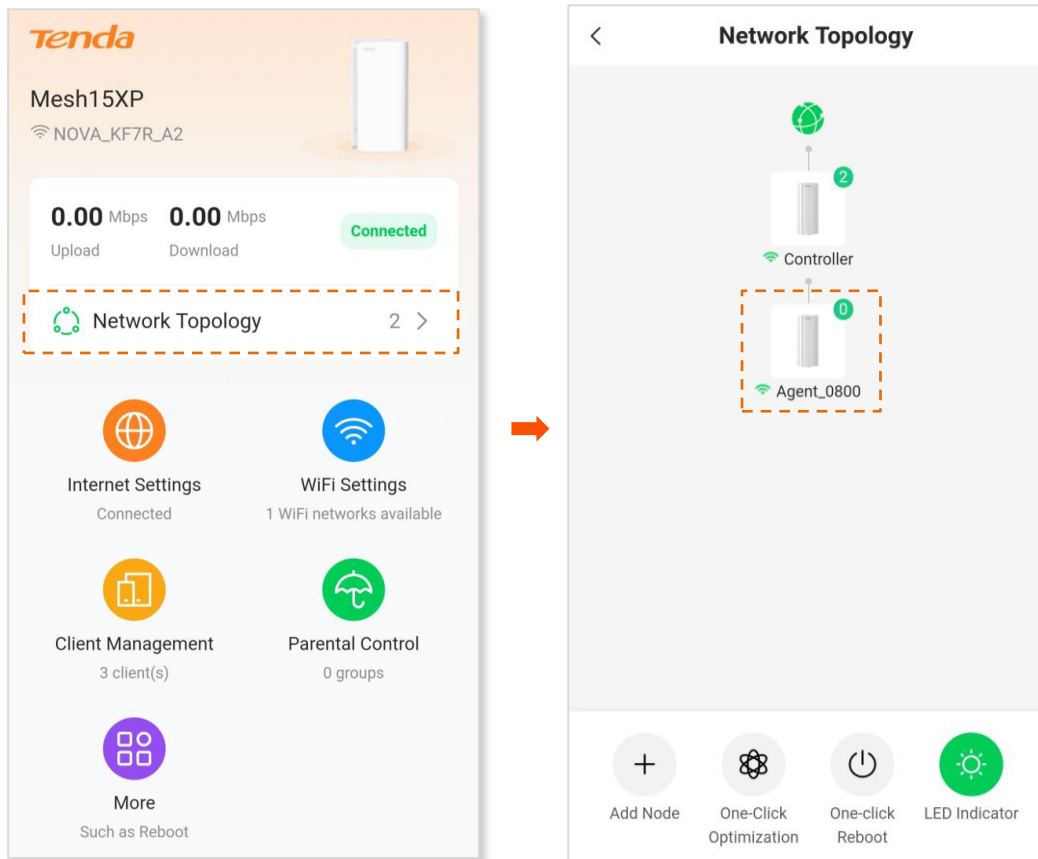
Parameter/Button	Description
Ethernet Port Status	<p>Indicates the status of the Ethernet ports of the primary node.</p> <p> TIP</p> <p>Currently, this parameter is only available for Mesh15XP, MX15 Pro, EX15 Pro, Mesh21XEP, MX21 Pro and EX21 Pro.</p> <p> : Indicates that the port is connected and used as a WAN port.</p> <p> : Indicates that the port is connected and used as a LAN port.</p> <p> : Indicates that the port is connected and used as an IPTV port.</p> <p> : Indicates that the port is not connected.</p>
Online Device	Shows the online clients that are connected to the primary node.
Offline Device	<p>Shows the offline clients that are connected to the primary node before.</p> <p> TIP</p> <p>A maximum of 30 offline clients can be displayed here. A client will be automatically deleted from the list if it is offline for 3 days. A client is displayed under Offline Device after it is disconnected from the network for 90 seconds (wired client)/60 seconds (wireless client).</p>
Reboot	Used to reboot the primary node.
LED Indicator	<p>Used to turn on/off the LED indicator of the primary node.</p> <p>You can use this function to check which device you are operating. Turn on/off all indicators prevails to this operation.</p>

Agent information

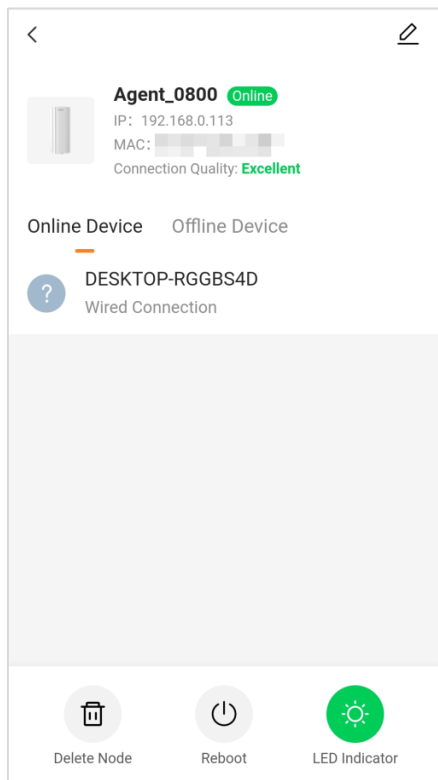
To view the information about and perform quick operations on the agents (secondary nodes) in the network:

Step 1 [Log in to the web UI \(mobile client\)](#).



Step 2 Tap **Network Topology** and then the target agent.



The following page is displayed.



---End

Parameter/Button	Description
	Used to modify the node name.
IP	Indicates the IP address of the secondary node.
MAC	Indicates the MAC address of the secondary node.
Connection Quality	Indicates the connection signal strength with the primary node.
Online Device	Shows the online clients that are connected to the secondary node.
	Shows the offline clients that are connected to the secondary node before.
Offline Device	 TIP A maximum of 30 offline clients can be displayed here. A client will be automatically deleted from the list if it is offline for 3 days. A client is displayed under Offline Device after it is disconnected from the network for 90 seconds (wired client)/60 seconds (wireless client).
Delete 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 .
Reboot	Used to reboot the secondary node.

Parameter/Button	Description
LED Indicator	Used to turn 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.

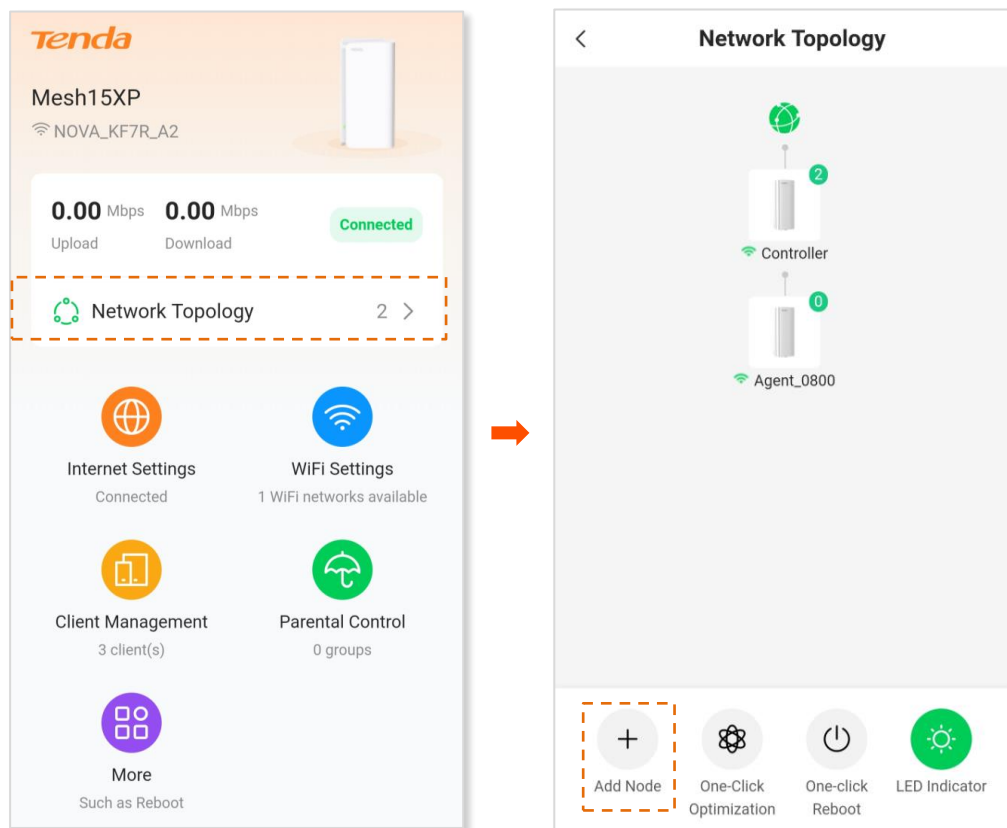
Add a node



- 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.

Step 1 [Log in to the web UI \(mobile client\).](#)

Step 2 Tap **Network Topology** and then **Add Node**.



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

Delete a node

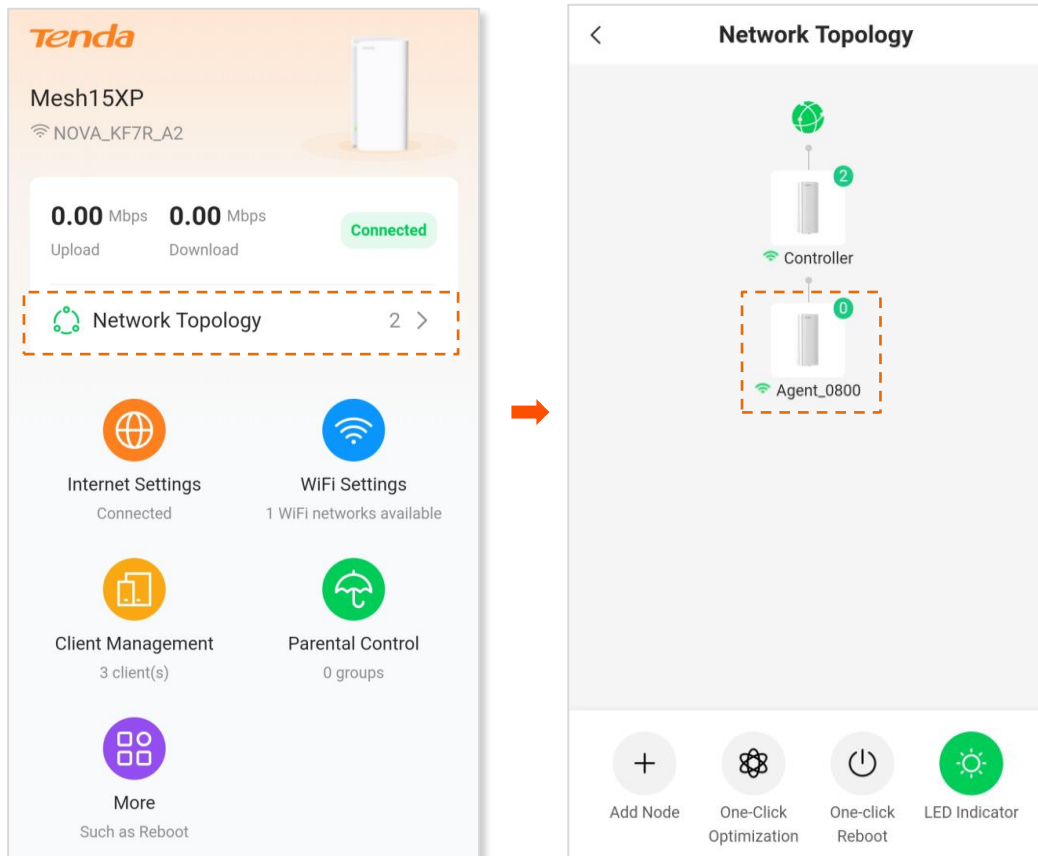


Removing a node will narrow the Wi-Fi coverage, and the removed node will no longer join the current network automatically. To add a removed node again, go to [Add a node](#).

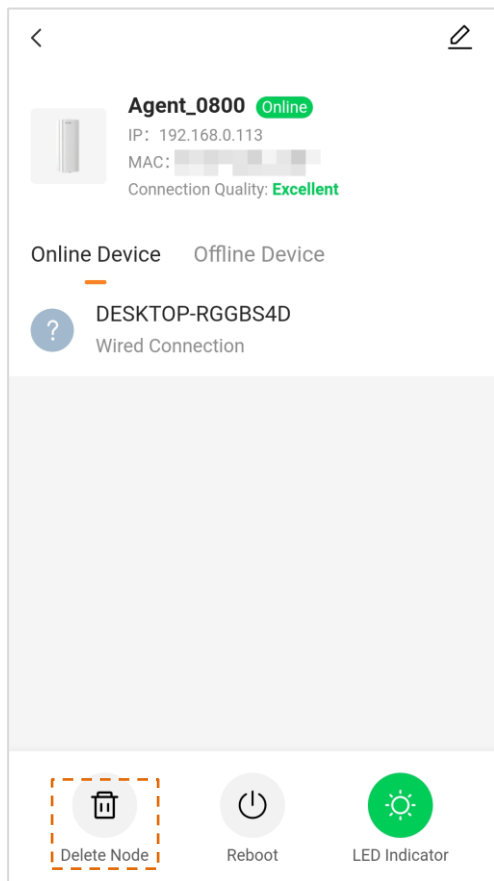
Step 1 [Log in to the web UI \(mobile client\)](#).

Step 2 Tap **Network Topology** and then the target agent.

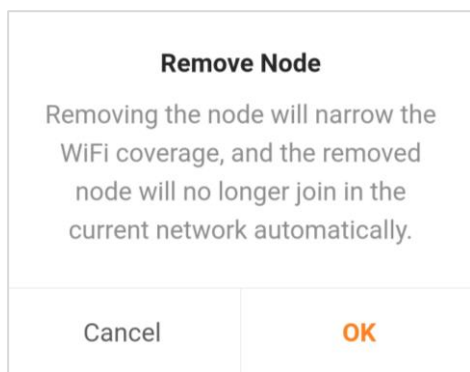
Agent_0800 is used as an example here.



Step 3 Tap **Delete Node**.



Step 4 Tap **OK**.



The secondary node is removed successfully.

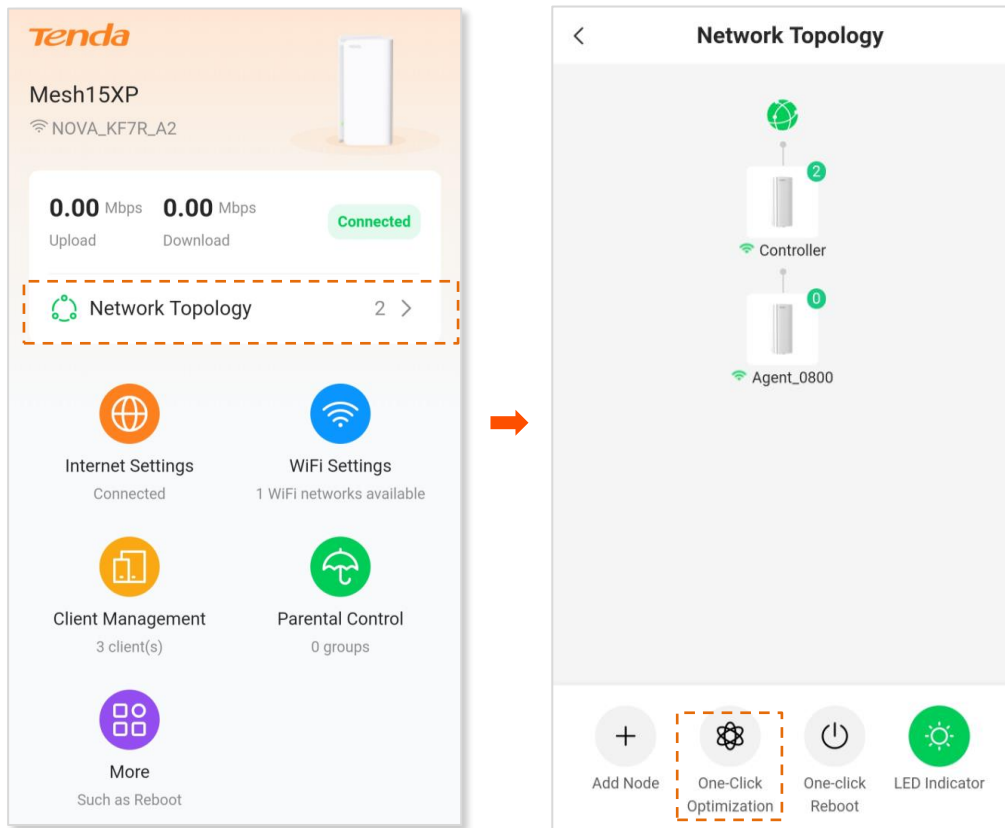
----End

One-click optimization

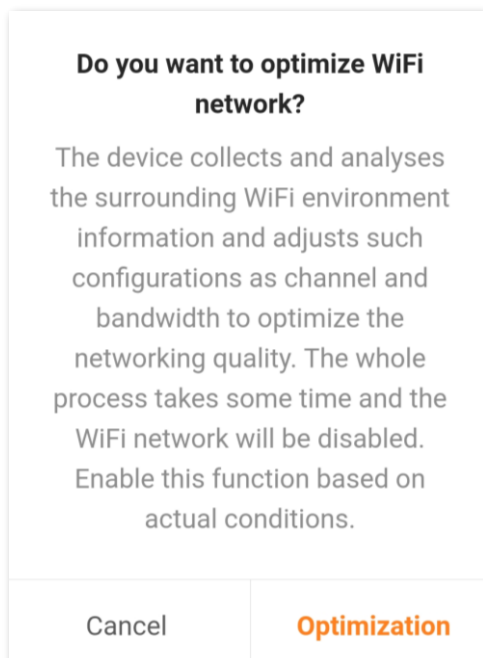
To optimize the Wi-Fi network with one click:

Step 1 [Log in to the web UI \(mobile client\).](#)

Step 2 Tap **Network Topology** and then **One-Click Optimization**.



Step 3 Tap **Optimization**.



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

---End

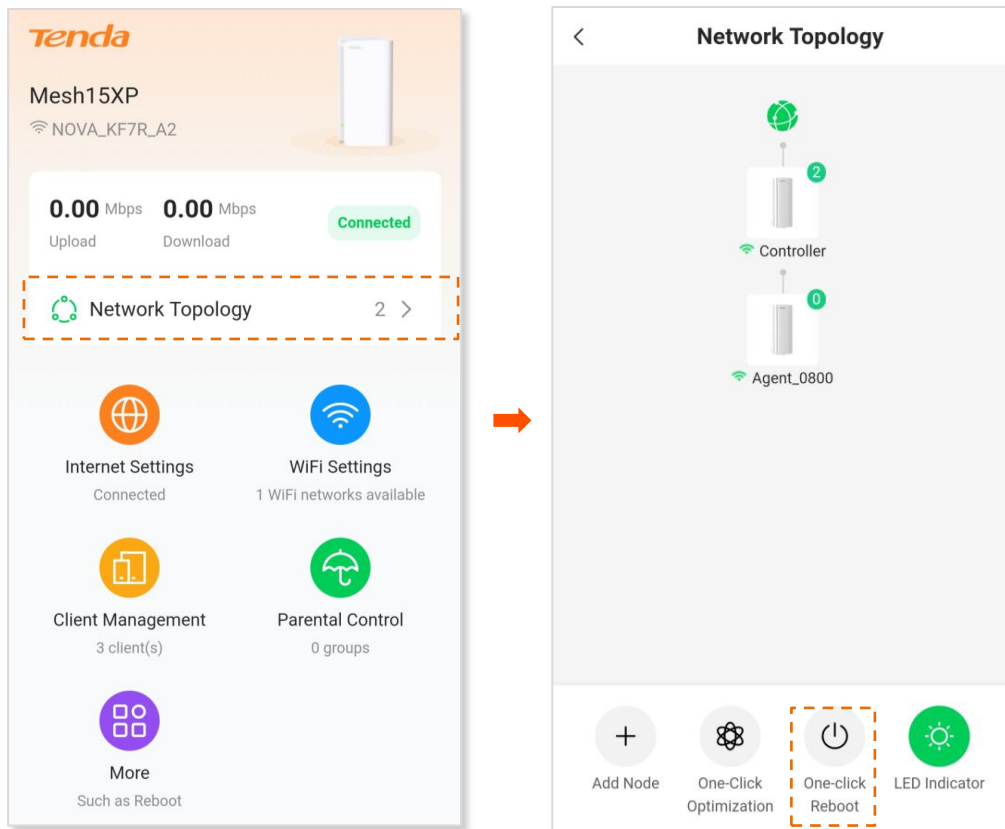
Reboot

Reboot all nodes

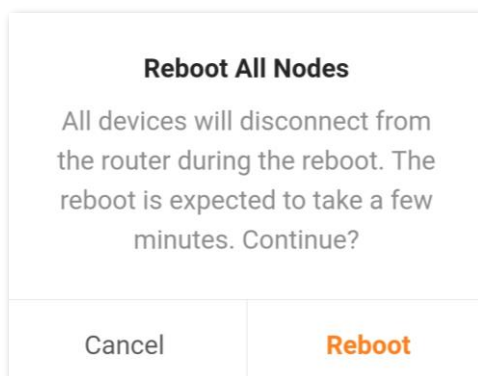
To reboot all nodes by one tap:

Step 1 [Log in to the web UI \(mobile client\)](#).

Step 2 Tap **Network Topology** and then **One-click Reboot**.



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



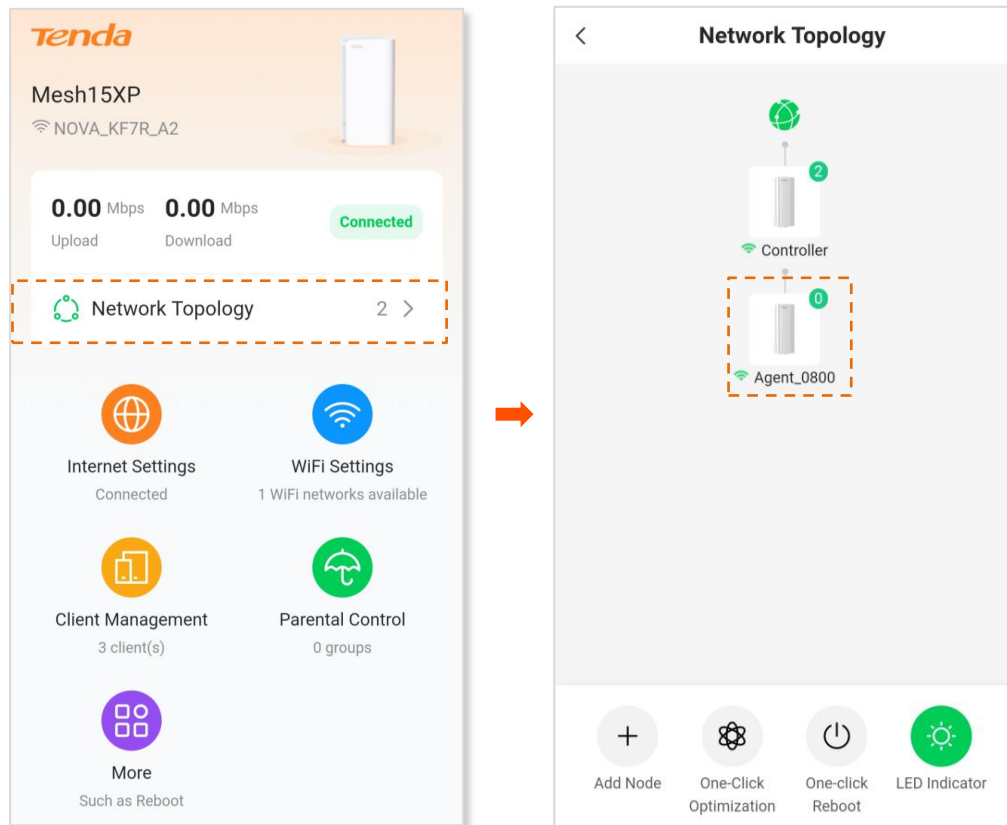
---End

Reboot a single node

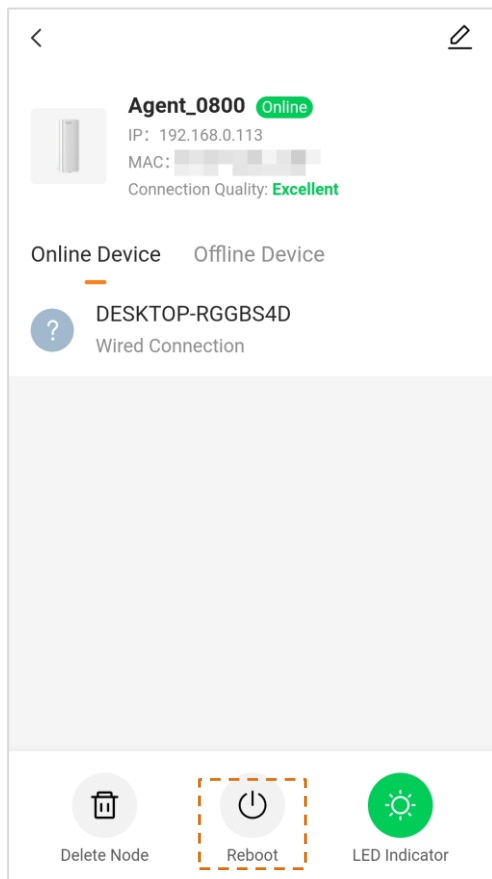
Step 1 [Log in to the web UI \(mobile client\).](#)

Step 2 Tap **Network Topology** and then the target node.

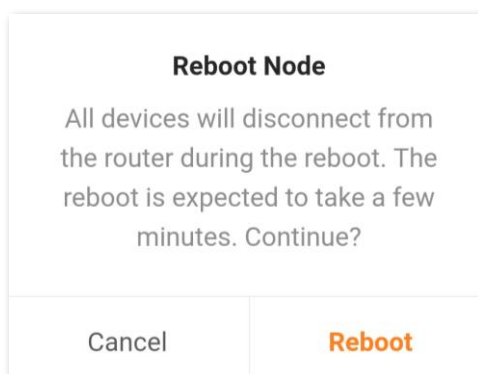
Agent_0800 is used as an example here.



Step 3 Tap **Reboot**.



Step 4 Tap **Reboot**. Wait until all nodes are restarted.



---End

Turn on/off LED indicators

Turn on/off all indicators

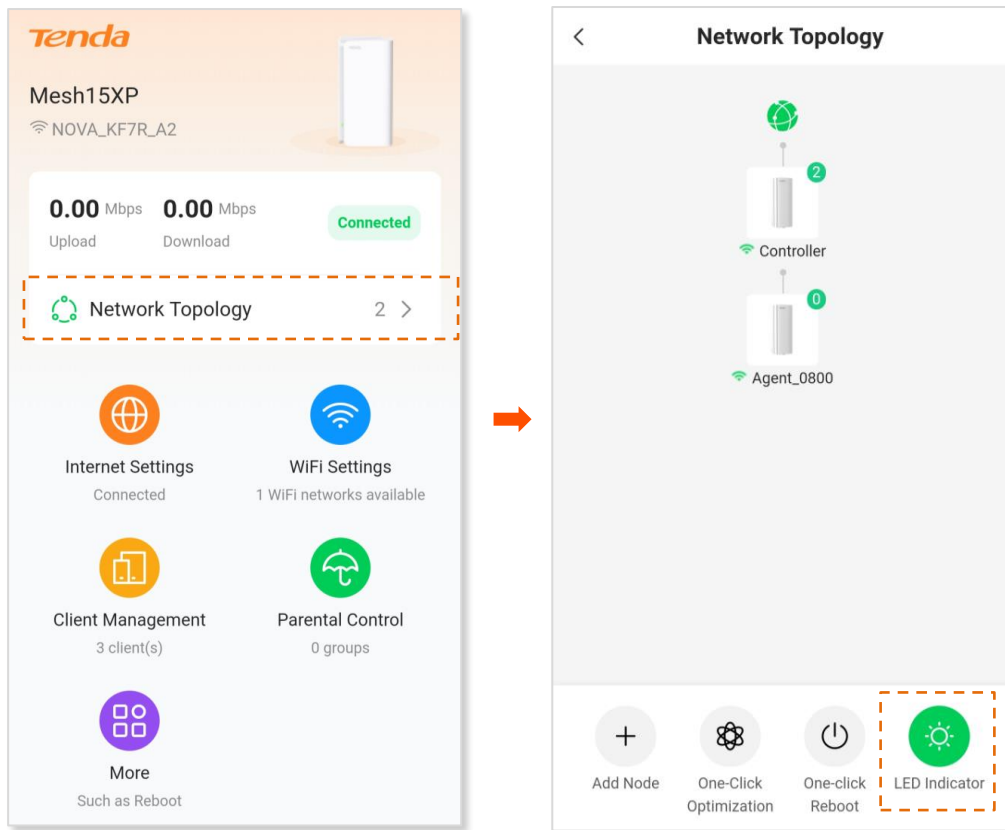


This operation prevails to LED indicator operations for each node and [Smart power saving](#).

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

Step 1 [Log in to the web UI \(mobile client\)](#).

Step 2 Tap **Network Topology** and then **LED Indicator**.



The indicators turn on/off immediately.

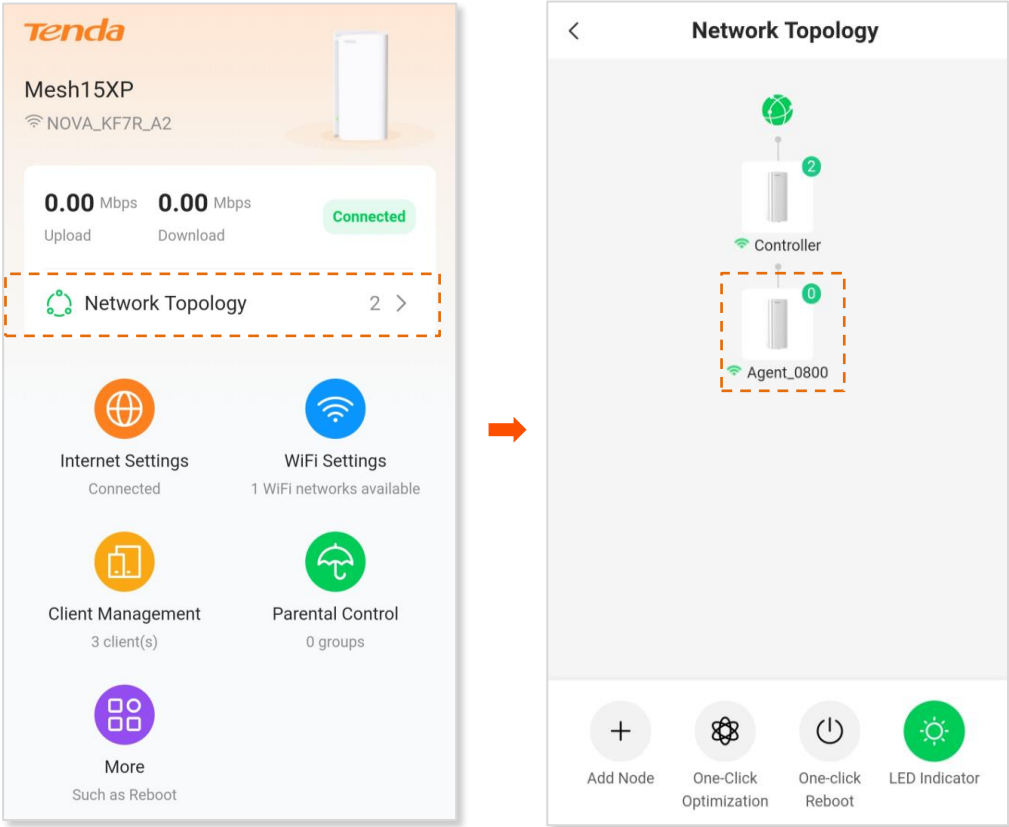
---End

Turn on/off LED indicator of a single node

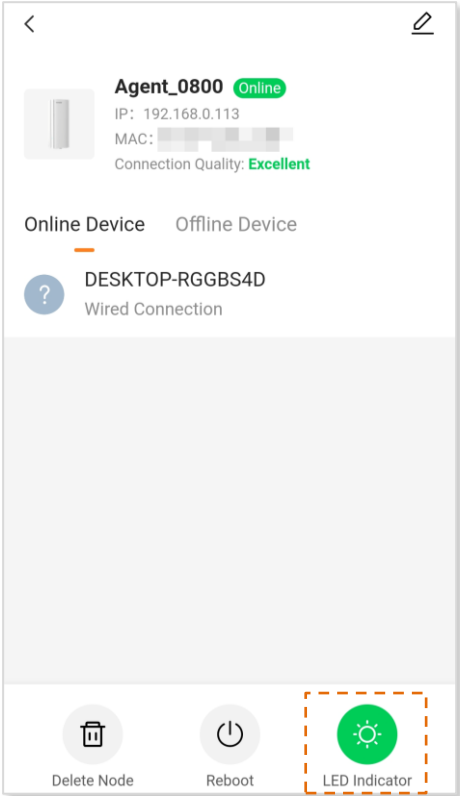
Step 1 [Log in to the web UI \(mobile client\)](#).

Step 2 Tap **Network Topology** and then the target node.

Agent_0800 is used as an example here.



Step 3 Tap LED Indicator.



The indicator turns on/off immediately.

---End

4.5 Internet settings

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

If you are configuring the 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:

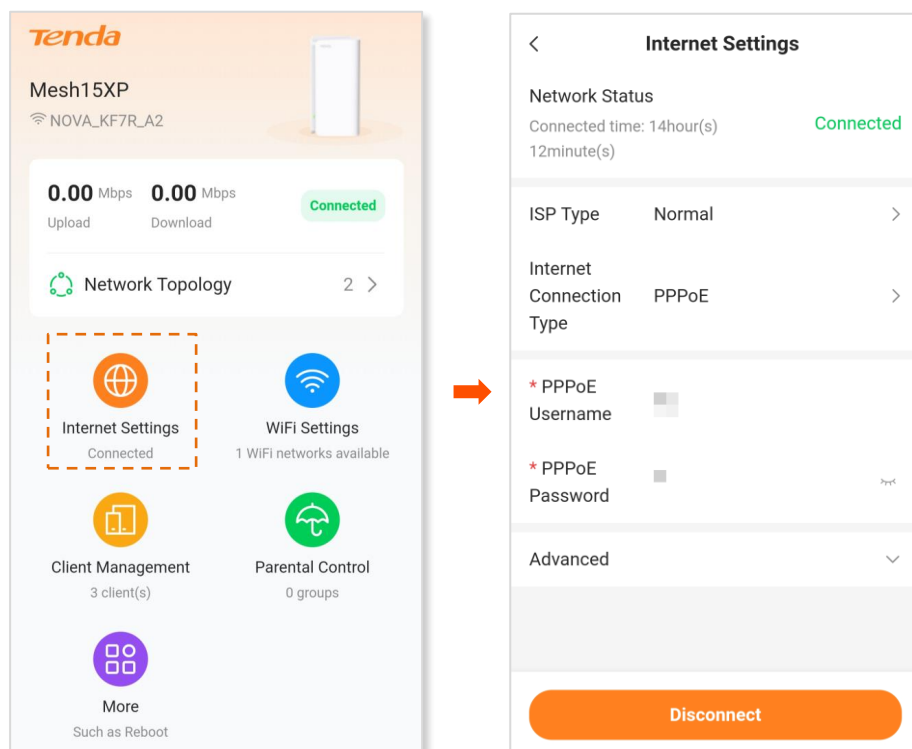
- [Overview](#)
- [Access the internet with a PPPoE account](#)
- [Access the internet through a dynamic IP address](#)
- [Access the internet with a set of static IP address information](#)
- [Set up dual access connection](#)

4.5.1 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 \(mobile client\)](#), and tap **Internet Settings**.



The following table describes the parameters displayed on this page.

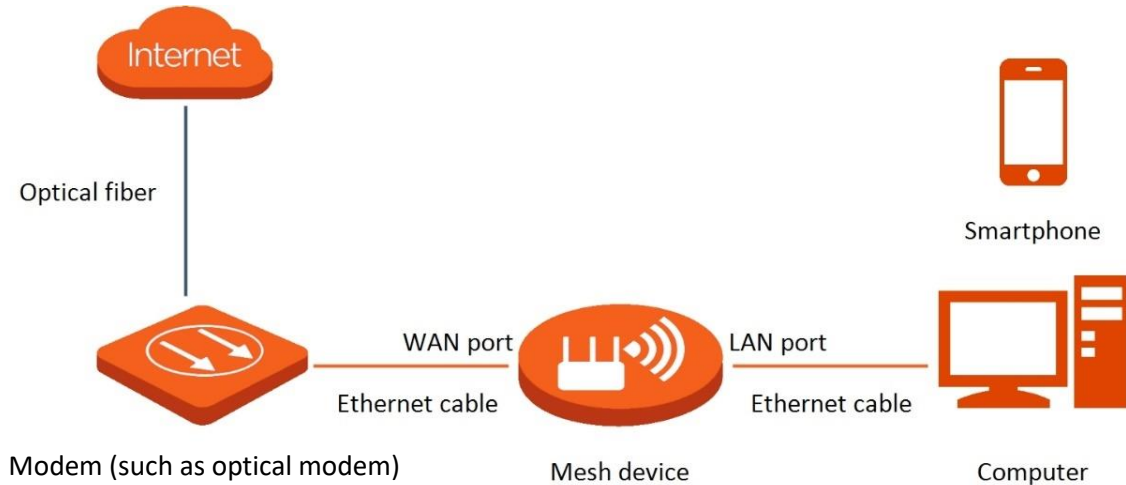
Parameter description

Parameter	Description
Network Status	<p>Indicates the internet connection status.</p> <ul style="list-style-type: none"> - 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/Connected time	Indicates the network connection time of the Mesh device.
ISP Type	
Internet Connection Type	
PPPoE Username	
PPPoE Password	
IP Address	
Subnet Mask	
Default gateway	
Primary DNS	
Secondary DNS	See Parameter description in Connect your primary node to the internet .
Address Type/DHCP	
DNS Settings	
Server IP Address/Domain Name	
User Name	
Password	
Area	
Internet VLAN ID	

Parameter	Description
IPTV VLAN ID	
Server Name	Displayed after you click Advanced if the connection type is PPPoE. They specify the PPPoE server name and PPPoE service name of the broadband service that you purchased.
Service Name	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	<p>Displayed after you click Advanced.</p> <p>It specifies the largest data packet transmitted by a network device. Do not change the value unless:</p> <ul style="list-style-type: none"> - 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. <p> TIP</p> <p>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.</p> <p>The MTU value range is as follows:</p> <ul style="list-style-type: none"> - When the internet connection type is PPPoE, the default value is 1480. Its allowed range is 1280 to 1492. - When the internet connection type is dynamic IP or static IP, the default value is 1500. Its allowed range is 1280 to 1500. - When the internet connection type is PPTP/L2TP, the default value is 1400. Its allowed range is 1280 to 1460.
MAC Address Clone	<p>Used to clone and change the MAC address of the WAN port of primary node.</p> <p>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.</p> <ul style="list-style-type: none"> - 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.

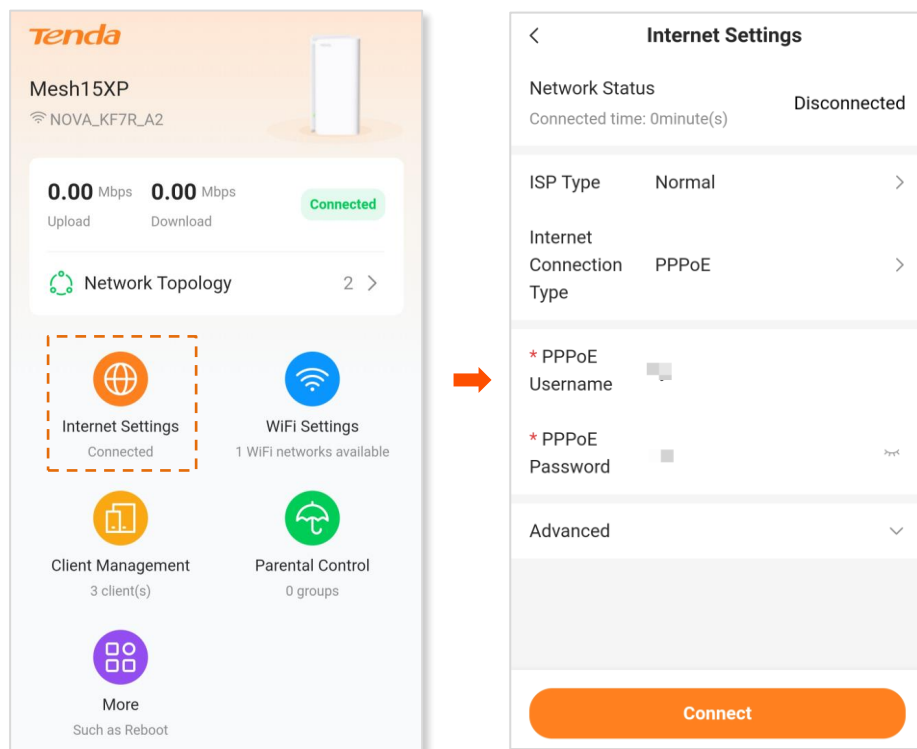
4.5.2 Access the internet with a PPPoE account

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



To access the internet with a PPPoE account:

Step 1 [Log in to the web UI \(mobile client\)](#), and tap **Internet Settings**.



Step 2 Set **ISP Type**.



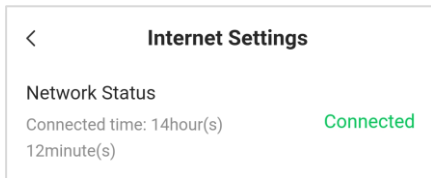
If you select **Manual** for **ISP Type**, enter **Internet VLAN ID** and **IPTV VLAN ID** (if any) provided by your ISP. Blank VLAN ID indicates that the IPTV function is disabled.

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

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

Step 5 Tap **Connect**.

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



---End



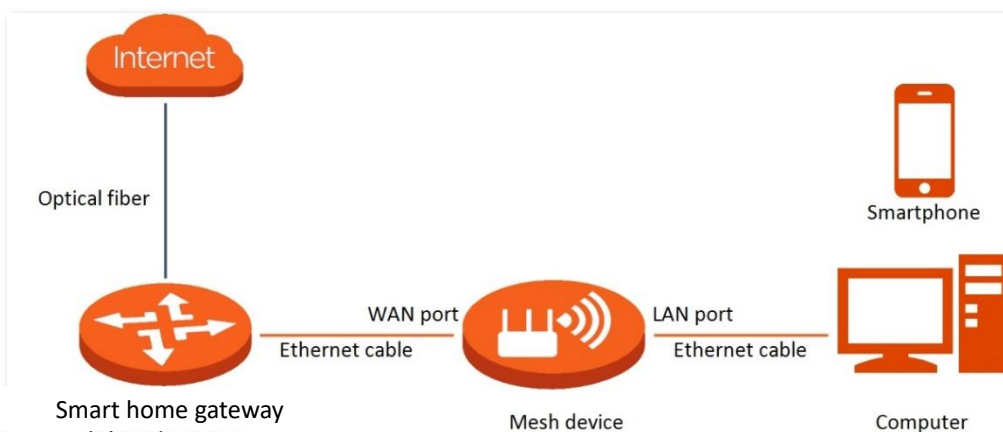
If there is no response from the remote server, troubleshoot as prompted under **Network Status** on the **Internet Settings** page.

4.5.3 Access the internet through a dynamic IP address

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

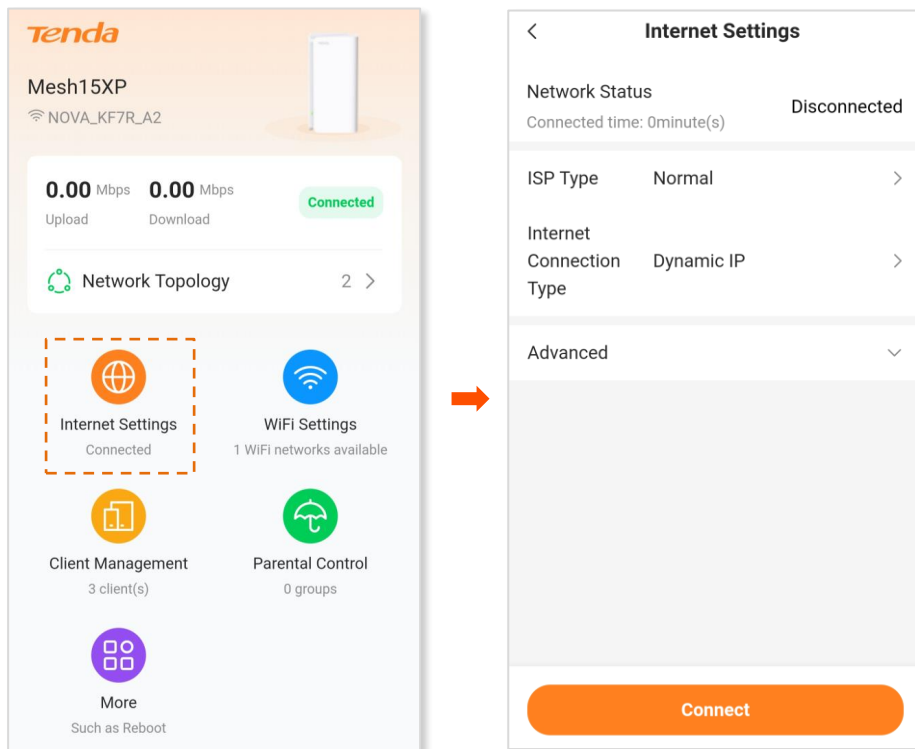
- Your ISP does not provide the PPPoE user name and password, or any other information including IP address, subnet mask, default gateway and DNS server.
- You already have a router with internet access and want to add another router.

The application scenario is shown below.



To access the internet through dynamic IP address:

Step 1 [Log in to the web UI \(mobile client\)](#), and tap **Internet Settings**.



Step 2 Set **ISP Type**.

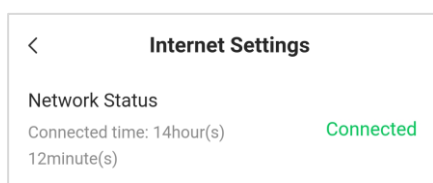


If you select **Manual** for **ISP Type**, enter **Internet VLAN ID** and **IPTV VLAN ID** (if any) provided by your ISP. Blank VLAN ID indicates that the IPTV function is disabled.

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

Step 4 Tap **Connect**.

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



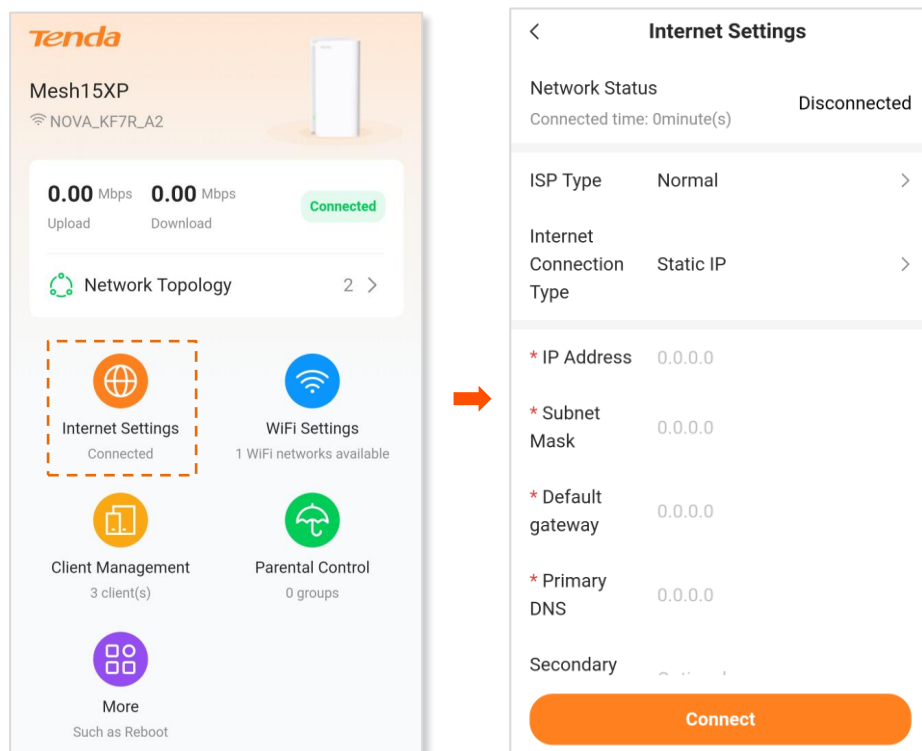
---End

4.5.4 Access the internet with a set of static IP address information

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

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

Step 1 [Log in to the web UI \(mobile client\)](#), and tap **Internet Settings**.



Step 2 Set ISP Type.



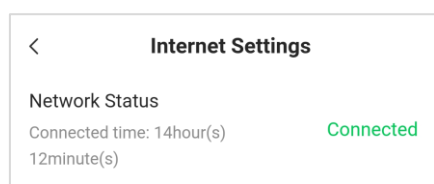
If you select **Manual** for **ISP Type**, enter **Internet VLAN ID** and **IPTV VLAN ID** (if any) provided by your ISP. Blank VLAN ID indicates that the IPTV function is disabled.

Step 3 Set Internet Connection Type to Static IP.

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

Step 5 Tap **Connect**.

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



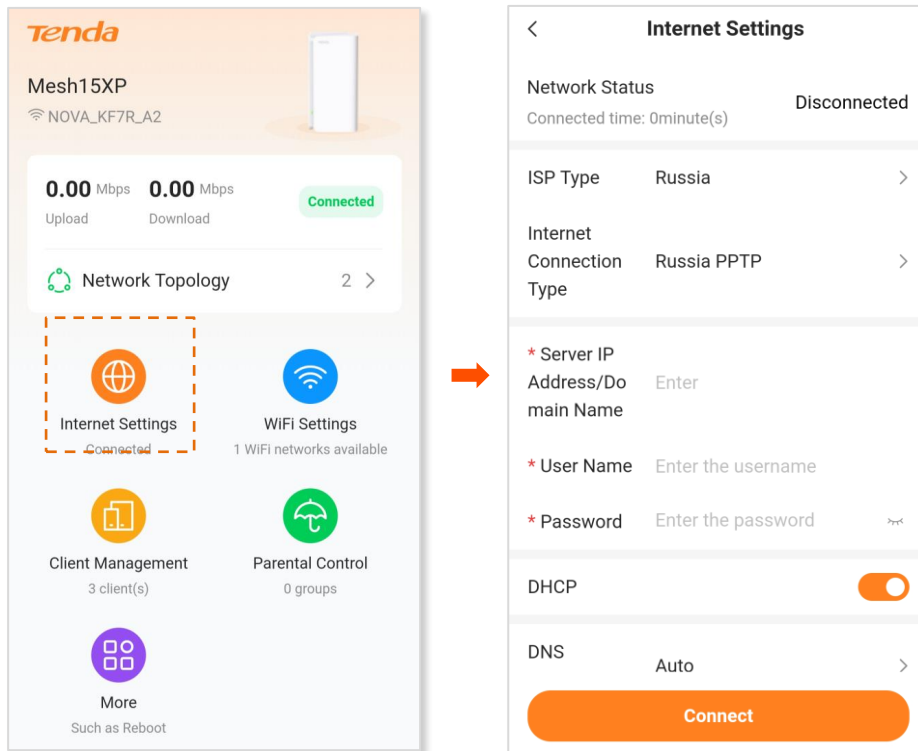
---End

4.5.5 Set up dual access connection

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

To set up dual access connection:

Step 1 [Log in to the web UI \(mobile client\)](#), and tap **Internet Settings**.

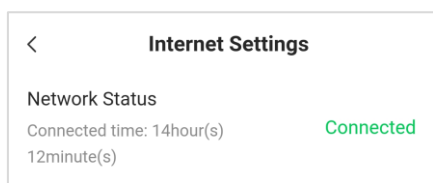


Step 2 Set **ISP Type** to **Russia**.

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

Step 4 Tap **Connect**.

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



---End

4.6 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.

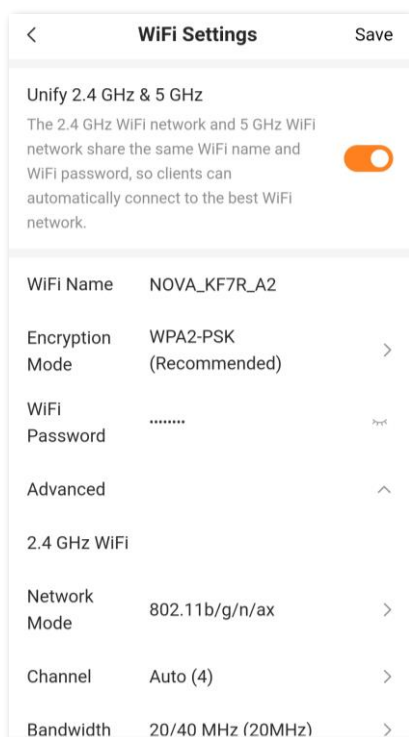
This section includes the following parts:

- [Basic settings](#)
- [Separate the Wi-Fi networks](#)
- [Unify the Wi-Fi networks](#)

4.6.1 Basic settings

To access the Wi-Fi settings page, [log in to the web UI \(mobile client\)](#), and tap **WiFi Settings**.




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





(MX15 Pro for example)

The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
Unify 2.4 GHz & 5 GHz	<p>Used to enable or disable the Unify 2.4 GHz & 5 GHz function.</p> <p>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 Wi-Fi networks and Unify the Wi-Fi networks.</p>
Unify 2.4 GHz & 5 GHz & 6 GHz	<p>Used to enable or disable the Unify 2.4 GHz & 5 GHz & 6 GHz function. It is available only for MX21 Pro/EX21 Pro/Mesh21XEP.</p> <p>When this function is enabled, the 2.4 GHz, 5 GHz and 6 GHz Wi-Fi networks share the same SSID and password. WiFi-enabled clients connected to it will use the frequency with better connection quality. For its operations, see Separate the Wi-Fi networks and Unify the Wi-Fi networks for reference.</p> <p> TIP</p> <p>If any device that supports 2.4 GHz network only needs to connect to the Wi-Fi network, do not enable this function.</p>
WiFi Name	Specifies the Wi-Fi network name (SSID) of the corresponding Wi-Fi network.
Encryption Mode	<p>Specifies the encryption mode supported by the Mesh device, including:</p> <ul style="list-style-type: none"> - 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. This option is only available for some models. Refer to the product you purchased. <p> TIP</p> <p>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).</p>
WiFi Password	<p>Specifies the password for connecting to the Wi-Fi network. You are strongly recommended to set a Wi-Fi password for security.</p> <p> TIP</p> <p>It is recommended to use the combination of numbers, uppercase letters, lowercase letters and special symbols in the password to enhance the security of the Wi-Fi network.</p>

Parameter	Description
Network Mode	<p>Specifies various protocols used for wireless transmission.</p> <p> TIP</p> <p>This parameter is available only for some models and the network modes vary with models. Refer to the product you purchased.</p> <p>2.4 GHz Wi-Fi network supports the 802.11b/g/n Mixed and 802.11b/g/n/ax Mixed modes.</p> <ul style="list-style-type: none"> - 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. <p>5 GHz WiFi network supports the 802.11a/n Mixed, 802.11a/n/ac Mixed and 802.11a/n/ac/ax Mixed modes.</p> <ul style="list-style-type: none"> - 802.11a/n: Indicates that devices compliant with the IEEE 802.11a protocol, and devices working at 5 GHz and compliant with the IEEE 802.11n can connect to the 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	<p>Specifies the channel in which the Wi-Fi network works. It is available only for some models.</p> <p>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.</p>

Parameter	Description
Bandwidth	<p>Specifies the bandwidth of the wireless channel of a Wi-Fi network. Please change the default settings only when necessary.</p> <p> TIP</p> <p>This parameter is available only for some models and the bandwidth varies with models. Refer to the product you purchased.</p> <ul style="list-style-type: none"> - 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.

4.6.2 Separate the Wi-Fi networks

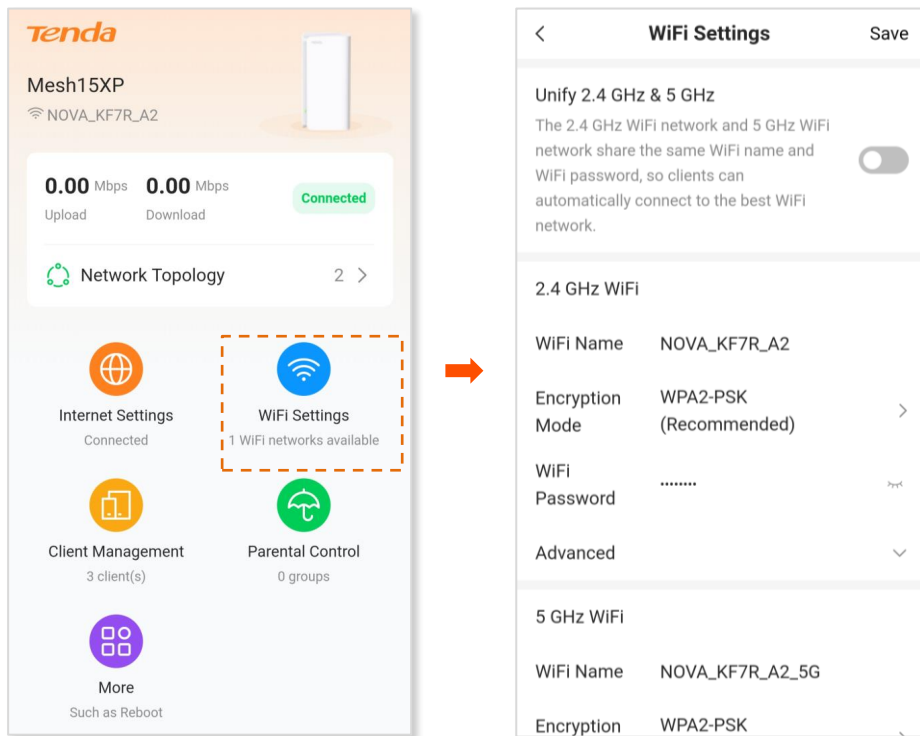
The Mesh device supports 2.4 GHz, 5 GHz and 6 GHz Wi-Fi networks, which are unified and only one Wi-Fi name is displayed by default.



The 6 GHz WiFi network is only supported by MX21 Pro/EX21 Pro/Mesh21XEP.

To separate the Wi-Fi names of the networks:

Step 1 [Log in to the web UI \(mobile client\)](#), and tap **WiFi Settings**.



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



For MX21 Pro/EX21 Pro/Mesh21XEP:

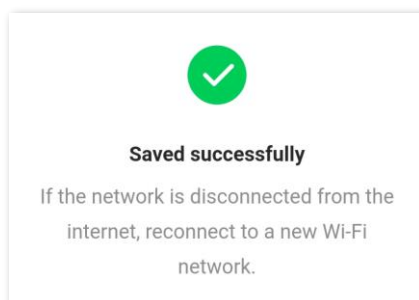
- To separate the Wi-Fi names of the three networks, disable **Unify 2.4 GHz & 5 GHz & 6 GHz**.
- To separate only the 6 GHz Wi-Fi name, enable **Unify 2.4 GHz & 5 GHz** but disable **Unify 2.4 GHz & 5 GHz & 6 GHz**.

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

MX15 Pro is used for example here. In this example, the 2.4 GHz Wi-Fi network is named **NOVA_KF7R_A2**, the 5 GHz Wi-Fi network is named **NOVA_KF7R_A2_5G**, and **WPA2-PSK (Recommended)** is selected for **Security**.

Step 4 Tap **Save** in the upper right corner.

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.

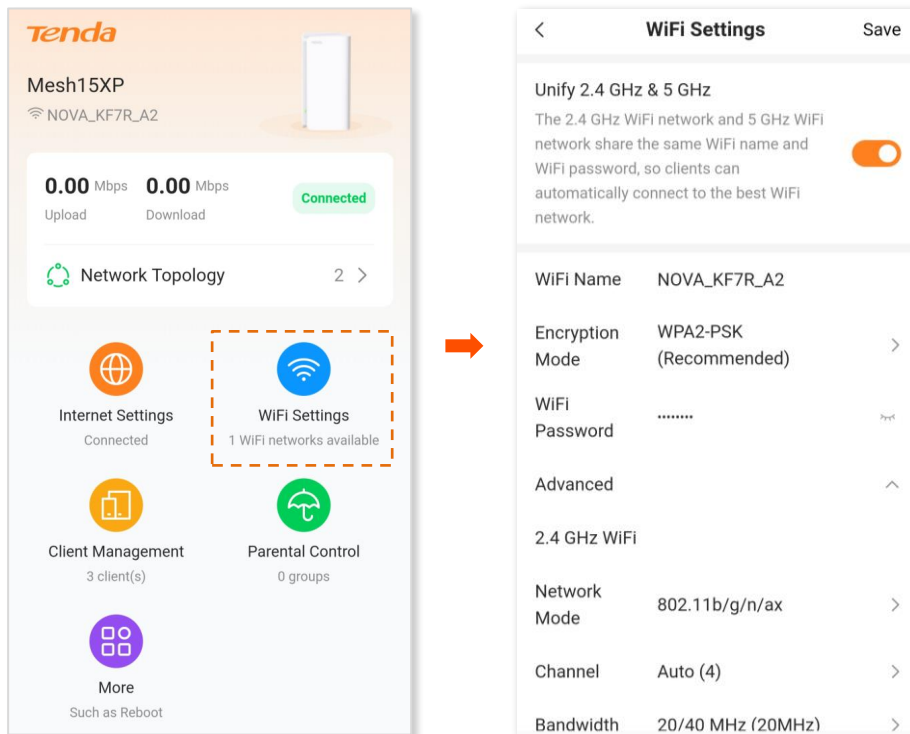
4.6.3 Unify the Wi-Fi networks

The Mesh device supports 2.4 GHz, 5 GHz and 6 GHz Wi-Fi networks. You can unify their Wi-Fi names and passwords as required.



The 6 GHz WiFi network is only supported by MX21 Pro/EX21 Pro/Mesh21XEP.

Step 1 [Log in to the web UI \(mobile client\)](#), and tap **WiFi Settings**.



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



For MX21 Pro/EX21 Pro/Mesh21XEP:

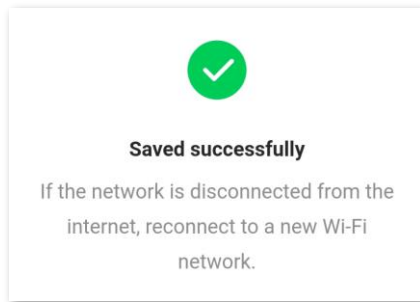
- To unify the Wi-Fi names of the three networks, enable **Unify 2.4 GHz & 5 GHz & 6 GHz**.
- To unify only the 2.4 GHz and 5 GHz Wi-Fi name, enable **Unify 2.4 GHz & 5 GHz** but disable **Unify 2.4 GHz & 5 GHz & 6 GHz**.

Step 3 Set **WiFi Name**, **Encryption Mode**, and **WiFi Password**.

MX15 Pro is used for example here. In this example, the Wi-Fi network is named **NOVA_KF7R_A2** and **WPA2-PSK (Recommended)** is selected for **Encryption Mode**.

Step 4 Tap **Save** in the upper right corner.

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



---End

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

4.7 Client management

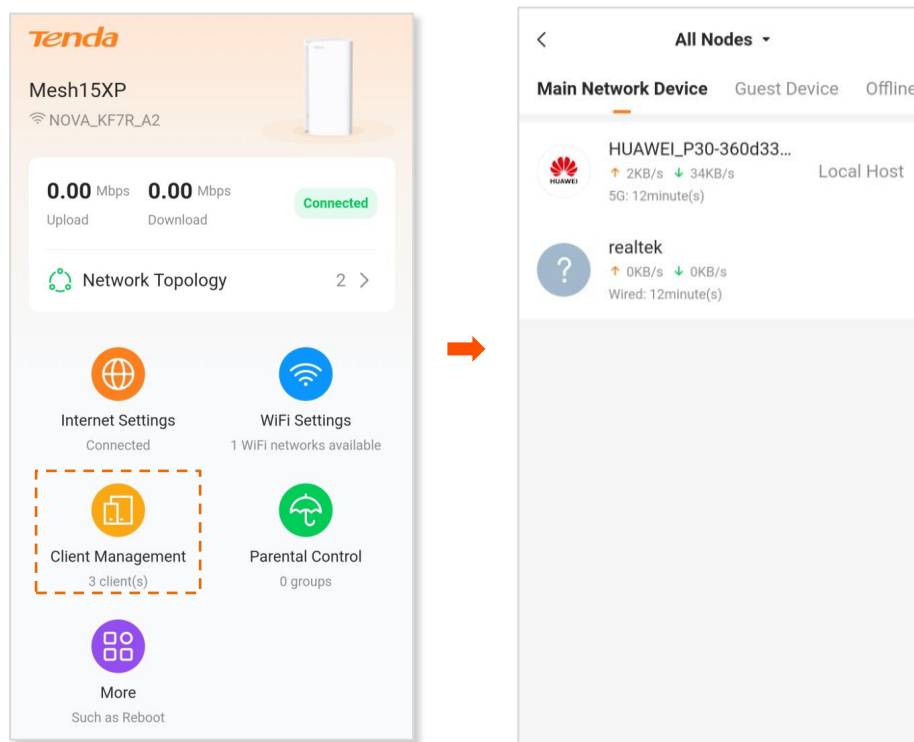
This section describes how to manage your clients, including:

- [View client information](#)
- [Change a client name](#)
- [Set speed limit](#)
- [Add a client to the blacklist](#)
- [Remove a client from the blacklist](#)
- [Delete an offline client](#)

4.7.1 View client information

To view information of clients:

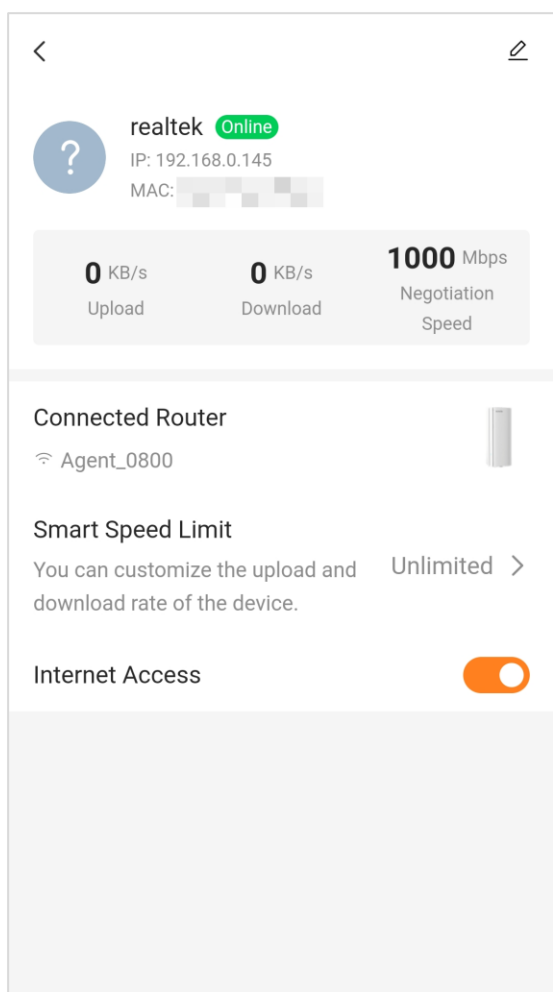
Step 1 [Log in to the web UI \(mobile client\)](#), and tap **Client Management**.





- The information of all online clients connected to the main network is displayed by default. To view clients connected to the guest network, offline clients and blacklisted clients, tap **Guest Device**, **Offline Device** and **Blacklist** respectively.
- To view information of only the clients connected to the controller (primary node), select the controller from the drop-down menu on the top. 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 menu on the top. You can change the agent names in [Agent information](#).


Step 2 Tap a client to view details. The client **realtek** is used as an example here.



---End

The following table describes the information displayed in **Client Management**.

Parameter/Button	Description
	Used to modify the client name.
IP	Indicates the IP address of the client.

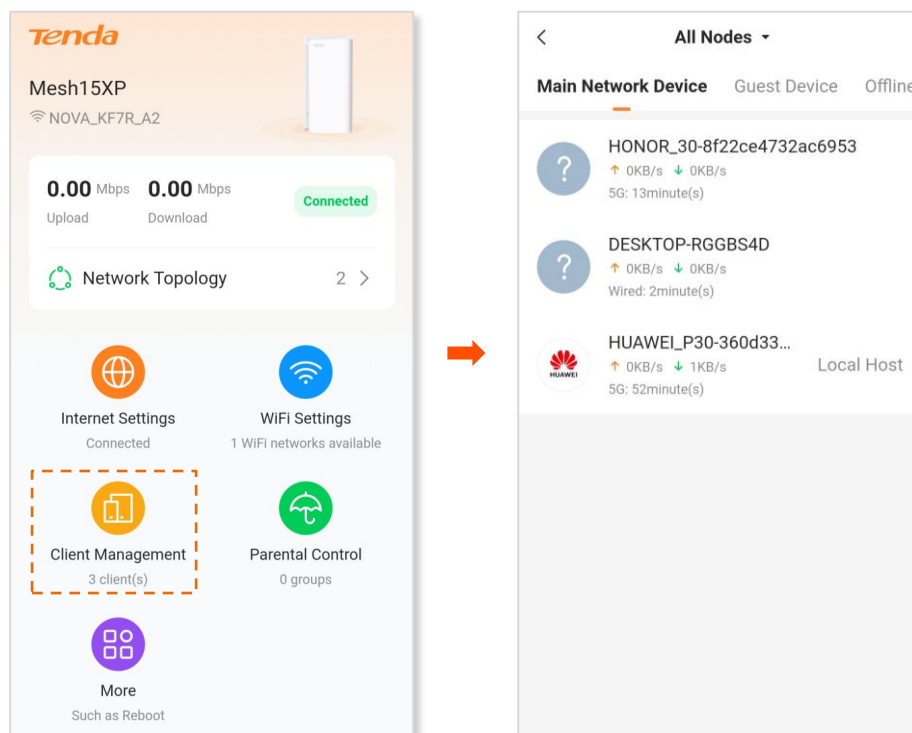
Parameter/Button	Description
MAC	Indicates the MAC address of the client.
Upload/Download	Indicates the real-time upload and download speeds.
Negotiation Speed	Indicates the speed of negotiation.
Connected Router	Indicates the node to which the client connects.
Smart Speed Limit	Used to set the maximum upload and download speeds for the client. For details, see Set speed limit .
Internet Access	Used to blacklist the client or remove the client from the blacklist.  TIP Once blacklisted, the client cannot access the internet through the Mesh system.


4.7.2 Change a client name

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

To change the name of a client:

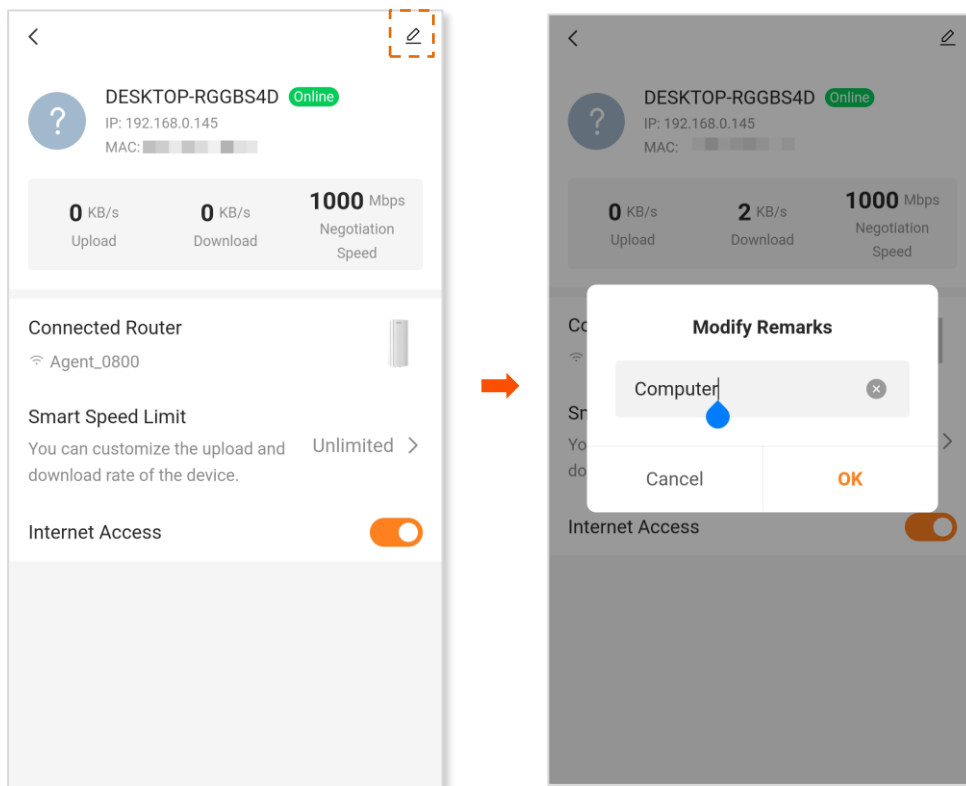
Step 1 [Log in to the web UI \(mobile client\)](#), and tap **Client Management**.



Step 2 Tap the target client and then tap  in the upper right corner.

DESKTOP-RGGBS4D is used as an example here.

Step 3 Enter a new name and tap **OK**.



The new client name is saved.

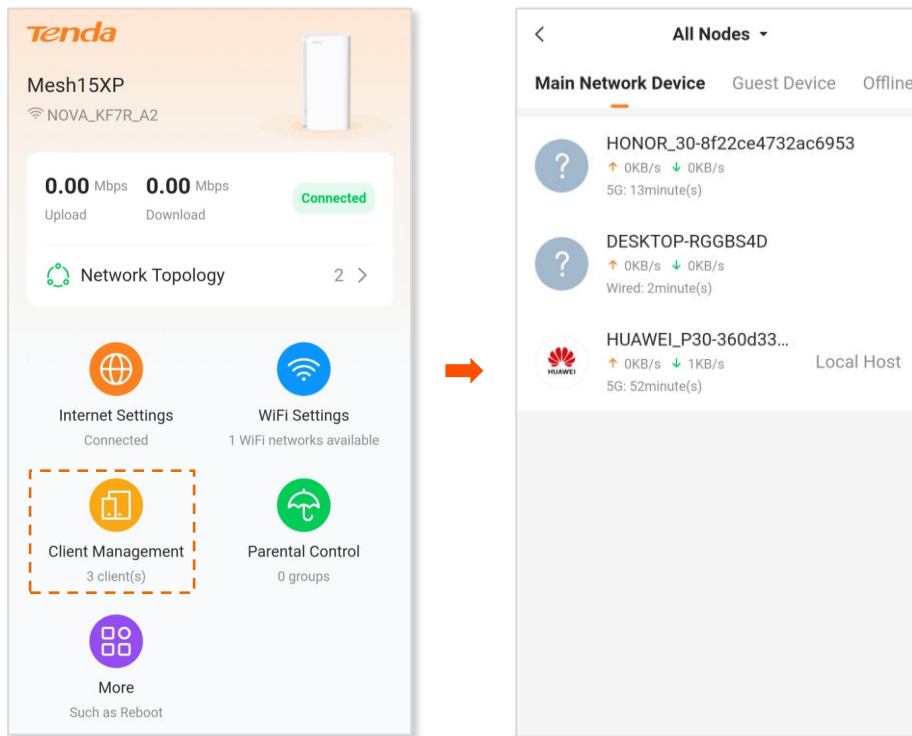
---End

4.7.3 Set speed limit

If multiple clients connect to your Mesh network and you want to limit the upload and download speed for a certain client, you can set speed limit here.

To set speed limit for a client:

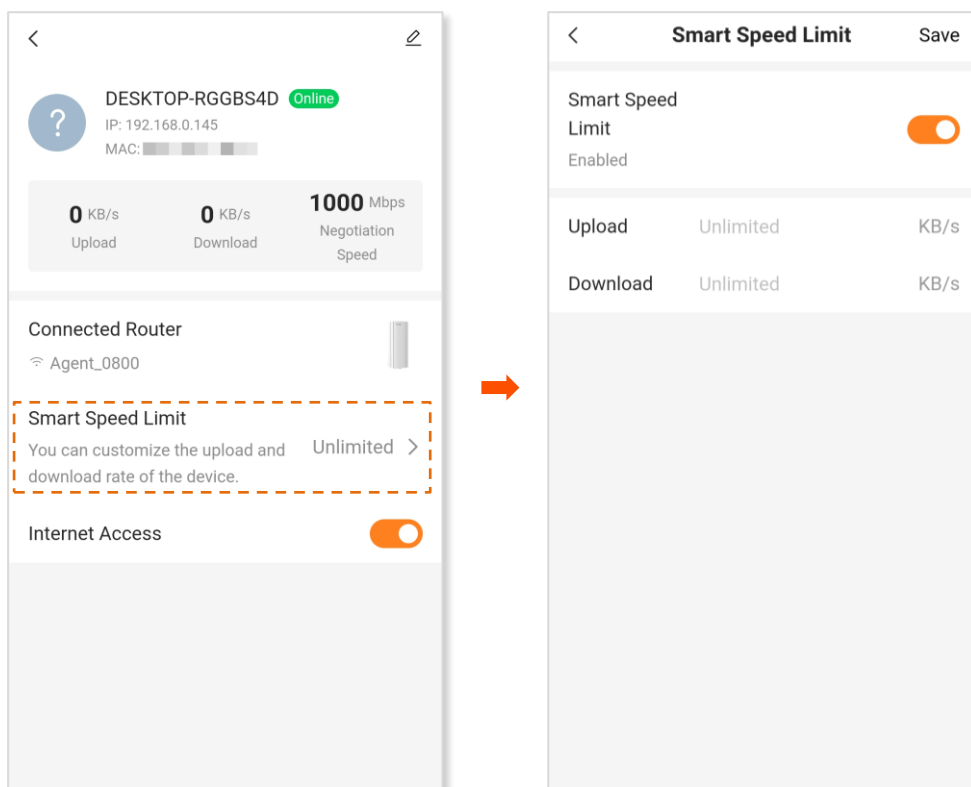
Step 1 [Log in to the web UI \(mobile client\)](#), and tap **Client Management**.



Step 2 Tap the target client and then tap **Smart Speed Limit**.

DESKTOP-RGGBS4D is used as an example here.

Step 3 Enable **Smart Speed Limit**. Set **Upload** and **Download** to the maximum upload and download speeds as required. Then, tap **Save**.



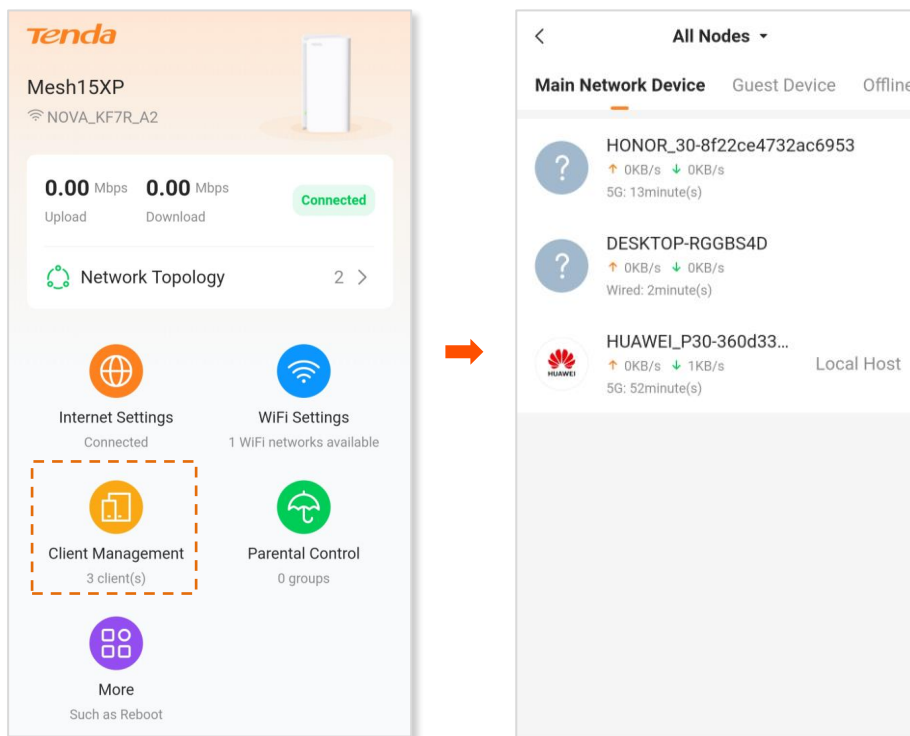
---End

4.7.4 Add a client to the blacklist

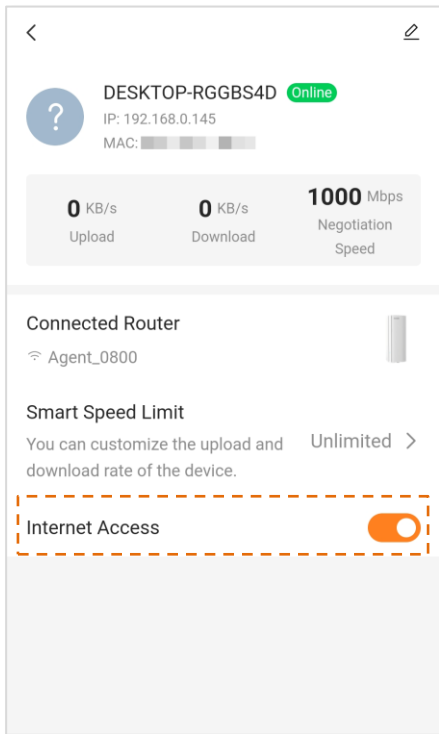
If you find any unknown client connects to your network and you want to block it from accessing your network, you can blacklist it here. All clients connected to the network can be blacklisted, except the local host. Here blacklisting a main network client is used as an example. The operations for blacklisting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

To blacklist a client:

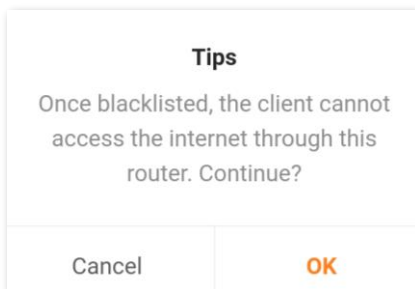
Step 1 [Log in to the web UI \(mobile client\)](#), and tap **Client Management**.



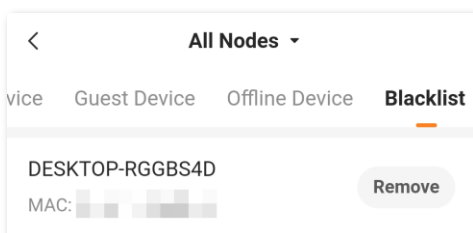
Step 2 Tap the target client and then disable **Internet Access**.
DESKTOP-RGGBS4D is used as an example here.



Step 3 Tap **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.
- The blacklist rule prevails when conflicting with the parent control rule.

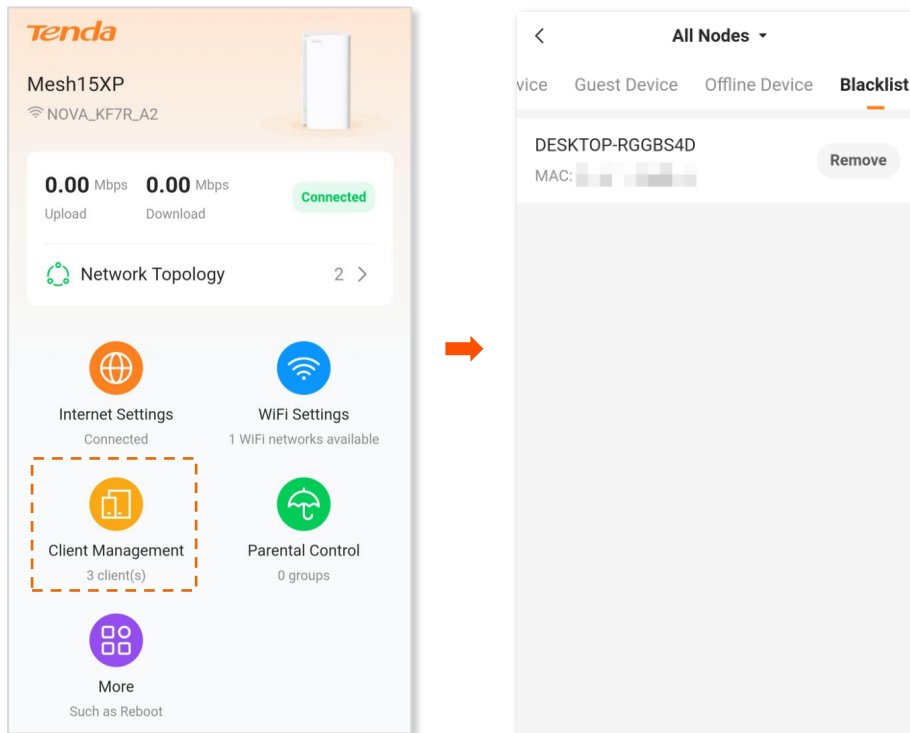
---End

4.7.5 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:

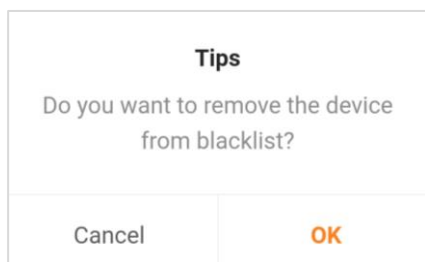
Step 1 [Log in to the web UI \(mobile client\)](#), and tap **Client Management**.



Step 2 Slide the menu bar to the right and tap **Blacklist**.

Step 3 Locate the target client, and tap **Remove** in the line of the client.

Step 4 Click **OK**.



The client is removed from the blacklist and displayed in **Main Network Device**, **Guest Device** or **Offline Device** now. It can access the network upon the next connection.

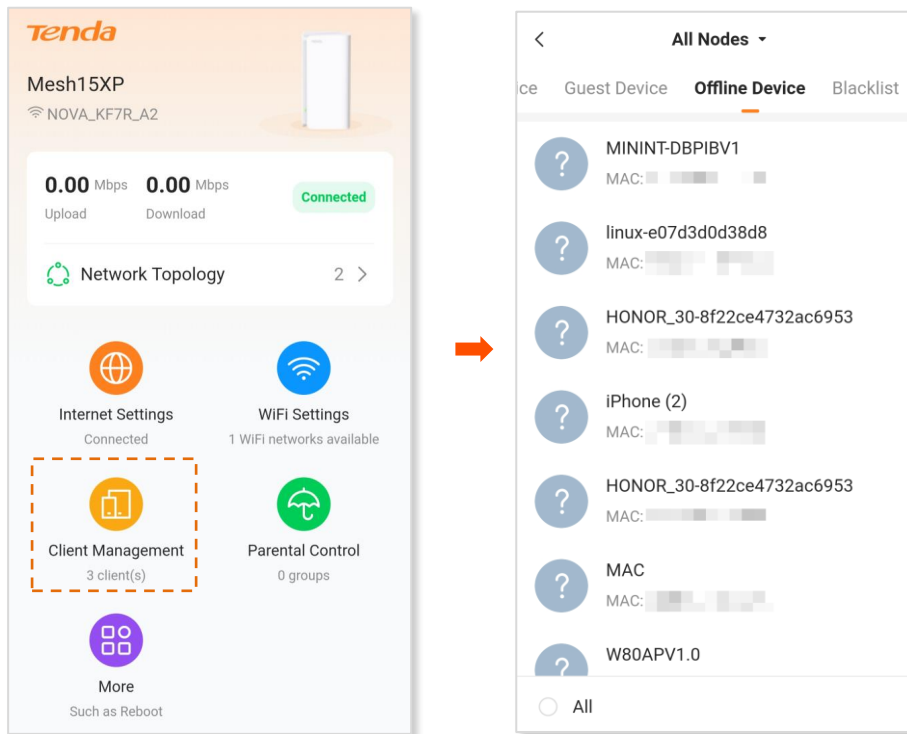
---End

4.7.6 Delete an offline client

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

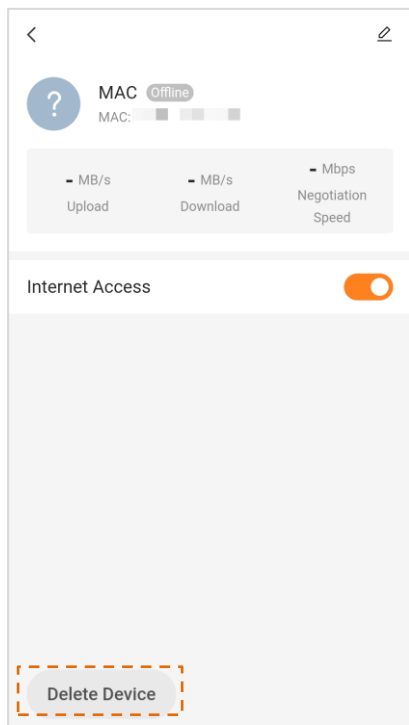
To delete an offline client:

Step 1 [Log in to the web UI \(mobile client\)](#), and tap **Client Management**.



Step 2 Tap the offline client to be deleted, and then tap **Delete Device**.

MAC is used as an example here.



The client you selected is removed from the device list.



- To delete all offline clients, select **All** on the **Offline Device** page and then tap **Delete**.
 - The deleted clients can be displayed in the device list again upon its next network access.
-

---End

4.8 Parental control

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

This section includes the following parts:

- [Create a parental control rule](#)
- [Disable a parental control rule](#)
- [Delete a parental control rule](#)

4.8.1 Create a parental control rule

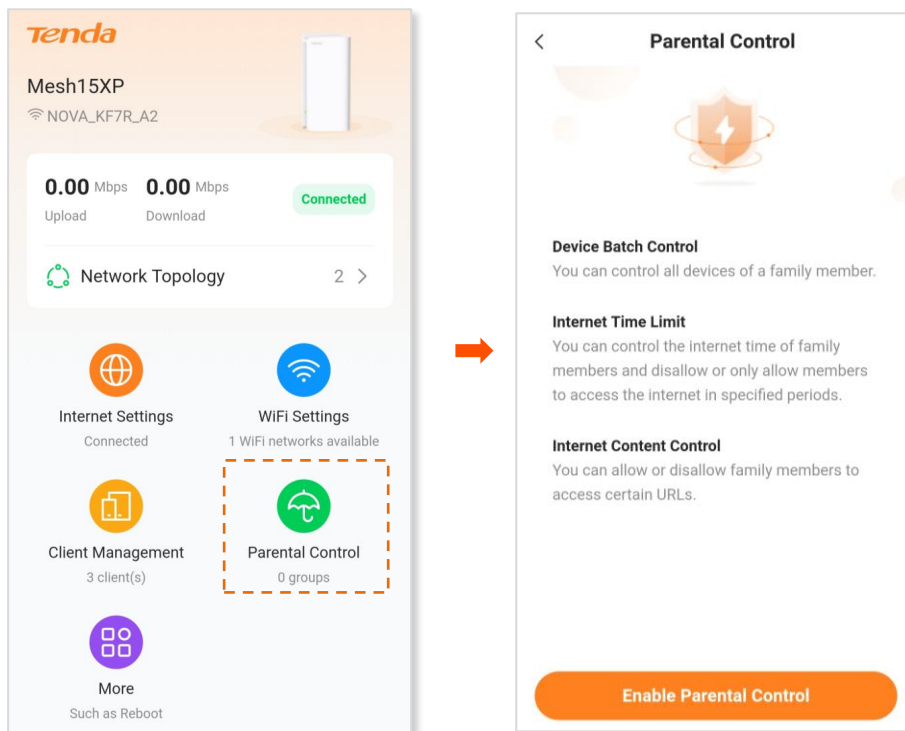
Add a parental control rule



- 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:

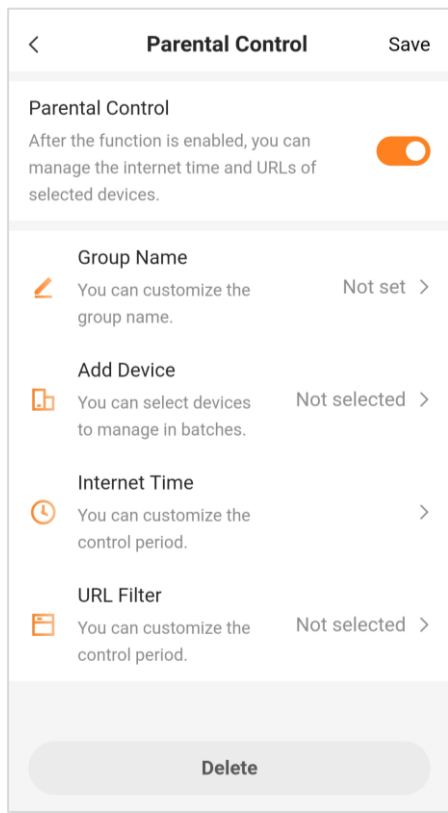
Step 1 [Log in to the web UI \(mobile client\)](#), and tap **Parental Control**.



Step 2 Tap **Enable Parental Control**.

Step 3 Set the parameters as required.**TIP**

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

**Step 4** Tap **Save** in the upper right corner.

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
Parental Control	Used to enable or disable the parental control rule.
Group Name	Specifies the name of the client group that the parental control rule applies to.
Add Device	Specifies the clients that the parental control rule applies to.
Internet Time	Specifies the period during which the parental rule takes effect.

Parameter	Description
URL Filter	<p>Specifies whether the URL filter rule is applied.</p> <ul style="list-style-type: none"> When it is enabled, Filter mode and URL must be set. The parental control rule takes effect on specific websites. When it is disabled, the URL filter rule is not applied.
Filter mode	<p>Required when URL Filter is enabled. Two modes are available here.</p> <ul style="list-style-type: none"> Block access to URLs: The Selected clients are only blocked from accessing the specified websites. Allow access to URLs: The Selected clients can only access the specified websites.

An example of adding parental control rules

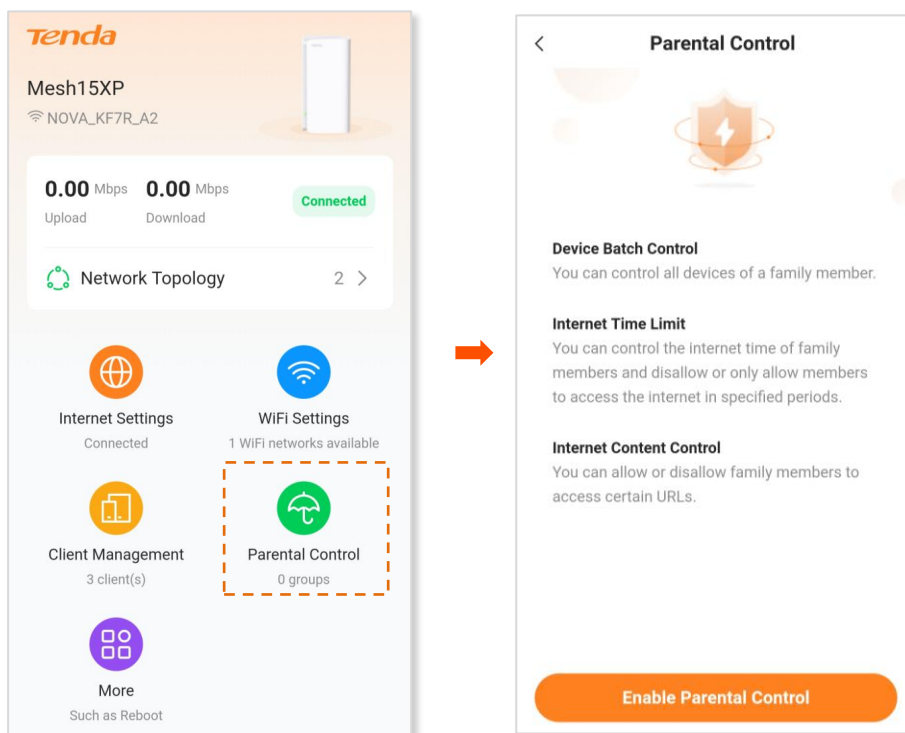
Scenario: The final exam for your kid is approaching and you want to configure your kid's internet access through the Mesh device.

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:

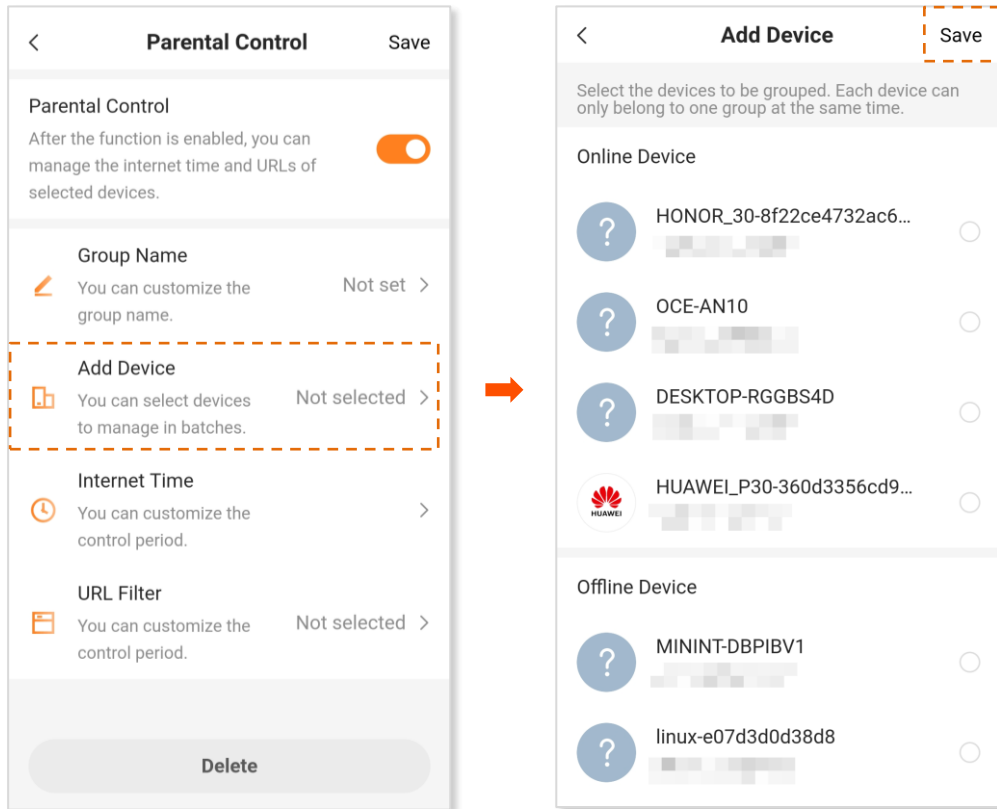
Step 1 [Log in to the web UI \(mobile client\)](#), and tap **Parental Control**.



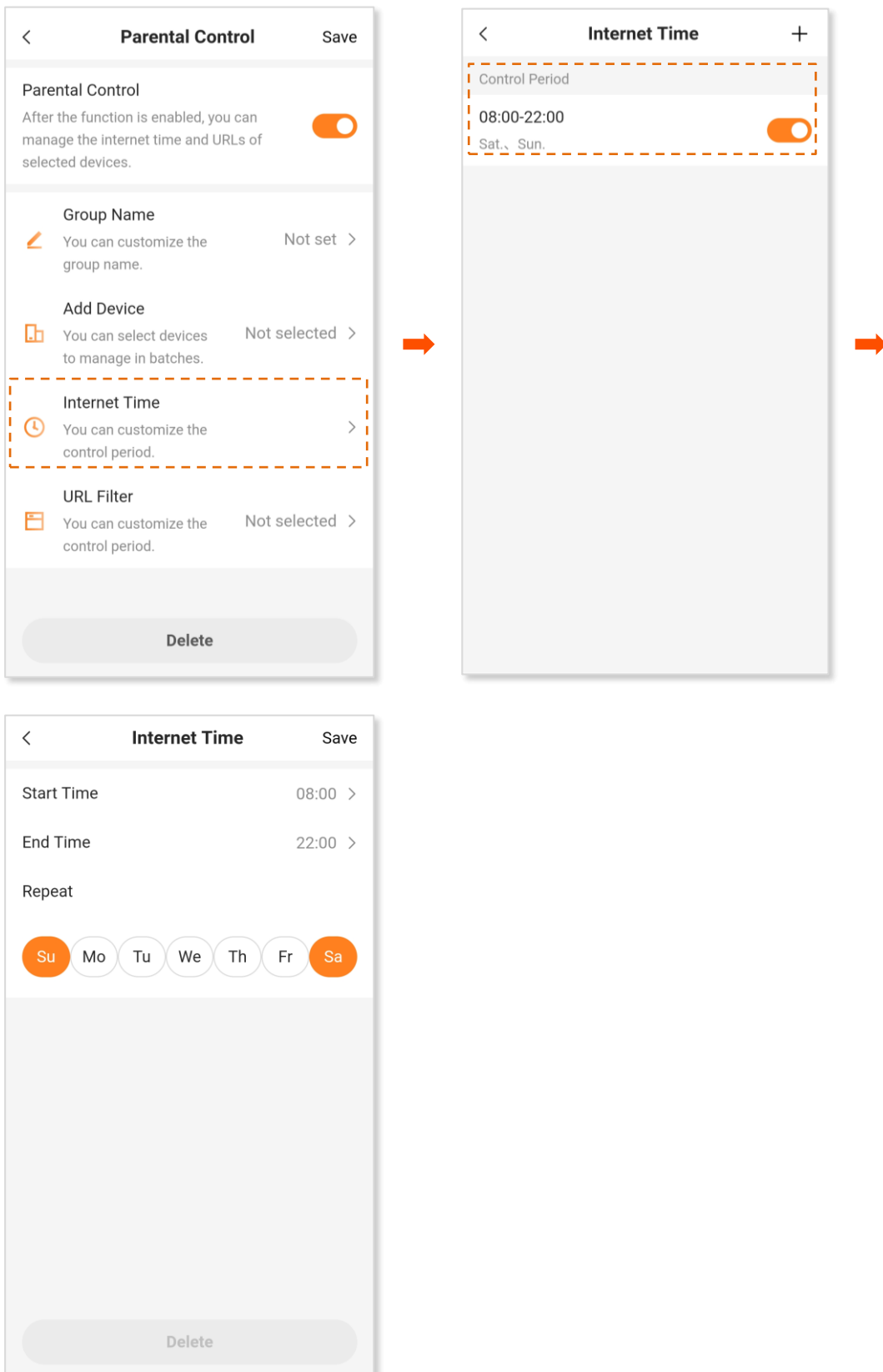
Step 2 Tap **Enable Parental Control**, and enable **Parental Control**.

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

Step 4 Tap **Add Device**. Then, select the target client, and tap **Save** in the upper right corner.

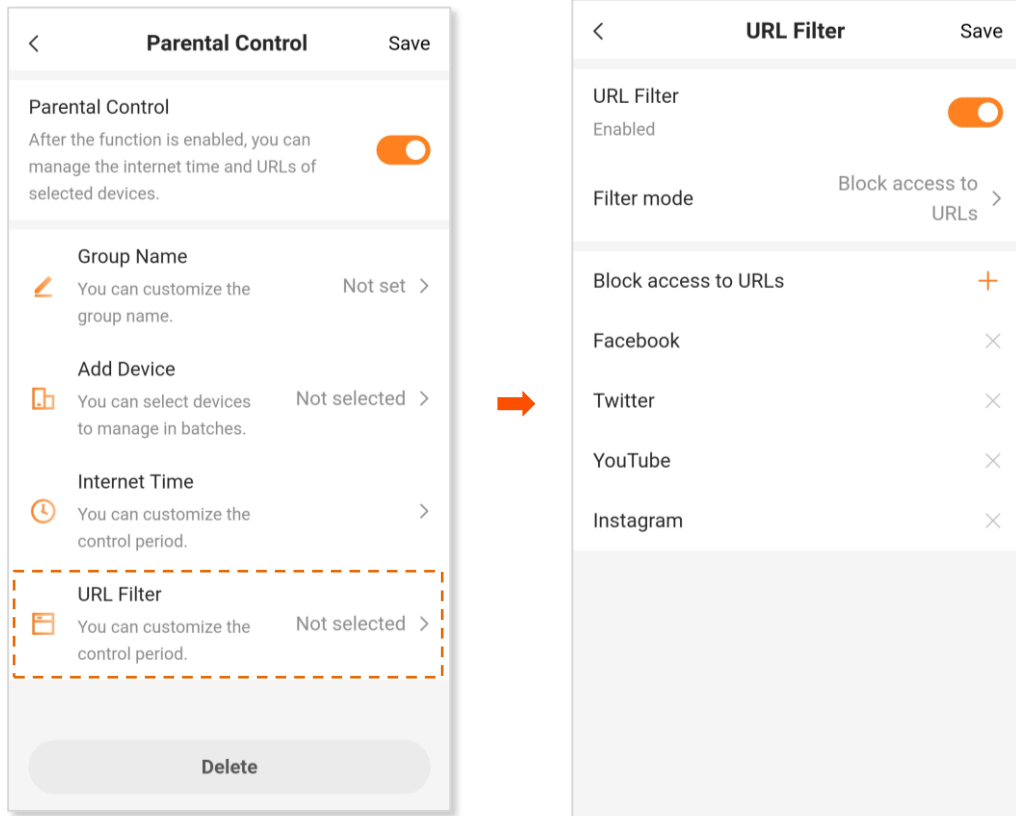


Step 5 Tap **Internet Time**. Then, specify the period during which the target websites are blocked, which is 08:00 to 22:00 on weekends in this example, and enable the control period.



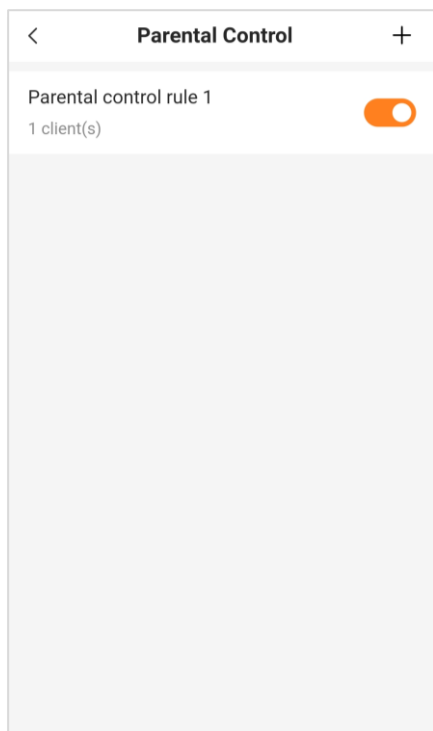
Step 6 Tap **URL Filter**. Then, enable **URL Filter** and select **Block access to URLs** for **Filter mode**.

Step 7 Tap **+** to add the websites to be blocked one by one, which are **Facebook**, **Twitter**, **YouTube**, and **Instagram** in this example.



Step 8 Tap **Save** in the upper right corner.

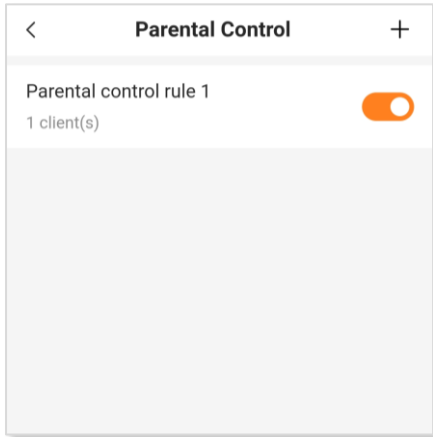
The following page is displayed, and your kid can access any websites except for Facebook, Twitter, YouTube and Instagram from 8:00 to 22:00 on weekends and cannot access the internet at all between 22:00 to 8:00 on weekends.



---End

4.8.2 Disable a parental control rule

By default, a parental control rule is enabled after you added it successfully, as shown in the following figure. You can disable it as required.



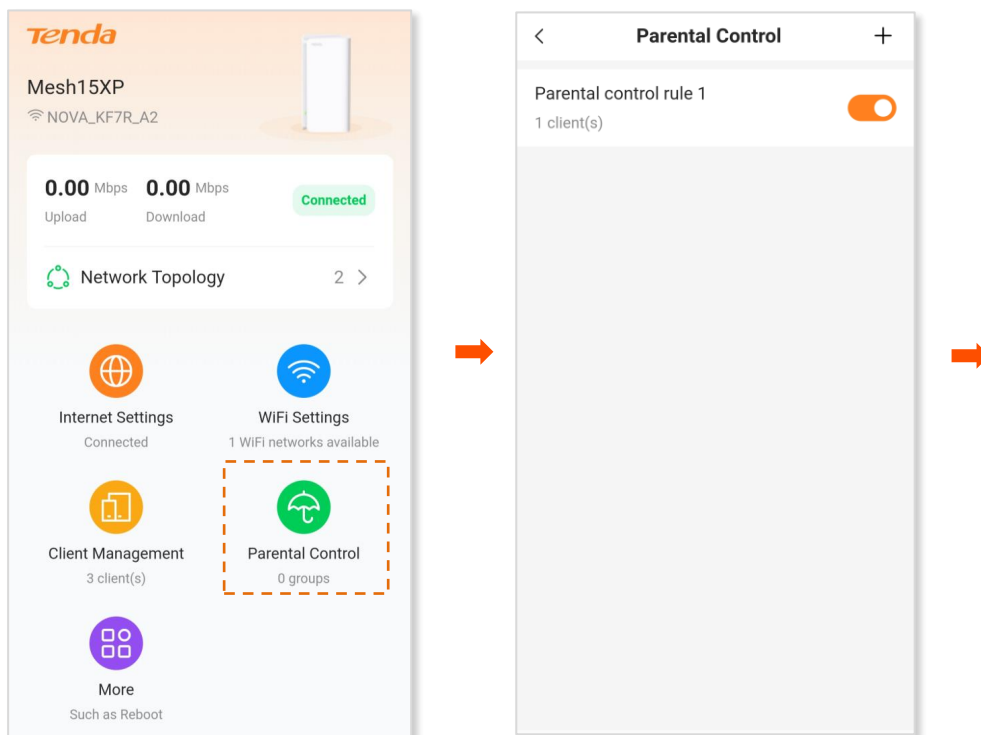
To disable a parental control rule, [log in to the web UI \(mobile client\)](#), tap **Parental Control**, and tap  to disable the corresponding rule.

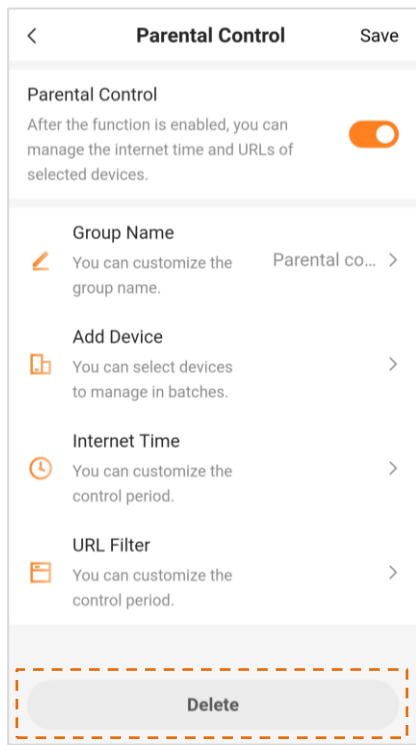
4.8.3 Delete a parental control rule

If you want to delete an unwanted parental control rule, perform the following steps:

Step 1 [Log in to the web UI \(mobile client\)](#), and tap **Parental Control**.

Step 2 Tap the target rule, and then tap **Delete**.





---End

4.9 More

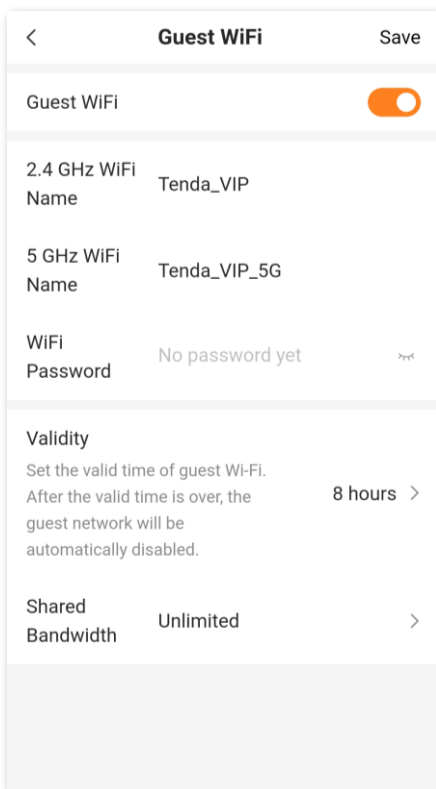
4.9.1 Guest Wi-Fi

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 \(mobile client\)](#) of the Mesh device and navigate to **More > Guest WiFi**. 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.

Parameter	Description
2.4 GHz WiFi Name	Specify the Wi-Fi name of the Mesh system's guest network.
5 GHz WiFi Name	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.
6 GHz WiFi Name	 TIP 6 GHz WiFi Name is only available for MX21 Pro/EX21 Pro/Mesh21XEP.
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:

- MX15 Pro used
- 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**
- Shared bandwidth for guests: **8 Mbps**

To achieve such a goal:

Step 1 [Log in to the web UI \(mobile client\)](#), and navigate to **More > Guest WiFi**.

Step 2 Enable **Guest WiFi**.

Step 3 Set **2.4 GHz WiFi Name**, which is **John_Doe** in this example.

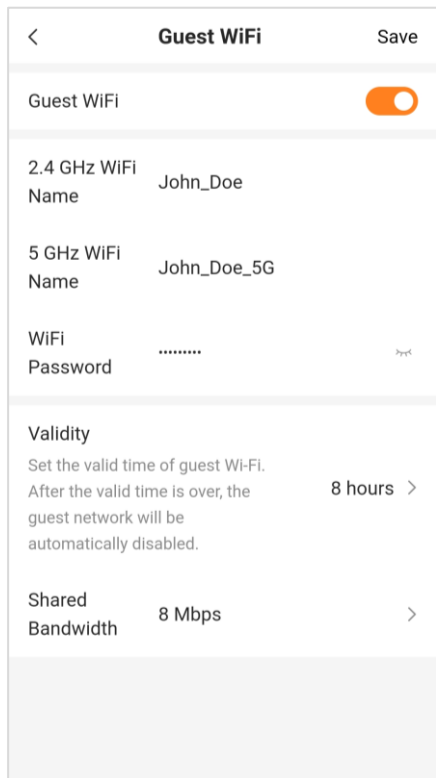
Step 4 Set **5 GHz WiFi Name**, which is **John_Doe_5G** in this example.

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

Step 6 Set **Validity**, which is **8 hours** in this example.

Step 7 Set **Shared Bandwidth**, which is **8 Mbps** in this example.

Step 8 Tap **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

4.9.2 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.



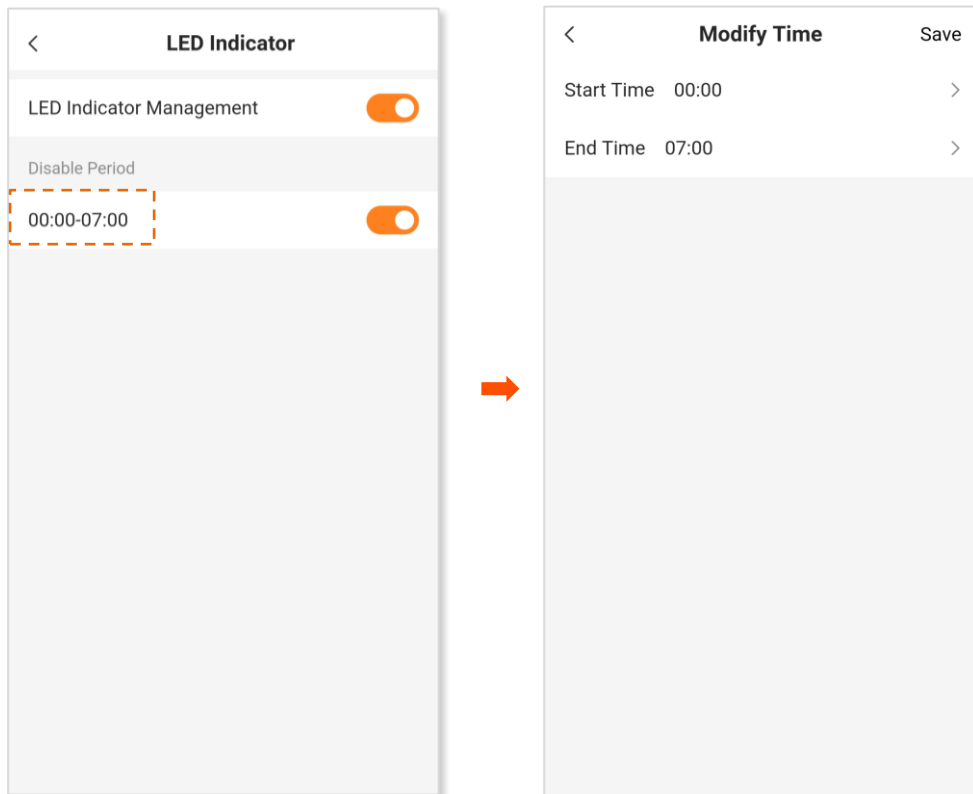
TIP
[Turn on/off all indicators](#) prevails to this operation.

To configure the power saving mode:

Step 1 [Log in to the web UI \(mobile client\)](#), and navigate to **More > LED Indicator**.

Step 2 Enable **LED Indicator Management**.

Step 3 Enable **Disable Period**. Then, tap the disable period to modify **Start Time** and **End Time**, and tap **Save** in the upper right corner.



“Saved successfully” is displayed, indicating that the settings are saved successfully.

---End

4.9.3 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 \(mobile client\)](#) and navigate to **More > 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](#).

4.9.4 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
<ul style="list-style-type: none"> The ISP does not provide any PPPoEv6 user name and password and information about the IPv6 address. You have a router that can access the IPv6 network. 	DHCPv6
IPv6 service is included in the PPPoE user name and password.	PPPoEv6
The ISP provides you with a set of information including IPv6 address, subnet mask, default gateway and DNS server.	Static IPv6 address

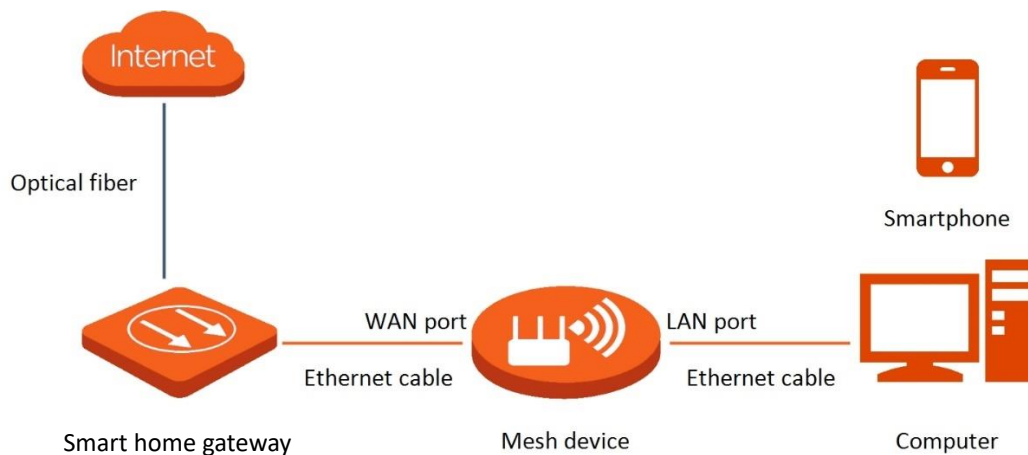
**TIP**

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

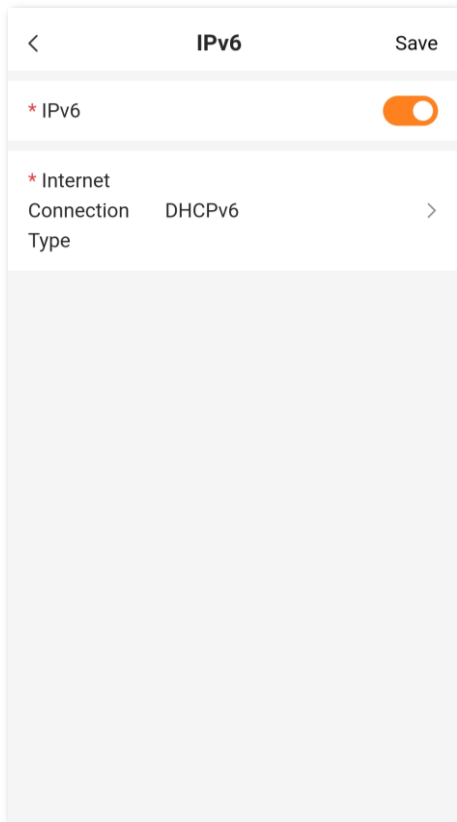
DHCPv6 enables the Mesh device to obtain an IPv6 address from the DHCPv6 server to access the internet. It is applicable in the following scenarios:

- 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 \(mobile client\)](#), and navigate to **More > IPv6**.
- Step 2** Enable the **IPv6** function.
- Step 3** Set **Internet Connection Type** to **DHCPv6**.
- Step 4** Tap **Save**.

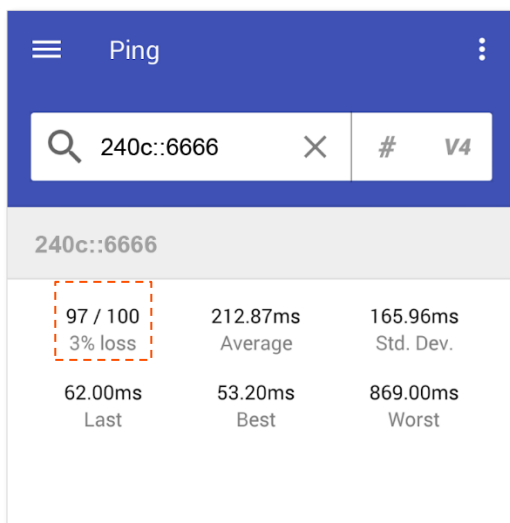


“Saved successfully” is displayed, indicating that the settings are saved successfully.

---End

Verification:

You can download a network diagnosis App (**HE.NET Network Tools** for example here) on your wireless client and ping an IPv6 website (**240c::6666** for example) to check whether the Mesh device accesses the IPv6 network successfully. As shown in the following figure, if the number of packets received is not 0, the Mesh device accesses the IPv6 network successfully.

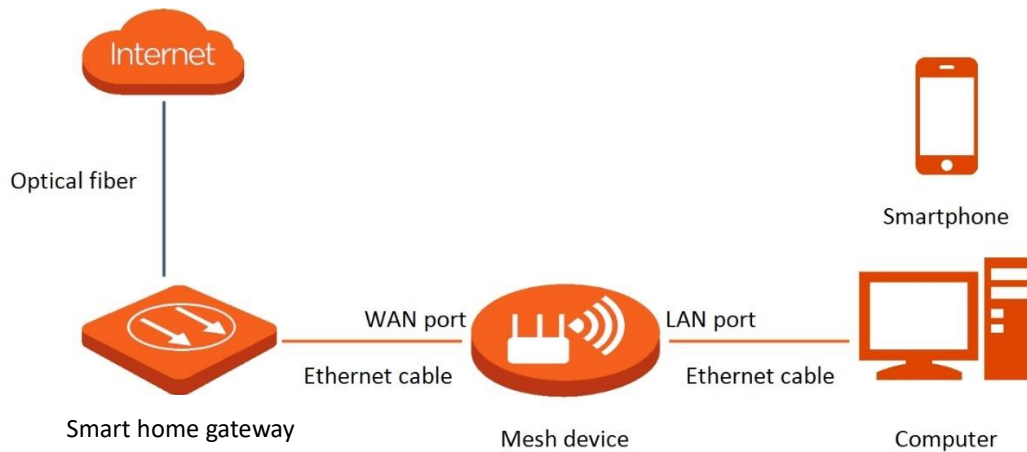


If the IPv6 network fails, try the following solutions:

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

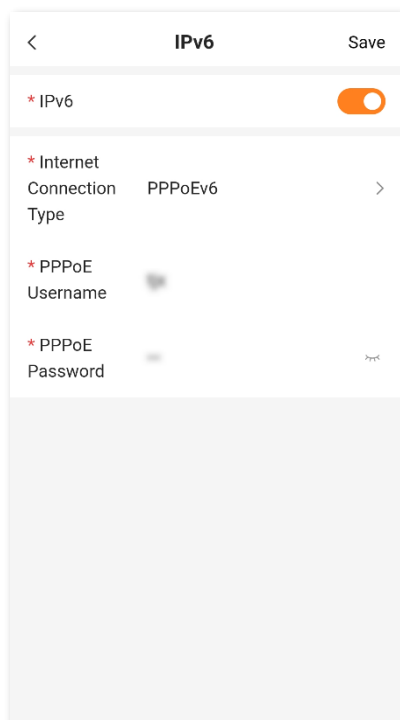
PPPoEv6

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 \(mobile client\)](#), and navigate to **More > IPv6**.
- Step 2** Enable the **IPv6** function.
- Step 3** Set **Internet Connection Type** to **PPPoEv6**.
- Step 4** Set **PPPoE Username** and **PPPoE Password** provided by your ISP, and tap **Save**.



Parameter description

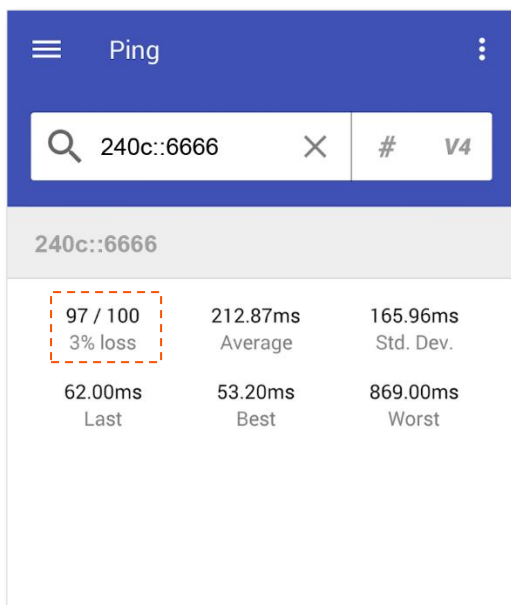
Parameter	Description
PPPoE Username	Specify the PPPoE user name and password provided by your ISP.
PPPoE Password	 TIP IPv4 and IPv6 services share the same PPPoE account.

“Saved successfully” is displayed, indicating that the settings are saved successfully.

---End

Verification:

You can download a network diagnosis App (**HE.NET Network Tools** for example here) on your wireless client and ping an IPv6 website (**240c::6666** for example) to check whether the Mesh device accesses the IPv6 network successfully. As shown in the following figure, if the number of packets received is not 0, the Mesh device accesses the IPv6 network successfully.



If the IPv6 network fails, try the following solutions:

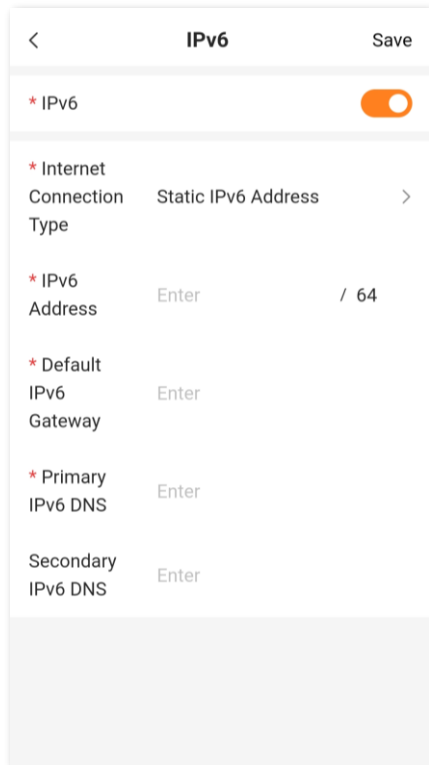
- Ensure that devices connected to Mesh device obtain their IPv6 addresses through DHCP.
- Consult your ISP for help.


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 \(mobile client\)](#), and navigate to **More > IPv6**.
- Step 2** Enable the **IPv6** function.
- Step 3** Set **Internet Connection Type** to **Static IPv6 Address**.
- Step 4** Enter the required parameters.
- Step 5** Tap **Save**.

**Parameter description**

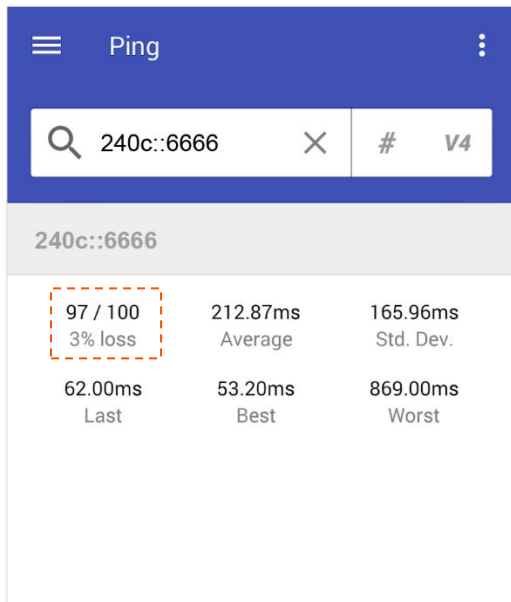
Parameter	Description
IPv6 Address	Specify the fixed IPv6 address information provided by your ISP.
Default IPv6 Gateway	 TIP
Primary IPv6 DNS	If your ISP only provides one DNS address, leave the secondary IPv6 DNS blank.
Secondary IPv6 DNS	

“Saved successfully” is displayed, indicating that the settings are saved successfully.

---End

Verification:

You can download a network diagnosis App (**HE.NET Network Tools** for example here) on your wireless client and ping an IPv6 website (**240c::6666** for example) to check whether the Mesh device accesses the IPv6 network successfully. As shown in the following figure, if the number of packets received is not 0, the Mesh device accesses the IPv6 network successfully.



If the IPv6 network fails, try the following solutions:

- Ensure that you have entered the correct WAN IPv6 address.
- Ensure that devices connected to Mesh device obtain their IPv6 addresses through DHCP.
- Consult your ISP for help.

4.9.5 Reset a node



- 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:

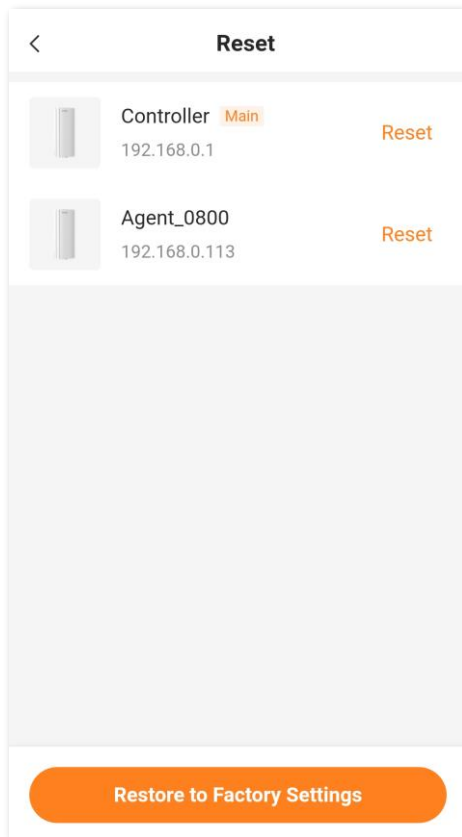
Step 1 [Log in to the web UI \(mobile client\)](#), and navigate to **More > Reset**.

Step 2 Tap **Reset** in the line of the node to be reset.

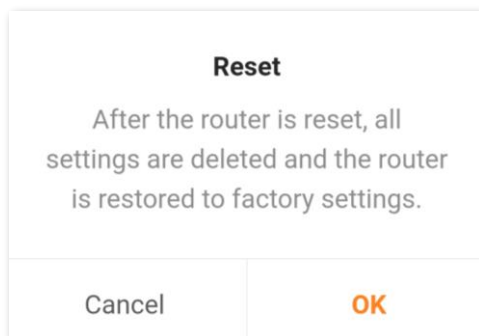


TIP

To reset all the nodes, tap **Restore to Factory Settings** at the bottom.



Step 3 Tap **OK**. Wait until the reset completes.



---End

4.9.6 Reboot a node



NOTE

Rebooting a node will disconnect all connections to the node. Please reboot the nodes when the network is idle.

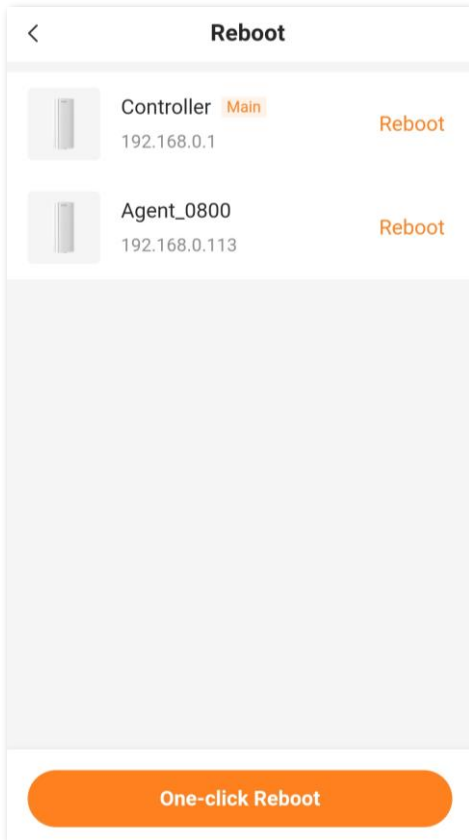
To reboot a node:

Step 1 [Log in to the web UI \(mobile client\)](#), and navigate to **More > Reboot**.

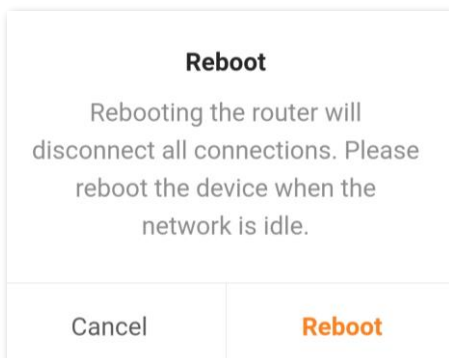
Step 2 Tap **Reboot** in the line of the node to be reset.



To reboot all the nodes, tap **One-click Reboot** at the bottom.



Step 3 Tap **Reboot**. Wait until the rebooting process completes.



---End

4.9.7 Firmware upgrade



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.

Upgrade a node

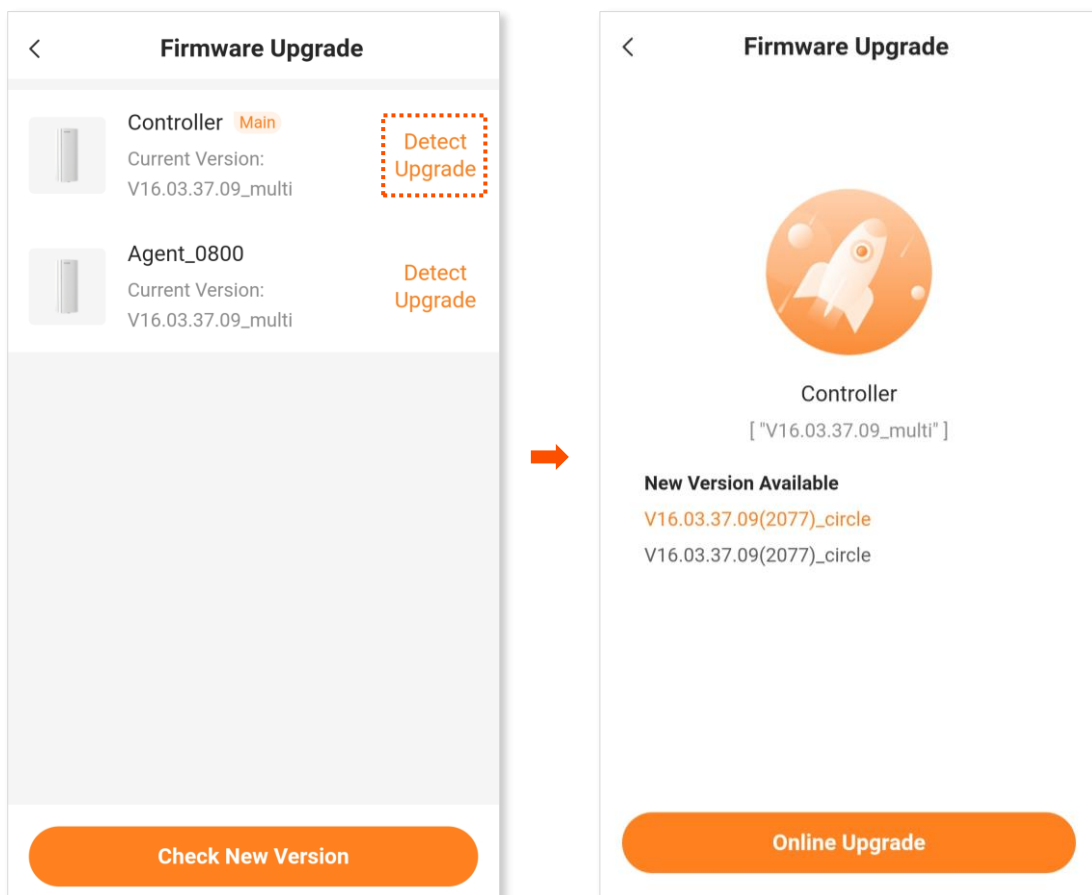
To perform online upgrade on a single node:

Step 1 [Log in to the web UI \(mobile client\)](#), and navigate to **More > Firmware Upgrade**.

Step 2 Tap **Detect Upgrade** for a node.

Controller is used for example.

Step 3 Tap **Online Upgrade**.



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

---End

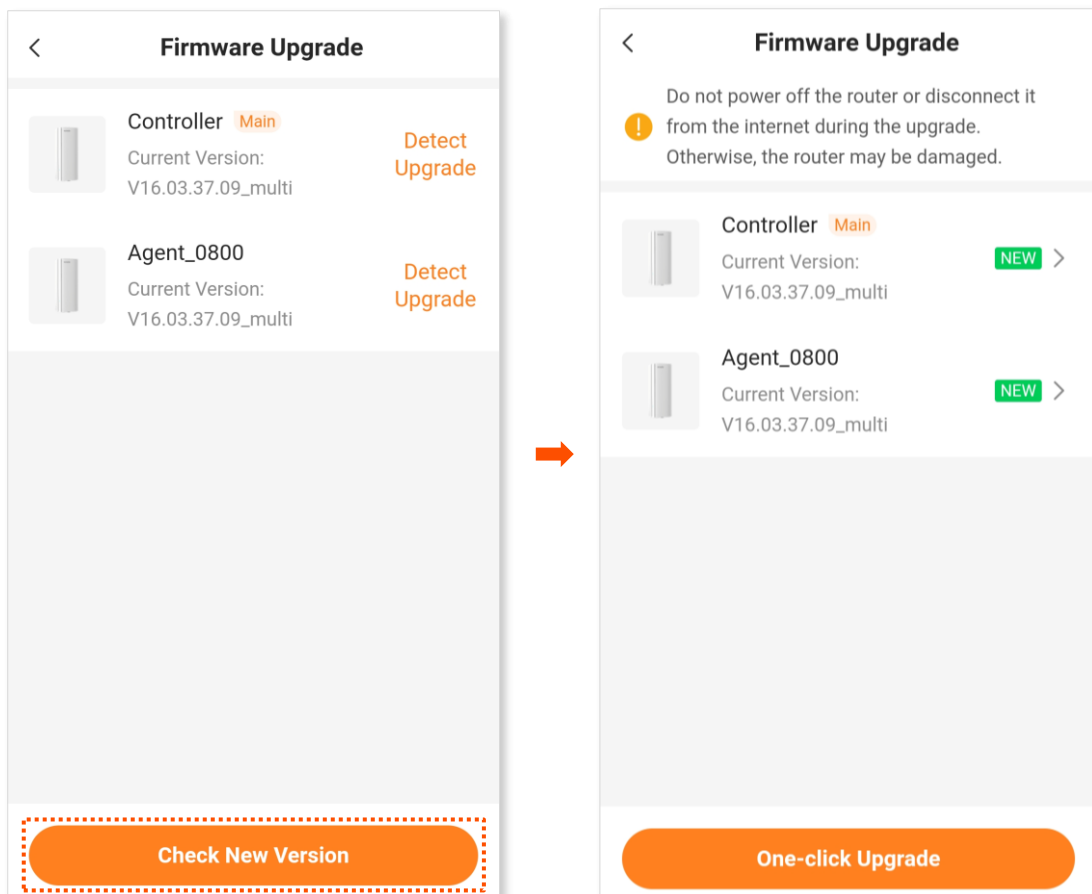
Upgrade all nodes

Step 1 [Log in to the web UI \(mobile client\)](#), and navigate to **More > Firmware Upgrade**.

Step 2 Tap **Check New Version**.

New appears if a new firmware version is detected.

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



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

---End

5 FAQ

5.1 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** and **Obtain DNS server 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.

5.2 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.

5.3 Failed to find or connect my wireless network

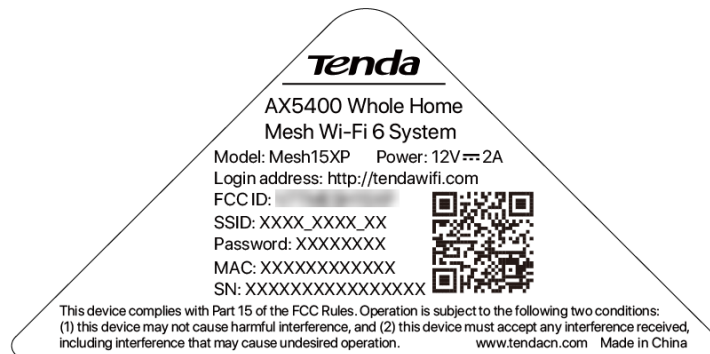
Use the following method to troubleshoot the fault.

- 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.

5.4 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.



(MX15 Pro for example)

- If you have changed the password, reset the primary node by holding down the reset (**RST/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	
Unify 2.4 GHz & 5 GHz & 6 GHz (MX21 Pro/EX21 Pro/Mesh21XEP)	Disabled	
Guest Wi-Fi	Disabled	
MESH button	Enabled	
VPN	Disabled	

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

A.2 Acronyms and Abbreviations

Acronym or Abbreviation	Full Spelling
ACS	Auto-Configuration Server
AES	Advanced Encryption Standard
AP	Access point
CPE	Customer Premises Equipment
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
FCC	Federal Communications Commission
FTP	File Transfer Protocol
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPTV	Internet Protocol television
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet service provider

Acronym or Abbreviation	Full Spelling
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
OS	Operating system
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point to Point Tunneling Protocol
RA	Router Advertisement
SSID	Service Set Identifier
STB	Set-top box
STUN	Session Traversal Utilities for NAT
TCP	Transmission Control Protocol
TR-069	Technical Report 069
UDP	User Datagram Protocol
UI	User interface
UPnP	Universal Plug and Play
URL	Uniform Resource Locator
VLAN	Virtual local area network
VPN	Virtual private network
WAN	Wide area network

Acronym or Abbreviation	Full Spelling
WLAN	Wireless local area network
WPA2-PSK	Wi-Fi Protected Access 2—Pre-Shared-Key
WPA3	Wi-Fi Protected Access 3
WPA3-SAE	WPA3-Simultaneous Authentication of Equals
WPS	Wi-Fi Protected Setup