



AX1800 Dual-band Whole Home Mesh Wi-Fi 6 System

User Guide

Copyright Statement

© 2021 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 AX1800 Dual-band Whole Home Mesh Wi-Fi 6 System, which can be managed on both the web UI and app. This user guide only introduces the operations on the web UI. For details about app operations, see *Tenda WiFi App User Guide For Whole Home Mesh WiFi System*. All the screenshots and product figures herein, unless otherwise specified, are taken from MX6.





- The web UI of different models may differ. The web UI actually displayed shall prevail.
- The AX1800 Dual-band Whole Home Mesh Wi-Fi 6 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
 NOTE	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configuration, loss of data or damage to device.
 TIP	This format is used to highlight a procedure that will save time or resources.

For more documents

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

The related documents are listed as below.

Document	Description
Data Sheet	It introduces the basic information of the device, including product overview, selling points, and specifications.
Quick Installation Guide	It introduces how to set up the device quickly for internet access, the descriptions of LED indicators, ports, and buttons, FAQ, statement information, and so on.
Tenda WiFi App User Guide for Whole Home Mesh WiFi System	It introduces how to set up more functions of the device for more requirements through the Tenda WiFi app.

Technical Support

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



Hotline

Global: (86) 755-27657180

(China Time Zone)

United States: 1-800-570-5892

(Toll Free: 7 x 24 hours)

Canada: 1-888-998-8966

(Toll Free: Mon - Fri 9 am - 6 pm PST)

Hong Kong: 00852-81931998



Email

support@tenda.com.cn



Website

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

Revision History

Tenda is constantly searching for ways to improve its products and documentation. The following table indicates any changes that might have been made since the MX6 was introduced.

Version	Date	Description
v1.0	2021-11-22	Original publication.

Contents

- 1 Get to know your device 1**
 - 1.1 Product overview 2
 - 1.2 Appearance 2
 - 1.2.1 LED indicator 2
 - 1.2.2 Buttons and Ports..... 4
 - 1.2.3 Label 5
- 2 Quick Setup 6**
 - 2.1 Connect your primary node 7
 - 2.1.1 Connect your primary node with a modem..... 7
 - 2.1.2 Connect your primary node without a modem 7
 - 2.2 Connect your primary node to the internet 7
 - 2.3 Extend your network..... 13
- 3 Web UI..... 15**
 - 3.1 Log in to the web UI 16
 - 3.2 Log out of the web UI..... 17
 - 3.3 Change the language..... 17
 - 3.4 Web UI layout..... 17
- 4 Network status 19**
 - 4.1 Network status 20
 - 4.2 Network topology 21
 - 4.2.1 Controller information 22
 - 4.2.2 Agent information 24
 - 4.2.3 Add a node 26
 - 4.2.4 One-click optimization 30
 - 4.2.5 Reboot all nodes 30

4.2.6 Turn on/off all indicators.....	31
5 Internet settings	32
5.1 Overview	33
5.2 Access the internet with a PPPoE account.....	36
5.3 Access the internet through a dynamic IP address.....	37
5.4 Access the internet with a set of static IP address information	39
5.5 Set up dual access connection	40
6 Wi-Fi Settings.....	42
6.1 Basic Settings.....	43
6.2 Separate the 2.4 GHz and 5 GHz Wi-Fi networks.....	44
7 Client management	46
7.1 View client information.....	47
7.2 Change a client name	49
7.3 Add a client to the blacklist.....	49
7.4 Remove a client from the blacklist.....	51
7.5 Delete an offline client	51
8 Parental control	53
8.1 Create a parental control rule	54
8.1.1 Add a parental control rule	54
8.1.2 An example of adding parental control rules.....	56
8.2 Other operations on the parental control rules.....	59
9 More.....	60
9.1 Router information.....	61
9.1.1 Basic information	62
9.1.2 WAN port information	62
9.1.3 LAN information	63
9.2 Guest Wi-Fi.....	63
9.2.1 Overview	63
9.2.2 An example of configuring the guest network.....	64

9.3 Working mode.....	65
9.3.1 Router mode	66
9.3.2 AP mode	68
9.4 IPv6.....	71
9.4.1 IPv6 WAN settings	71
9.4.2 IPv6 LAN settings.....	78
9.5 Smart power saving.....	79
9.6 Advanced Wi-Fi Settings.....	80
9.6.1 Channel & bandwidth	80
9.6.2 WPS	83
9.6.3 MESH button	85
9.7 Network settings	86
9.7.1 LAN Settings	86
9.7.2 VPN.....	89
9.7.3 IPTV	98
9.7.4 WAN parameters.....	102
9.8 Advanced.....	103
9.8.1 App remote management.....	103
9.8.2 MAC address filter.....	104
9.8.3 Firewall	107
9.8.4 DMZ host.....	108
9.8.5 Remote web management.....	113
9.8.6 Static routing	116
9.8.7 DDNS	120
9.8.8 UPnP.....	125
9.8.9 Port mapping.....	126
9.9 System settings.....	128
9.9.1 Login password.....	128
9.9.2 System time.....	129

- 9.9.3 Firmware upgrade 131
- 9.9.4 Backup & restore 135
- 9.9.5 Auto system maintenance 138
- 9.9.6 System log 139
- 10 FAQ..... 140**
- 10.1 Failed to access the web UI 140
- 10.2 Internet detection failed upon the first setup 140
- 10.3 Failed to find or connect my wireless network 141
- 10.4 Forgot my password 141
- Appendixes 142**
- A.1 Factory settings 142
- A.2 Acronyms and Abbreviations 144

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

1.2 Appearance

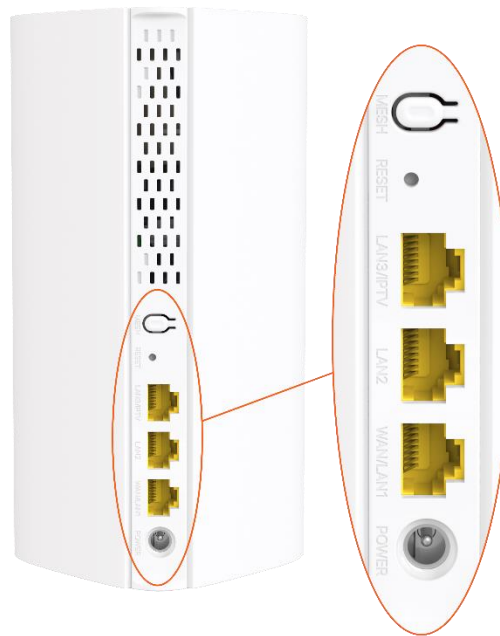
1.2.1 LED indicator




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

LED indicator	Stage	Status	Description
LED indicator	Before networking	Solid green	System started
		Blinking green slowly	Waiting for networking
	During networking	Blinking green slowly	Networking...  TIP This status only exists during the first-time networking.
		Solid on	Networking completed <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 failed
	WPS	Blinking green quickly	WPS started Device connecting...
		Solid green	Device connected
	Reset	Blinking red quickly	Reset started
		Solid green	Restarting...
		Blinking green slowly	Reset completed

1.2.2 Buttons and Ports



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

Jack/Port/Button	Description
MESH	<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>

Jack/Port/Button	Description
LAN2	LAN port.
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.
POWER	Power jack.

1.2.3 Label

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



Model: Specifies the device model.

Power: Specifies the power of the device.

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.

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

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

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

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

2 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 chapter 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 Connect your primary node

2.1.1 Connect your primary node with a modem

To connect your primary node with a modem:

Step 1 Power off your modem.

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

Step 3 Power on your modem.

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

---End

2.1.2 Connect your primary node without a modem

To directly connect your primary node without a modem:

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

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

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

---End

2.2 Connect your primary node to the internet

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

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

Step 1 Use an Ethernet cable to connect your computer to the **LAN2** or **LAN3/IPTV** port of the primary node, or use your smartphone to access the Wi-Fi network of the primary node.

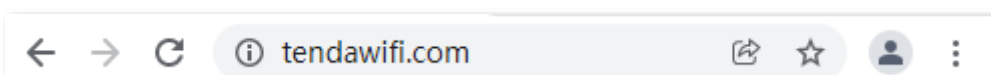
In the following steps, computer connection is used for illustration.

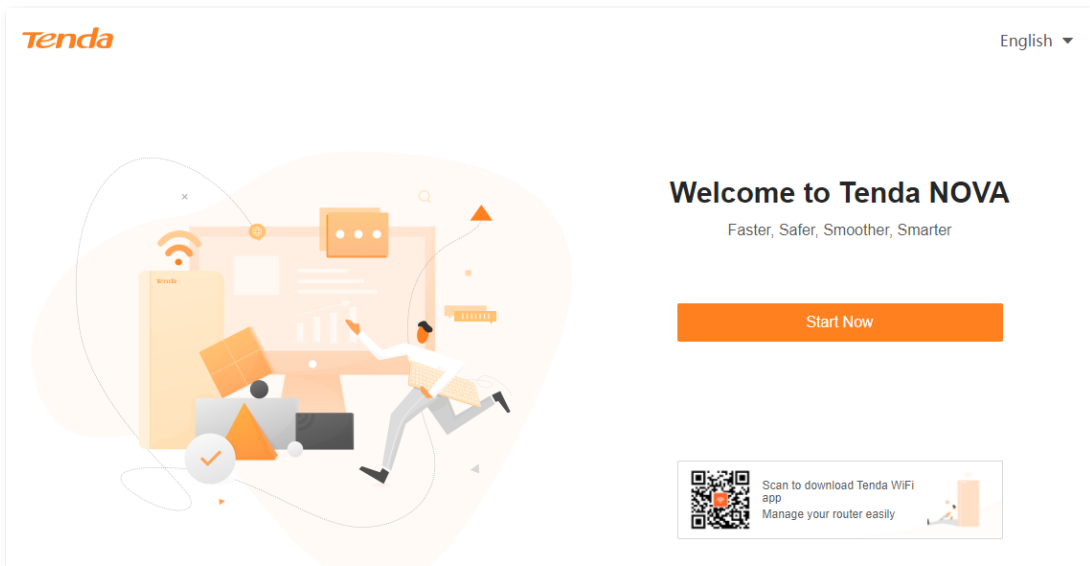


TIP

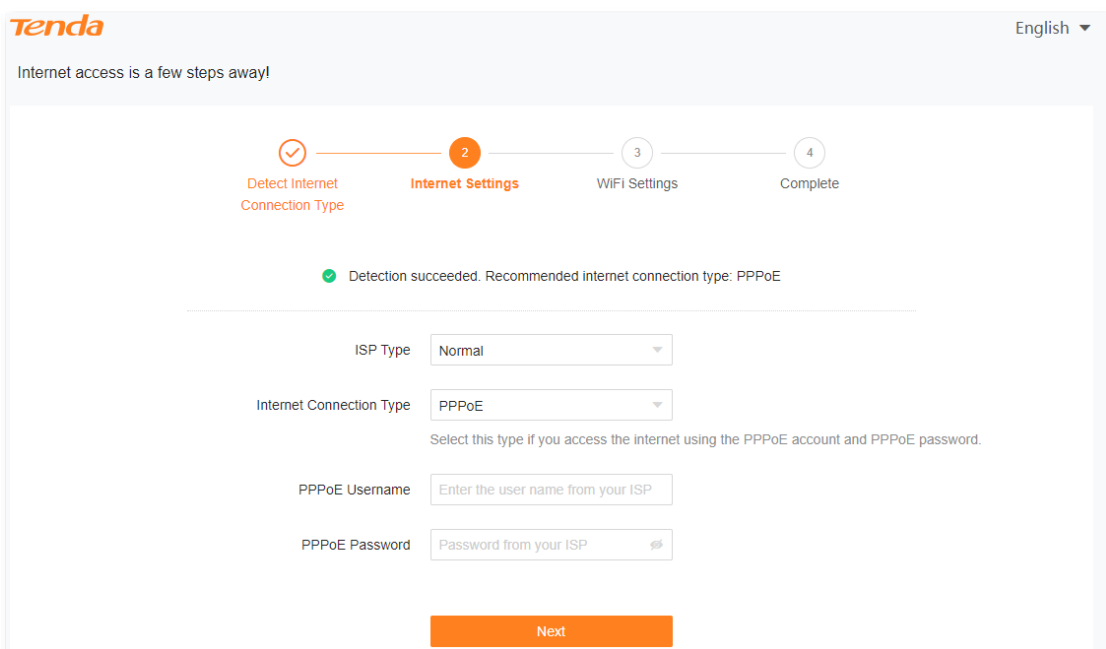
The default Wi-Fi name and password can be found on the bottom label of the device.

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

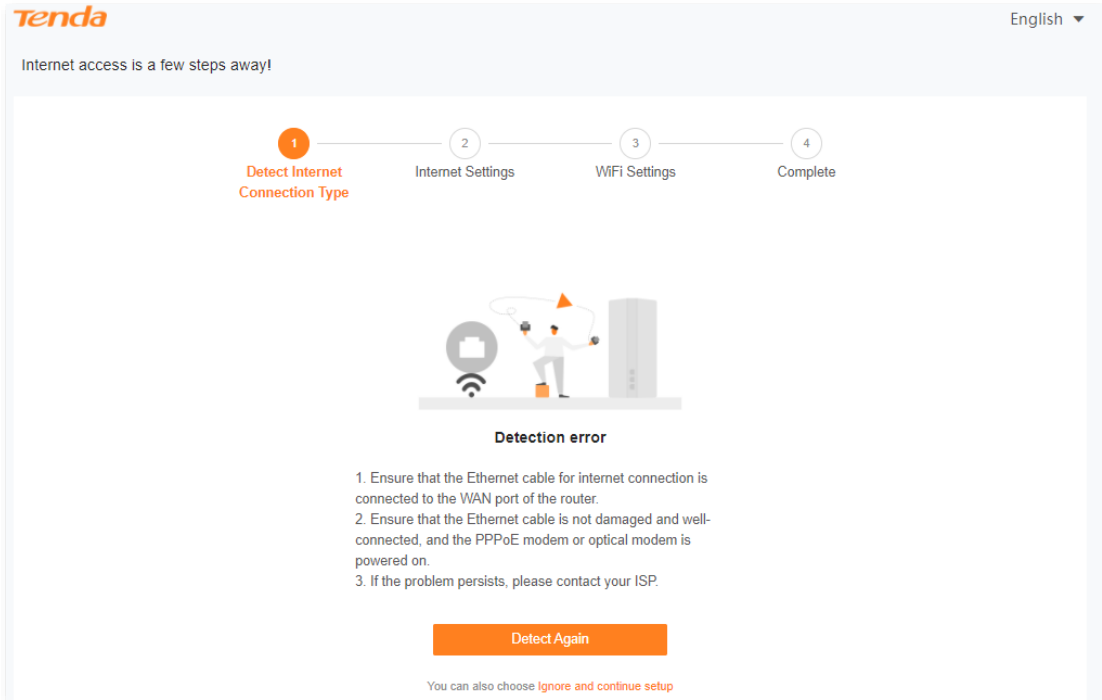


Step 3 Click **Start Now**.

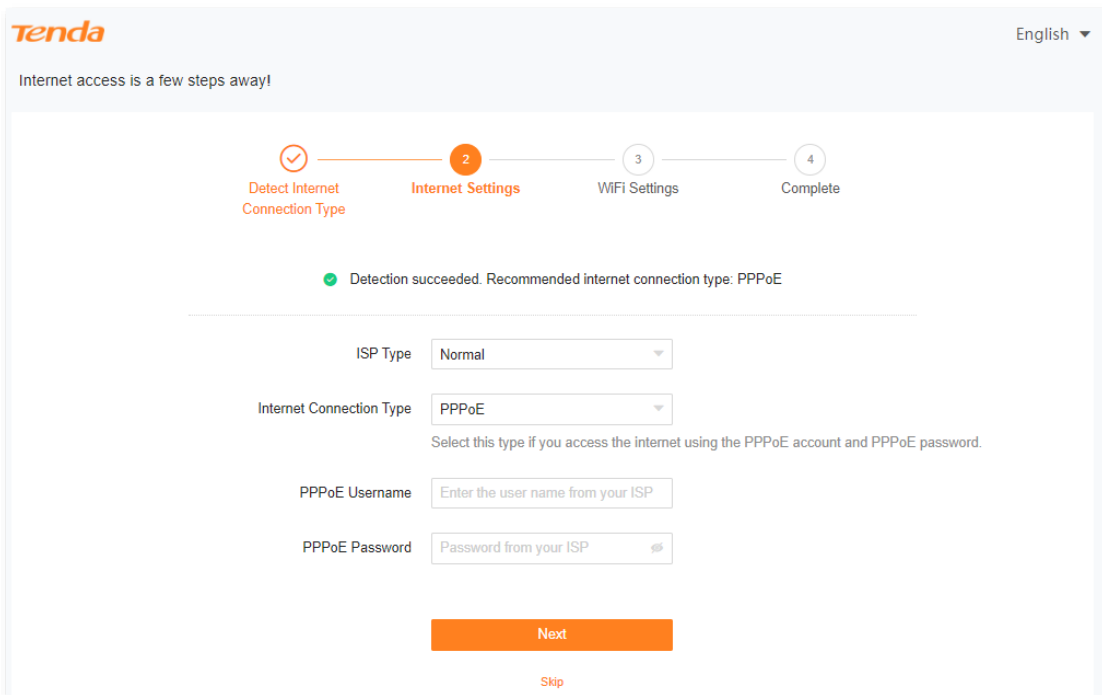
- If your internet connection is normal, the following page is displayed and you can continue the setup in **Step 4**.



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




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



The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
ISP Type	<p>Specifies the type of your ISP, such as Normal, Russia, Unifi, Maxis, Maxis-Special, and Manual. Parameters required for each option may differ.</p> <p>Refer to the following to choose your connection type:</p> <ul style="list-style-type: none"> • Normal, Unifi, Maxis, and Maxis-Special: Select these options when your ISP provides no setup information, except for the PPPoE user name and password, or static IP address information. • Russia: Select this option when your ISP provides dual access information, such as PPTP, L2TP connection information. • Manual: Select this option when your ISP provides VLAN ID information, besides the PPPoE user name and account, or static IP address. <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	When the internet connection type is static IP, you need to enter the fixed IP address information provided by your ISP.
Subnet Mask	
Gateway	
Primary DNS	If your ISP provides only one DNS server, you can leave Secondary DNS blank.
Secondary DNS	
Address Type	<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	
Internet VLAN ID	<p>When you select Manual for ISP Type, you can configure these parameters.</p> <p> TIP</p>
IPTV VLAN ID	<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 parameters as required, and click **Next**.



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

Tenda English ▾

Internet access is a few steps away!

Detect Internet Connection Type
 Internet Settings
 WiFi Settings
 Complete

WiFi Name: NOVA_9JK3_A3

WiFi Password: Not encrypted

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
 Complete

Configuration completes. You can access the internet now

Current WiFi network is cut off. Please connect to the new WiFi network

WiFi Name: NOVA_...

WiFi Password: _____

Login Password: _____

Complete

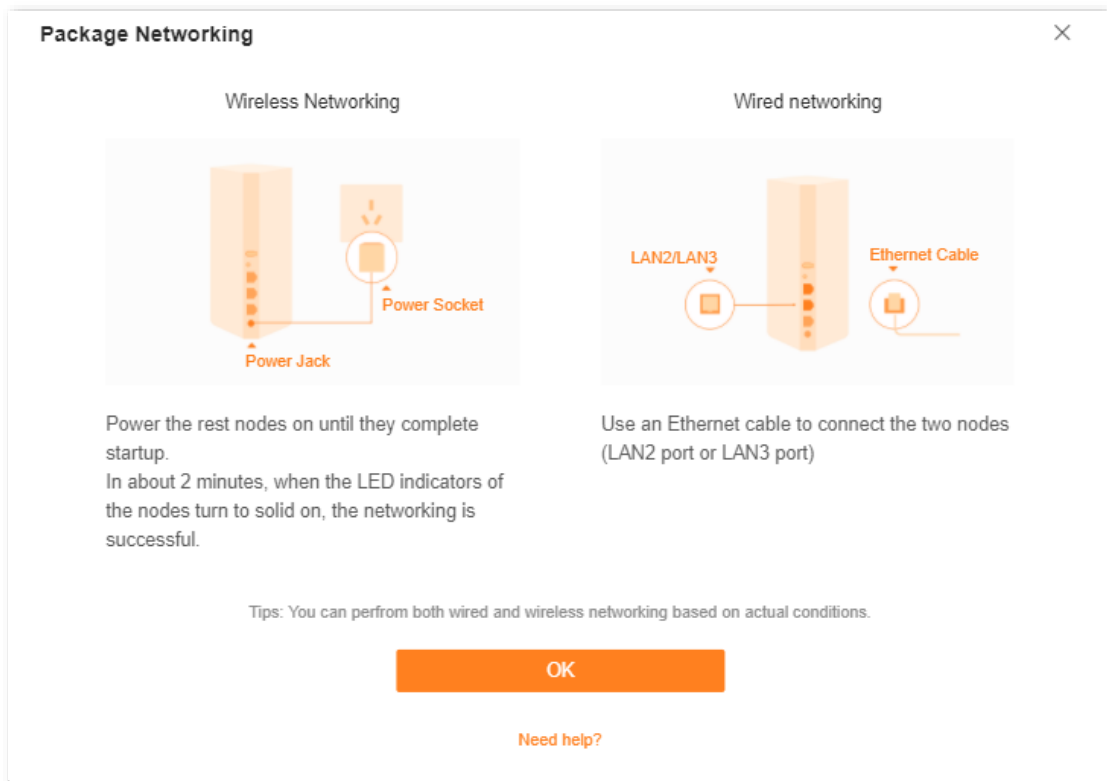
---End

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

2.3 Extend your network

Upon your first login, the following information is displayed to tell you how to extend the network.



To extend your network:

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

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

Step 2 Relocate the secondary nodes to a proper position.



TIP

- Ensure that the distance between any two nodes is less than 10 meters.
- Keep your nodes away from electronics with strong interference, such as microwave ovens, induction cookers, and refrigerators.
- Place the nodes in a high position with few obstacles.

Step 3 Power on the secondary nodes again. Wait until these LED indicators blink green slowly.



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.)

3 Web UI

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

[Log in to the web UI](#)

[Log out of the web UI](#)

[Change the language](#)

[Web UI layout](#)

3.1 Log in to the web UI

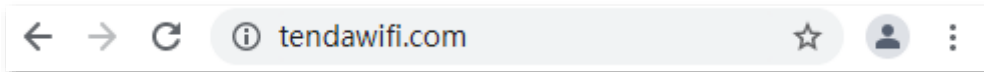
To log in to the web UI, perform the following steps:

- Step 1** Use an Ethernet cable to connect your computer to the **LAN2** or **LAN3/IPTV** port of the primary node, or use your smartphone to access the Wi-Fi network of the primary node. In the following steps, computer connection is used for illustration.

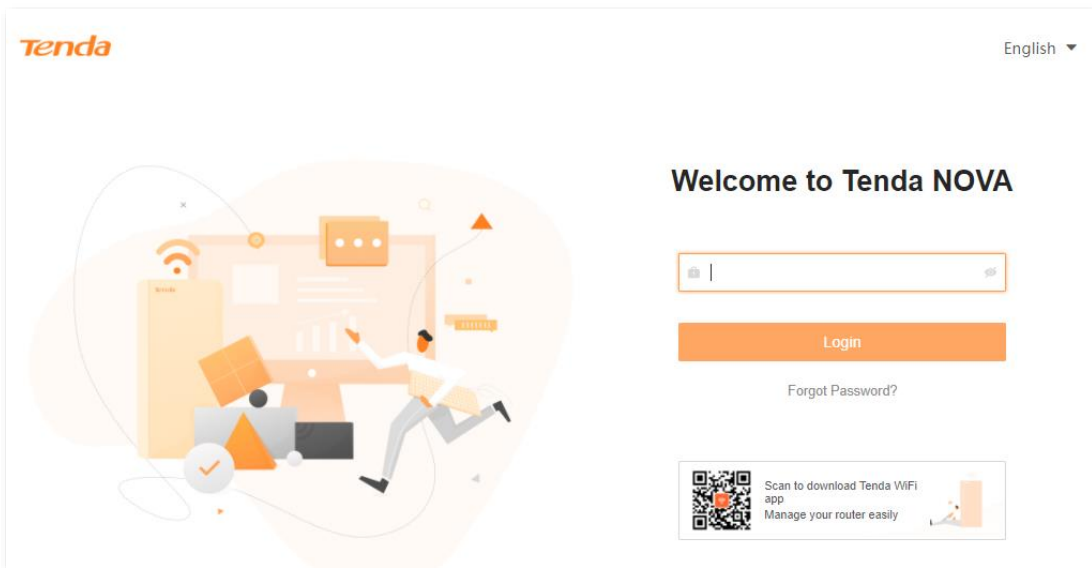


The default Wi-Fi name and password can be found on the bottom label of the Mesh device.

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



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



- 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](#).

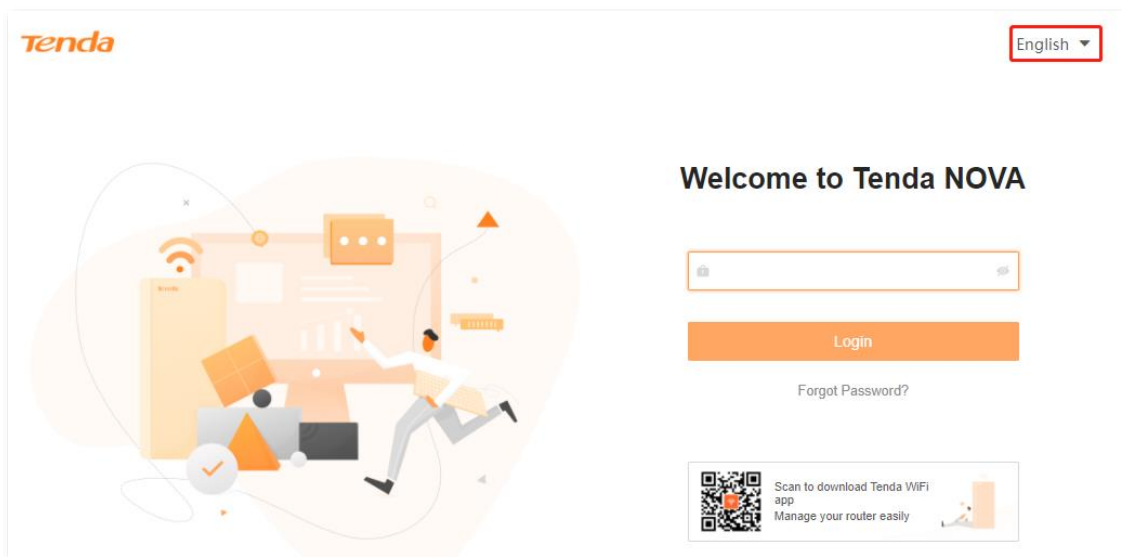
---End

3.2 Log out of the web UI

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

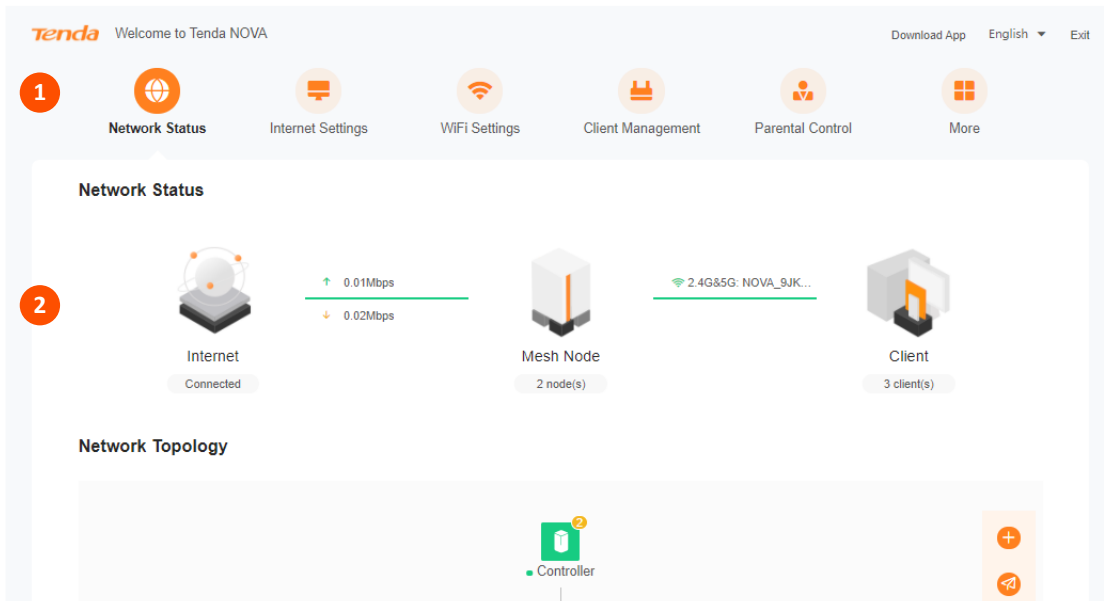
3.3 Change the language

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



3.4 Web UI layout

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



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

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

4 Network status

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

This chapter includes the following sections:

[Network status](#)

[Network topology](#)

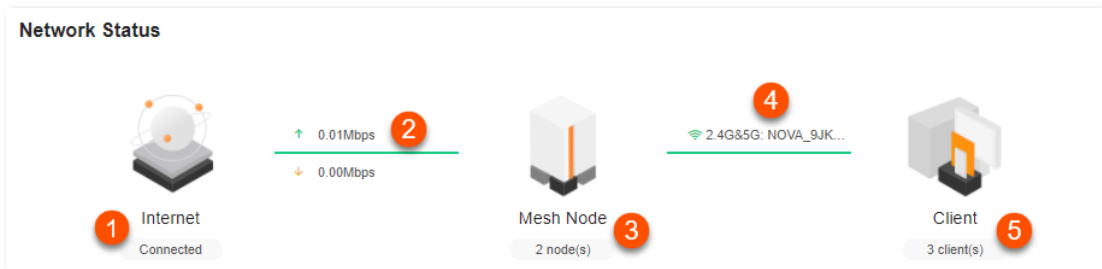
4.1 Network status

To view the network status:

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

Step 2 Choose **Network Status**.

The following page is displayed.



---End

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

No.	Description
1	<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.
3	Indicates the number of Mesh nodes connected in the network.
4	Indicates the Wi-Fi name and frequency band.
5	Indicates the number of clients connected in the network, including secondary Mesh nodes.

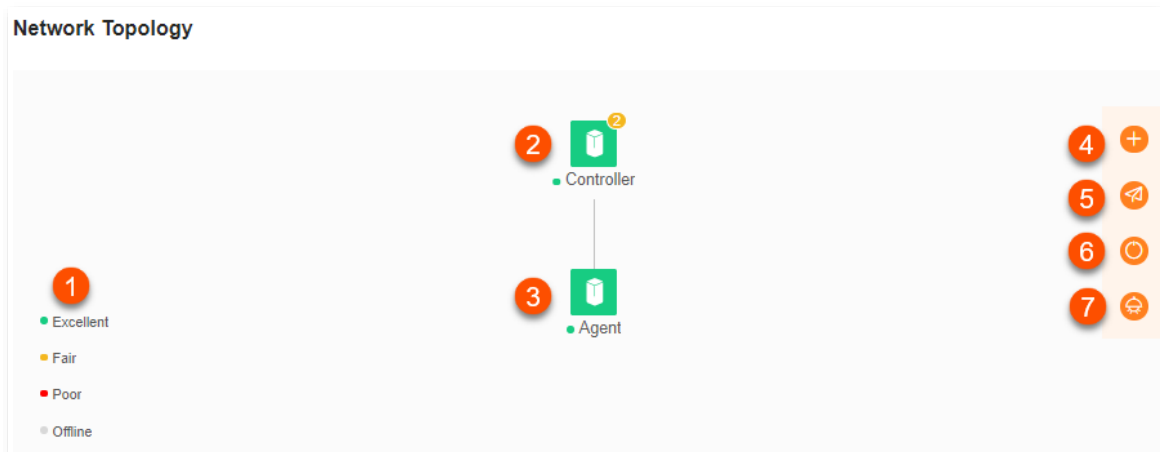
4.2 Network topology

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

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

Step 2 Choose **Network Status**.

The following page is displayed.



---End


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

No.	Description
1	Explains the node status indicated by different colors. <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 .
6	Used to Reboot all nodes .
7	Used to Turn on/off all indicators .

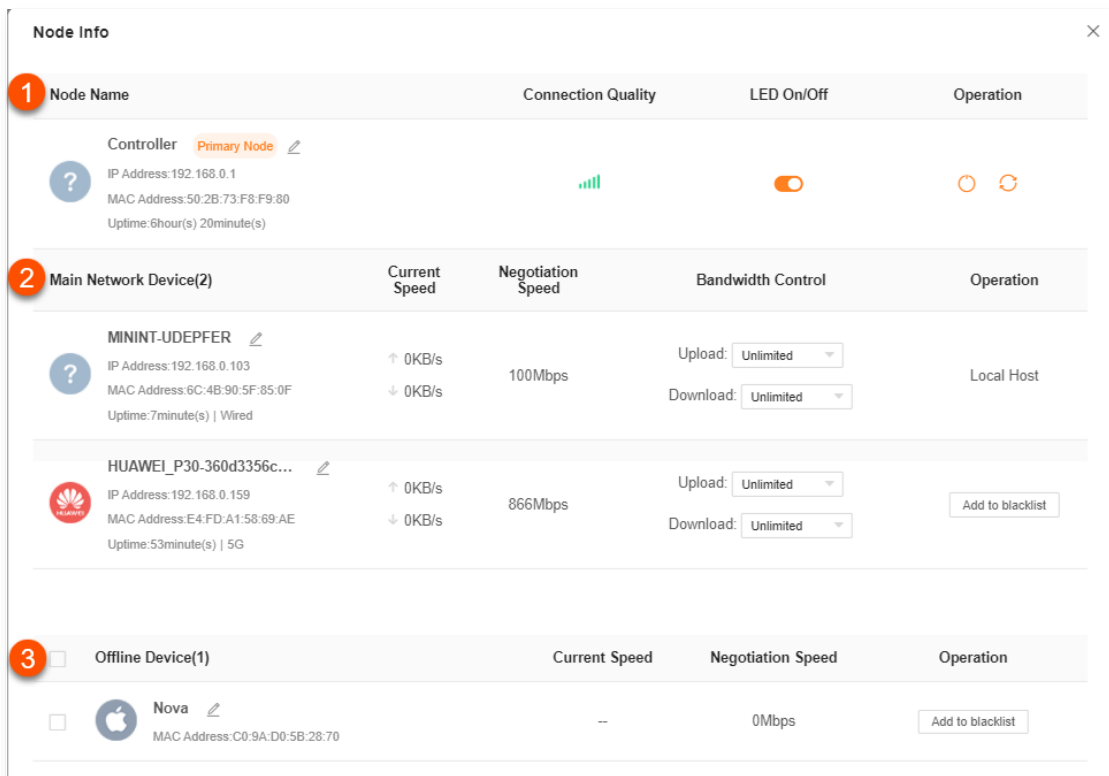
4.2.1 Controller information

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

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

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

The following dialog box is displayed.



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






- Section 1:** A table with columns: Node Name, Connection Quality, LED On/Off, and Operation. It lists the 'Controller' (Primary Node) with IP 192.168.0.1, MAC 50:2B:73:F8:F9:80, and uptime of 6h 20m. Connection quality is shown as a green signal icon, and the LED is turned on.
- Section 2:** A table with columns: Main Network Device(2), Current Speed, Negotiation Speed, Bandwidth Control, and Operation. It lists two devices: 'MININT-UDEPFER' (Local Host) and 'HUAWEI_P30-360d3356c...' (5G). Both show 0KB/s current speed and 100Mbps/866Mbps negotiation speed. Bandwidth control is set to 'Unlimited' for both.
- Section 3:** A table with columns: Offline Device(1), Current Speed, Negotiation Speed, and Operation. It lists 'Nova' with MAC C0:9A:D0:5B:28:70 and 0Mbps negotiation speed.

---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.
- **Connection Quality:** Shows the connection signal strength with the primary node. You can hover your mouse over  to see the strength value.
- **LED On/Off:** Provides a  button for turning on/off the LED indicator of the primary node. You can use this function to check which device you are operating. [Turn on/off all indicators](#) prevails to this operation.
- **Operation:** Provides a  button for rebooting the primary node and a  button for resetting the primary node.

1




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

No.	Description
	<p>This area 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.
2	<ul style="list-style-type: none"> • 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.
	<p>This area 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: Displays the speed of negotiation.
3	<ul style="list-style-type: none"> • Operation: Provides an Add to blacklist button for blacklisting clients. Once blacklisted, the client cannot access the internet through the Mesh system. <p> TIP</p> <p>A maximum of 20 offline clients can be displayed here. A client will be automatically deleted from the list if it is offline for 3 days. A client is displayed under Offline Device after it is disconnected from the network for 90 seconds (wired client)/60 seconds (wireless client).</p>

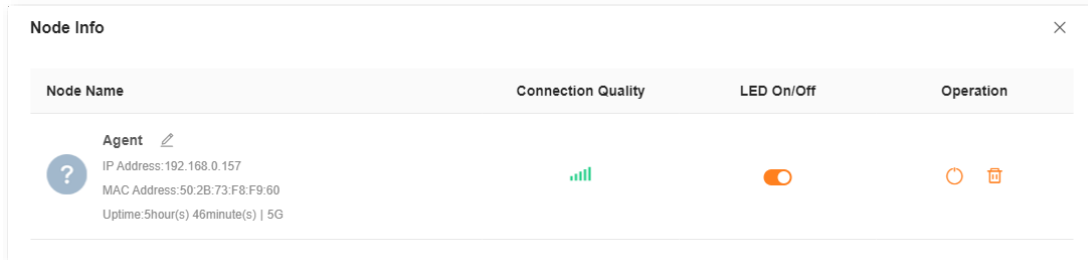
4.2.2 Agent information

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

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






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


4.2.3 Add a node



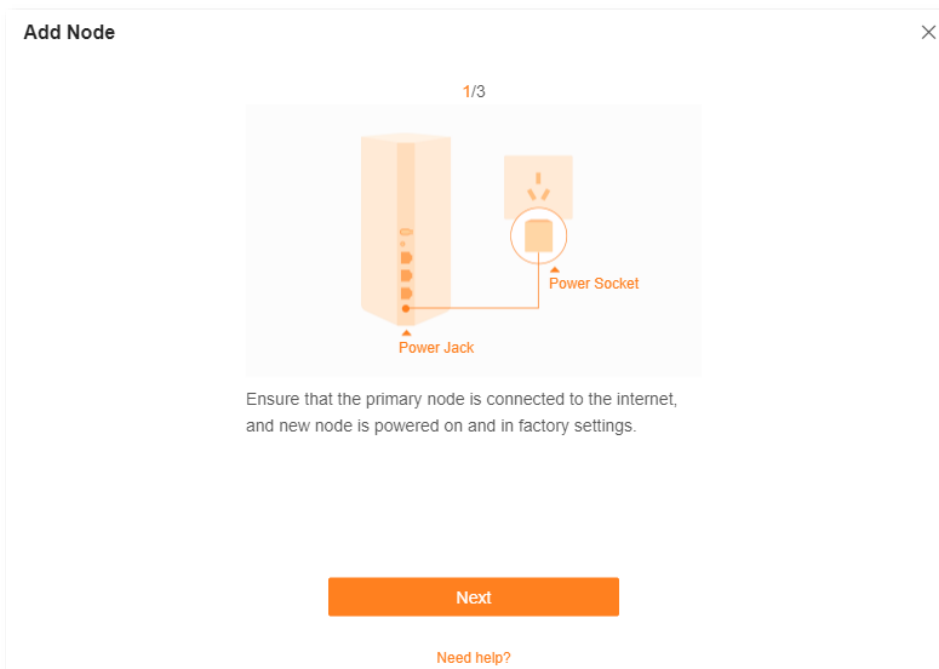
- The node to be added must support the EasyMesh or Xmesh protocol.
- The node to be added must be located within the signal coverage of the primary node.
- A maximum of nine nodes can be added to a Mesh network.

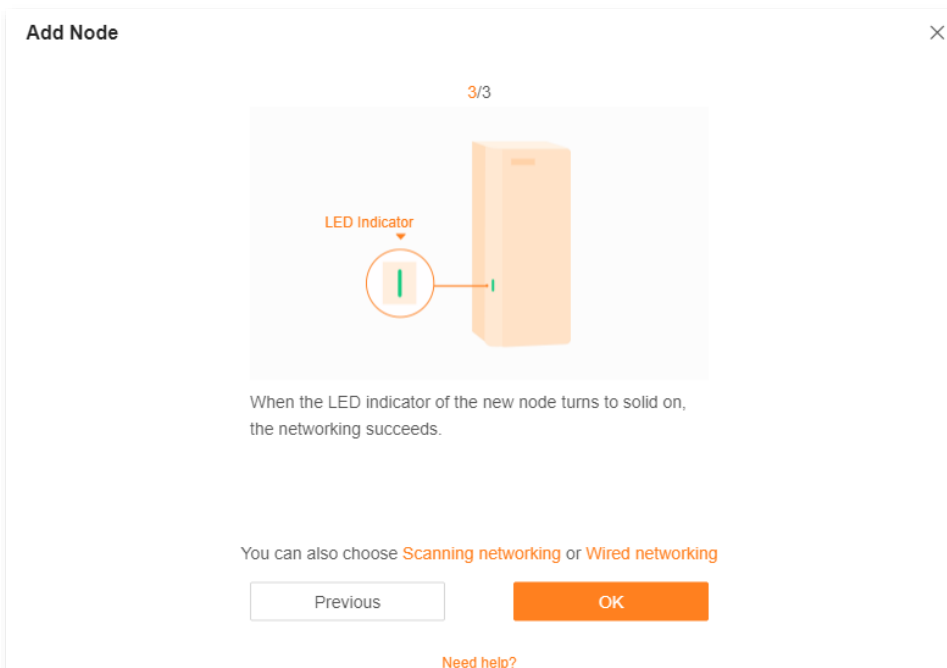
To add a node:

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

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

Step 3 Follow the instructions displayed.





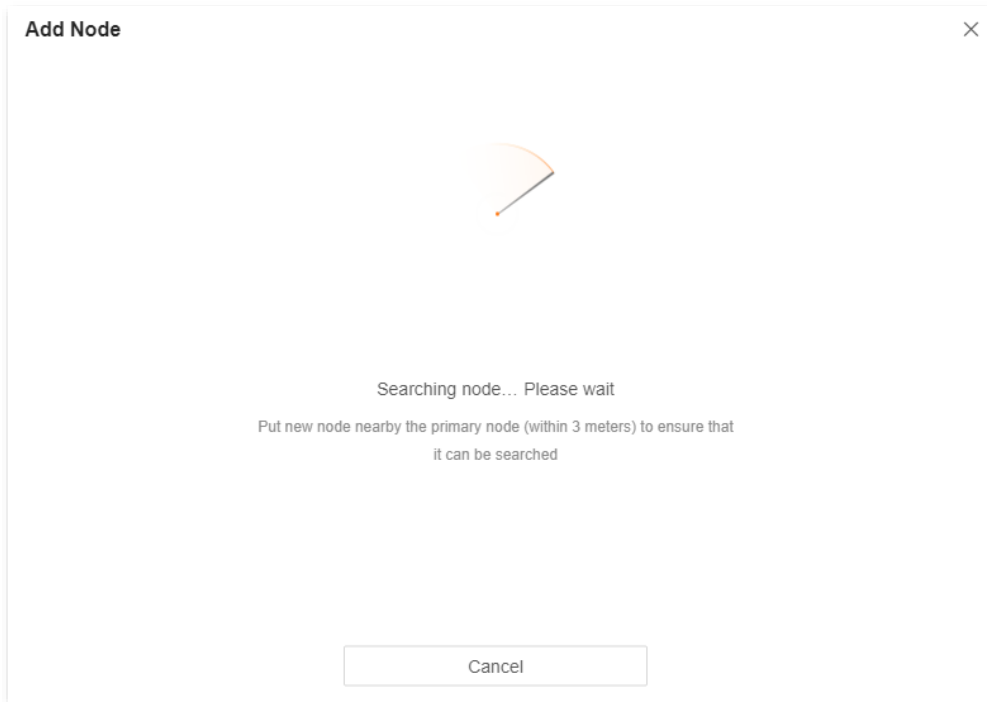
If the LED indicator of new node lights solid on and the new node is displayed in **Network Topology**, the node is added successfully.

---End

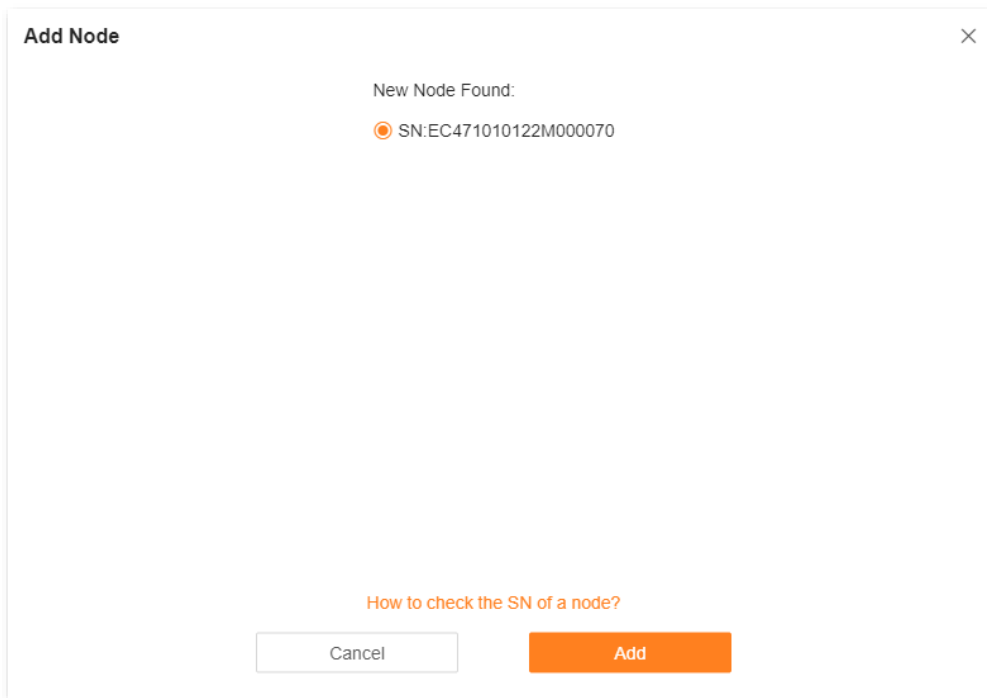
If you cannot add a node by following the preceding instructions, try the following two methods by clicking **Scanning networking** or **Wired networking** shown in the preceding figure:

- To scan a new node:

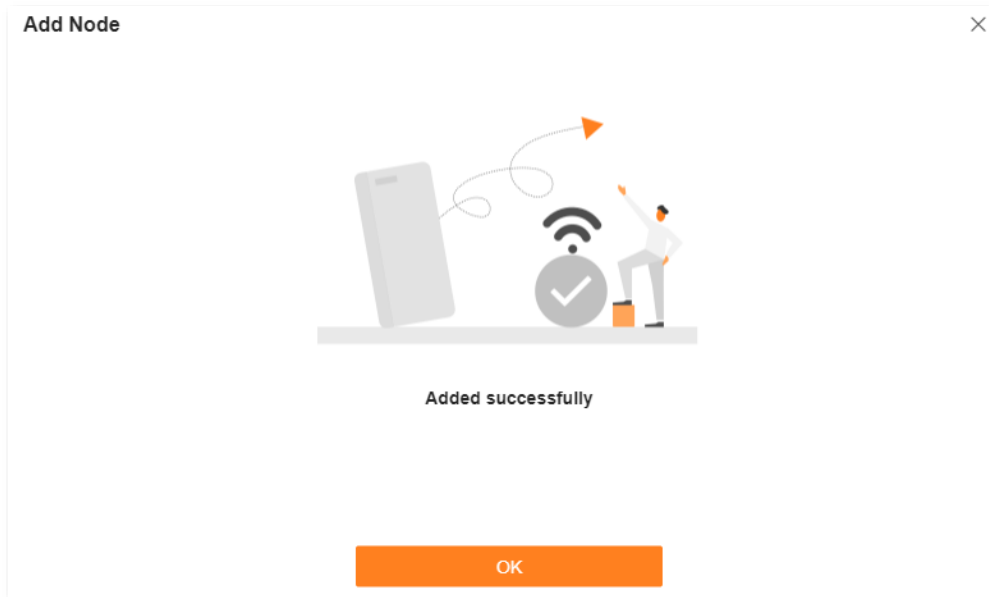
Step 1 Click Scanning networking.



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



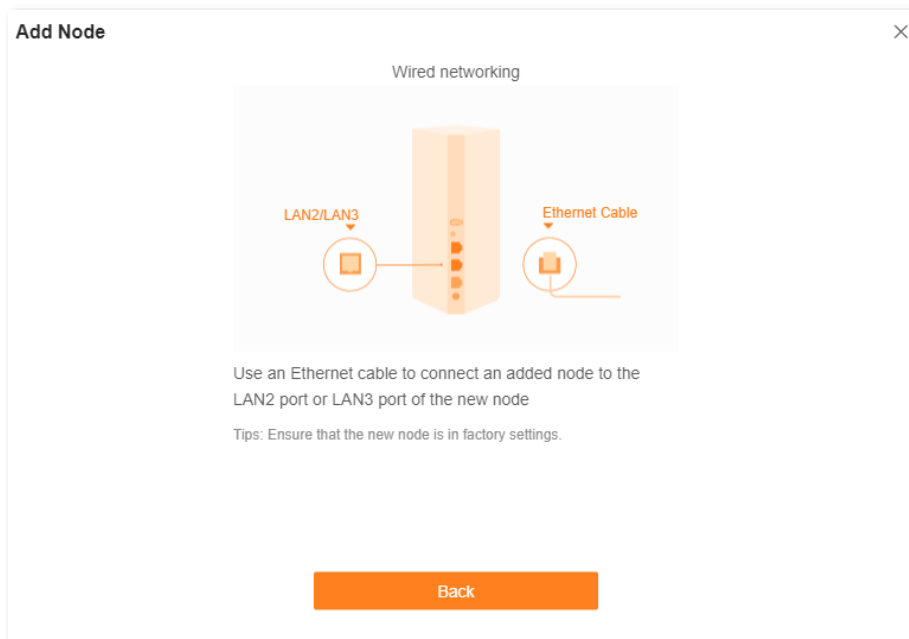
Step 3 Wait until the ongoing process is complete.



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

---End

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




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

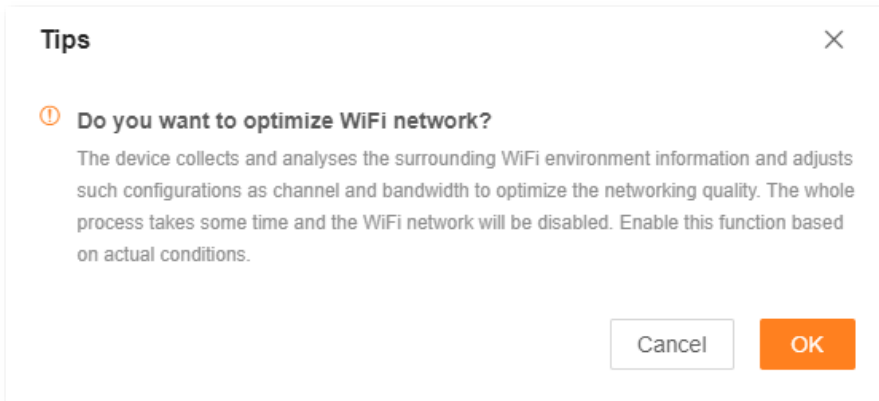
4.2.4 One-click optimization

To optimize the Wi-Fi network with one click:

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

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

Step 3 Click **OK**.




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

---End

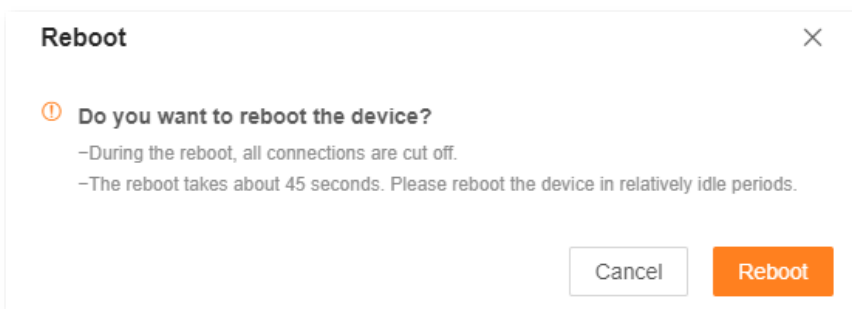
4.2.5 Reboot all nodes

To reboot all nodes by one click:

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

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

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



---End


4.2.6 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  under **Network Topology**.

The indicators turn on/off immediately.

---End

5 Internet settings

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

If you are configuring the 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 chapter includes the following sections:

[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](#)

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](#), 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

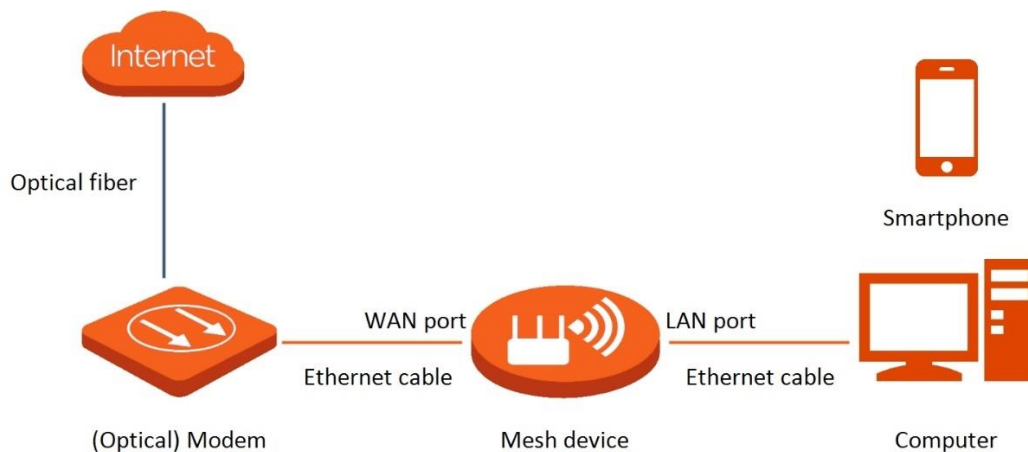
Parameter	Description
Network Status	<p>Indicates the internet connection status.</p> <ul style="list-style-type: none"> • Connected: The internet connection is successful. • Other information (for example, No Ethernet cable is connected to the WAN port): The internet connection failed. Perform troubleshooting according to the tips displayed.

Parameter	Description
Uptime	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	
Internet VLAN ID	
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.

Parameter	Description
	<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>
MTU	<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	<p>Required when you select Custom for MAC Address Clone under Advanced. You can enter the customized MAC address here.</p>

5.2 Access the internet with a PPPoE account

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



To access the internet with a PPPoE account:

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

Step 2 Set **ISP Type**.



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 Normal

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

PPPoE Username

PPPoE Password

Advanced ∨

Connect

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

Internet Settings

Network Status Connected

---End



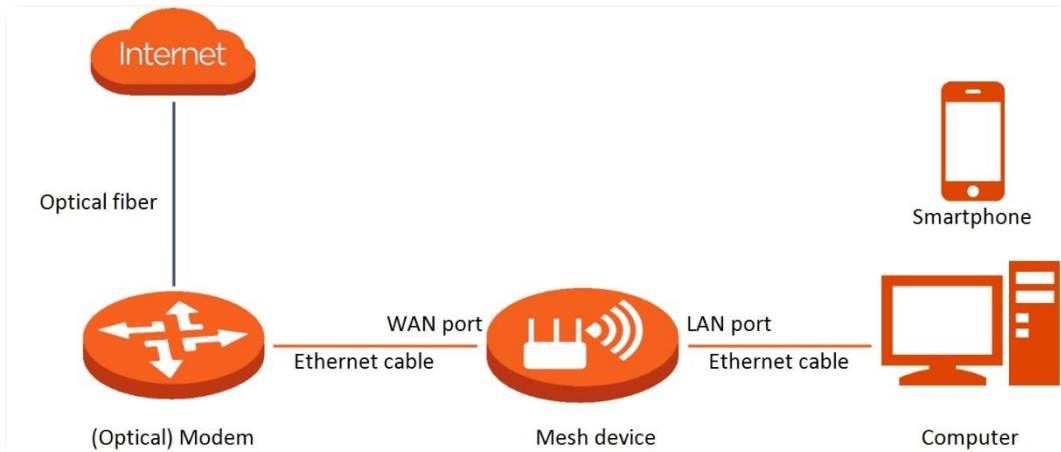
If there is no response from the remote server, troubleshoot as prompted under **Network Status** on the **Internet Settings** page.

5.3 Access the internet through a dynamic IP address

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

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

The application scenario is shown below.



To access the internet through dynamic IP address:

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

Step 2 Set **ISP Type**.



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:

Internet Connection Type:

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

Advanced ▼

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

Internet Settings

Network Status: Connected

---End

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

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

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

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

Step 2 Set **ISP Type**.



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: . . .

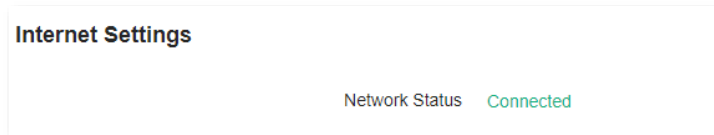
Primary DNS: . . .

Secondary DNS: . . .

Advanced ▾

Connect

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



---End

5.5 Set up dual access connection

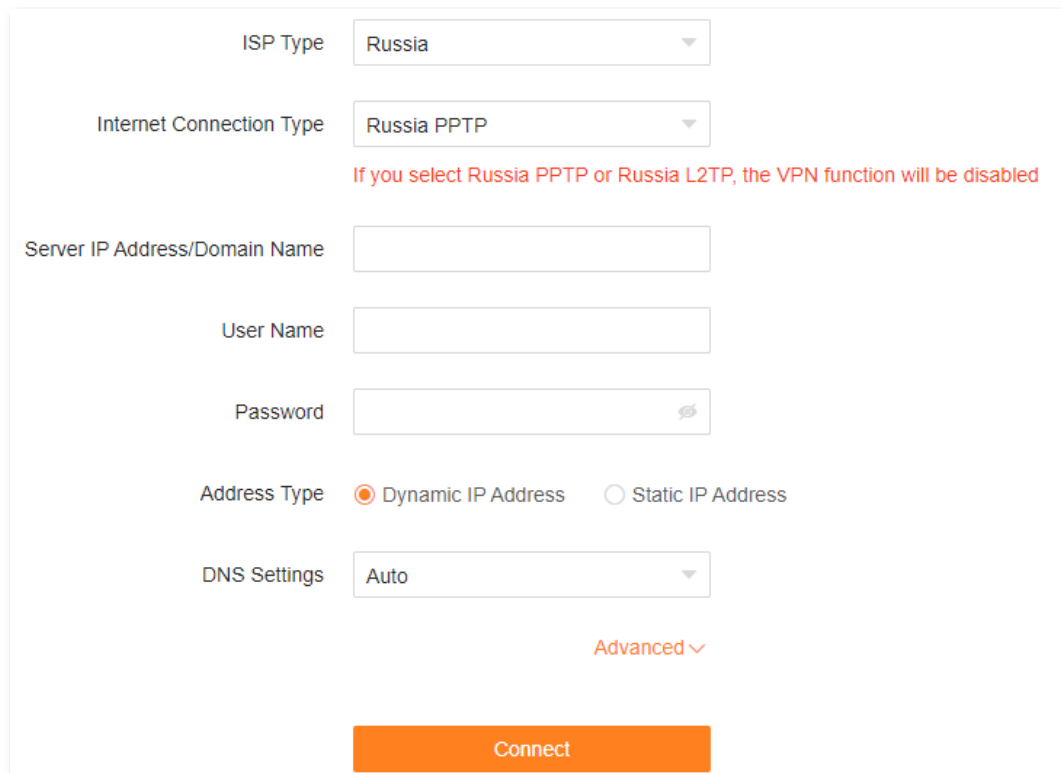
In countries like Russia, the ISP may require you to set up dual access. One is for access to the internet through PPPoE, PPTP or L2TP, and the other is for access to the “local” resources where the ISP is located through DHCP or static IP address. If your ISP provides such connection information, you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

To set up dual access connection:

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

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

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

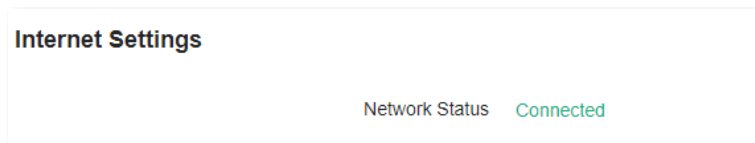
A screenshot of the "Internet Settings" configuration form. It includes the following fields and options:

- ISP Type: A dropdown menu with "Russia" selected.
- Internet Connection Type: A dropdown menu with "Russia PPTP" selected.
- A red warning message: "If you select Russia PPTP or Russia L2TP, the VPN function will be disabled".
- Server IP Address/Domain Name: An empty text input field.
- User Name: An empty text input field.
- Password: An empty password input field with a visibility toggle icon.
- Address Type: Two radio buttons, "Dynamic IP Address" (selected) and "Static IP Address".
- DNS Settings: A dropdown menu with "Auto" selected.
- An "Advanced" link with a downward arrow.
- A large orange "Connect" button at the bottom.

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

Step 5 Click **Connect**.

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



---End

6 Wi-Fi Settings

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

This chapter includes the following sections:

[Basic Settings](#)

[Separate the 2.4 GHz and 5 GHz Wi-Fi networks](#)

6.1 Basic Settings

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

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

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	Used to enable or disable the Unify 2.4 GHz & 5 GHz function. When this function is enabled, the 2.4 GHz and 5 GHz Wi-Fi networks share the same SSID and password. WiFi-enabled clients connected to it will use the frequency with better connection quality. For details, see Separate the 2.4 GHz and 5 GHz Wi-Fi networks .
WiFi Name	Specifies the Wi-Fi network name (SSID) of the corresponding Wi-Fi network.
Security	Specifies the encryption mode supported by the Mesh device, including: <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. <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>

Parameter	Description
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>

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

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

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

- Step 1** [Log in to the web UI](#), and choose **WiFi Settings**.
- Step 2** Toggle off **Unify 2.4 GHz & 5 GHz**.
- Step 3** Set **WiFi Name** and **WiFi Password** of each WiFi network.

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

- Step 4** Click **Save**.

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 ⓘ

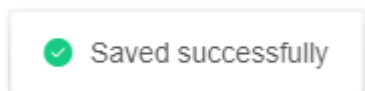
5 GHz WiFi

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.

7

Client management

This chapter 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](#)

7.1 View client information

To view information of clients:

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

Step 2 Choose **Client Management**.



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

The following page is displayed.



Client Management

All Nodes All Devices Blacklist

1	Main Network Device(1)	Current Speed	Negotiation Speed	Bandwidth Control	Operation
	MININT-UDEPFER IP Address: 192.168.0.103 MAC Address: 6C:4B:90:5F:85:0F Uptime: 1hour(s) 6minute(s) Wired	↑ 0KB/s ↓ 1KB/s	1000Mbps	Upload: Unlimited Download: Unlimited	Local Host
2	Guest Device(0)	Current Speed	Negotiation Speed	Operation	
	No Data				
3	Offline Device(1)	Current Speed	Negotiation Speed	Operation	
	<input type="checkbox"/> HUAWEI_P30-360d3356c... MAC Address: E4:FD:A1:58:69:AE	--	0Mbps	<input type="button" value="Add to blacklist"/>	

---End

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


No.	Description
1	<p>This area 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.
2	<p>This area 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.
3	<p>This area 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 20 offline clients can be displayed here. A client is displayed under Offline Device after it is disconnected from the network for 90 seconds (wired client)/60 seconds (wireless client). A client will be automatically deleted from this list if it is offline for 3 days.</p>

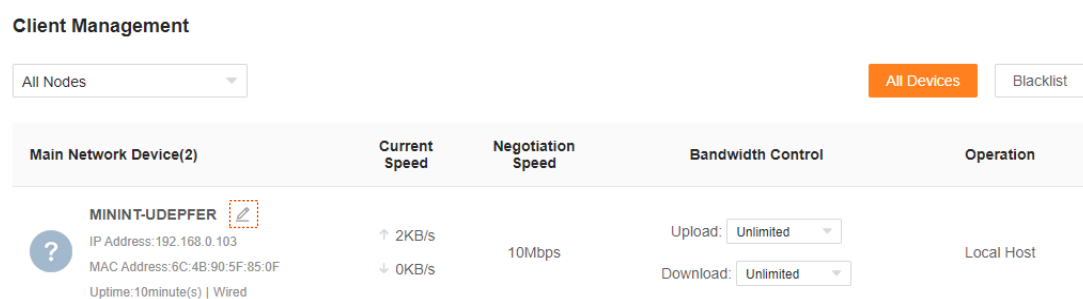
7.2 Change a client name

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

To change the name of a client:

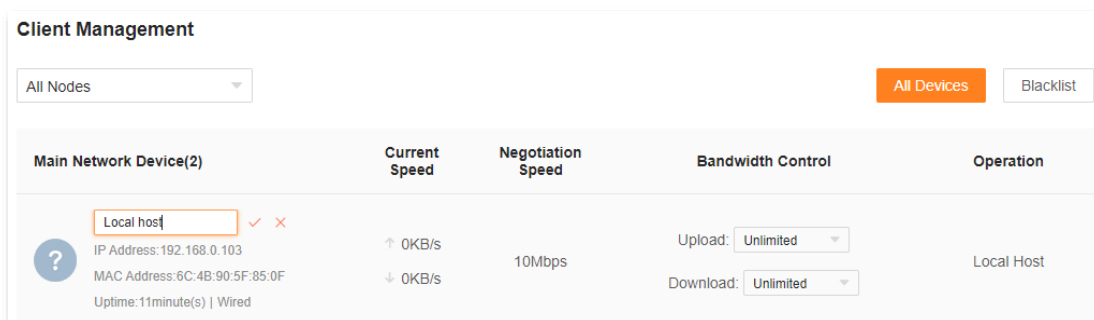
Step 1 [Log in to the web UI](#), and choose **Client Management**.

Step 2 Click  beside the client name.



The screenshot shows the 'Client Management' interface. At the top, there is a dropdown menu set to 'All Nodes' and two buttons: 'All Devices' (orange) and 'Blacklist' (grey). Below this is a table with the following columns: 'Main Network Device(2)', 'Current Speed', 'Negotiation Speed', 'Bandwidth Control', and 'Operation'. The table contains one row for a client named 'MININT-UDEPFER'. The client's details include a question mark icon, IP Address: 192.168.0.103, MAC Address: 6C:4B:90:5F:85:0F, and Uptime: 10minute(s) | Wired. The 'Current Speed' is 2KB/s (upload) and 0KB/s (download). The 'Negotiation Speed' is 10Mbps. The 'Bandwidth Control' section has 'Upload: Unlimited' and 'Download: Unlimited' dropdown menus. The 'Operation' column shows 'Local Host'. An edit icon (pencil) is visible next to the client name.

Step 3 Enter a new name and click .



This screenshot shows the same 'Client Management' interface as the previous one, but the client name has been changed to 'Local host'. The name is now enclosed in a text input field with a checkmark icon (✓) and a close icon (✗) to its right. All other details, including IP Address, MAC Address, speeds, and bandwidth controls, remain the same.

The new client name is saved.

---End

7.3 Add a client to the blacklist

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

To blacklist a client:

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

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

Client Management

All Nodes All Devices Blacklist

Main Network Device(2)	Current Speed	Negotiation Speed	Bandwidth Control	Operation
MININT-UDEPFER ? IP Address:192.168.0.103 MAC Address:6C:4B:90:5F:85:0F Uptime:14minute(s) Wired	↑ 0KB/s ↓ 0KB/s	1000Mbps	Upload: Unlimited Download: Unlimited	Local Host
HUAWEI_P30-360d3356c... IP Address:192.168.0.159 MAC Address:E4:FD:A1:58:69:AE Uptime:2minute(s) 5G	↑ 0KB/s ↓ 0KB/s	780Mbps	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

All Devices **Blacklist**

Device Name	MAC Address	Operation
HUAWEI_P30-360d3356cd98fc	E4:FD:A1:58:69:AE	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.
- A maximum of 80 clients can be blacklisted.
- The blacklist rule prevails when conflicting with the parent control rule.

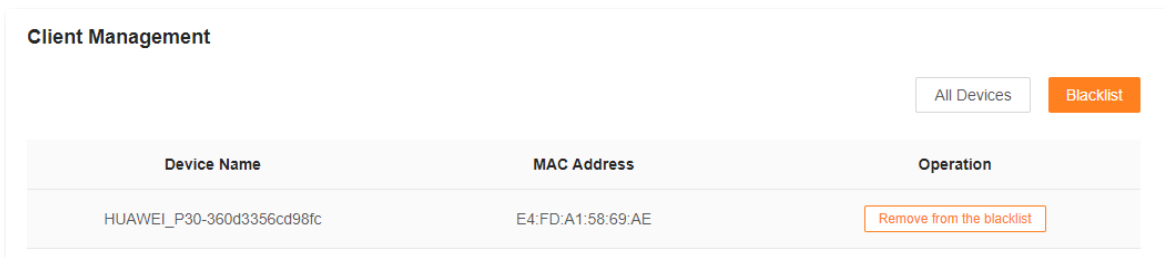
---End

7.4 Remove a client from the blacklist

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

To remove a client from the blacklist:

- Step 1** [Log in to the web UI](#), and choose **Client Management**.
- Step 2** Choose **Blacklist** on the right.
- Step 3** Click **Remove from the blacklist** under **Operation** in the line of the client to be removed from the blacklist.



- Step 4** Click **OK**.



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


---End

7.5 Delete an offline client

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

To delete an offline client:

- Step 1** [Log in to the web UI](#), and choose **Client Management**.
- Step 2** Select the offline client to be deleted, and click **Delete** on the upper right corner of **Offline Device**.

Offline Device(1)		Current Speed	Negotiation Speed	Operation
<input checked="" type="checkbox"/>	 HUAWEI_P30-360d3356c... MAC Address: E4:FD:A1:58:69:AE	--	0Mbps	<input type="button" value="Add to blacklist"/>

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

8 Parental control

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

This chapter includes the following sections:

[Create a parental control rule](#)

[Other operations on the parental control rules](#)

8.1 Create a parental control rule

8.1.1 Add a parental control rule

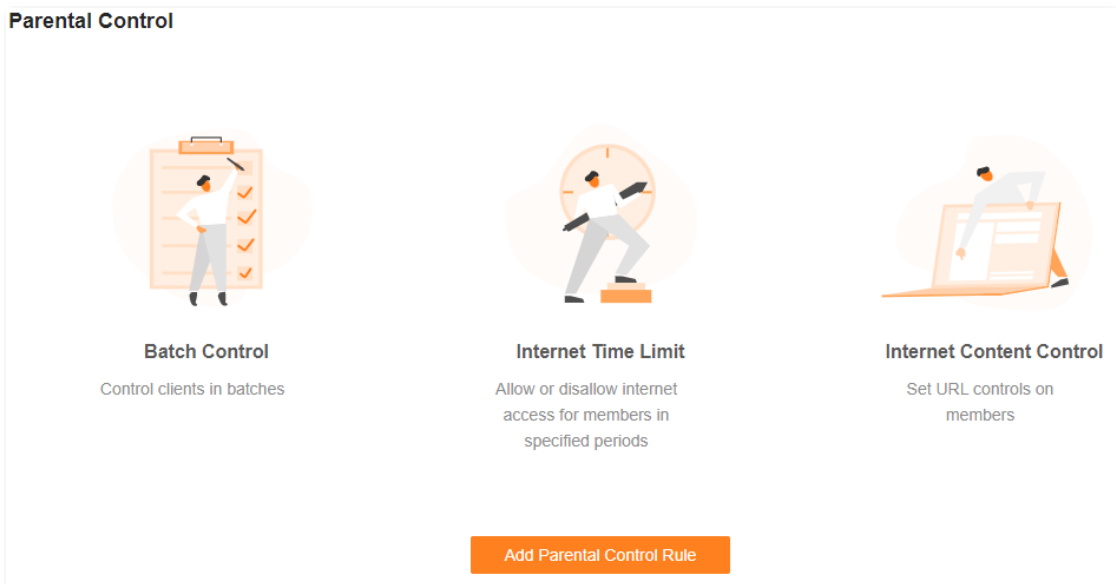


- The blacklist rule prevails when conflicting with the parent control rule.
- A maximum of 10 rules can be added.
- A maximum of 30 clients can be controlled.

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.

The screenshot shows a 'Parental Control' dashboard with a table of existing rules. A plus icon is visible in the top right corner.

Group Name	Control Period	URL Filter	Parental Control	Operation
Blacklist1	06:00-22:00 Mon. ~ Sun.	baidu	Disallowed	<input checked="" type="checkbox"/>

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

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

Internet Access Mon. ✕ +6

Add control period

URL Filter

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

URL

Add URL

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.

Parameter	Description
	Specifies whether the parental control rule takes effect.
Control Period	<ul style="list-style-type: none"> When it is toggled on, internet access is allowed only in the period specified by Internet Access. When it is toggled off, internet access is allowed all the time.
Internet Access	<p>Required when Control Period is toggled on.</p> <p>It specifies the period during which the client can access the internet.</p>
Add control period	Available when Control Period is toggled on. 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 toggled on, Filter mode and URL must be set. The parental control rule takes effect on specific websites. When it is toggled off, the URL filter rule is not applied.
Filter mode	<p>Required when URL Filter is toggled on. 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 toggled on. If you want to set multiple URLs, click this button.

8.1.2 An example of adding parental control rules

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

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


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

To add such a rule:

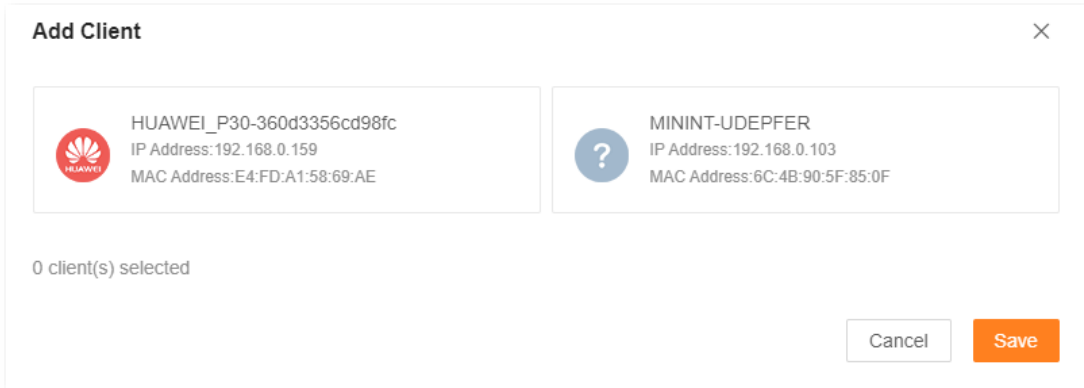
Step 1 [Log in to the web UI](#), and choose **Parental Control**.

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

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

Step 4 Click  beside **Selected clients**.

The following dialog box is displayed.

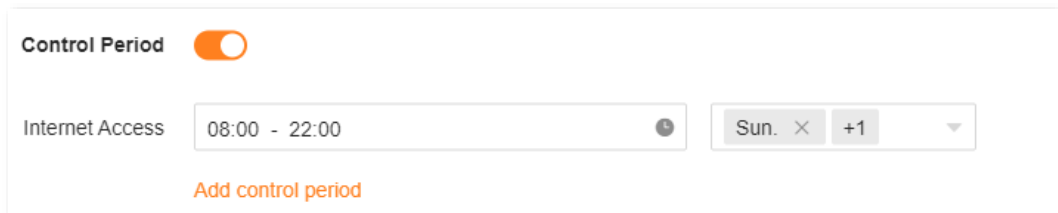


Step 5 Select the clients to which this parental control rule is applied, and click **Save**.

Step 6 Toggle on **Control Period**.

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

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



Step 8 Toggle on **URL Filter**.

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

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

URL Filter

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

URL ●

●

●

●

[Add URL](#)

Step 11 Click **Save**.

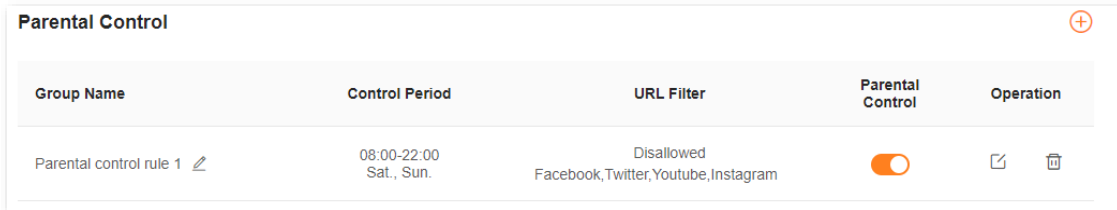
The following page is displayed, and your kid can access any websites except for Facebook, Twitter, Youtube and Instagram from 8:00 to 22:00 on weekends and cannot access the internet at all between 22:00 to 8:00 on weekends.




Parental Control +				
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

8.2 Other operations on the parental control rules




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



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.

9 More

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

[Router information](#)

[Guest Wi-Fi](#)

[Working mode](#)

[IPv6](#)

[Smart power saving](#)

[Advanced Wi-Fi Settings](#)

[Network settings](#)

[Advanced](#)

[System settings](#)

9.1 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.

The screenshot displays the 'Router Info' page in a web interface. On the left is a navigation menu with options: Router Info (selected), Guest WiFi, Working Mode, IPv6, Smart Power Saving, WiFi Settings, Network Settings, Advanced, and System Settings. The main content area is titled 'Router Info' and includes a sub-header 'You can check the information of the router here.' Below this, the page is organized into three sections: 'Basic Info', 'WAN Port Info', and 'LAN Info'. Each section contains a list of key-value pairs for various system and network parameters.

Router Info	
You can check the information of the router here.	
Basic Info	
Product Model	Mesh6X
System Time	2021-09-13 09:11:07
Uptime	38minute(s)
Firmware Version	V16.03.16.11_multi
Hardware Version	V1.1
WAN Port Info	
Internet Connection Status	Connected
Internet Connection Type	PPPoE
Uptime	37minute(s)
IP Address	172.16.200.14
Subnet Mask	255.255.255.255
Gateway	172.16.200.1
Primary DNS	114.114.114.114
Secondary DNS	223.5.5.5
MAC Address	50:2B:73:F8:F9:81
LAN Info	
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
MAC Address	50:2B:73:F8:F9:80
2.4 GHz WiFi	
Status	Visible
WiFi Name	NOVA_9JK3_A3
Security	WPA2-PSK (Recommended)
Channel	1
Bandwidth	20
MAC Address	50:2B:73:F8:F9:82
5 GHz WiFi	
Status	Visible
WiFi Name	NOVA_9JK3_A3
Security	WPA2-PSK (Recommended)
Channel	40
Bandwidth	80
MAC Address	50:2B:73:F8:F9:8A

---End

9.1.1 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. Mesh6X is used as an example here.
System Time	Specifies the current system time.
Uptime	Specifies the network connection time of the primary node.
Firmware Version	Specifies the firmware version of the primary node.
Hardware Version	Specifies the hardware version of the primary node.

9.1.2 WAN port information



This part is displayed only in the router mode.

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

Parameter description

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

9.1.3 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.
WiFi Name	Specifies the Wi-Fi name of the respective Wi-Fi network.
Security	Specifies the security mode of the respective Wi-Fi network.
Channel	Specifies the channel that the respective Wi-Fi network works in.
Bandwidth	Specifies the bandwidth of the respective Wi-Fi network.
MAC Address	Specifies the MAC address of the respective Wi-Fi network.

9.2 Guest Wi-Fi

9.2.1 Overview

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

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

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

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	Specifies the Wi-Fi name of the Mesh system's guest network. By default, NOVA_VIP is for the 2.4 GHz Wi-Fi network and NOVA_VIP_5G for the 5 GHz Wi-Fi network.
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.
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 .

9.2.2 An example of configuring the guest network

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

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

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

Assume that:

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

To achieve such a goal:

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

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

Step 3 Enable **Guest WiFi**.

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

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

Step 6 Set **WiFi Password**, which is **Tenda+245** in this example.

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

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

Step 9 Click **Save**.

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

---End

9.3 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.

Working Mode

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

Router Mode


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



[Current Mode](#)

AP 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.



[Switch 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.

9.3.1 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**.

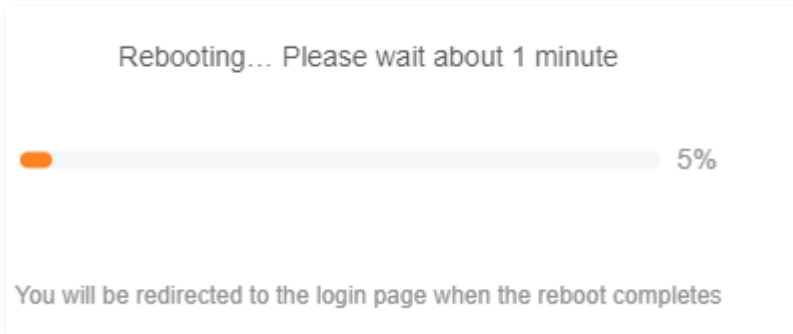
Tips

ⓘ Do you want to switch to router mode?

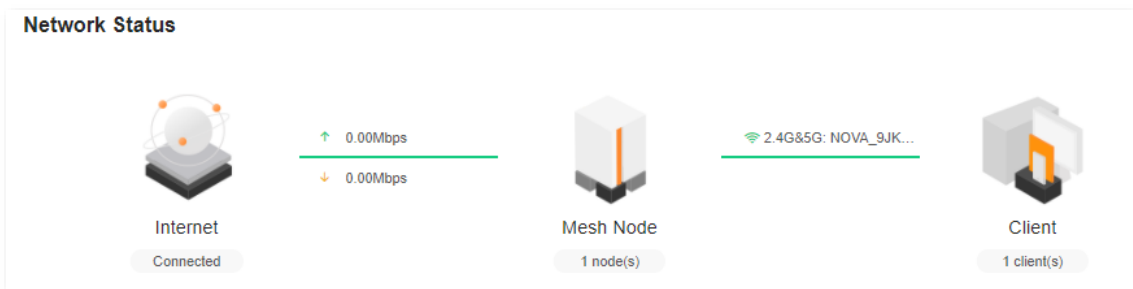
1. After the router mode is enabled, the device will reboot, and the configuration takes effect after the device is rebooted.
2. Under the router mode, you can use either the LAN IP address or `tendawifi.com` to log in to the web UI.
3. Under the router mode, the Ethernet cable for internet connection 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.



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

9.3.2 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.



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:



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

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


Current Mode



AP 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.

Switch Mode



Step 4 Click **OK**.

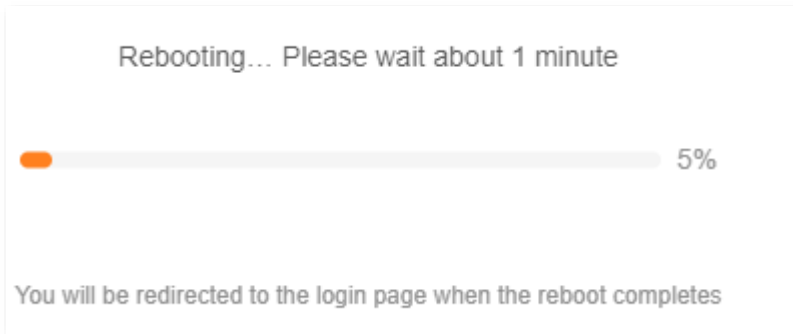
Tips

Do you want to switch to AP mode?

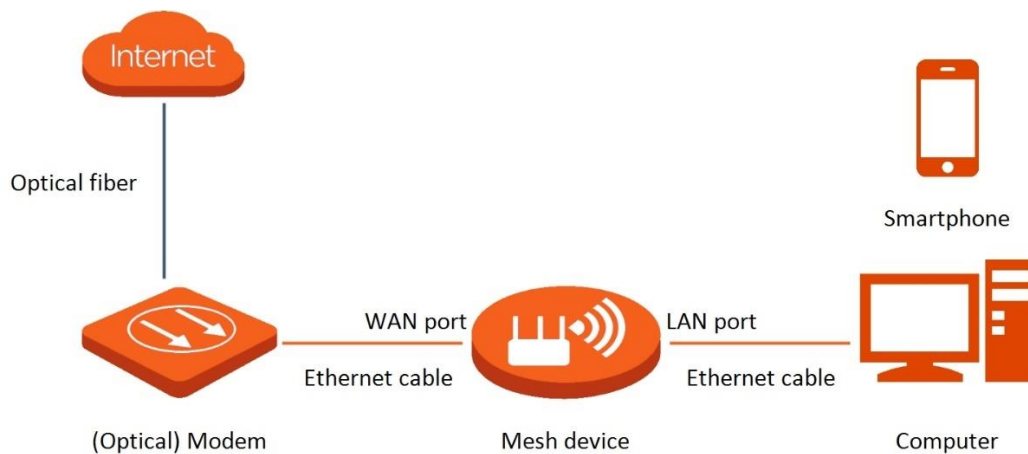
1. After the AP mode is enabled, the device will reboot, and the configuration takes effect after the device is rebooted.
2. Under the AP mode, some functions are unavailable, such as Internet Settings, Parental Control, VPN, and Port Mapping.
3. Under the AP mode, all Ethernet ports are LAN ports, and 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

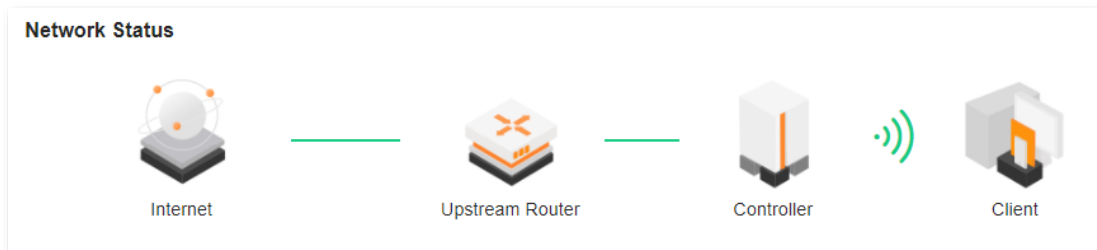
Step 5 Wait until the devices are restarted.



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



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.

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



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.

9.4 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](#)

9.4.1 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. 	DHCPv6

Scenario	Connection Type
<ul style="list-style-type: none"> You have a router that can access the IPv6 network. 	
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

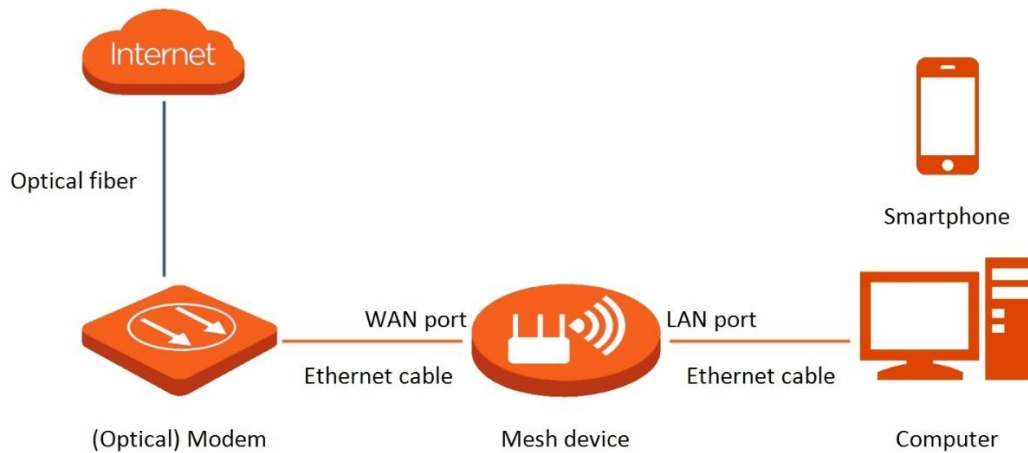


Before configuring the IPv6 function, ensure that you are within the coverage of the IPv6 network and already subscribe to the IPv6 internet service. Contact your ISP for any doubt about it.

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 **DHCP**.
- Step 5** Click **Save**.

IPv6

This device supports IPv6 and can access IPv6 network.


IPv6

IPv6 WAN

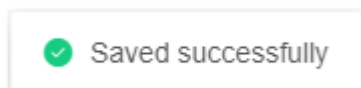
Internet Connection Type DHCP

Obtain IPv6 Prefix Delegation

Parameter description

Parameter	Description
Obtain IPv6 Prefix Delegation	<p>When the option is selected, the LAN port of Mesh device obtains the IPv6 prefix from its upstream device. The LAN port might not obtain the PD prefix if the upstream device does not support PD prefix delivery. Contact your ISP for relevant solutions.</p> <p> TIP</p> <p>The Mesh device supports NAT6. When the connection type is DHCPv6, it is recommended to disable Obtain IPv6 Prefix Delegation, and the clients obtain IPv6 prefix from the Mesh device.</p>

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



---End

IPv6 network test:

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

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

The screenshot shows the 'Test your IPv6 connectivity' website. It displays the following information:

- Your IPv4 address on the public Internet appears to be 113.104.250.31 (CHINANET-BACKBONE No.31, Jin-rong Street)
- Your IPv6 address on the public Internet appears to be 240e:fa:c68e:df00:91e2:c8c2:e4fc:c940 (CHINANET-GUANGDONG-SHENZHEN-MAN CHINANET Guangdong province Shenzhen MAN network)
- Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites. [\[more info\]](#)
- Your browser has real working IPv6 address - but is avoiding using it. We're concerned about this. [\[more info\]](#)
- It appears that you use a tunnel mechanism for either IPv4 or IPv6. If you are using a VPN, your VPN is only protecting one protocol, not both.
- [HTTPS](#) support is now available on this site. [\[more info\]](#)
- Your DNS server (possibly run by your ISP) appears to have IPv6 Internet access.

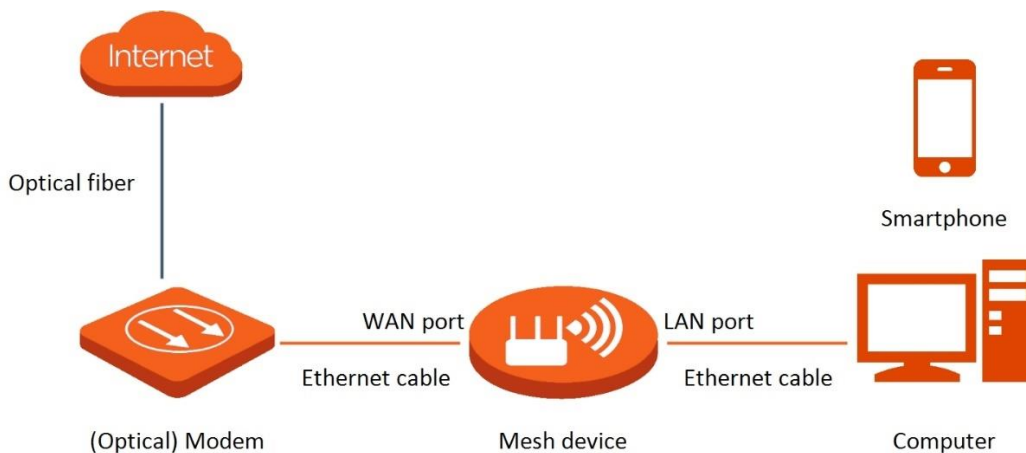
Your readiness score
10/10
for your IPv6 stability and readiness, when publishers are forced to go IPv6 only

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

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

PPPoEv6

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



Configuration procedure:

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

IPv6

This device supports IPv6 and can access IPv6 network.

IPv6

IPv6 WAN



Internet Connection Type

PPPoE Username

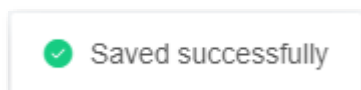
PPPoE Password

Obtain IPv6 Prefix Delegation

Parameter description

Parameter	Description
PPPoE Username	Specify the PPPoE user name and password provided by your ISP.
PPPoE Password	<p> TIP</p> <p>IPv4 and IPv6 services share the same PPPoE account.</p>
Obtain IPv6 Prefix Delegation	<p>When the option is selected, the LAN port of Mesh device obtains the IPv6 prefix from its upstream device. If the LAN port cannot obtain the PD prefix, it is because the upstream device does not support PD prefix delivery. Contact your ISP to solve this problem.</p> <p> TIP</p> <p>The Mesh device supports NAT6. When the connection type is PPPoE, it is recommended to disable Obtain IPv6 Prefix Delegation, and the clients obtain IPv6 prefix from the Mesh device.</p>

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



---End

IPv6 network test:

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

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

The screenshot shows the 'Test your IPv6 connectivity' page. It displays the following information:

- Your IPv4 address on the public Internet appears to be 113.104.250.31 (CHINANET-BACKBONE No.31,Jin-rong Street)
- Your IPv6 address on the public Internet appears to be 240e:fa:e68e:d100:91e2:e802:e4fc:0840 (CHINANET-GUANGDONG-SHENZHEN-MAN CHINANET Guangdong province Shenzhen MAN network)
- Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites. [\[more info\]](#)
- Your browser has real working IPv6 address - but is avoiding using it. We're concerned about this. [\[more info\]](#)
- It appears that you use a tunnel mechanism for either IPv4 or IPv6. If you are using a VPN, your VPN is only protecting one protocol, not both.
- HTTPS support is now available on this site. [\[more info\]](#)
- Your DNS server (possibly run by your ISP) appears to have IPv6 Internet access.

Your readiness score
10/10
 for your IPv6 stability and readiness, when publishers are forced to go IPv6 only

Click to see [Test Data](#)
 (Updated server side IPv6 readiness stats)

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

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

Static IPv6 Address

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

Configuration procedure:

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

IPv6 WAN

Internet Connection Type: Static IPv6 Address


IPv6 Address: / 64

Default IPv6 Gateway:

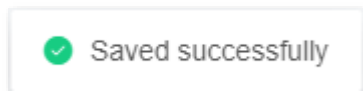
Primary IPv6 DNS:

Secondary IPv6 DNS:

Parameter description

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

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

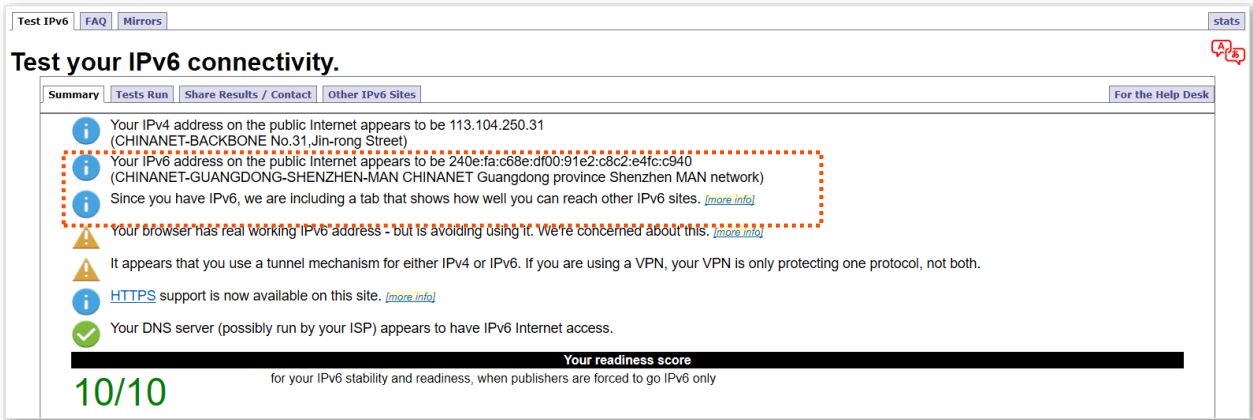


---End

IPv6 network test:

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

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



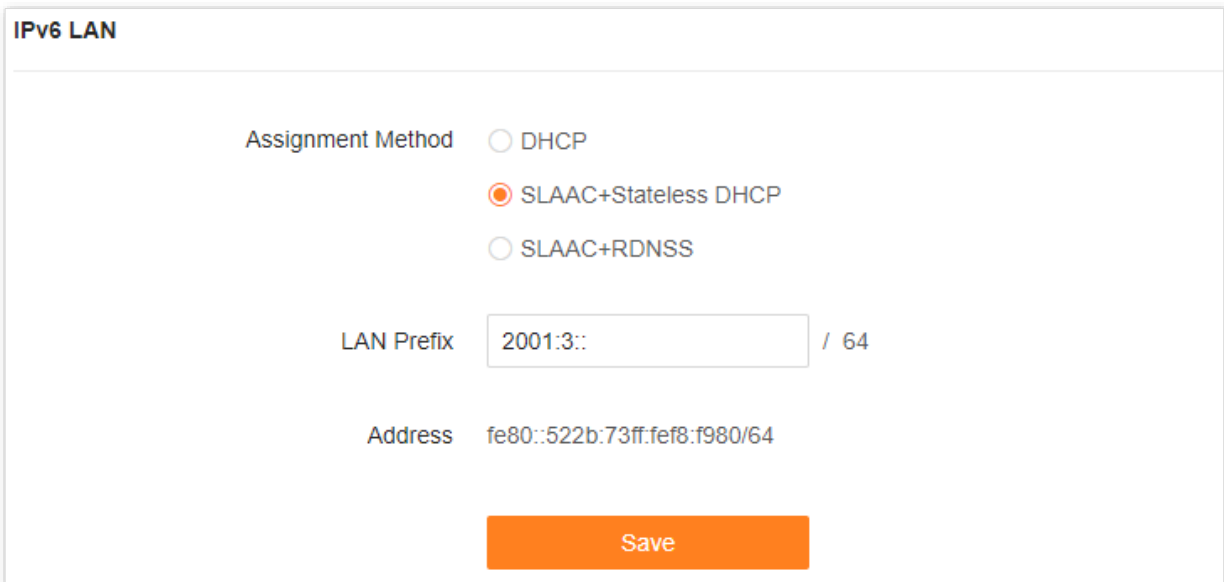
If the IPv6 network test fails, try the following solutions:

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

9.4.2 IPv6 LAN settings

To access the page, [log in to the web UI](#) of the Mesh device and choose **More > IPv6**.

You can change the IPv6 LAN settings here.



The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
Assignment Method	<p>Specifies how the Mesh device assigns IPv6 addresses to its clients.</p> <ul style="list-style-type: none"> • DHCP: Dynamic Host Configuration Protocol for IPv6 (DHCPv6) indicates that a client obtains the complete IPv6 address information from the DHCPv6 server, including the DNS server address. The gateway address is obtained through Router Advertisement (RA). • SLAAC+Stateless DHCP: Indicates that a client obtains the IPv6 prefix and gateway address through RA, and DNS server address from the DHCPv6 server. And the client generates its unique IPv6 address using the IPv6 prefix contained in the RA and interface ID which is generated using the EUI-64 method or generated randomly by the client. • SLAAC+RDNSS: Indicates that a client obtains an IPv6 prefix and gateway address through RA and DNS server address from the RDNSS option. And the client generates its unique IPv6 address using the IPv6 prefix contained in the RA and interface ID which is generated using the EUI-64 method or generated randomly by the client.
LAN Prefix	<p>Specifies the LAN IPv6 prefix.</p> <ul style="list-style-type: none"> • If you enable the Obtain IPv6 Prefix Delegation option in IPv6 WAN settings, the Mesh device obtains its LAN IPv6 prefix from its upstream device. • If you disable the Obtain IPv6 Prefix Delegation option in IPv6 WAN settings, you can configure the LAN IPv6 prefix manually.

9.5 Smart power saving

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



TIP

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

To configure the power saving mode:

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

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

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

- To turn on all indicators, select **Enable**.
- To turn off all indicators all the time, select **Disable**.

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

Step 4 Click **Save**.

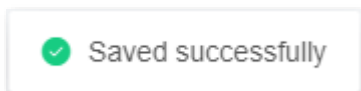
LED Indicator

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

LED Indicator

Turn Off at

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



---End

9.6 Advanced Wi-Fi Settings

9.6.1 Channel & bandwidth

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



In order not to influence 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>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.
Network Mode	<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.</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>
Bandwidth	<p>Specifies the bandwidth of the wireless channel of a Wi-Fi network. Please change the default settings only when necessary.</p> <ul style="list-style-type: none"> • 20MHz: Indicates that the channel bandwidth used by the 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. • 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.

9.6.2 WPS

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

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



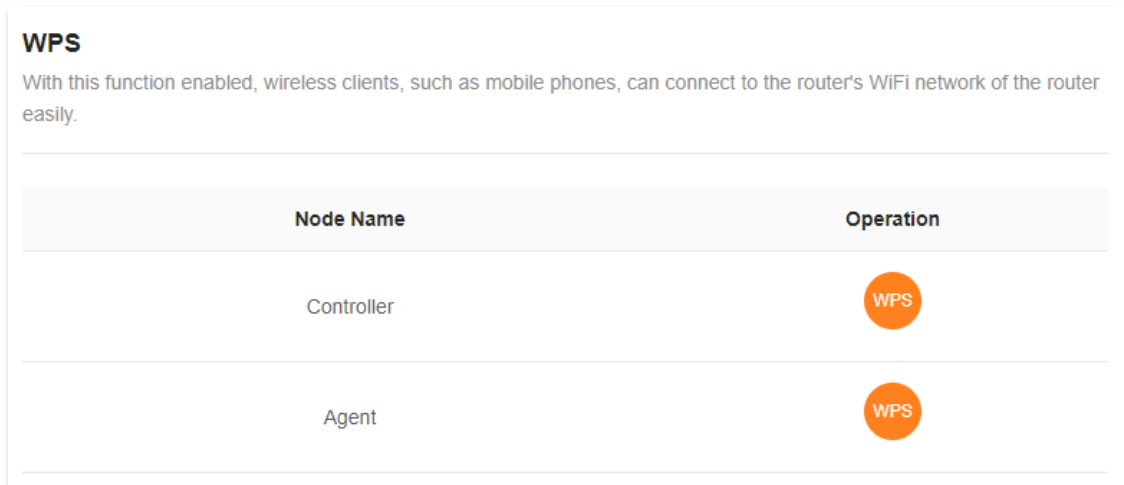
- This function only applies to WPS-enabled Wi-Fi devices. It is enabled by default and cannot be disabled.
- Wi-Fi networks encrypted with WPA3 cannot be connected through WPS.
- The WPS negotiation times out in 120 seconds. The **WPS** button is disabled during WPS negotiation.

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

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

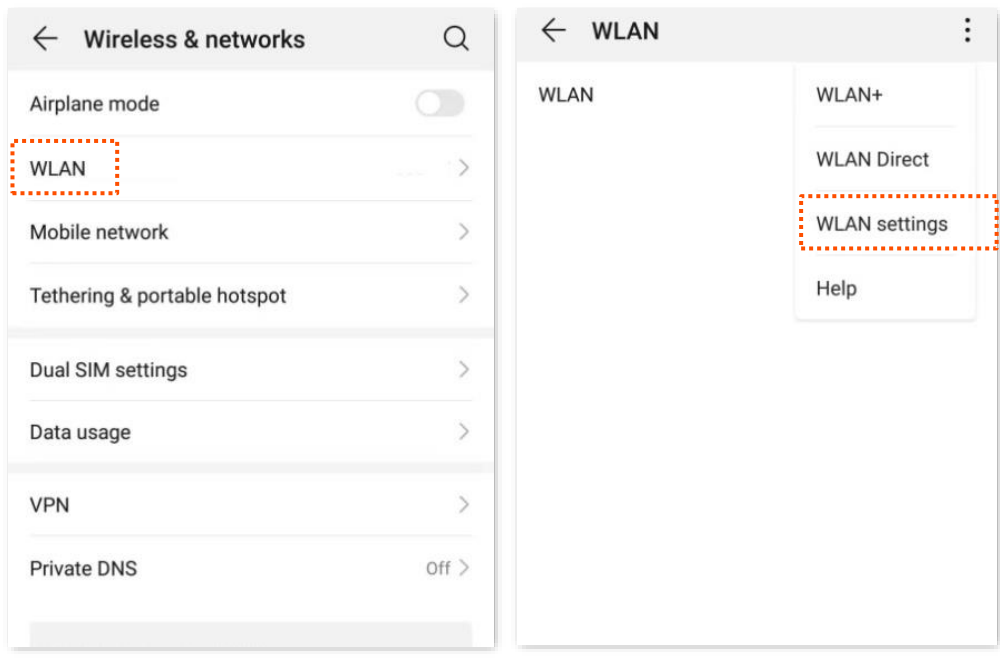
Step 2 Choose **More > WiFi Settings > WPS**.

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

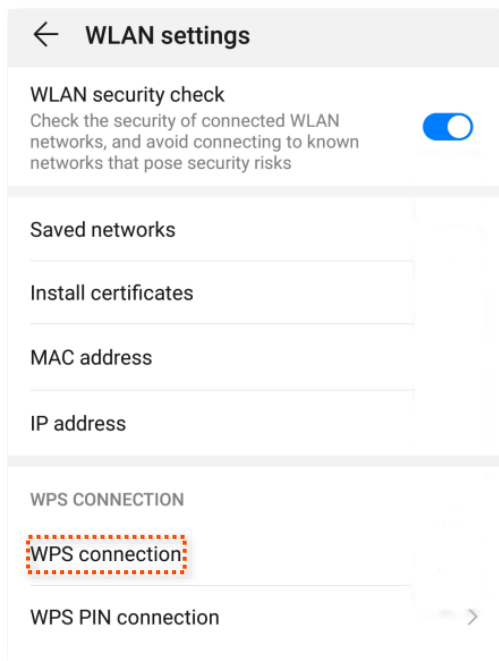


Step 4 Configure the WPS function on your WiFi-enabled devices **within 2 minutes**. Configuration on various devices may differ (Example: HUAWEI P10).

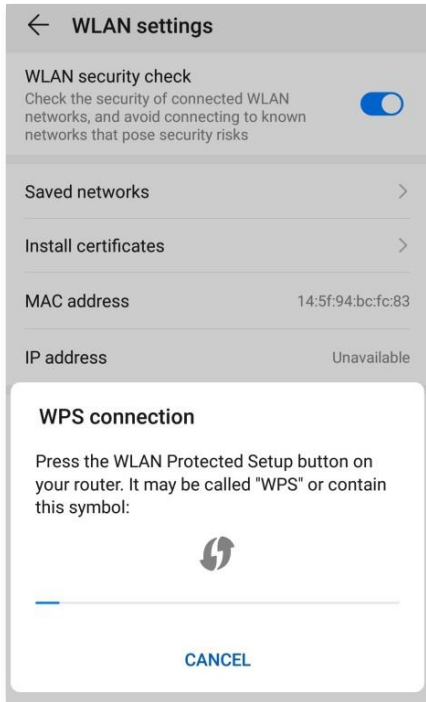
1. Find **WLAN** settings on your phone.
2. Tap , and choose **WLAN settings**.



3. Choose WPS connection.



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



---End

9.6.3 MESH button

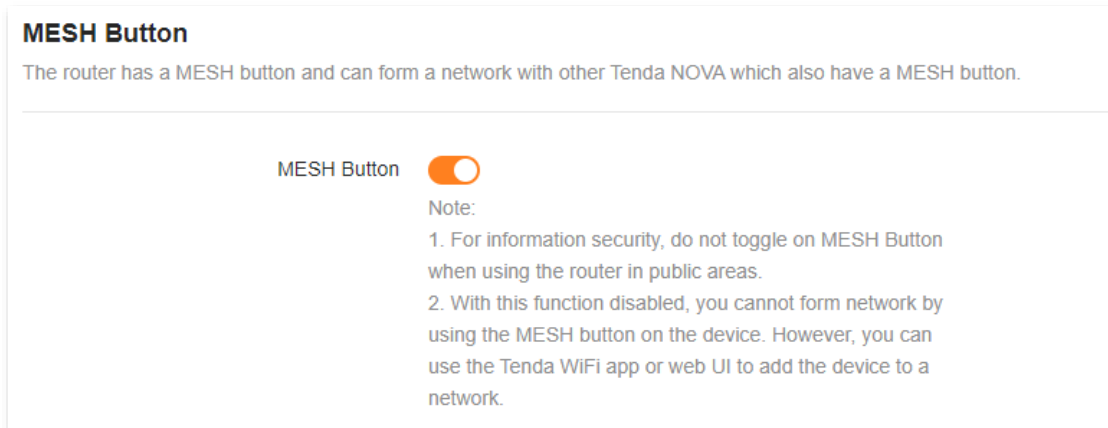
You can use the **MESH** button to network your NOVA devices which also have a **Mesh** button. On this page, you can enable or disable the **MESH** button as required.



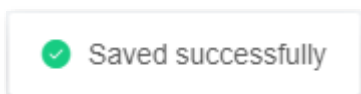
- For information security, do not toggle on **MESH Button** when using the Mesh device in public areas.
- With this function disabled, you cannot form a network by using the **MESH** button on the device. However, you can use the Tenda WiFi app or web UI to add the device to a network.

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

- Step 1** [Log in to the web UI.](#)
- Step 2** Choose **More > WiFi Settings > MESH Button.**
- Step 3** Toggle on or off **MESH Button.**



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



---End

9.7 Network settings

9.7.1 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 192.168.0. -

Lease Time ⓘ

DNS





Static IP Reservation List +

Device Name	IP Address	MAC Address	Operation
123	192.168.0.143	c0:9a:d0:5b:28:70	<input type="button" value="✎"/> <input type="button" value="✖"/>

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>The available options include:</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:

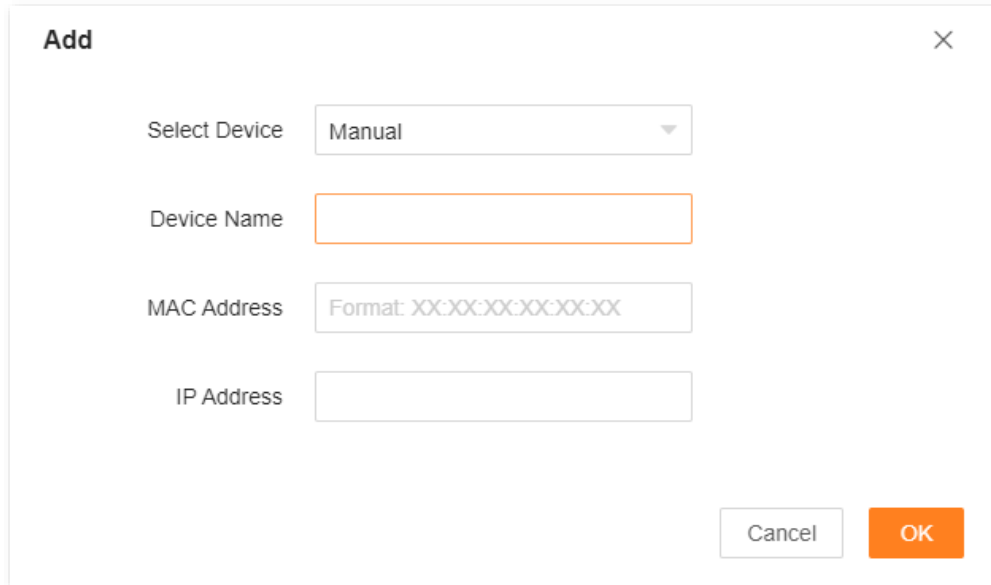
Step 1 [Log in to the web UI.](#)

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

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

Step 4 Set **Select Device.**

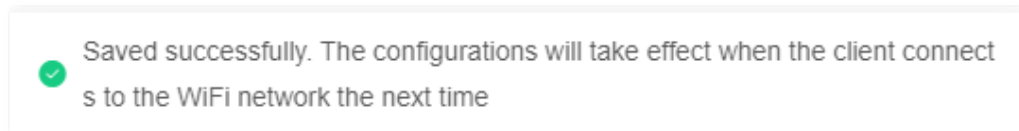
- You can directly select a client from the drop-down list box, which requires no further settings on **MAC Address** and **IP Address**.
- If you select **Manual**, you need to set **Device Name**, **MAC Address**, and **IP Address** manually.



The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. It contains four input fields: "Select Device" with a dropdown menu showing "Manual", "Device Name" with an empty text box, "MAC Address" with a text box containing the placeholder "Format: XX:XX:XX:XX:XX:XX", and "IP Address" with an empty text box. At the bottom right, there are two buttons: "Cancel" and "OK".

Step 5 Click **OK**.

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

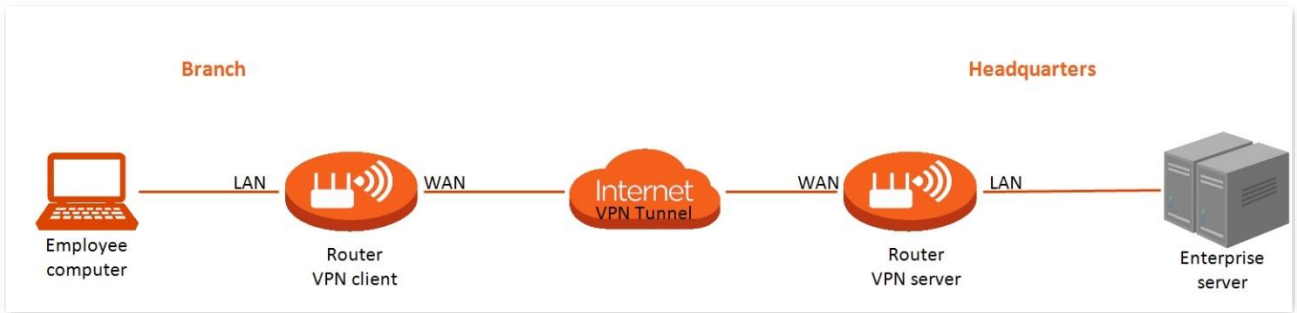


---End

9.7.2 VPN

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

The typology of a VPN network is shown below.



PPTP server

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

To access the configuration page, [log in to the web UI](#) of the 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 -

MPPE Encryption

[Save](#)

PPTP Account +





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

- **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:

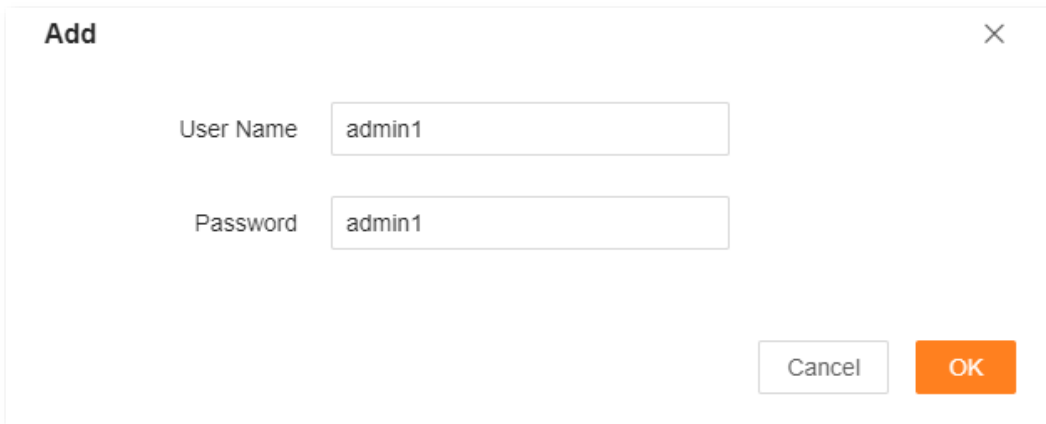
Step 1 [Log in to the web UI](#).

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".

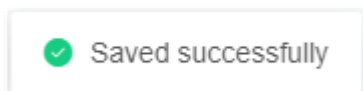
Step 5 Click . Set **User Name** and **Password** for the PPTP server, which are both **admin1** in this example. Then, click **OK**.



The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. It contains two text input fields: "User Name" with the value "admin1" and "Password" with the value "admin1". At the bottom right, there are two buttons: "Cancel" and "OK".


Step 6 Click **Save**.

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



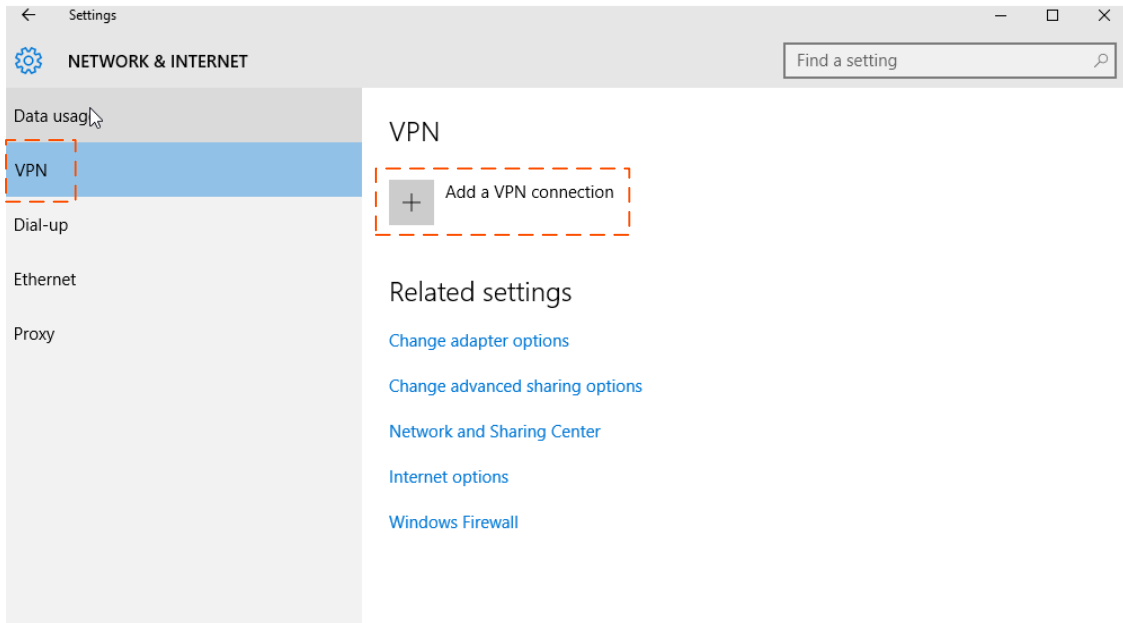
---End

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**.

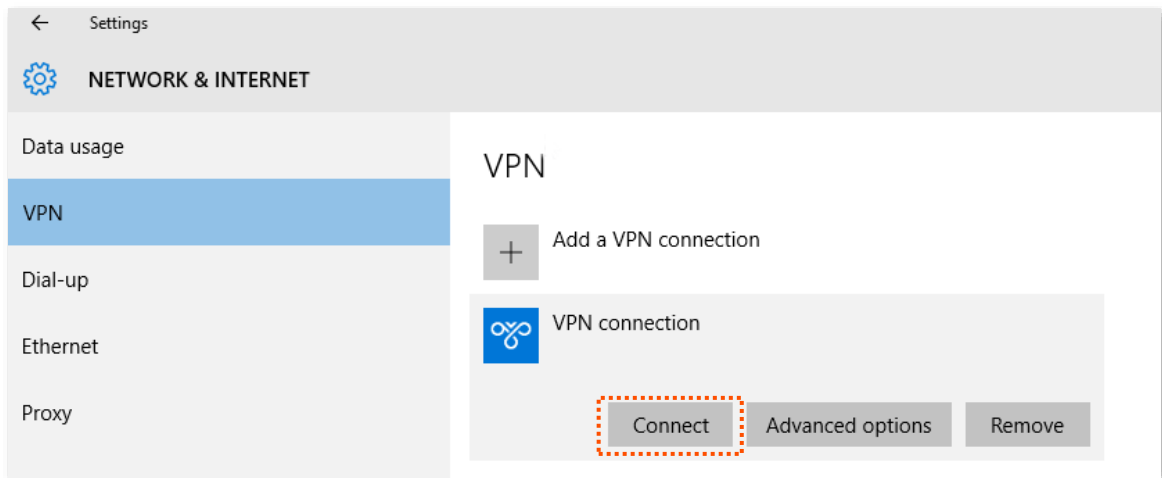



Step 3 Configure the VPN parameters.

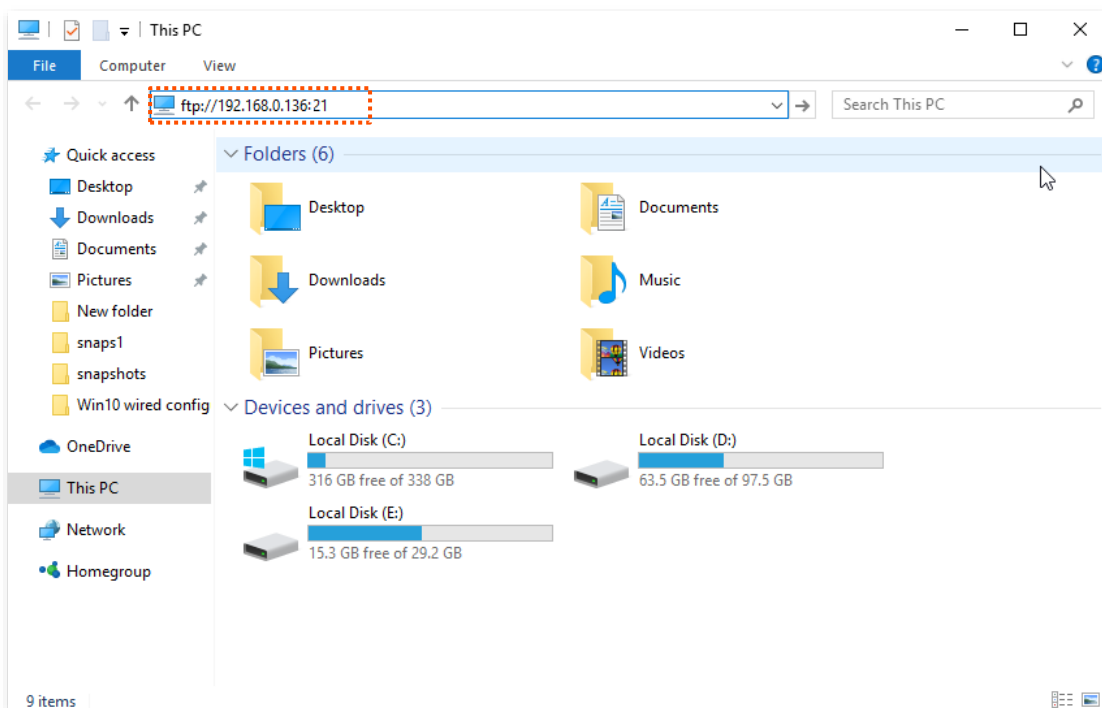
1. Enter a connection name, such as **VPN connection**.
2. Enter the server address, which is **113.88.112.220** in this example.
3. Select a VPN type, which is **Point to Point Tunneling Protocol (PPTP)** in this example.
4. Select a type of sign-in info, which is **User name and password** in this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

A screenshot of the 'Add a VPN connection' dialog box in Windows. The dialog has a blue background and contains several input fields and dropdown menus. The 'Connection name' field contains 'VPN connection'. The 'Server name or address' field contains '113.88.112.220'. The 'VPN type' dropdown menu is set to 'Point to Point Tunneling Protocol (PPTP)'. The 'Type of sign-in info' dropdown menu is set to 'User name and password'. The 'User name (optional)' field contains 'admin1'. The 'Password (optional)' field contains a series of dots. At the bottom right, there are 'Save' and 'Cancel' buttons.

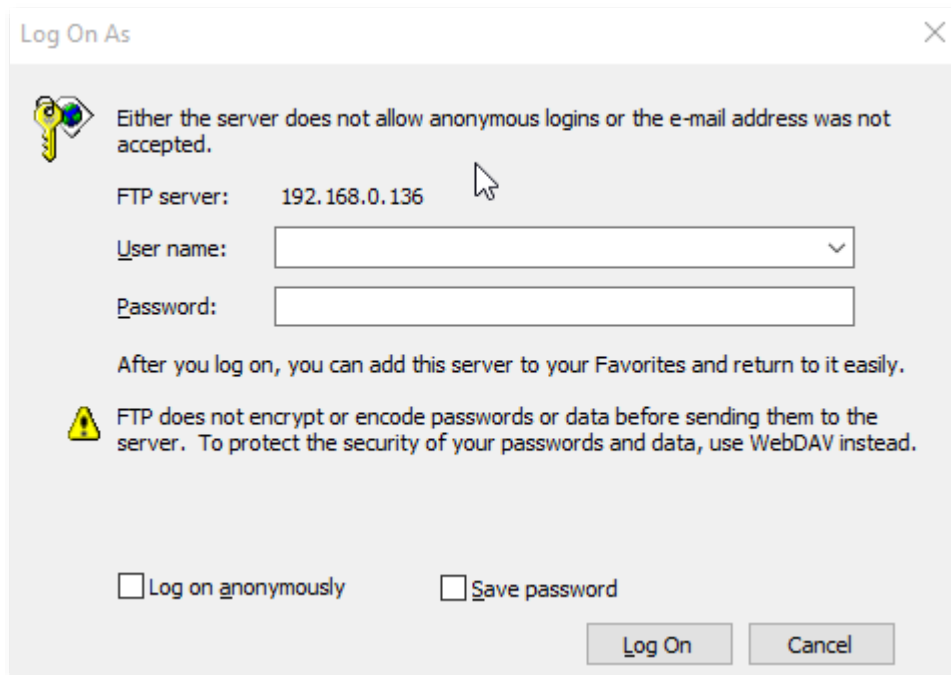
Step 4 Find the VPN connection added, and click **Connect**.



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



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



---End

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

PPTP/L2TP client

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

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

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

Parameter description

Parameter	Description
PPTP/L2TP Client	Used to enable or disable the PPTP/L2TP client function.
Client Type	Specifies the client type that the Mesh device serves as, either PPTP or L2TP. <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 Address/Domain Name	Specifies the IP address or domain name of the PPTP/L2TP server that the Mesh device connects to. Generally, when a Mesh device serves as the PPTP/L2TP server at the peer side, the domain name or IP address should be that of the WAN port whose PPTP/L2TP server function is enabled.
User Name	Specifies the user name and password that the PPTP/L2TP server assigns to the PPTP/L2TP clients.
Password	
Status	Specifies the connection status of the VPN connection.

- **Access VPN resources with the Mesh device**

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

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

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

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

Configuration procedure:

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

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

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

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

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

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

Step 7 Click **Save**.

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

---End

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

9.7.3 IPTV

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

You can set the multicast and STB functions here.

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

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

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

IPTV

You can configure multicast and IPTV functions here.

Multicast

STB

VLAN

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 ▾

The following table describes the parameters displayed on this page.

Parameter description

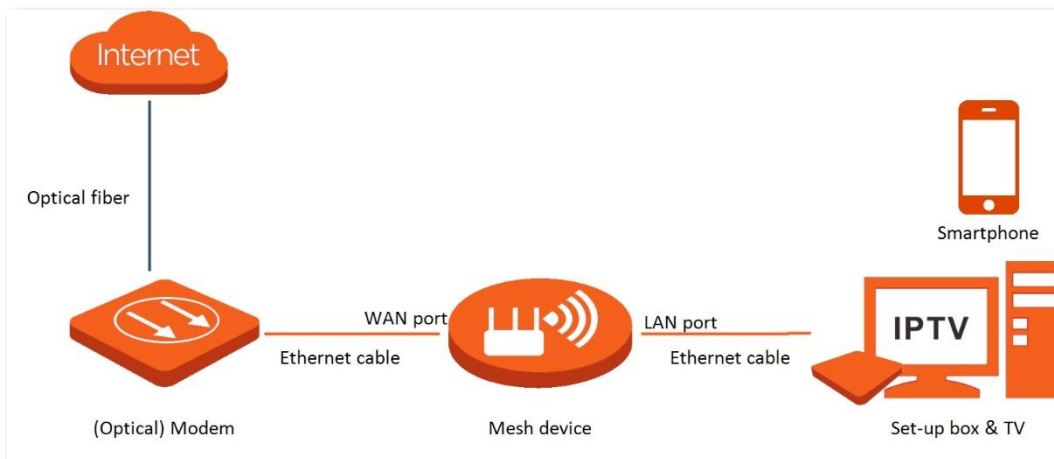
Parameter	Description
Multicast	Used to enable or disable the multicast function.
STB	Used to enable or disable the IPTV function of the Mesh device. When this function is enabled, the port LAN3/IPTV can be used only as an IPTV port and be connected to an IPTV set-top box.
VLAN	Specifies the VLAN ID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

Watch IPTV programs through the Mesh device

Scenario: The IPTV service is included in your broadband service. You have obtained the IPTV account and password from your ISP, but no VLAN information.

Goal: Watch IPTV programs through the Mesh device.

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



Configuration procedure:

Step 1 Set your Mesh device.

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

IPTV

You can configure multicast and IPTV functions here.

Multicast

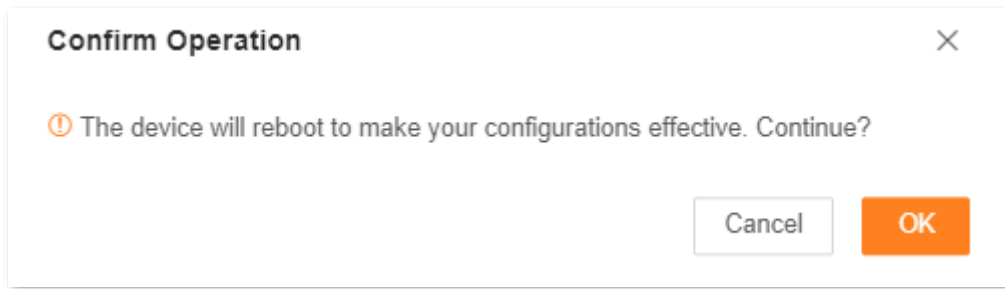
Once enabled, you can watch the multicast video source on the WAN side of the router from your client.

STB

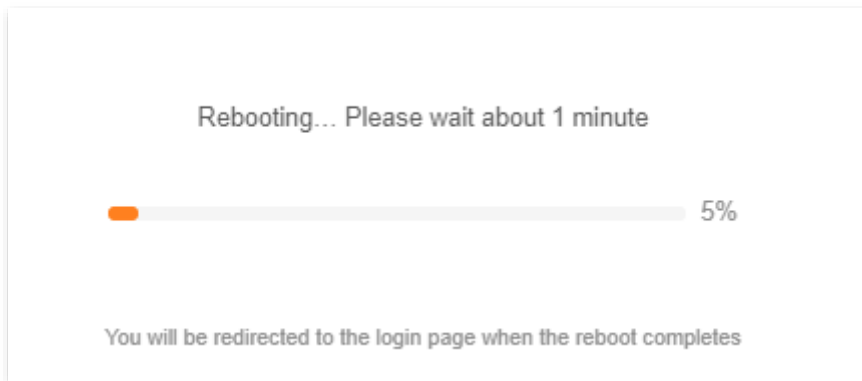
Connect the IPTV STB to the IPTV port of the router.

VLAN

5. Click **OK**.



Wait until the Mesh device is restarted.



Step 2 Configure the set-top box.

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

---End

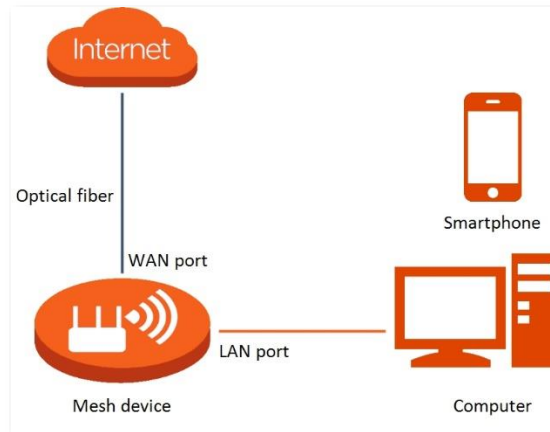
After completing the configuration, you can watch IPTV programs on your TV.

Watch multicast videos through the Mesh device

Scenario: You have the address of multicast videos.

Goal: You can watch multicast videos.

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



Configuration procedure:

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

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.

9.7.4 WAN parameters

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

To access the configuration page, [log in to the web UI](#) of the 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.
100 Mbps full duplex	Indicates that the WAN port is working at the speed of 100 Mbps, and the port can receive and send data packets at the same time.
100 Mbps half duplex	Indicates that the WAN port is working at the speed of 100 Mbps, but the port can only receive or send data packets alternately.
10 Mbps full duplex	Indicates that the WAN port is working at the speed of 10 Mbps, and the port can receive and send data packets at the same time.
10 Mbps half duplex	Indicates that the WAN port is working at the speed of 10 Mbps, but the port can only receive or send data packets alternately.

9.8 Advanced

9.8.1 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 mesh

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.
ID	Specifies the ID of the Mesh node, which is automatically allocated.
Cloud Account	Specifies the account bound on your Tenda WiFi app.

9.8.2 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**.

MAC Address Filter

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

MAC Address Filter

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

Blacklist Device +

Device Name	MAC Address	Operation
No Data		

The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description	
MAC Address Filter	Used to enable or disable the MAC address filter function.	
Filter mode	Specifies the MAC address filter mode. <ul style="list-style-type: none"> • Blacklist: WiFi-enabled clients listed are unable to connect to the Wi-Fi network of the Mesh device. 	
Blacklist Device	Device Name	Specifies the name of the blacklisted client.
	MAC Address	Specifies the MAC address of the blacklisted client.
	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  .

MAC Address Filter

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

MAC Address Filter

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

Blacklist Device 

Device Name	MAC Address	Operation
No Data		

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 +

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

1 items in total

Save

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.

9.8.3 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.

9.8.4 DMZ host

Overview

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



- 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

The following table describes the parameters displayed on this page.

Parameter description

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

An example of enabling internet users to access LAN resources

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

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

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

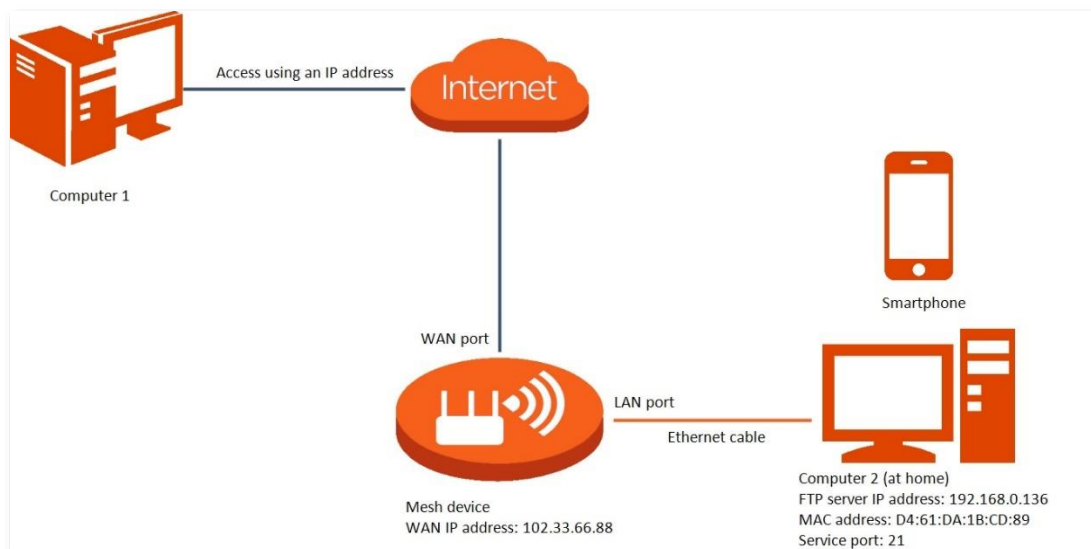
Assume that the information of the FTP server includes:

- IP address: **192.168.0.136**
- MAC address: **D4:61:DA:1B:CD:89**
- Service port: **21**
- WAN IP address of the Mesh device: **102.33.66.88**



TIP

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



Configuration procedure:

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

Step 2 Set the server host as the DMZ host.

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

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 .
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 +			
Device Name	IP Address	MAC Address	Operation
FTP server	192.168.0.136	d4:61:da:1b:cd:89	 

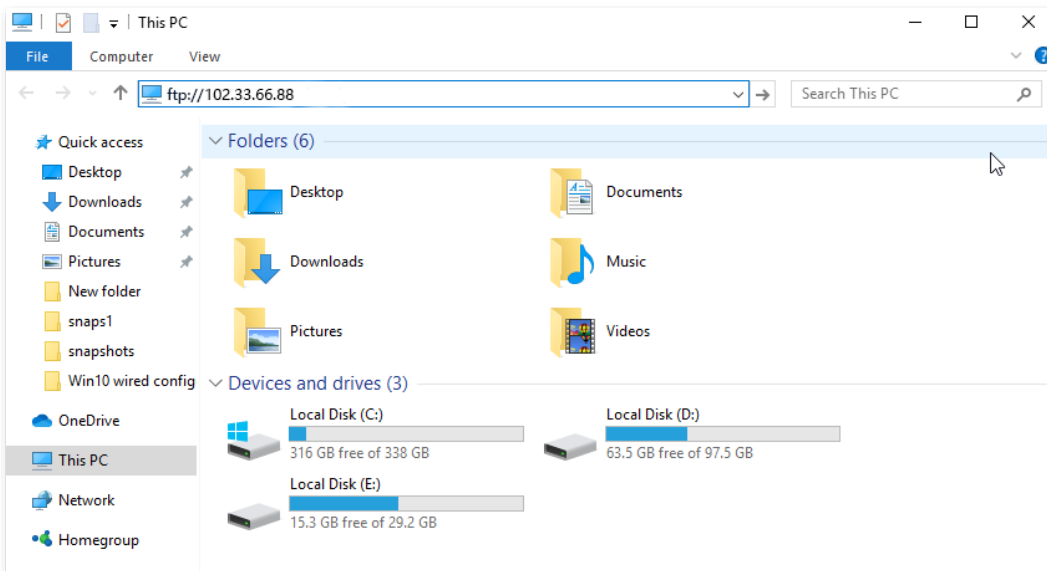
----End

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"*.

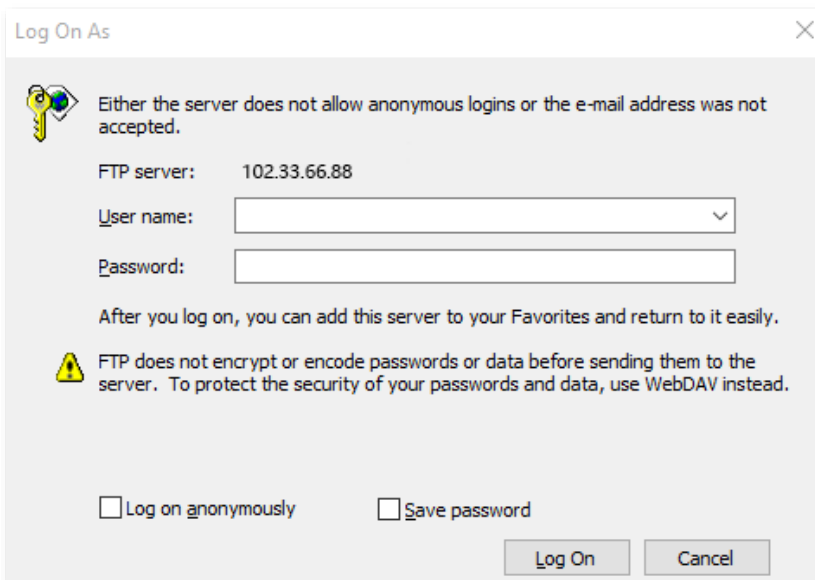
In this example, the address is “<ftp://102.33.66.88>”. You can find the WAN IP address of the Mesh device in [WAN port information](#).



If the default intranet service port number is 80, change the service port number to an uncommon one (1024–65535), such as 9999.



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



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



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

9.8.5 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.

Parameter	Description
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).
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 number from 1 to 1024 has been occupied by familiar services. It is strongly recommended to enter a port number from 1025 to 65535 to prevent conflict. • Remote web management can be achieved by visiting “<i>http://WAN IP address of the Mesh device:Port number</i>”. If the DDNS host function is enabled, the web UI can also be accessed through “<i>http://Domain name of the Mesh device’s WAN port:Port number</i>”.

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

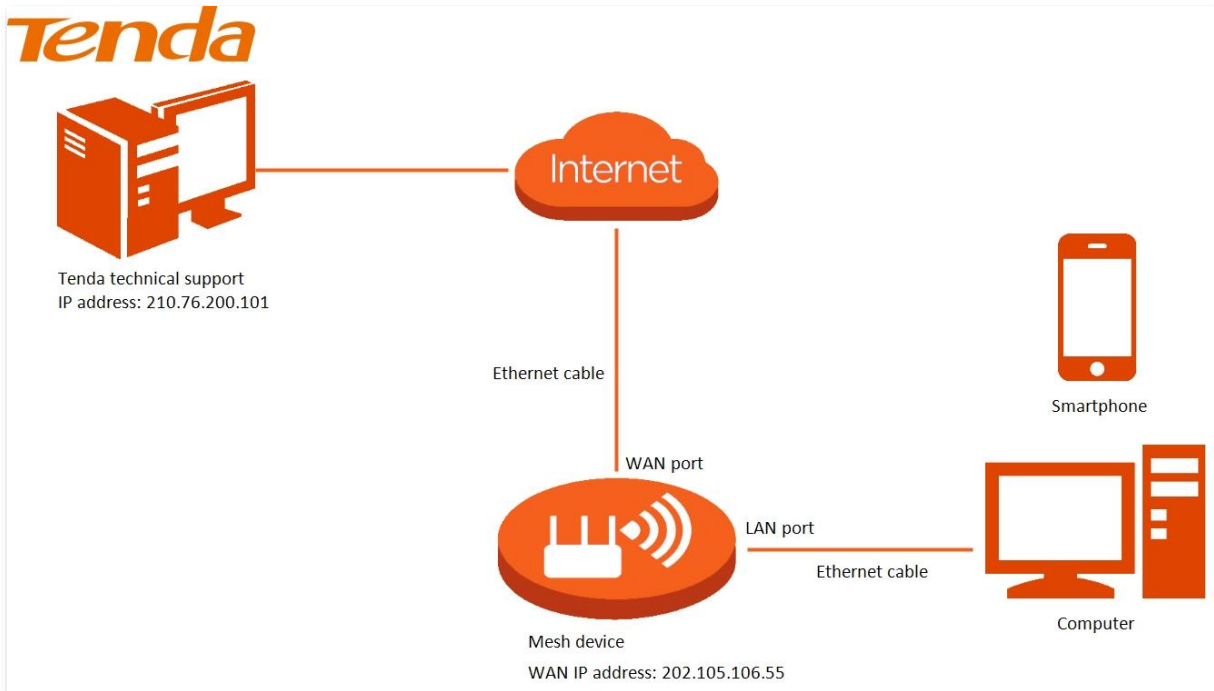
Scenario: You encounter a problem in configuring the Mesh device, and the Mesh device can access the internet.

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

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

Assume that:

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



Configuration procedure:

- Step 1** [Log in to the web UI.](#)
- Step 2** Choose **More > Advanced > Remote Web Management.**
- Step 3** Enable **Remote Web Management.**
- Step 4** Select **Specified IP Address** for **Remote Web Management.**
- Step 5** Enter the IP address that is allowed to access the web UI remotely for **Specified IP Address**, which is **210.76.200.101** in this example.
- Step 6** Click **Save.**

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

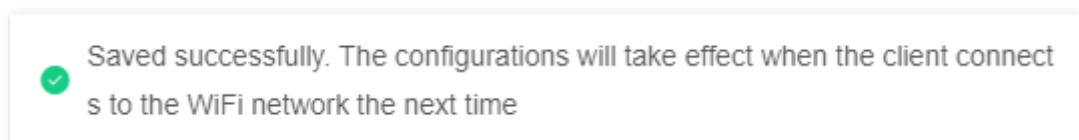
Remote IP Address Specified IP Address ▼

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.

9.8.6 Static routing

Overview

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



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

To access the configuration page, [log in to the web UI](#) of the 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 +

Destination Network	Subnet Mask	Gateway	WAN	Operation
172.16.105.0	255.255.255.0	192.168.10.20	WAN1	 
0.0.0.0	0.0.0.0	172.16.200.1	WAN1	System
172.16.200.1	255.255.255.255	0.0.0.0	WAN1	System
192.168.0.0	255.255.255.0	0.0.0.0	br0	System
224.0.0.0	240.0.0.0	0.0.0.0	br0	System
239.0.0.0	255.0.0.0	0.0.0.0	br0	System

The following table describes the parameters displayed on this page.

Parameter description

Parameter	Description
Destination Network	<p>Specifies the IP address of the destination network.</p> <p>If Destination Network and Subnet Mask are both 0.0.0.0, this is the default route.</p> <p> TIP</p> <p>When no route of packets can be found under Routing Table, the 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.

Parameter	Description
	The available options include:
Operation	 : Used to modify a static routing rule.  : Used to delete a static routing rule.

An example of adding a static routing rule

Scenario: You have a Mesh device and another two routers. Router1 is connected to the internet and its DHCP server is enabled. Router2 is connected to an intranet and its DHCP server is disabled.

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

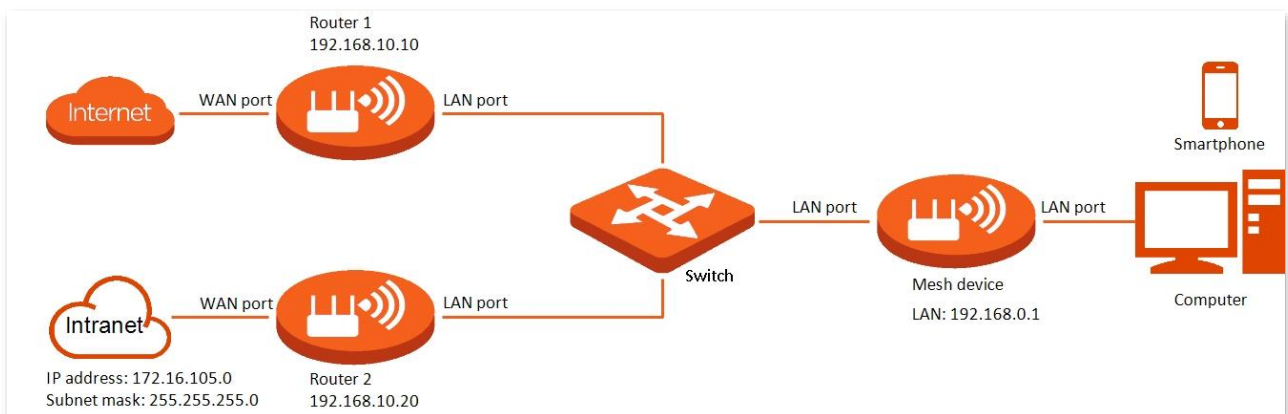
Solution: You can configure the static routing function to reach the goal.

Assume the LAN IP addresses of these devices are:

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

Information about the intranet:

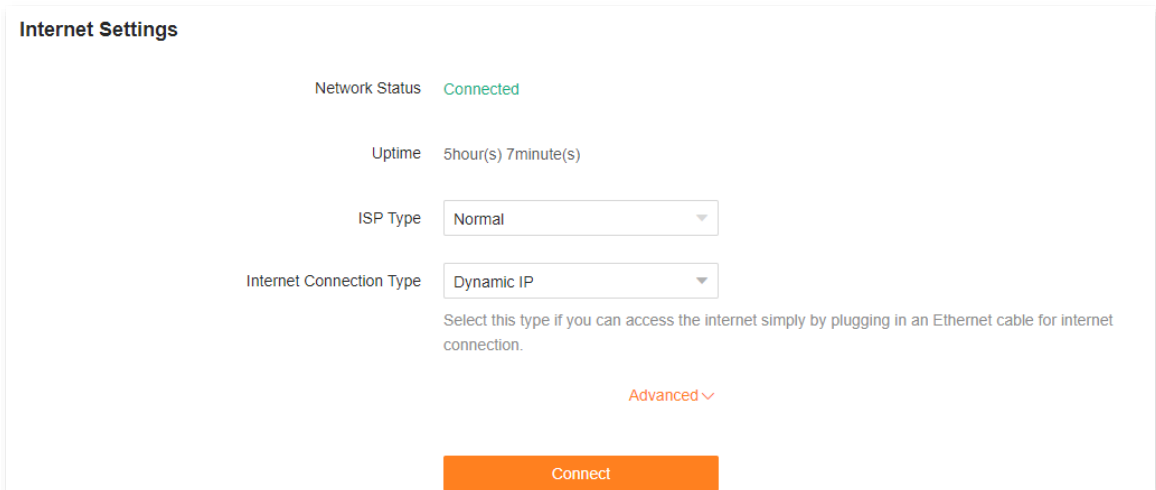
- IP address: 172.16.105.0
- Subnet mask: 255.255.255.0



Configuration procedure:

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

Step 2 Refer to [Access the internet through a dynamic IP address](#) to configure the internet access for MX6.



Internet Settings

Network Status Connected

Uptime 5hour(s) 7minute(s)


ISP Type

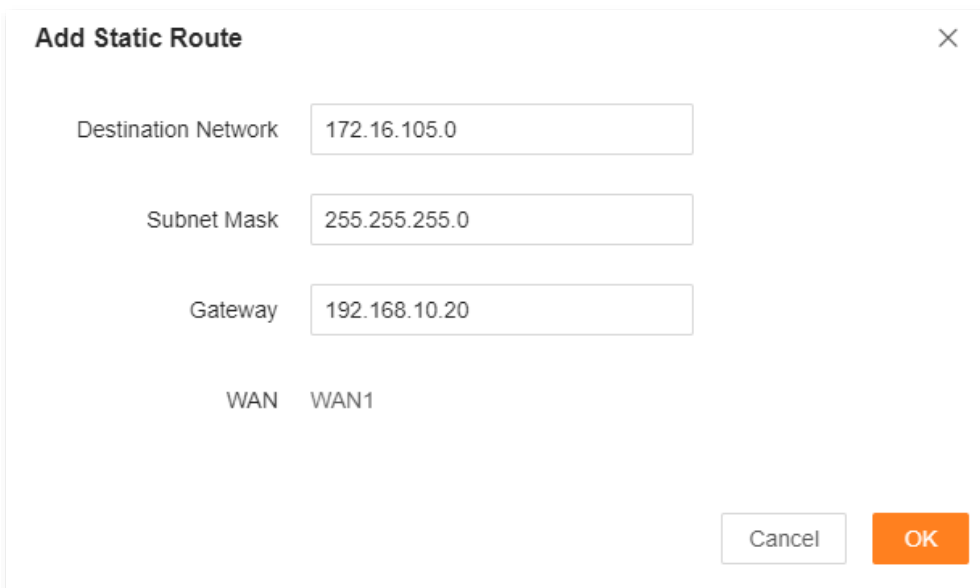
Internet Connection Type

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

[Advanced](#) ∨

Step 3 Add a static routing rule on MX6.

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



Add Static Route ×

Destination Network

Subnet Mask

Gateway


WAN

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

Static Routing

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

Routing Table +

Destination Network	Subnet Mask	Gateway	WAN	Operation
172.16.105.0	255.255.255.0	192.168.10.20	WAN1	 

---End

After completing the configuration, you can access both the internet and intranet through MX6 at the same time.

9.8.7 DDNS

Overview

DDNS normally interworks with the port mapping, DMZ host and remote web management, so that internet users can be free from the influence of dynamic WAN IP address and access the internal server or the 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

The following table describes the parameters displayed on this page.

Parameter description

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

An example of enabling internet users to access LAN resources using a domain name

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

Goal: Open the FTP server to internet users and enable family members who are not at home to access the resources of the FTP server from the internet with a domain name.

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

Assume that the information of the FTP server includes:

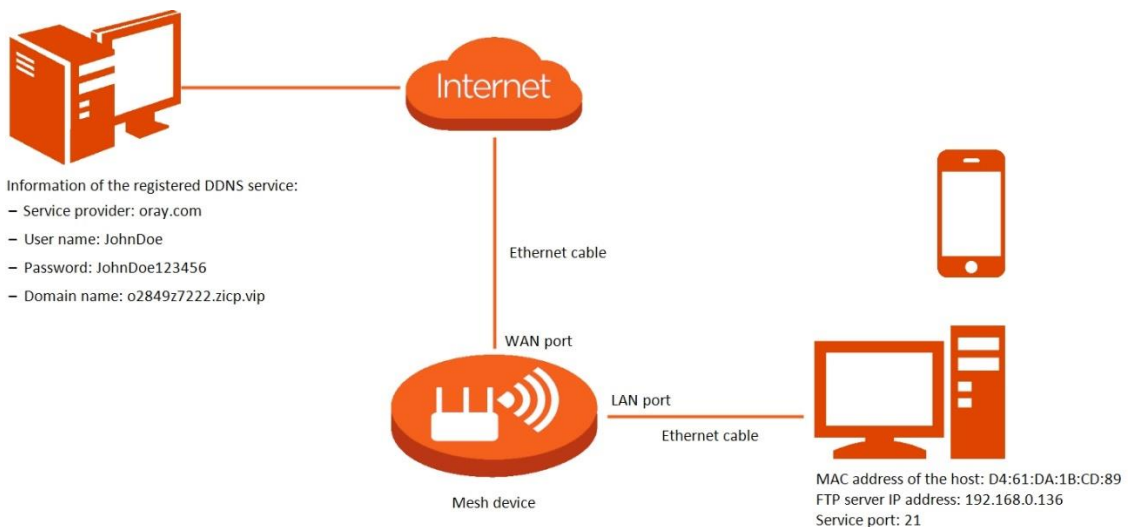
- IP address: **192.168.0.136**
- MAC address of the host: **D4:61:DA:1B:CD:89**
- Service port: **21**

Information of the registered DDNS service:

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



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

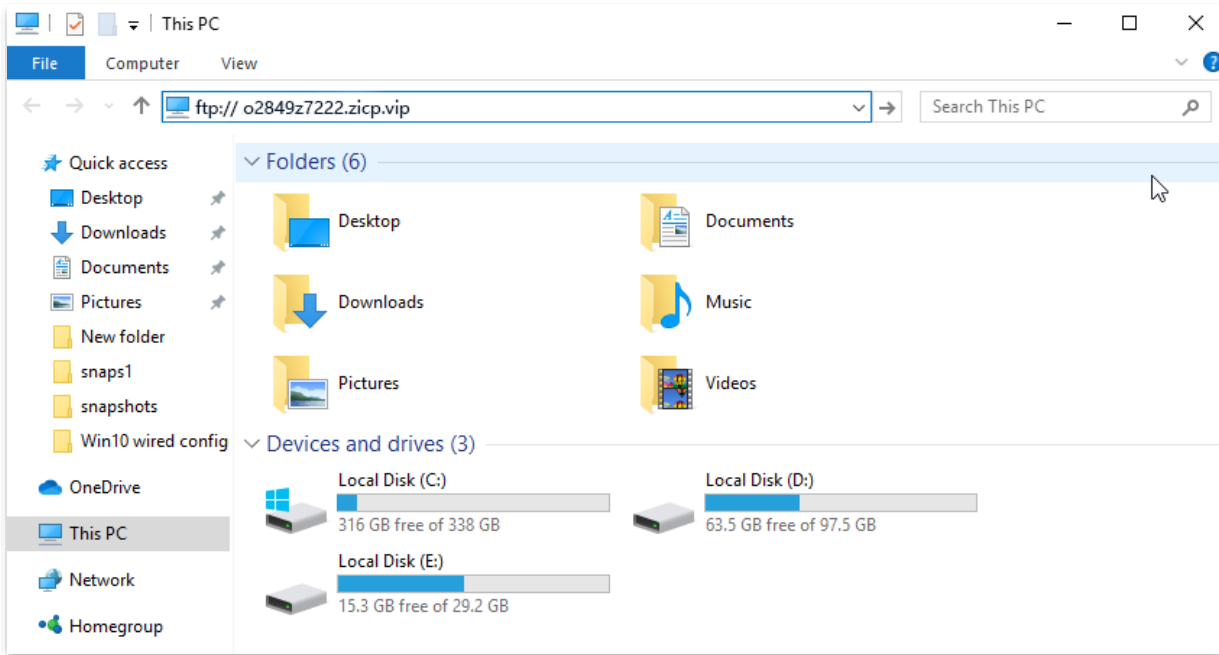
Connection Status Disconnected

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

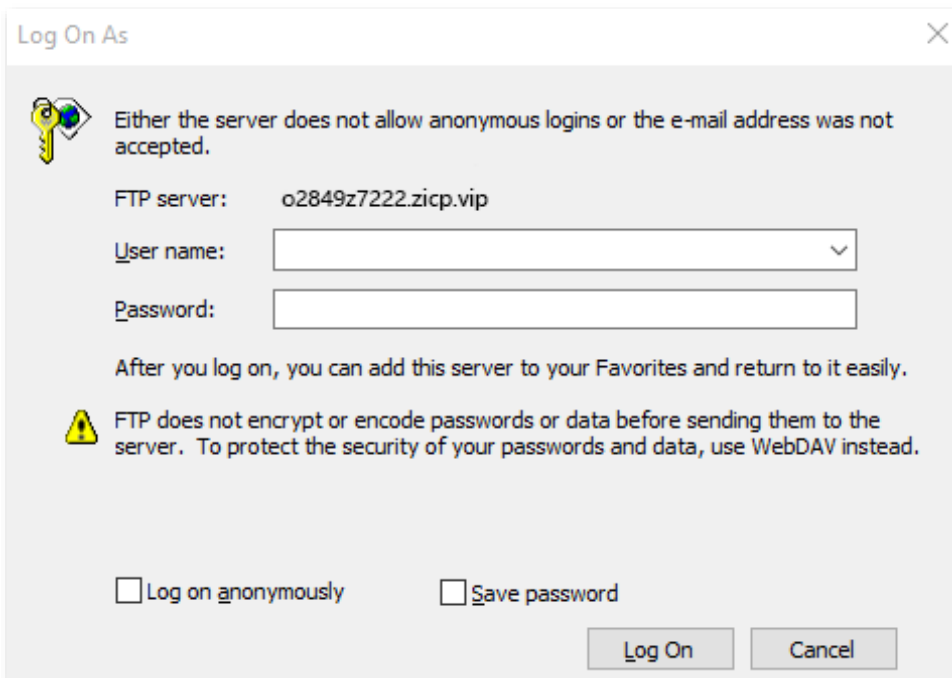
Step 3 Configure the port mapping function by following the steps in [Port mapping](#).

---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.





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

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

9.8.8 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.

Parameter	Description
Internal Host	Specifies the address of inner host to receive and send responses.
Internal Port	Specifies the host port which needs to be mapped.
Protocol	Specifies the mapping protocol.

9.8.9 Port mapping

Overview



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

To access the configuration page, [log in to the web UI](#) of the 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 +

Internal IP Address	Internal Port	External Port	Protocol	Operation
192.168.0.103	21	21	TCP&UDP	 

The following table describes the parameters displayed on this page.

Parameter description

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

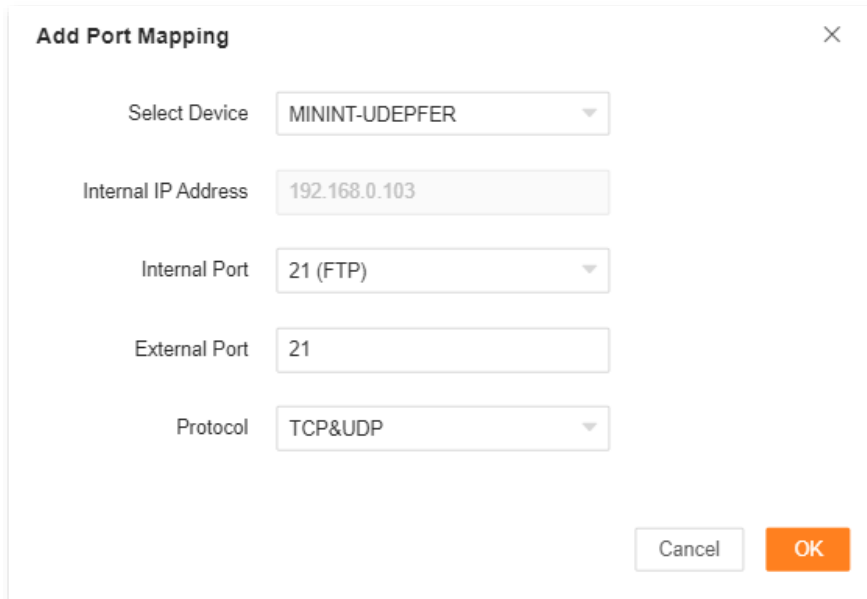
Step 3 Click .

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**.



Add Port Mapping [X]

Select Device: MININT-UDEPFER

Internal IP Address: 192.168.0.103

Internal Port: 21 (FTP)

External Port: 21

Protocol: TCP&UDP

Cancel OK

---End

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

9.9 System settings

9.9.1 Login password

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

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

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

Login Password

You can modify the login password of the router here.

Old Password

New Password

Confirm Password

Save

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](#).

9.9.2 System time

You can change the time settings on this page. The time-based functions require an accurate system time. The system time of the 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 .

Parameter	Description
	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.

9.9.3 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 <small>New Version Available: V16.03.16.12(11225) Details</small>	V16.03.16.11_multi	Online Upgrade Local Upgrade
Agent <small>New Version Available: V16.03.16.12(11225) Details</small>	V16.03.16.11_multi	Online Upgrade Local Upgrade

[One-click 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	Detect New Version Local Upgrade
Agent	V16.03.16.11_multi	Detect New Version Local Upgrade

[Detect New Version](#)

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% <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% <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



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



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.

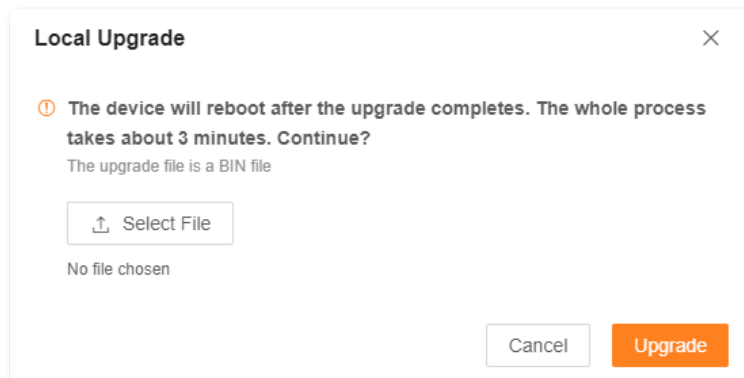
Step 1 Go to www.tendacn.com. Download an applicable firmware of the Mesh device to your local computer and unzip it.

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



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.

9.9.4 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"/>

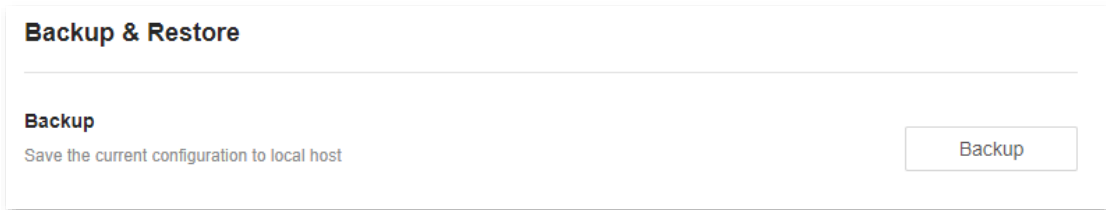
Back up the configuration of the Mesh device

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**.



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

---End

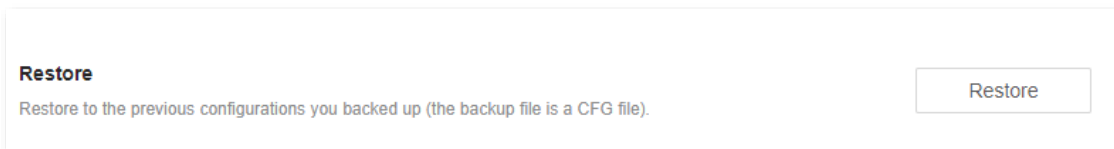
Restore the previous configuration of the Mesh device

To restore the previous configuration of the Mesh device:

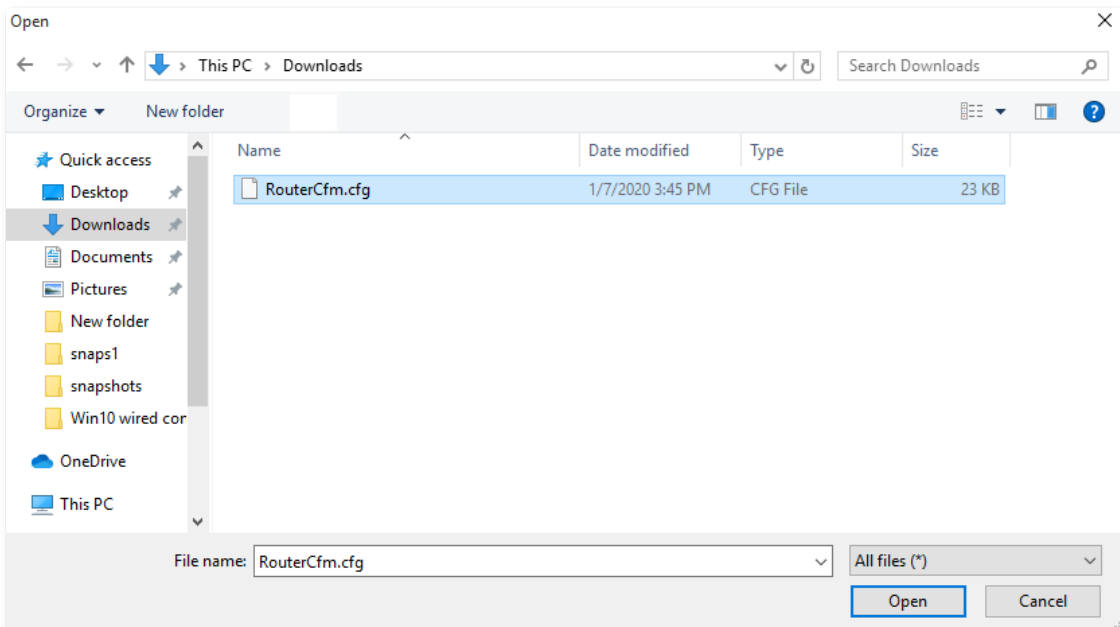
Step 1 [Log in to the web UI.](#)

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

Step 3 Click **Restore.**



Step 4 Select the configuration file to be restored (extension: cfg), 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:

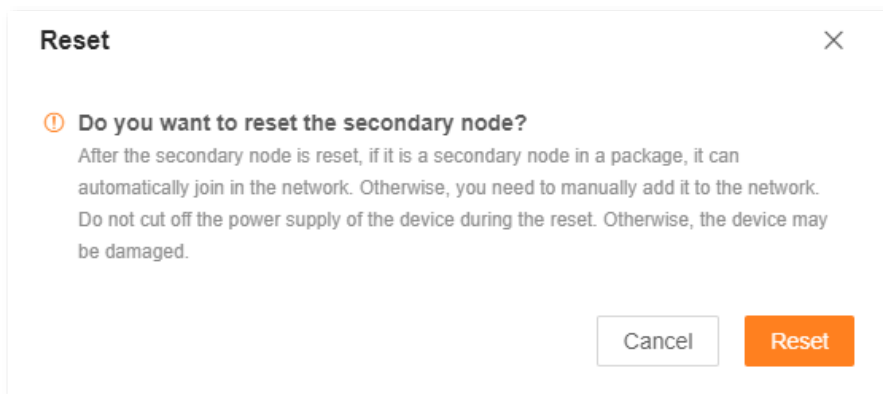
Step 1 [Log in to the web UI.](#)

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

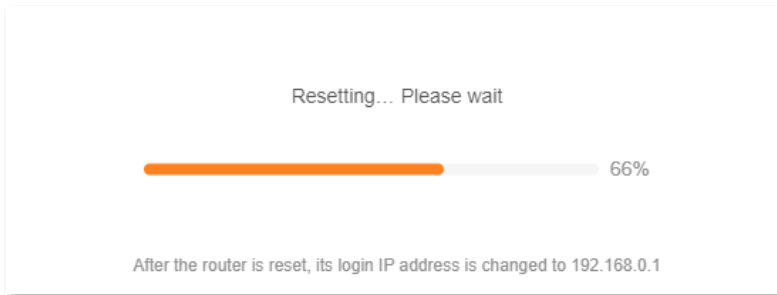
Step 3 Click **Reset** in the line of the node to be reset.

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

9.9.5 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

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.

Parameter	Description
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.

9.9.6 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.

No.	Time	Type	Log Content
1	2000-01-01 00:33:22	system	Sync time failed!
2	2000-01-01 00:32:26	system	Sync time failed!
3	2000-01-01 00:31:31	system	Sync time failed!
4	2000-01-01 00:30:36	system	Sync time failed!
5	2000-01-01 00:29:41	system	Sync time failed!
6	2000-01-01 00:29:38	system	Client Offline: MAC:c8:3a:35:9c:5fe1, IP:192.168
7	2000-01-01 00:29:38	system	Client Offline: MAC:c8:3a:35:12:34:f5, IP:192.168
8	2000-01-01 00:29:24	system	Client Offline: MAC:00:b0:4c:51:15:7e, IP:192.168
9	2000-01-01 00:28:46	system	Sync time failed!
10	2000-01-01 00:27:51	system	Sync time failed!

147 items in total < 1 2 3 4 5 6 7 ... 15 >



TIP Rebooting the Mesh device will clear all previous system logs.

10 FAQ

10.1 Failed to access the web UI

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

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

10.2 Internet detection failed upon the first setup

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

- Ensure that the Ethernet cable for internet connection is connected to the WAN port of the 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.

10.3 Failed to find or connect my wireless network

Use the following method to troubleshoot the fault.

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

10.4 Forgot my password

Use the following method to troubleshoot the fault.

- If you used the same password for Wi-Fi login and web UI login:
 - If you used the default password and forgot it, find it on the bottom label.



- If you have changed the password, reset the primary node by holding down the **RESET** button with a needle-like item (such as a pin) for about 8 seconds, and perform settings again.
- If you used different passwords for Wi-Fi login and web UI login:
 - The default Wi-Fi password can be found on the bottom label. If you have changed the password, [log in to the web UI](#), and navigate to [Wi-Fi Settings](#) to find the password.
 - If you also forgot the web UI login password, reset the primary node by holding down the **RESET** button with a needle-like item (such as a pin) for about 8 seconds, and perform settings again.

Appendixes

A.1 Factory settings

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

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

A.2 Acronyms and Abbreviations

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

Acronym or Abbreviation	Full Spelling
RA	Router Advertisement
SSID	Service Set Identifier
STB	Set-top box
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UI	User interface
UPnP	Universal Plug and Play
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual local area network
VPN	Virtual private network
WAN	Wide area network
WLAN	Wireless local area network
WPA	Wi-Fi Protected Access
WPA-PSK	WPA Pre-shared Key
WPA3-SAE	WPA3-Simultaneous Authentication of Equals
WPS	Wi-Fi Protected Setup