



User Guide

BBA Mesh

Contents

About This Guide	1
 Chapter 1. Get to Know About Your Device	 3
1. 1. Product Overview.....	4
1. 2. Appearance	4
 Chapter 2. Connect the Device.....	 6
2. 1. Position the Device	7
2. 2. Connect Your Device	7
 Chapter 3. Log In to Your Device.....	 10
 Chapter 4. Set Up Internet Connection	 12
4. 1. Use Quick Setup Wizard	13
4. 2. Quick Setup Via TP-Link Aginet App	14
4. 3. Manually Set Up Your Internet Connection	15
4. 4. Set Up the Mesh Device as an Access Point.....	17
4. 5. Set Up an IPv6 Internet Connection	18
4. 6. IPv6 Tunnel	22
 Chapter 5. Setup Your Network via TP-Link Aginet App	 25
5. 1. Set Up Your Mesh Device	26
5. 2. Dashboard.....	29
5. 3. Add More Mesh Devices	31
5. 4. Check Mesh Device Status	32
5. 5. Remove/Reboot Mesh Devices	35
5. 6. Manage Connected Devices	36
5. 7. Create a New Network	37
5. 8. Parental Controls	38
5. 9. Wi-Fi Settings	39
5. 10. Guest Network.....	40
5. 11. Internet Connection	41
5. 12. Block List.....	43
5. 13. Upgrade Your Mesh Device	44
5. 14. Advanced Features	45

Chapter 6. Customize Your Network Settings..... 49

6. 1.	Configure LAN Settings.....	50
6. 1. 1.	Change the LAN IP Address	50
6. 1. 2.	Use the Mesh Device as a DHCP Server	51
6. 1. 3.	Reserve LAN IP Addresses	52
6. 2.	Configure IPv6 LAN Settings.....	52
6. 2. 1.	Configure the RADVD Address Type.....	53
6. 2. 2.	Configure the DHCPv6 Server Address Type	53
6. 3.	Set Up a Dynamic DNS Service Account	54
6. 4.	Create Static Routes.....	55
6. 5.	RIP Settings	58
6. 6.	Specify Wireless Settings.....	59
6. 6. 1.	Change Basic Wireless Settings	59
6. 6. 2.	Advanced Wireless Settings.....	61
6. 6. 3.	View Wireless Information	64
6. 7.	Schedule Your Wireless Function	65
6. 8.	Use WPS for Wireless Connection	66

Chapter 7. Multi-SSID 69

Chapter 8. TP-Link Cloud Service 71

8. 1.	Register a TP-Link ID.....	72
8. 2.	Change Your TP-Link ID Information.....	72
8. 3.	Manage the User TP-Link IDs	73
8. 3. 1.	Add TP-Link ID to Manage the Mesh Device	74
8. 3. 2.	Remove TP-Link ID(s) from Managing the Mesh Device	74
8. 4.	Manage the Mesh Device via the TP-Link Aginet App.....	75

Chapter 9. EasyMesh with Seamless Roaming..... 76

9. 1.	Set Up a EasyMesh Network	77
9. 2.	Manage Devices in the EasyMesh Network.....	79

Chapter 10. Guest Network..... 81

10. 1.	Create a Network for Guests	82
10. 2.	Customize Guest Network Options.....	82

Chapter 11. NAT Forwarding..... 84

11. 1.	ALG	85
--------	-----------	----

11. 2. Set Up Public Services on The Local Network by Virtual Servers.....	85
11. 3. Open Ports Dynamically by Port Triggering.....	87
11. 4. Make Applications Free from Port Restriction by DMZ.....	89
11. 5. Make Xbox Online Games Run Smoothly by UPnP.....	90

Chapter 12.Parental Controls 92

Chapter 13.Quality of Service..... 97

Chapter 14.Network Security 102

14. 1. Firewall & DoS Protection.....	103
14. 2. Service Filtering.....	104
14. 3. Access Control.....	105
14. 4. IP & MAC Binding.....	107
14. 5. IPv6 Firewall.....	109

Chapter 15.VPN Server&Client..... 111

15. 1. Use OpenVPN to Access Your Home Network.....	112
15. 2. Use PPTP VPN to Access Your Home Network.....	113
15. 3. Use IPSec VPN to Access Your Home Network.....	117
15. 4. VPN Connections.....	126

Chapter 16.Manage Your Mesh Device 127

16. 1. Set System Time.....	128
16. 2. Control the LED.....	129
16. 3. Test Internet Connectivity.....	129
16. 4. Update the Firmware.....	131
16. 5. Back Up and Restore Configuration Settings.....	132
16. 6. Reboot the Mesh Device.....	133
16. 7. Administration Management.....	134
16. 7. 1.Change the Login Password.....	134
16. 7. 2.Local Management.....	135
16. 7. 3.Remote Management.....	136
16. 7. 4.HTTP Referer Head Check.....	137
16. 7. 5.ICMP Ping.....	137
16. 7. 6.Session ID.....	138
16. 8. System Log.....	138
16. 9. CWMP Settings.....	140
16. 10. SNMP Settings.....	141

16. 11. Monitor the Internet Traffic Statistics.....143

16. 12. Port Mirror.....143

FAQ 145

About This Guide

This guide is a complement of Quick Installation Guide. The Quick Installation Guide instructs you on quick internet setup, and this guide provides details of each function and shows you the way to configure these functions appropriate to your needs.

Note: Features available in the mesh device may vary by model and software version. Mesh device availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual mesh device experience.

Conventions

In this guide the following conventions are used:

Convention	Description
<u>Underlined</u>	Underlined words or phrases are hyperlinks. You can click to redirect to a website or a specific section.
Teal	Contents to be emphasized and texts on the web page are in teal, including the menus, items, buttons, etc.
>	The menu structures to show the path to load the corresponding page. For example, Advanced > Wireless > WDS means the WDS function page is under the Wireless menu that is located in the Advanced tab.
 Note:	Ignoring this type of note might result in a malfunction or damage to the device.
 Tips:	Indicates important information that helps you make better use of your device.
symbols on the web page	 Click to edit the corresponding entry.  Click to delete the corresponding entry.  click to enable or disable the corresponding entry.  Click to view more information about items on the page.

More Info

The latest software, management app and utility can be found at [Download Center](https://www.tp-link.com/support/download/) at <https://www.tp-link.com/support/download/>.

The Quick Installation Guide can be found where you find this guide or inside the package of the mesh device.

Specifications can be found on the product page at <https://www.tp-link.com>.

TP-Link Community is provided for you to discuss our products and share knowledge at <https://community.tp-link.com>.

Our Technical Support contact information can be found at the [Contact Technical Support](https://www.tp-link.com/support/) page at <https://www.tp-link.com/support/>.

*Maximum wireless signal rates are the physical rates derived from IEEE Standard 802.11 specifications. Actual wireless data throughput and wireless coverage are not guaranteed and will vary as a result of 1) environmental factors, including building materials, physical objects, and obstacles, 2) network conditions, including local interference, volume and density of traffic, product location, network complexity, and network overhead, and 3) client limitations, including rated performance, location, connection, quality, and client condition.

*Use of Wi-Fi 6 (802.11ax), and features including OFDMA, MU-MIMO, 1024-QAM, and HT160 require clients to also support the corresponding features.

*Saving clients' battery power requires clients to also support the 802.11ax Wi-Fi standard. Actual power reduction may vary as a result of network conditions, client limitations, and environmental factors.

*Use of WPA3 requires clients to also support the corresponding feature.

*This mesh device may not support all the mandatory features as ratified in Draft 3.0 of IEEE 802.11ax specification.

*Further software upgrades for feature availability may be required.

Chapter 1

Get to Know About Your Device

This chapter introduces what your device can do and shows its appearance.

It contains the following sections:

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

1.1. Product Overview

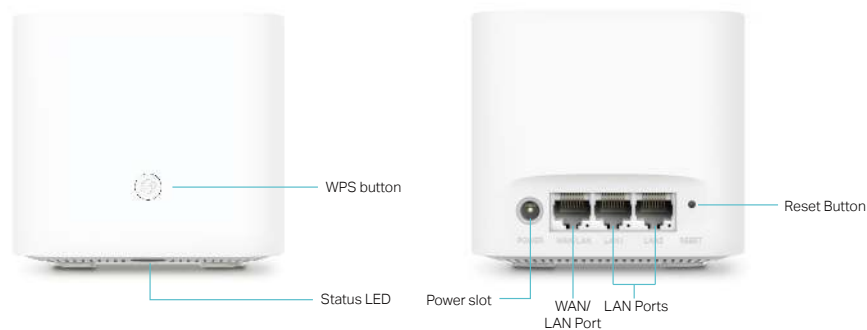
The Whole Home Mesh Wi-Fi AP is designed to extend your network coverage. You can use multiple APs to create a seamless, intelligent and easy-to-configure mesh network that covers the entire home.

The Mesh Wi-Fi system consists of a Main AP, one or more agents. The Main AP connects to a wired router, a modem or gateway, the agents extend the wireless coverage of your network.

1.2. Appearance

The device has an LED that changes its behavior according to its working status, and a WPS button, three RJ-45 Ethernet ports, a power port, and a RESET button.

Note: The appearance of the product is for illustration only, it may be different from your device, please refer to the actual product.



You can check the device's working status by following the LED Explanation table.

LED Explanation	
Status	Indication
Flashing yellow	The device is starting up or resetting.
Yellow	The connection quality of the device is normal.
Flashing blue	The device is ready for setup.
Fast flashing blue	The device is establishing a WPS or mesh connection.
Blue	The device has been set up, but the internet is unavailable.
Flashing white/green	The device is upgrading the firmware.
White/green	The device is all set up and connected to internet.
Flashing red	The device has lost connection.

LED Explanation	
Status	Indication
Red	The device has an issue.
Off	Power is off, or the status LED is turned off.

For information about the button and ports, you can refer to the explanation table below.

Item	Description
 WPS button	Press the button to start a WPS or mesh sync process.
Power port	For connecting the device to a power socket via the provided power adapter.
WAN/LAN port	For connecting the device to: a) a wired router(access point mode) b) a DSL/Cable modem, the Ethernet outlet or other internet devices(router mode). c) your PC or other Ethernet network devices.
LAN1, LAN2 ports	For connecting your PC or other Ethernet network devices.
RESET button	Press and hold the button for at least 5 seconds to reset the device into its factory default settings.

Chapter 2

Connect the Device

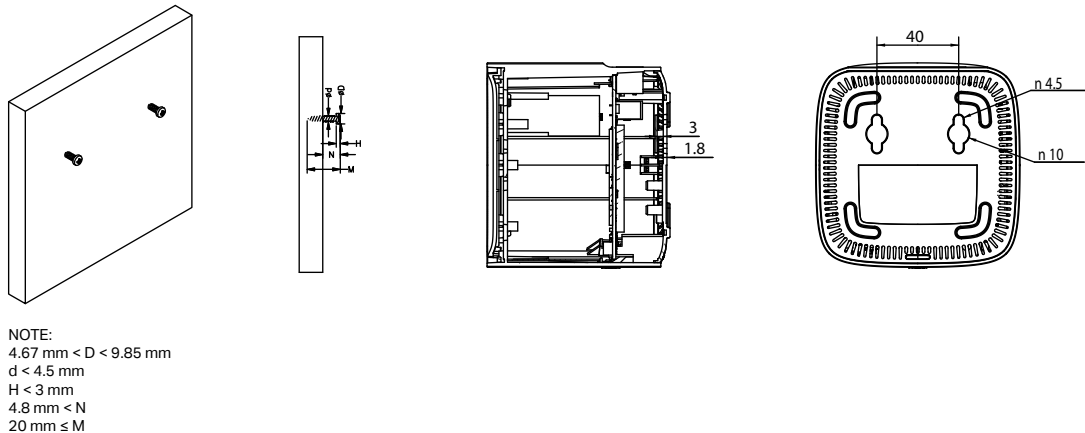
This chapter contains the following sections:

- [Position the Device](#)
- [Connect Your Device](#)

2.1. Position the Device

- The device should not be located in a place where it will be exposed to moisture or excessive heat.
- Place the device in a location where it can be connected to multiple devices as well as to a power source.
- Make sure the cables and power cord are safely placed out of the way so they do not create a tripping hazard.
- Keep the device away from devices with strong electromagnetic interference, such as Bluetooth devices, cordless phones and microwaves.
- The device can be placed on a shelf or desktop.

Generally, the device is placed on a horizontal surface, such as on a shelf or desktop. The device also can be mounted on the wall as shown in the following image.

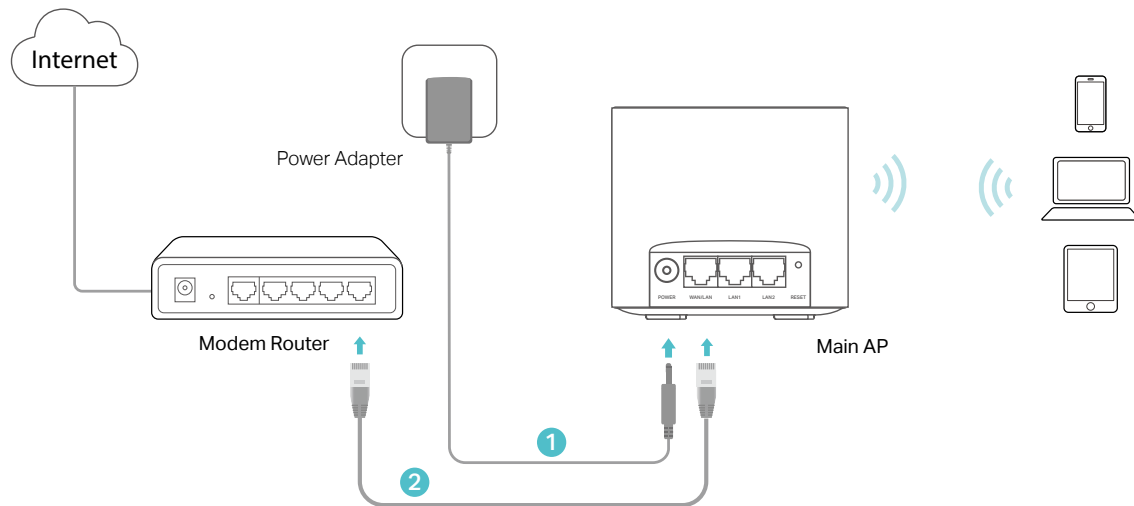


Note:

The diameter of the screw should be between 4.67 mm and 9.85 mm, and the center distance of two screws is 40 mm. The screws should be at least 20 mm in length to hold the device, and the screw head raised above the wall surface should be about 4.8 mm.

2.2. Connect Your Device

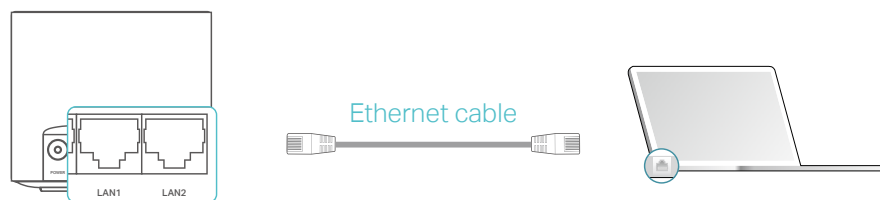
If you want to set up this device as a regular router or as the Main AP for Mesh Wi-Fi system, follow the steps below to connect your device.



1. Connect the power adapter to the AP.
2. Connect the WAN/LAN port of the AP to your wired router's Ethernet port via an Ethernet cable.
3. Verify the status LED (on the bottom of the device) is flashing blue before continuing with the configuration.
4. Connect your computer to the AP.

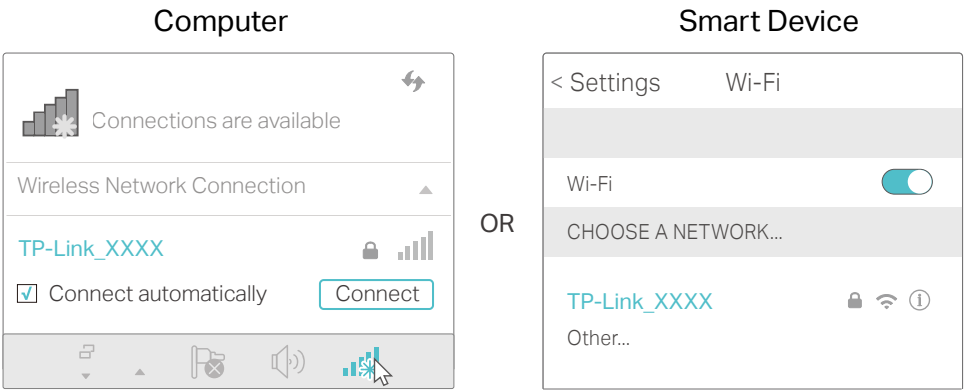
- **Method 1: Wired**

Turn off the Wi-Fi on your computer and connect the computer to the LAN port of the AP using an Ethernet cable.



- **Method 2: Wireless**

- 1) Find the SSID (Network Name) and Wireless Password printed on the label at the bottom of the AP.
- 2) Click the network icon of your computer or go to Wi-Fi Settings of your smart device, and then select the SSID to join the network.



Chapter 3

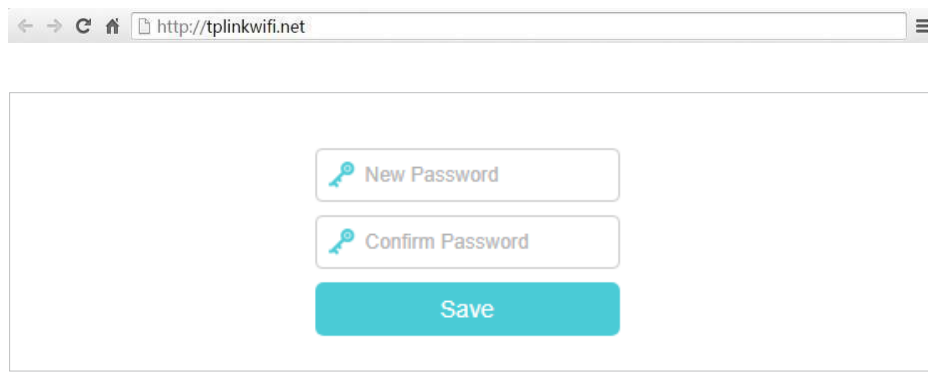
Log In to Your Device

This chapter introduces how to log in to the web management page of the device.

With the web management page, it is easy to configure and manage your device. The web management page can be used on any Windows, Macintosh or UNIX OS with a Web browser, such as Microsoft the Internet Explorer, Mozilla Firefox or Apple Safari.

Follow the steps below to log in to your device.

1. Set up the TCP/IP Protocol in [Obtain an IP address automatically](#) mode on your computer.
2. Launch a web browser and enter <http://tplinkwifi.net> or <http://192.168.88.1> in the address bar. Create a strong login password for secure management and click [Save](#). Then, enter the password again on the login window and click [Log in](#) to log in to your AP.



Note:

1. If the dialog boxes shown in the images above do not appear, it suggests that your IE Web-browser has been set to a proxy. You can go to [Tools > Internet Options > Connections > LAN Settings](#), and clear the [Using Proxy](#) check box, and click [OK](#).
2. If the login window does not appear, please refer to the [FAQ](#) section.

Chapter 4

Set Up Internet Connection

This chapter introduces how to connect your mesh device to the internet. The mesh device is equipped with a web-based Quick Setup wizard. It has necessary ISP information built in, automates many of the steps and verifies that those steps have been successfully completed. Furthermore, you can also set up an IPv6 connection if your ISP provides IPv6 service.

It contains the following sections:

- [Use Quick Setup Wizard](#)
- [Quick Setup Via TP-Link Aginet App](#)
- [Manually Set Up Your Internet Connection](#)
- [Set Up the Mesh Device as an Access Point](#)
- [Set Up an IPv6 Internet Connection](#)

4.1. Use Quick Setup Wizard

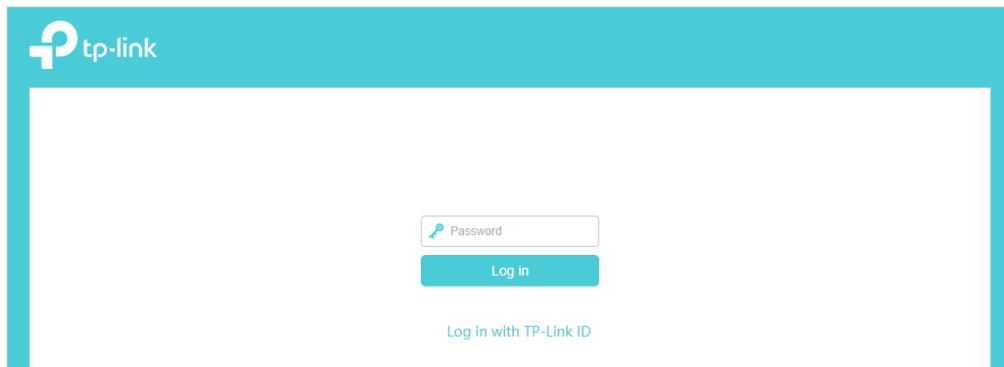
The Quick Setup Wizard will guide you to set up your mesh device.

🔗 **Tips:**

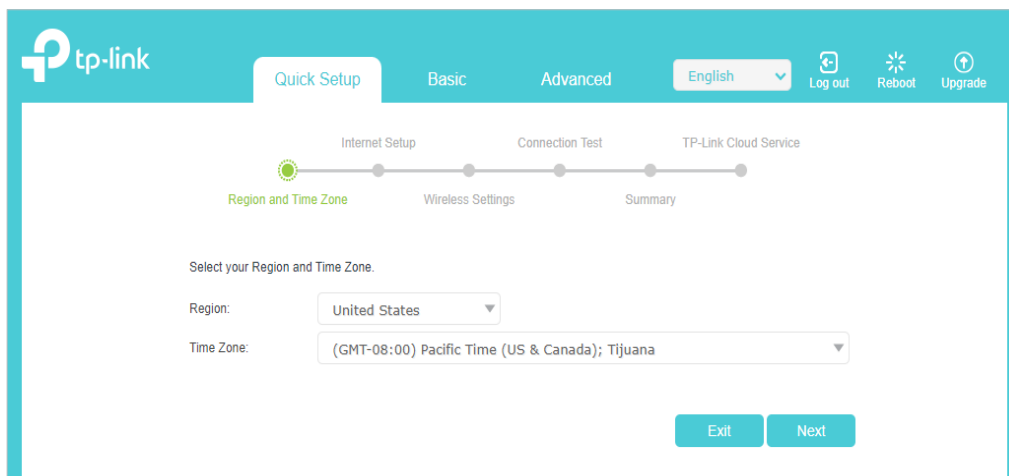
If you need the IPv6 internet connection, please refer to the section of [Set Up an IPv6 Internet Connection](#).

Follow the steps below to set up your mesh device.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.



2. Follow the step-by-step instructions to complete Quick Setup configuration or go to [Quick Setup](#) for configuration to connect your mesh device to the internet. Then follow the step-by-step instructions to connect your mesh device to the internet.



3. To enjoy a more complete service from TP-Link (remote management, TP-Link DDNS, and more.), log in with your TP-Link ID or click [Sign Up Now](#) to get one. Then follow the instructions to bind the mesh device to your TP-Link ID.

Get TP-Link Cloud Service

Log in to bind the router to your TP-Link ID. You can manage your network remotely via the Tether app, get notified of the latest firmware updates and more.

TP-Link ID (Email):

Password:

LOG IN

[Sign Up Now](#) [Forgot Password?](#)

SKIP

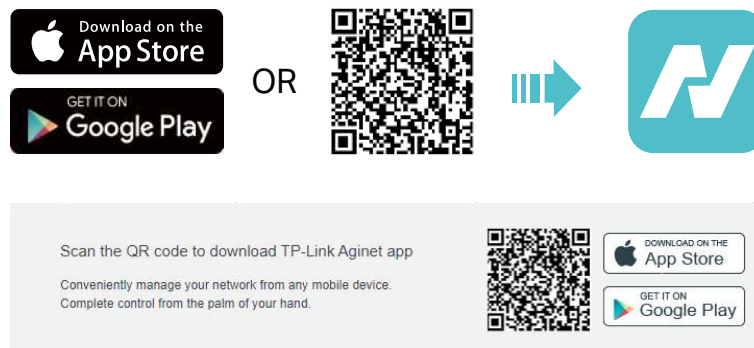
Note:

- To learn more about the TP-Link Cloud service, please refer to the [TP-Link Cloud Service](#) section.
- If you do not want to register a TP-Link ID now, you may click [Skip](#) to proceed.
- If you have changed the preset wireless network name (SSID) and wireless password during the Quick Setup process, all your wireless devices must use the new SSID and password to connect to the mesh device.

4.2. Quick Setup Via TP-Link Aginet App

The Aginet app runs on iOS and Android devices, such as smartphones and tablets.

1. Launch the Apple App Store or Google Play store and search “TP-Link Aginet” or simply scan the QR code to download and install the app.



2. Launch the Aginet app and log in with your TP-Link ID.

Note: If you don't have a TP-Link ID, create one first.

3. Tap the [Create a Network](#) button and select how you will connect your device to the internet. Follow the steps to complete the setup and connect to the internet.
4. Connect your devices to the newly configured wireless networks of the mesh device and enjoy the internet!

4.3. Manually Set Up Your Internet Connection

In this part, you can check your current internet connection settings. You can also modify the settings according to the service information provided by your ISP.

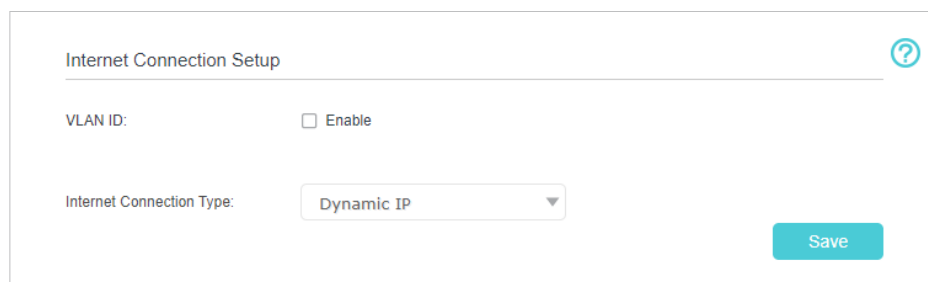
Follow the steps below to check or modify your internet connection settings.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
2. Go to **Basic > Internet**.
3. Follow the instructions on the page to continue the configuration. Parameters on the figures are just used for demonstration.

Note:

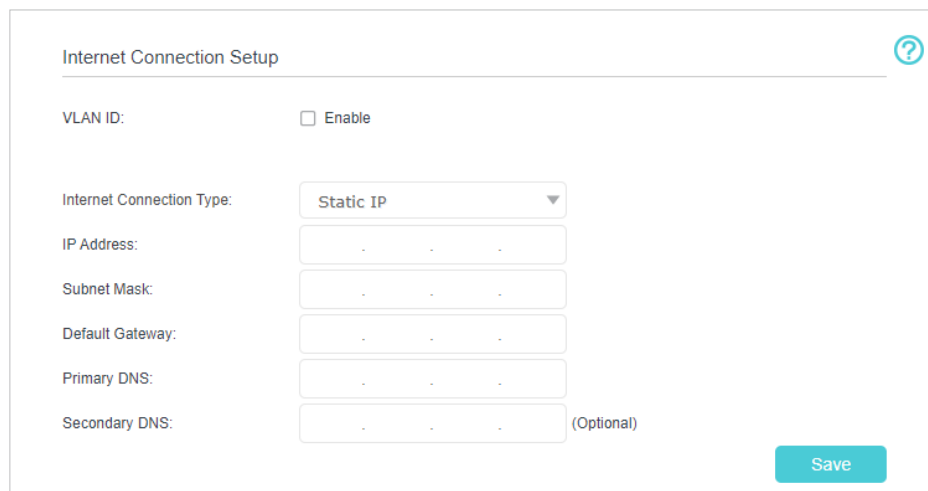
Since different connection types require different cables and connection information, you can also refer to the demonstrations to determine your connection type.

- 1) If you choose **Dynamic IP**, the IP address and Subnet Mask are assigned automatically by the ISP. Dynamic IP users are usually equipped with a cable TV or fiber cable.



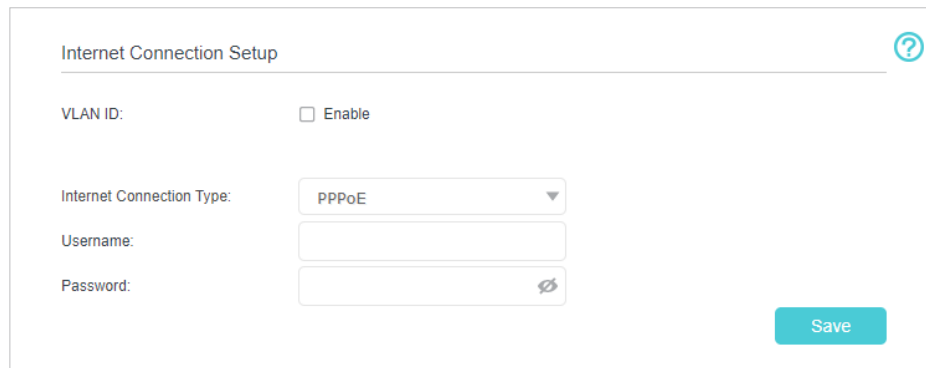
The screenshot shows the 'Internet Connection Setup' page. At the top, there is a title bar with a question mark icon. Below it, there is a 'VLAN ID' section with an 'Enable' checkbox. The 'Internet Connection Type' is set to 'Dynamic IP' in a dropdown menu. A 'Save' button is located at the bottom right.

- 2) If you choose **Static IP**, enter the information provided by your ISP in the corresponding fields.



The screenshot shows the 'Internet Connection Setup' page with 'Static IP' selected in the 'Internet Connection Type' dropdown. Below this, there are input fields for 'IP Address', 'Subnet Mask', 'Default Gateway', 'Primary DNS', and 'Secondary DNS' (marked as optional). A 'Save' button is located at the bottom right.

- 3) If you choose **PPPoE**, enter the **username** and **password** provided by your ISP. PPPoE users usually have DSL cable modems.



Internet Connection Setup

VLAN ID: ☐ Enable

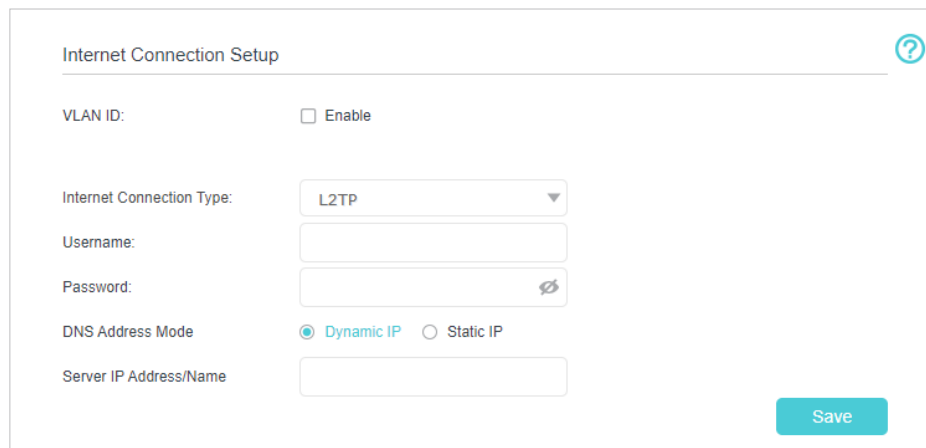
Internet Connection Type:

Username:

Password:

Save

- 4) If you choose **L2TP**, enter the **username** and **password** and choose the **Secondary Connection** provided by your ISP. Different parameters are needed according to the Secondary Connection you have chosen.



Internet Connection Setup

VLAN ID: ☐ Enable

Internet Connection Type:

Username:

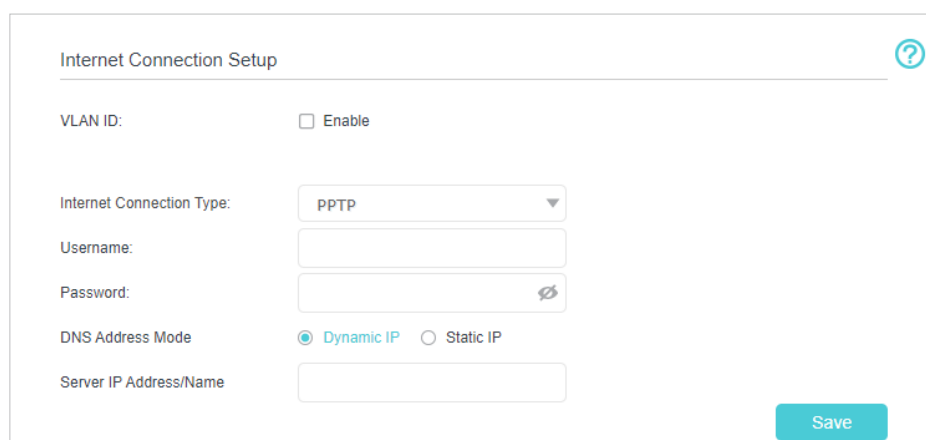
Password:

DNS Address Mode ☒ Dynamic IP ☐ Static IP

Server IP Address/Name

Save

- 5) If you choose **PPTP**, enter the **username** and **password**, and choose the **Secondary Connection** provided by your ISP. Different parameters are needed according to the Secondary Connection you have chosen.



Internet Connection Setup

VLAN ID: ☐ Enable

Internet Connection Type:

Username:

Password:

DNS Address Mode ☒ Dynamic IP ☐ Static IP

Server IP Address/Name

Save

4. Click **Save**.

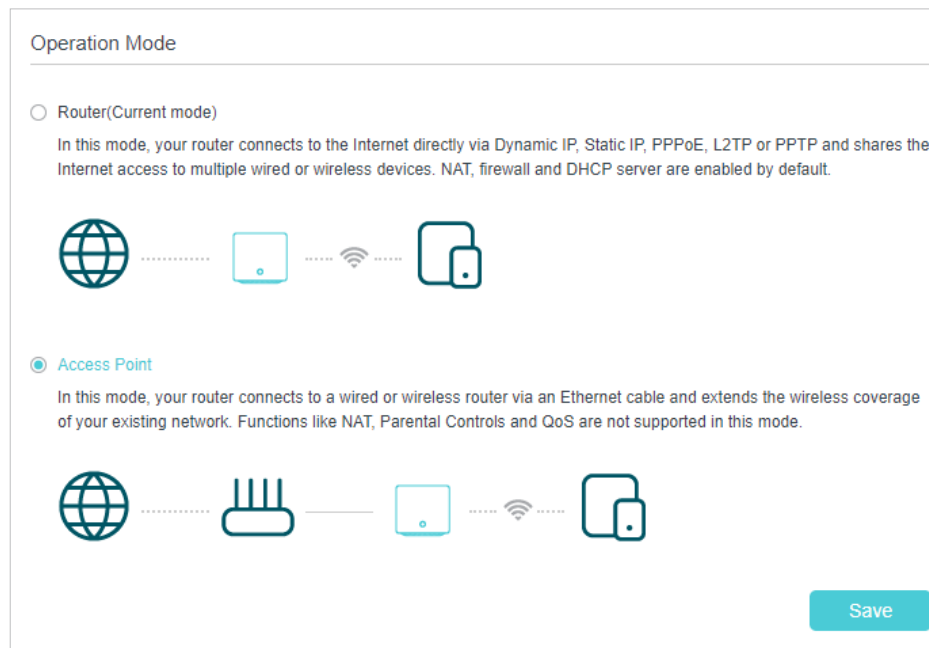
 Tips:

- If you use [Dynamic IP](#) and [PPPoE](#) and you are provided with any other parameters that are not required on the page, please go to [Advanced](#) > [Network](#) > [Internet](#) to complete the configuration.
- If you still cannot access the internet, refer to the [FAQ](#) section for further instructions.

4.4. Set Up the Mesh Device as an Access Point

The mesh device can work as an access point, transforming your existing wired network to a wireless one.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
2. Go to [Advanced](#) > [Operation Mode](#), select [Access Point](#) and click [Save](#). The mesh device will reboot and switch to Access Point mode.



3. After rebooting, connect the mesh device to your existing wired router via an Ethernet cable.
4. Log in again to the web management page <http://tplinkwifi.net> or <http://192.168.88.1>, and go to [Quick Setup](#).
5. Configure your wireless settings and click [Next](#).
6. Confirm the information and click [Save](#). Now, you can enjoy Wi-Fi.

☛ **Tips:**

- Functions, such as Parental Controls, QoS and NAT Forwarding, are not supported in the Access Point mode.
- Functions, such as Guest Network, are the same as those in the Router mode.

4.5. Set Up an IPv6 Internet Connection

Your ISP provides information about one of the following IPv6 internet connection types: PPPoE(SLAAC/DHCPv6/AUTO/Passthrough), Dynamic IP(SLAAC/DHCPv6/AUTO/Passthrough), Static IP.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
2. Go to **Advanced > Network > Internet**.
3. Click **Add** and enable IPv6 and select the internet connection type provided by your ISP.

Default Gateway

Default Gateway:

DNS Lookup: (Optional)

IPv4 Ping: (Optional)

IPv6 Ping: (Optional)

Save

Internet Setup

Refresh Add Delete All

Connection Name	Service Type	VLAN ID	Status	Operation	Enable	Modify
ipoe_0_0_d	Internet	N/A	Disconnected	Connect		

Tips:

If you do not know what your internet connection type is, contact your ISP or judge according to the already known information provided by your ISP.

4. Fill in information as required by different connection types.

- 1) **Static IP:** Fill in blanks and click **OK**.

Connection Name: (Optional)

☒ [Enable This Entry](#)

Service Type: ☒ [Internet](#) ☐ IPTV ☐ TR069 ☐ Others

Default Gateway:

Internet Connection Type:

VLAN ID: ☐ Enable

IPv4: ☒ [Enable](#)

IP Address:

Subnet Mask:

Default Gateway:

Primary DNS:

Secondary DNS: (Optional)

IPv6: ☒ [Enable](#)

IPv6 Address:

Prefix Length:

IPv6 Gateway:

IPv6 DNS Server:

Secondary DNS: (Optional)

☒ Advanced

- 2) [Dynamic IP\(SLAAC/DHCPv6/AUTO/Passthrough\)](#): Click [Advanced](#) to input further information if your ISP requires. Click [OK](#).

Connection Name:		(Optional)
	☒ Enable This Entry	
Service Type:	☒ Internet ☐ IPTV ☐ TR069 ☐ Others	
Default Gateway:	Auto	
Internet Connection Type:	Dynamic IP	
VLAN ID:	☐ Enable	
IPv4:	☒ Enable	
IP Address:	0.0.0.0	
Subnet Mask:	0.0.0.0	
Gateway:	0.0.0.0	
IPv6:	☒ Enable	
IPv6 Address:	::	
Prefix Length:	0	
IPv6 Gateway:	::	
Addressing Type:	AUTO	
☒ Advanced		

- 3) **PPPoE(SLAAC/DHCPv6/AUTO/Passthrouth):** Click [Advanced](#) to input further information if your ISP requires. Click [OK](#).

Connection Name: (Optional)

☒ Enable This Entry

Service Type: ☒ Internet ☐ IPTV ☐ TR069 ☐ Others

Default Gateway:

Internet Connection Type:

VLAN ID: ☐ Enable

Username:

Password:

Confirm Password:

Connection Mode: ☒ Auto ☐ On Demand ☐ Manually

Authentication Type:

IPv4: ☒ Enable

IPv6: ☒ Enable

Addressing Type:

5. Configure LAN ports. Go to [Advanced](#) > [Network](#) > [LAN Settings](#). Fill in [Site Prefix Type](#) provided by your ISP, and click [Save](#).

DHCP Server IPv4 **IPv6** ?

Group: Default

Address Type: ☒ RADVD ☐ DHCPv6 Server

Enable RDNSS: ☐ Enable

Enable ULA Prefix: ☐ Enable

Site Prefix Type: ☒ Delegated ☐ Static

WAN Connection:

6. Click [Advanced](#) > [Status](#) to check whether you have successfully set up an IPv6 connection.

Tips:

Visit the [FAQ](#) section if there is no internet connection.

4.6. IPv6 Tunnel

IPv6 Tunnel is a transition mechanism that enables IPv6-only hosts to reach IPv4 services or vice versa and allows isolated IPv6 hosts and networks to reach each other over IPv4-only infrastructure before IPv6 completely supplants IPv4. It is a temporary solution for networks that do not support native dual-stack, where both IPv6 and IPv4 run independently.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
2. Go to **Advanced > Network > Internet**.
3. Click **Add** and enable IPv6 and Click **Advanced** to view more advanced settings.
4. Select the checkbox to enable IPv6 Tunnel.

Advanced

IPv6 Tunnel: ☒ Enable

Mechanism: DS-Lite

Configuration Type: ☒ Auto ☐ Manual

MTU Size: 1500 (bytes. (The default is 1500, do not change unless necessary.))

NAT: ☒ Enable

Full-cone NAT: ☐ Enable

IGMP Proxy: ☒ Enable

Get IP Using Unicast DHCP: ☐ Enable (It is usually not required.)

Use the Following DNS Addresses: ☐ Enable

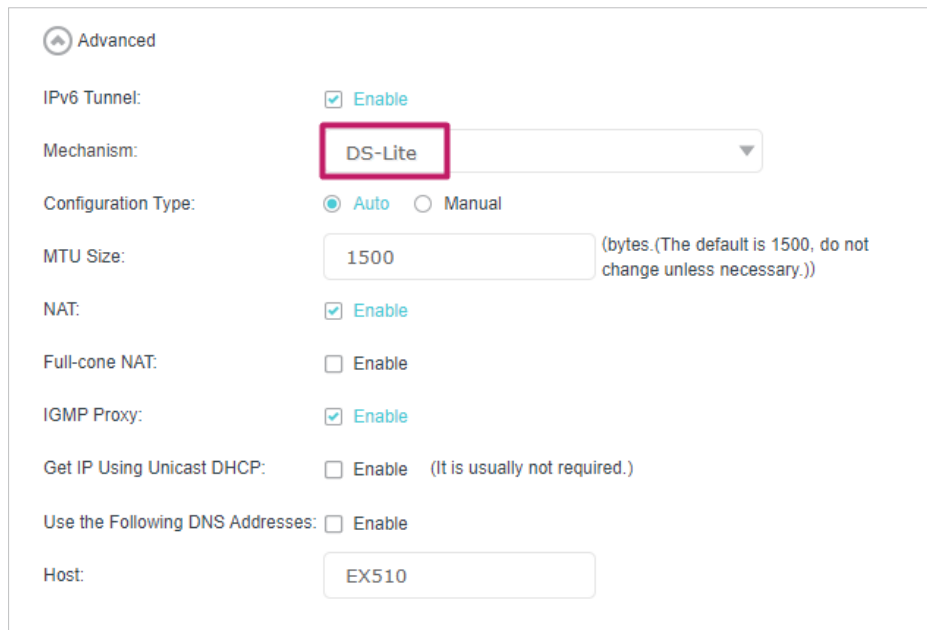
Host: EX510

Tips:

Please check the IPv6 tunnel settings each time while reconfiguring WAN connection, as WAN connection configuration may take effect on tunnel settings.

5. Fill in information as required by different tunneling mechanisms.

- 1) **DS-Lite**: Fill in blanks and click **OK**. Select this tunneling mechanism if your ISP uses DS-Lite deployment for assigning address.



The screenshot shows the 'Advanced' configuration window for an internet connection. The 'IPv6 Tunnel' is enabled. The 'Mechanism' dropdown is set to 'DS-Lite', which is highlighted with a red box. The 'Configuration Type' is set to 'Auto'. The 'MTU Size' is 1500. The 'NAT' is enabled. The 'Full-cone NAT' is disabled. The 'IGMP Proxy' is enabled. The 'Get IP Using Unicast DHCP' is disabled. The 'Use the Following DNS Addresses' is disabled. The 'Host' is set to 'EX510'.

Advanced

IPv6 Tunnel: ☒ Enable

Mechanism: **DS-Lite**

Configuration Type: ☒ Auto ☐ Manual

MTU Size: 1500 (bytes. (The default is 1500, do not change unless necessary.))

NAT: ☒ Enable

Full-cone NAT: ☐ Enable

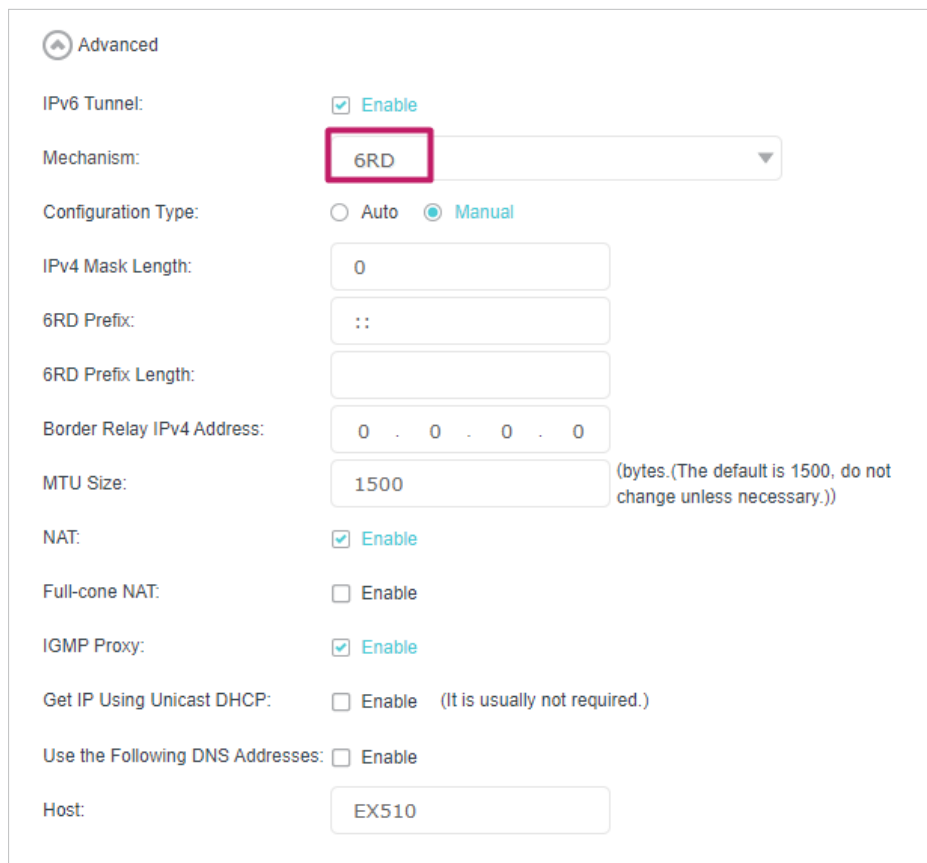
IGMP Proxy: ☒ Enable

Get IP Using Unicast DHCP: ☐ Enable (It is usually not required.)

Use the Following DNS Addresses: ☐ Enable

Host: EX510

- 2) **6rd**: Fill in blanks and click **OK**. Select this tunneling mechanism if your ISP uses 6rd deployment for assigning address.



The screenshot shows the 'Advanced' configuration window for an internet connection. The 'IPv6 Tunnel' is enabled. The 'Mechanism' dropdown is set to '6RD', which is highlighted with a red box. The 'Configuration Type' is set to 'Manual'. The 'IPv4 Mask Length' is 0. The '6RD Prefix' is '::'. The '6RD Prefix Length' is empty. The 'Border Relay IPv4 Address' is '0 . 0 . 0 . 0'. The 'MTU Size' is 1500. The 'NAT' is enabled. The 'Full-cone NAT' is disabled. The 'IGMP Proxy' is enabled. The 'Get IP Using Unicast DHCP' is disabled. The 'Use the Following DNS Addresses' is disabled. The 'Host' is set to 'EX510'.

Advanced

IPv6 Tunnel: ☒ Enable

Mechanism: **6RD**

Configuration Type: ☐ Auto ☒ Manual

IPv4 Mask Length: 0

6RD Prefix: ::

6RD Prefix Length:

Border Relay IPv4 Address: 0 . 0 . 0 . 0

MTU Size: 1500 (bytes. (The default is 1500, do not change unless necessary.))

NAT: ☒ Enable

Full-cone NAT: ☐ Enable

IGMP Proxy: ☒ Enable

Get IP Using Unicast DHCP: ☐ Enable (It is usually not required.)

Use the Following DNS Addresses: ☐ Enable

Host: EX510

- 3) **6to4**: Fill in blanks and click **OK**. Select this tunneling mechanism if your ISP uses 6to4 deployment for assigning address.

 Advanced

IPv6 Tunnel:

☒ Enable

Mechanism:

6to4

▼

MTU Size:

1500

(bytes. (The default is 1500, do not change unless necessary.))

NAT:

☒ Enable

Full-cone NAT:

☐ Enable

IGMP Proxy:

☒ Enable

Get IP Using Unicast DHCP:

☐ Enable (It is usually not required.)

Use the Following DNS Addresses:

☐ Enable

Host:

EX510

Chapter 5

Setup Your Network via TP-Link Aginet App

This chapter guides you on how to setup your Whole Home Mesh Wi-Fi System via TP-Link Aginet app, as well as regulatory information. Features available in Aginet app may vary by model and software version. Aginet app availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual mesh experience.

5.1. Set Up Your Mesh Device

The intuitive Aginet app guides you through an easy setup process that gets each unit up and all your devices connected.

Follow the steps below to set up your Whole Home Mesh Wi-Fi System.

1. Download and install the Aginet app

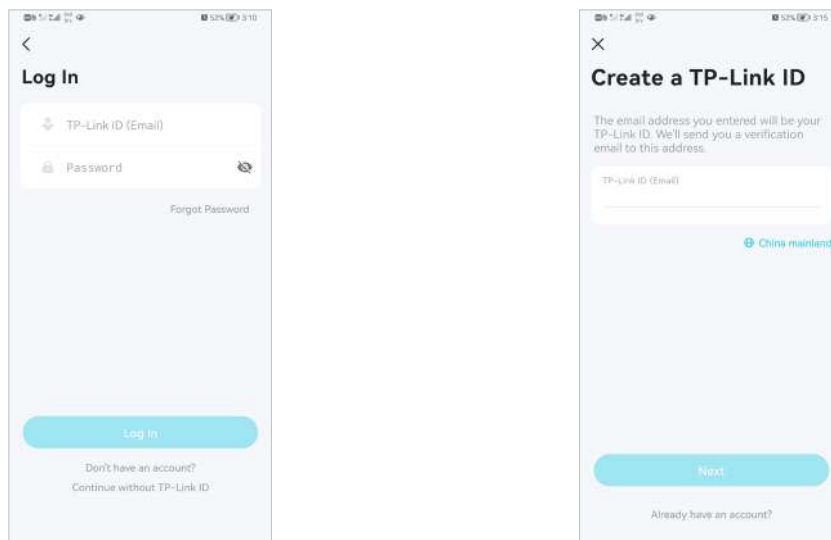
Scan the QR code below or go to Google Play or the App Store to download the Aginet app. Install the app on your Android or iOS smartphone or tablet.



2. Log in or sign up with TP-Link ID.

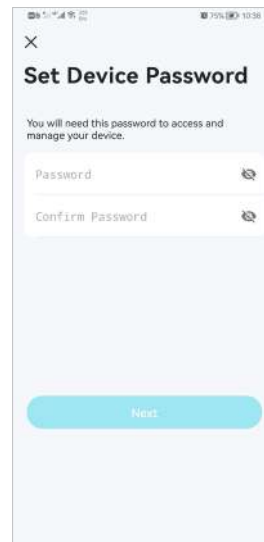
Open the Aginet app. Use your TP-Link ID to log in. If you don't have a TP-Link ID, tap [Don't have an account?](#) and sign up first.

Note: If you forgot your login password, tap [Forgot Password](#). The Aginet app will guide you through the rest.



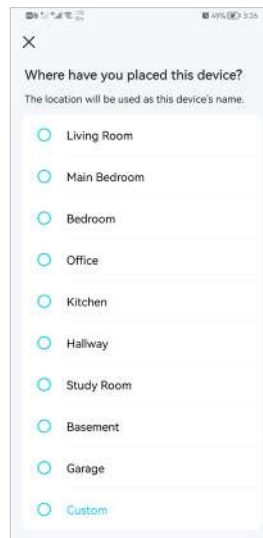
3. Plug in and power on mesh device.

Power off your modem. Connect your mesh device to the modem and power them both on. If you don't have a modem, connect the Ethernet outlet directly to your mesh device.



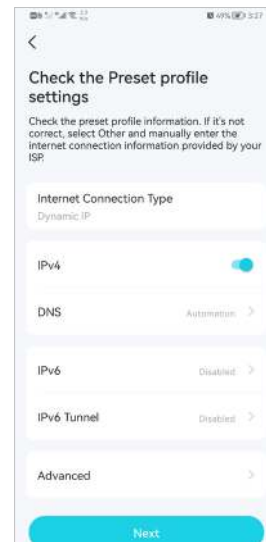
4. Select a location.

Select a location for this mesh device. If its location is not listed, you can create a new one by choosing **Custom**. This will be the name of your mesh device.



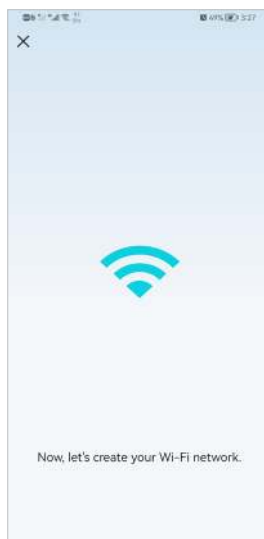
5. Set up internet connection.

Select the internet connection type and enter the information. If you are not sure, contact your internet service provider.



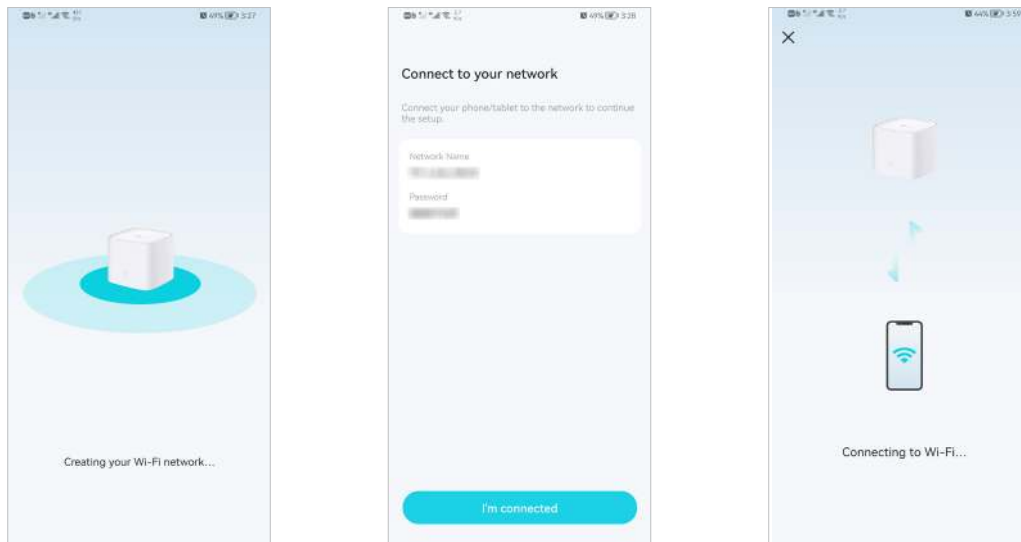
6. Create your Wi-Fi network.

Set a network name and a password. These will be the name and password you use to connect your devices to Wi-Fi.



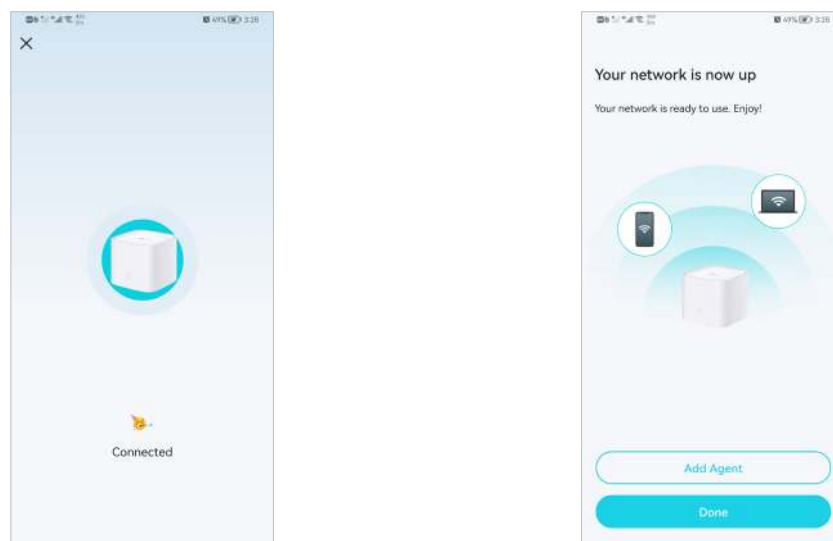
7. Connect to your Wi-Fi network.

Connect your phone/tablet to the mesh device's Wi-Fi.



8. Setup complete.

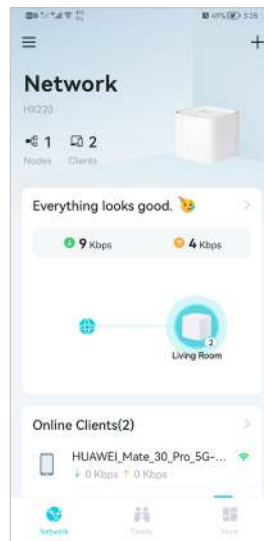
Your mesh network is now up. Connect all devices to the mesh network. You can also [Add Agent](#) to expand the Wi-Fi coverage.



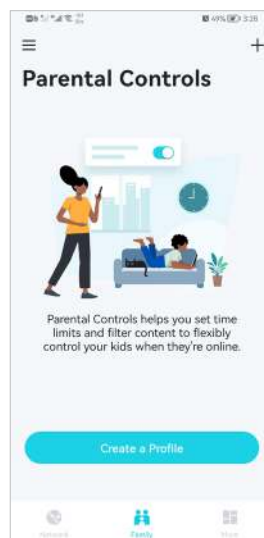
5.2. Dashboard

After you successfully set up your mesh network, you will see the dashboard of the Aginet app. Here you can get an overview of the network status, create family profiles, and customize your home network and set up various advanced features.

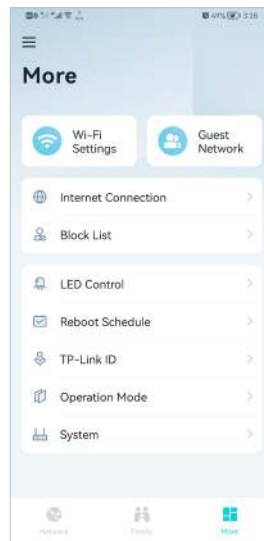
1. Tap  to get an overview of the network status.



2. Tap  to create family profiles.



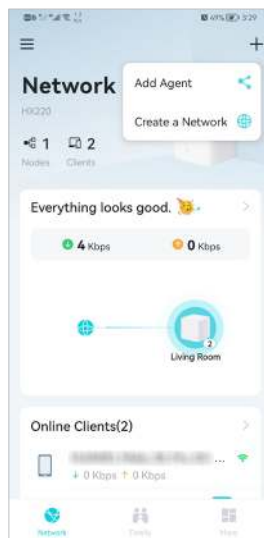
3. Tap  for more features.



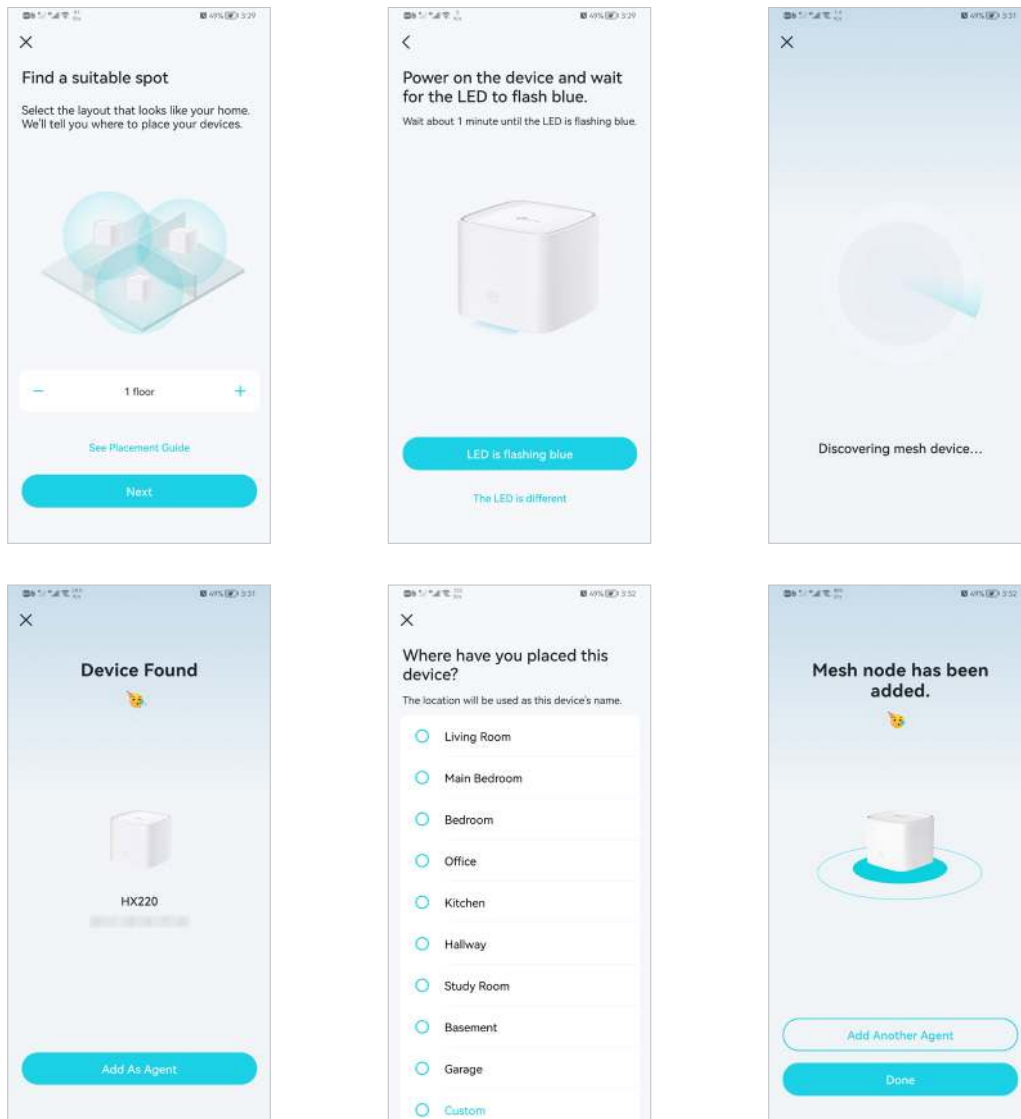
5.3. Add More Mesh Devices

After creating a mesh network, you can add more mesh devices to the network to expand the Wi-Fi coverage and manage them easily on your Aginet app.

1. In **Network**, tap **+** > **Add Agent**. Then select the **Mesh Device**.



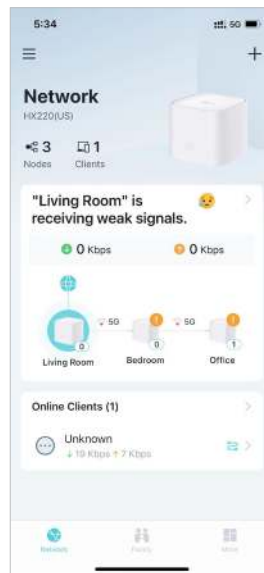
2. Follow app instructions to complete the setup.



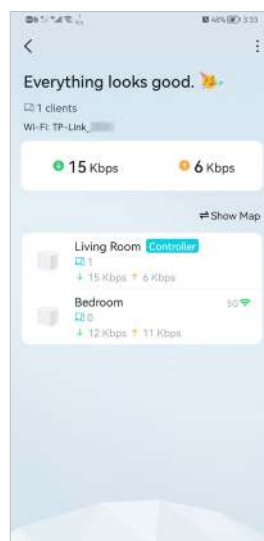
5.4. Check Mesh Device Status

In [Network](#), you can check the working status (online/offline) of all the mesh devices, check the details (speed/mesh device's IP address & MAC address/connected clients) of each mesh device, change the mesh device's location/name, and more.

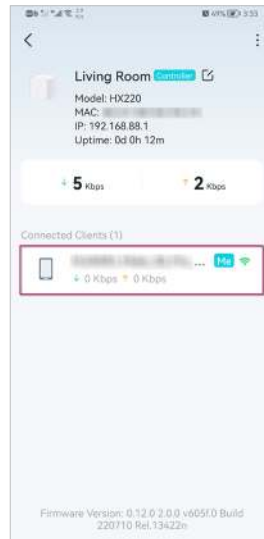
1. Tap  to check all mesh devices' status.



2. Tap a mesh device to check more details.



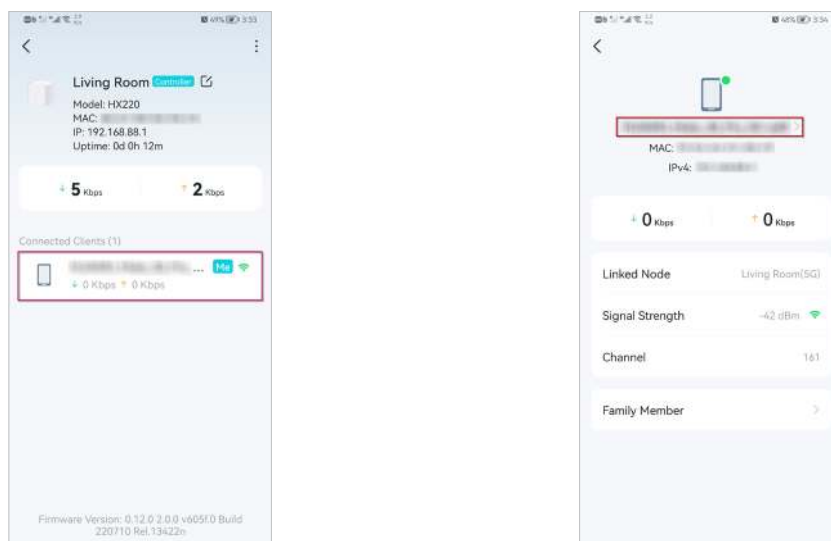
3. Check download/upload speed of the mesh device.



4. Tap  and change or customize the location/name of the mesh device.



5. Check the clients connected to the mesh device.



6. Tap the client's name. Change or customize client's information.

5.5. Remove/Reboot Mesh Devices

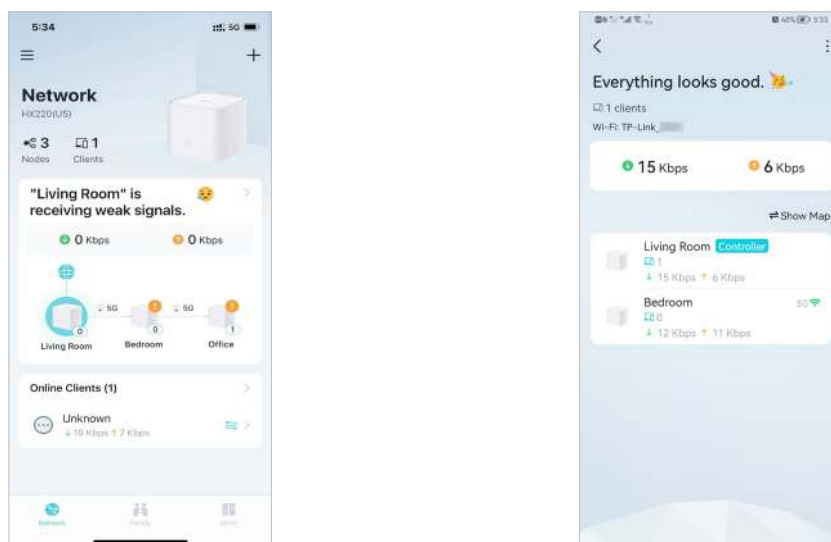
You can reset your mesh device to factory default settings or reboot your mesh device to clear cache and enhance running performance easily in the Aginet app. Follow the steps below.

Note:

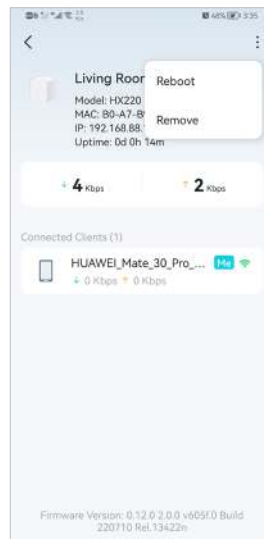
Rebooting your mesh device will keep the current settings on it.

Removing your mesh device will reset it to factory default settings and you will need to set up your mesh device again. You can also press and hold the Reset button for at least 5 second to quickly reset your mesh device to factory default settings.

In **Network**, tap . Select a mesh device.



7. Tap  to remove or reboot the mesh device.

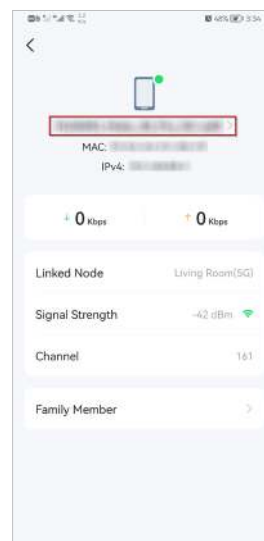
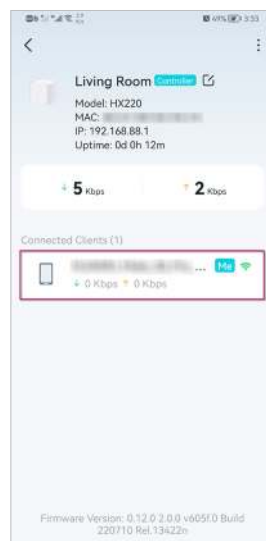
**Note:**

If the LED light of mesh device does not turn flashing blue after tapping **Remove**, press and hold the Reset button for at least 5 seconds to reset it.

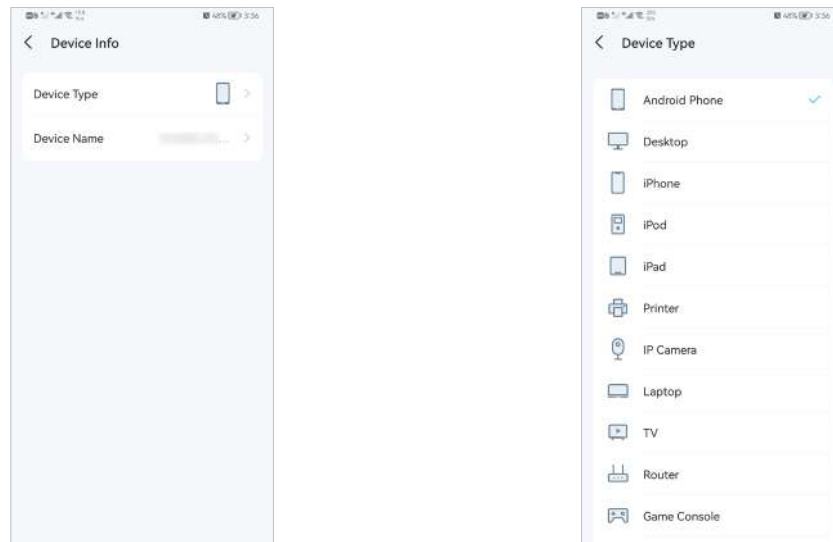
5.6. Manage Connected Devices

In **Network**, you can manage your connected devices easily, such as changing the device name and type.

1. Tap a connected device to check the details (e.g. real-time upload and download speeds, device name/profile, etc.).



2. Change the **Device Type** and **Device Name** as needed.

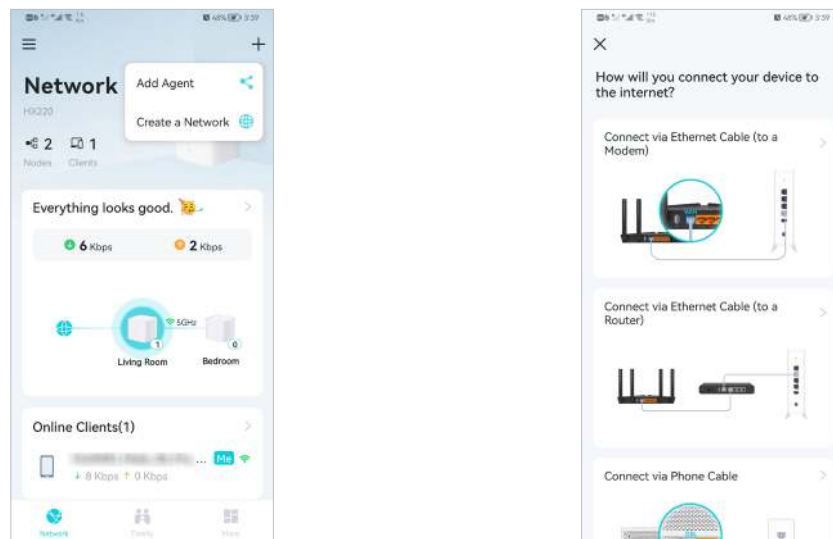


5.7. Create a New Network

In the Aginet app, you can create different mesh networks with your TP-Link ID and manage them conveniently from the Aginet app with one account. You can also help family or friends manage their networks with your Aginet app. Two methods are provided as below to create a new network.

Method 1. Create a new network from the Overview page

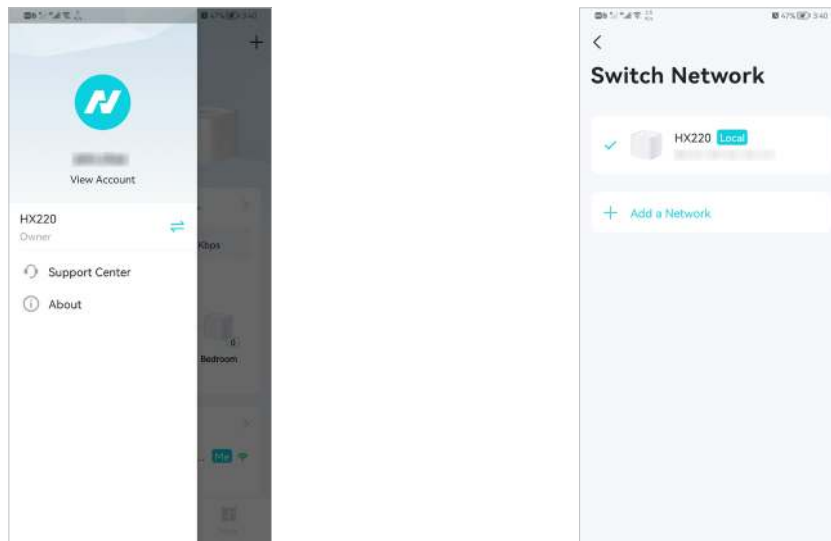
1. Tap **+** > [Create a Network](#).
2. Then follow app instructions to complete the setup.



Method 2. Create a new network from the Menu page

1. Tap to open the menu. Tap > [Add a Network](#).

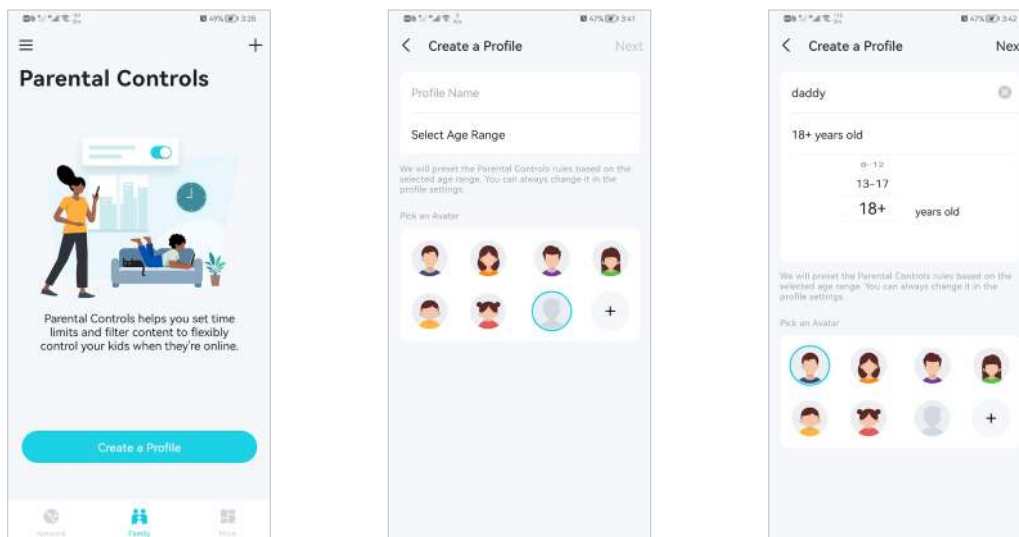
2. Then follow app instructions to complete the setup.

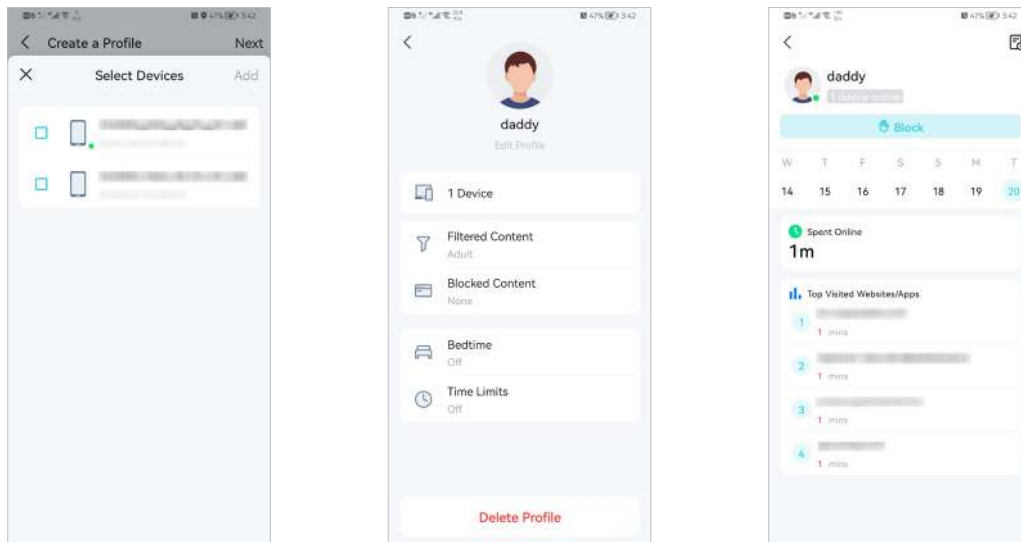


5.8. Parental Controls

Parental Controls helps you set time limits and filter content to flexibly control your kids when they're online.

1. In **Family**, tap **Create a Profile**.
2. Then follow app instructions to complete the setup.

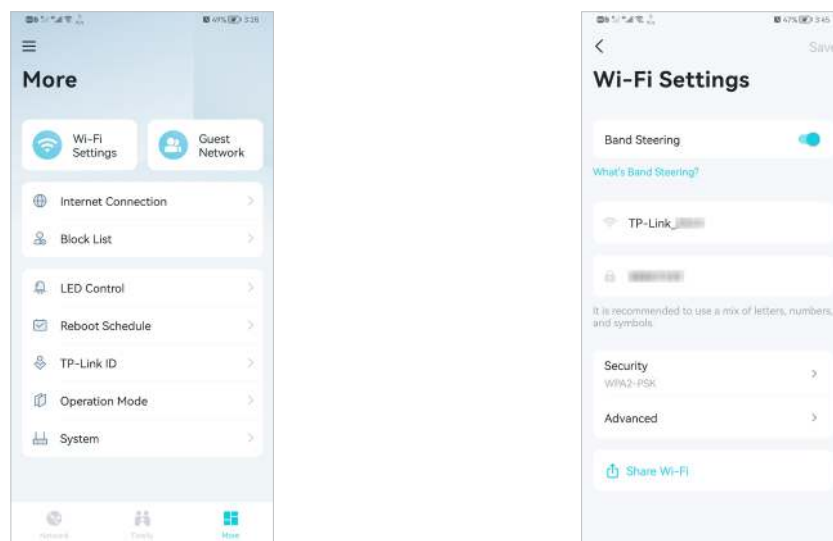




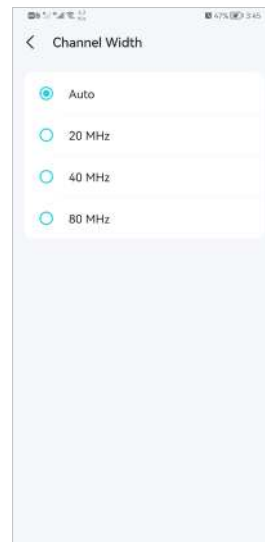
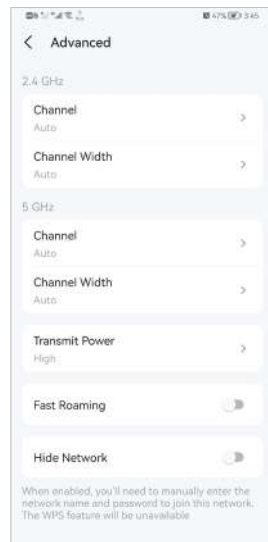
5.9. Wi-Fi Settings

You can change the network name and password of your main network at any time and share the network easily with family and friends.

1. In [More](#), Tap [Wi-Fi Settings](#).



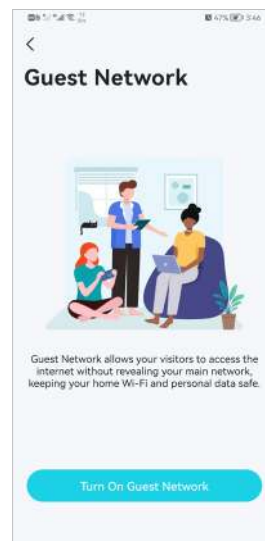
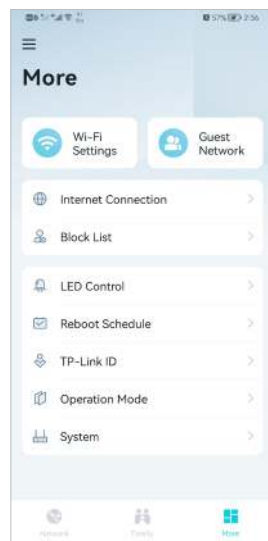
2. Manage main network (e.g. change your main network's Wi-Fi name and password, hide the network from Wi-Fi list, etc.).
3. Tap Advanced. For better Wi-Fi performance, set the channel width for 2.4GHz and 5GHz Wi-Fi as needed. (It is recommended to use the default settings.)



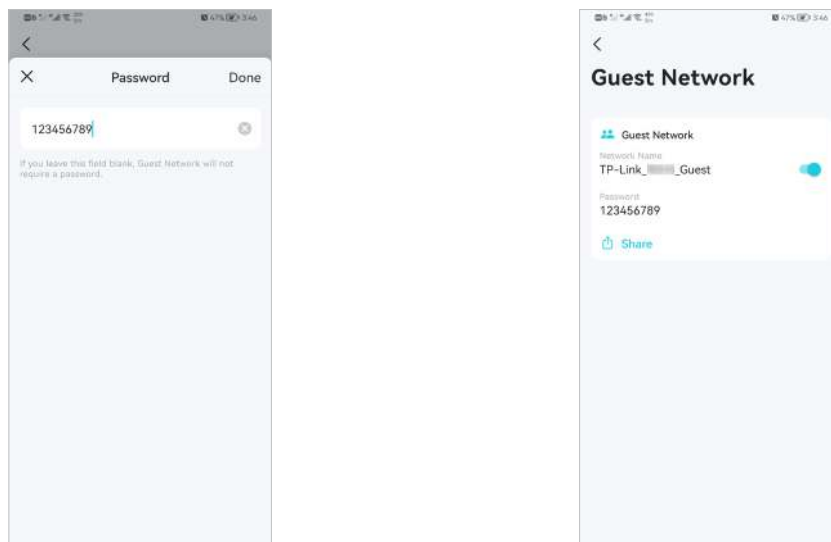
5. 10. Guest Network

You can create and share a separate network for guests to guarantee the security and privacy of your main network.

1. In **More**, Tap **Guest Network**.



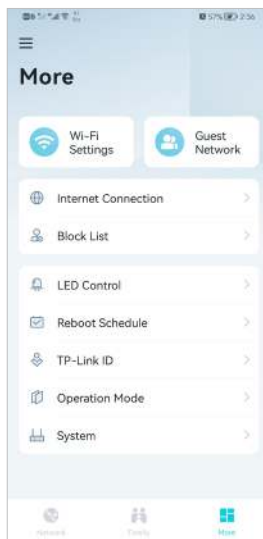
2. Set a Wi-Fi name and password for the guest network.



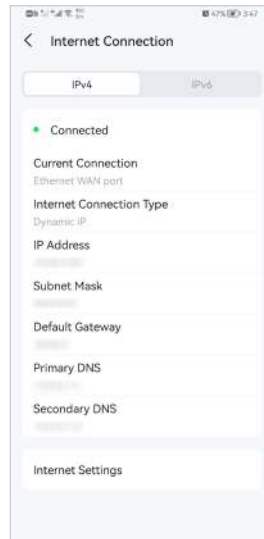
5. 11. Internet Connection

In Internet Connection, You can modify WAN settings (IPv4 & IPv6), enable MAC Clone mode.

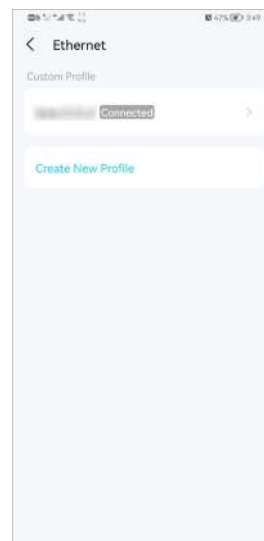
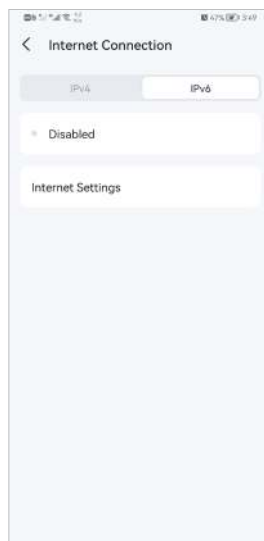
1. In [More](#), Tap [Internet Connection](#).

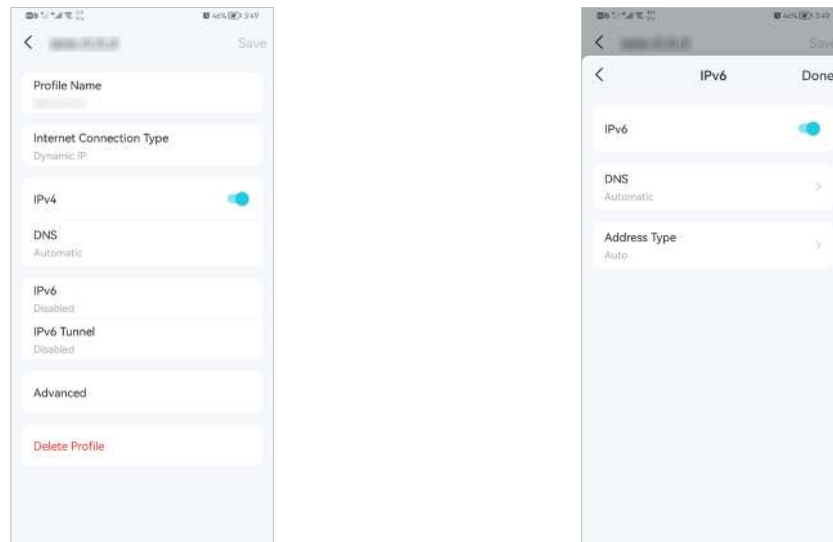


2. View [IPv4](#) details or change the internet connection type.



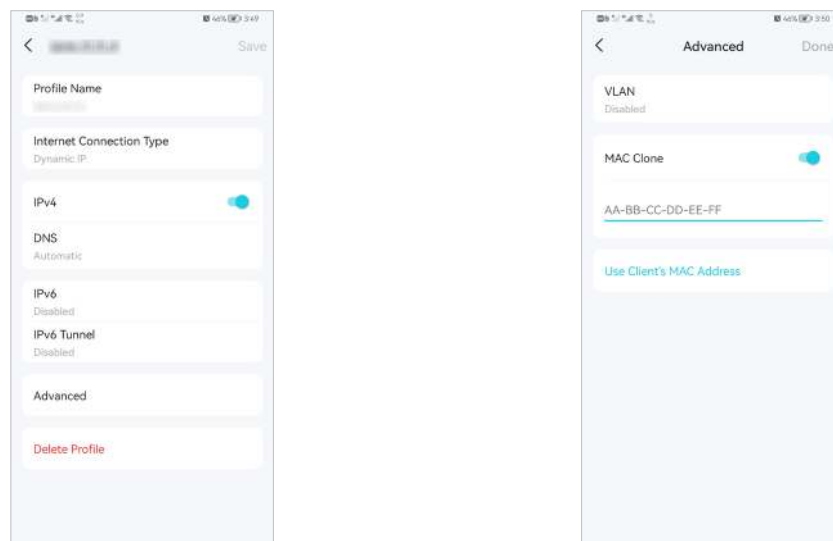
3. Enable **IPv6** to set up an IPv6 internet connection.





4. Tap **Advanced** and enable **MAC Clone** as needed.

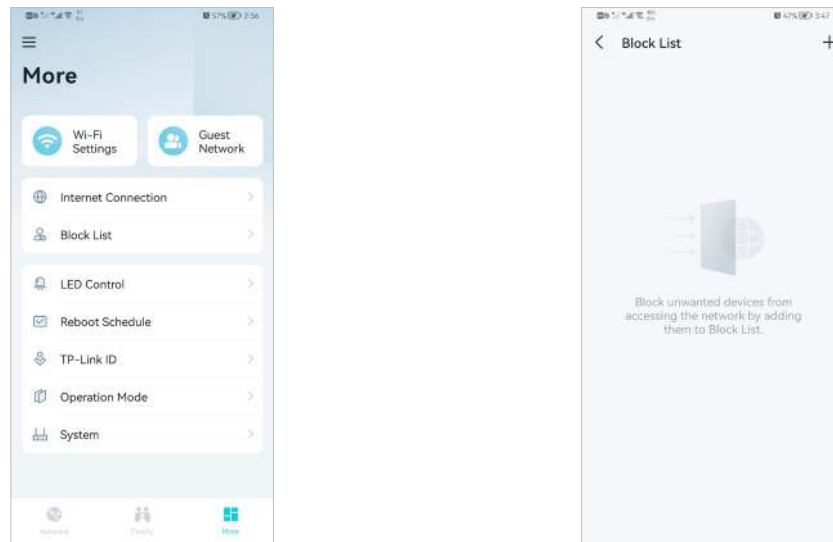
Tip: For more about MAC Clone, refer to <https://www.tp-link.com/support/faq/2925/>



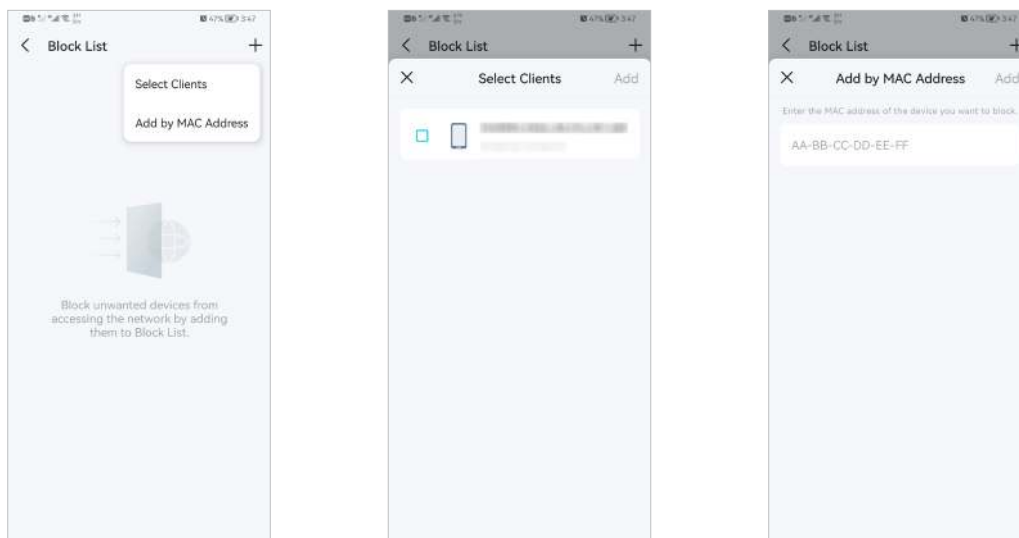
5. 12. Block List

Add devices to the block list to prevent the devices from accessing your network, ensuring the safety of your personal information shared in the network.

1. In **More**, Tap **Block List**.



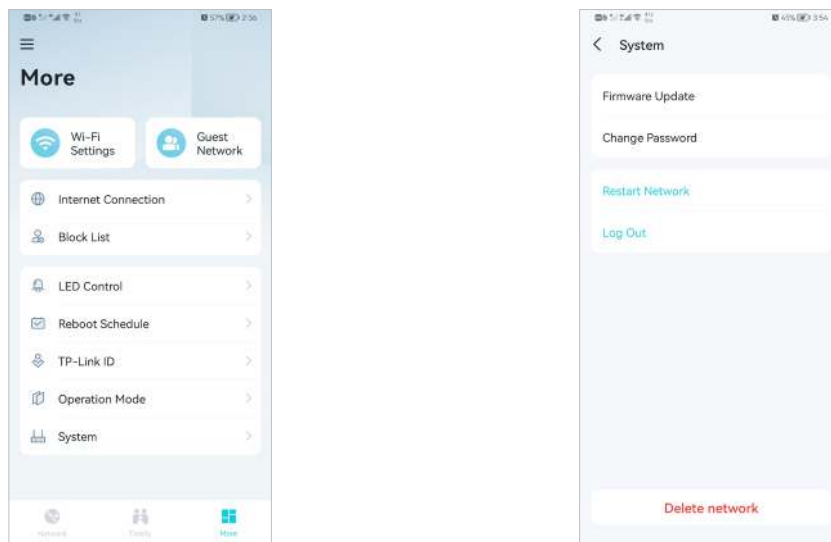
2. Tap **+** and add clients or other devices to the block list.



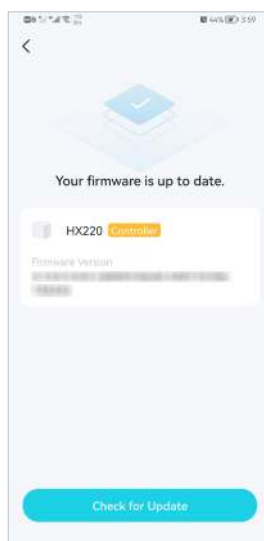
5. 13. Upgrade Your Mesh Device

TP-Link is dedicated to improving product features and providing a better customer experience. An up-to-date firmware provides better and more stable network performance. Always update your mesh device to the latest firmware version when prompted in the Aginet app.

1. In **More**, Tap **System** and **Firmware Update**.



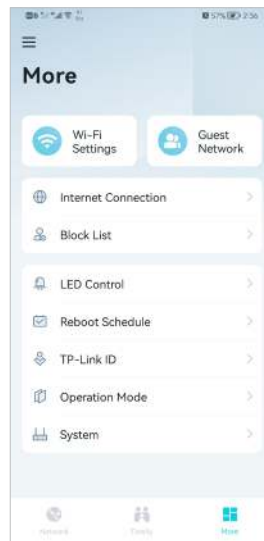
2. Download and install the firmware (if any) and follow app instructions to update your mesh device to the latest version.



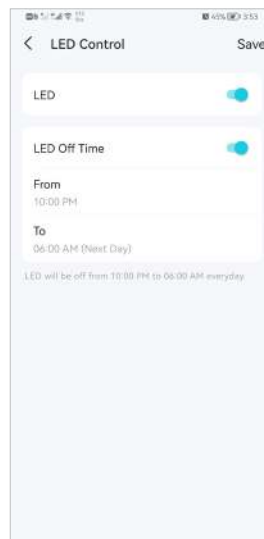
5. 14. Advanced Features

Additional features are available under the Advanced menu. You can control mesh device's LED, enable reboot schedule, bind your TP-Link ID, change the operation mode, configure system settings.

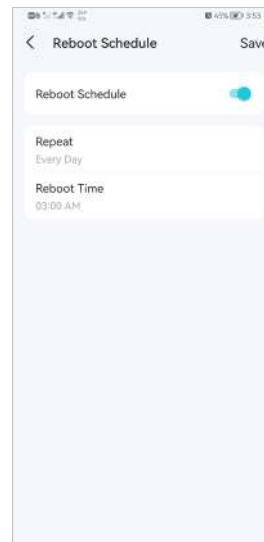
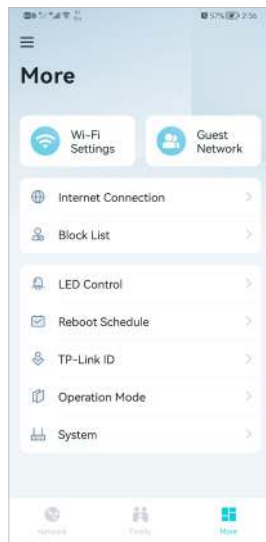
1. In [More](#), Tap [LED Control](#).



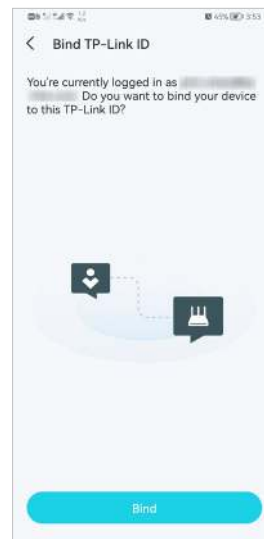
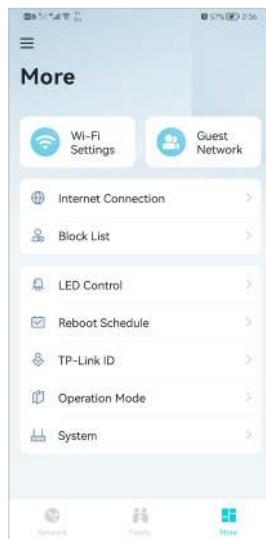
2. Toggle off **LED** to turn off the light on mesh device. Configure the **LED Off Time** to turn off the LED light at bedtime only.



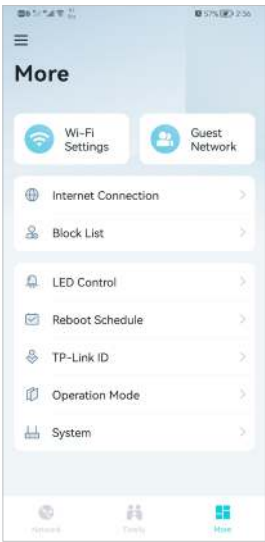
3. Enable **Reboot Schedule** as needed.



4. Bind your **TP-Link ID**.



5. Change the **Operation Mode** as needed.



Chapter 6

Customize Your Network Settings

This chapter introduces how to change the default settings or adjust the basic configuration of the mesh device using the web management page.

It contains the following sections:

- [Configure LAN Settings](#)
- [Configure IPv6 LAN Settings](#)
- [Set Up a Dynamic DNS Service Account](#)
- [Create Static Routes](#)
- [RIP Settings](#)
- [Specify Wireless Settings](#)
- [Schedule Your Wireless Function](#)
- [Use WPS for Wireless Connection](#)

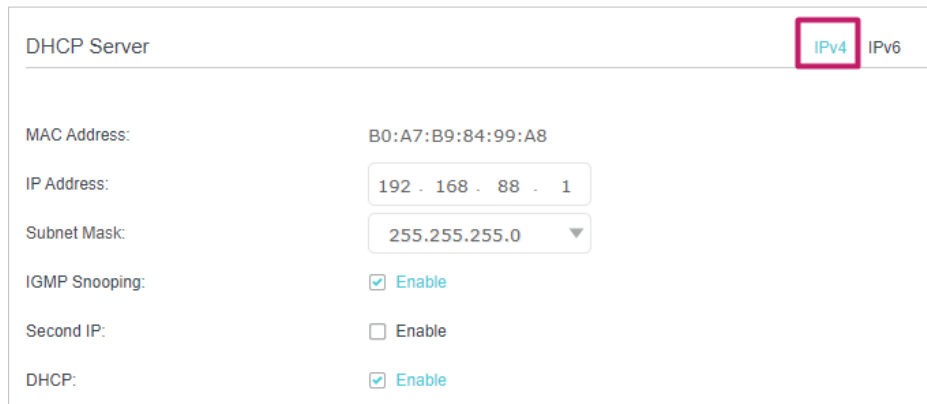
6.1. Configure LAN Settings

6.1.1. Change the LAN IP Address

The mesh device is preset with a default LAN IP 192.168.88.1, which you can use to log in to its web management page. The LAN IP address together with the Subnet Mask also defines the subnet that the connected devices are on. If the IP address conflicts with another device in your local network or your network requires a specific IP subnet, you can change it.

Follow the steps below to change your IP address.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [Network](#) > [LAN Settings](#) page and select [IPv4](#).



The screenshot shows the 'DHCP Server' configuration page. At the top right, there are two tabs: 'IPv4' (which is selected and highlighted with a red box) and 'IPv6'. Below the tabs, the following settings are visible:

- MAC Address: B0:A7:B9:84:99:A8
- IP Address: 192 . 168 . 88 . 1
- Subnet Mask: 255.255.255.0 (with a dropdown arrow)
- IGMP Snooping: ☒ Enable
- Second IP: ☐ Enable
- DHCP: ☒ Enable

3. Enter a new [IP Address](#) appropriate to your needs.
4. Select the [Subnet Mask](#) from the drop-down list. The subnet mask together with the IP address identifies the local IP subnet.
5. Keep [IGMP Snooping](#) enabled by default. IGMP snooping is the process of listening to IGMP (Internet Group Management Protocol) network traffic. The function prevents hosts on a local network from receiving traffic for a multicast group they have not explicitly joined.
6. You can configure the mesh device's [Second IP](#) and [Subnet Mask](#) for LAN interface through which you can also access the web management page.
7. Keep the rest settings as the default settings.
8. Click [Save](#) to make the settings effective.

6.1.2. Use the Mesh Device as a DHCP Server

You can configure the mesh device to act as a DHCP server to assign IP addresses to its clients. To use the DHCP server function of the mesh device, you must configure all computers on the LAN to obtain an IP Address automatically.

Follow the steps below to configure DHCP server.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [Network](#) > [LAN Settings](#) page and select [IPv4](#).

DHCP: ☒ Enable

☒ DHCP Server ☐ DHCP Relay

IP Address Pool: 192 . 168 . 88 . 2 - 192 . 168 . 88 . 249

Address Lease Time: 120 minutes. (1-2880. The default value is 1440.)

Default Gateway: 0 . 0 . 0 . 0 (Optional)

Default Domain: (Optional)

Primary DNS: 0 . 0 . 0 . 0 (Optional)

Secondary DNS: 0 . 0 . 0 . 0 (Optional)

Save

3. Enable [DHCP](#) function and select [DHCP Server](#).
4. Specify the [IP Address Pool](#), the start address and end address must be on the same subnet with LAN IP. The mesh device will assign addresses within this specified range to its clients. It is from 192.168.88.2 to 192.168.88.249 by default.
5. Enter a time duration in the [Address Lease Time](#) field. The [Address Lease Time](#) is the amount of time in which a DHCP client can lease its current dynamic IP address assigned by the mesh device. After the dynamic IP address expires, the user will be automatically assigned a new dynamic IP address.
6. Keep the rest settings as the default settings and click [Save](#).

Note:

1. The mesh device can be configured to work as a [DHCP Relay](#). A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. If it is enabled, the DHCP requests from local PCs will be forwarded to the DHCP server that runs on WAN side.
2. You can also appoint IP addresses within a specified range to devices of the same type by using [Condition Pool](#) feature. For example, you can assign IP addresses within the range (192.168.88.50 to 192.168.88.80) to Camera devices, thus facilitating the network management. Enable DHCP feature and configure the parameters according to your situation on the [Advanced](#) > [Network](#) > [LAN Settings](#) page.

6.1.3. Reserve LAN IP Addresses

You can view and add a reserved address for a client. When you specify an IP address for a device on the LAN, that device will always receive the same IP address each time when it accesses the DHCP server. If there are some devices in the LAN that require permanent IP addresses, please configure Address Reservation on the mesh device for the purpose.

Follow the steps below to reserve an IP address for your devices.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [Network](#) > [LAN Settings](#) page, and select [IPv4](#).
3. Scroll down to the [Address Reservation](#) section, and click [Add](#) to add an address reservation entry for your device.

The screenshot displays the 'Address Reservation' section of a network configuration interface. At the top, there are '+ Add' and '- Delete' buttons. Below is a table with the following structure:

☐	MAC Address	Reserved IP Address	Group	Enable	Modify
--	--	--	--	--	--

Below the table, there is a form to add a new entry:

- MAC Address: [Input field with dashes]
- IP Address: [Input field with dots]
- Group: [Dropdown menu showing 'Default']
- ☒ Enable This Entry
- [Scan] button
- [Cancel] and [OK] buttons

4. Enter the [MAC Address](#) of the device for which you want to reserve IP address.
5. Specify the [IP address](#) which will be reserved by the mesh device.
6. Select the [Enable This Entry](#) check box and click [OK](#) to make the settings effective.

6.2. Configure IPv6 LAN Settings

Based on the IPv6 protocol, the mesh device provides two ways to assign IPv6 LAN addresses:

- Configure the RADVD (Mesh Device Advertisement Daemon) address type
- Configure the DHCPv6 Server address type

6.2.1. Configure the RADVD Address Type

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [Network](#) > [LAN Settings](#).
3. Select [IPv6](#) to configure IPv6 LAN parameters.

DHCP Server IPv4 **IPv6**

Group: Default

Address Type: ☒ RADVD ☐ DHCPv6 Server

Enable RDNSS ☐ Enable

Enable ULA Prefix ☐ Enable

Site Prefix Type: ☒ Delegated ☐ Static

WAN Connection: No available interface ▼

Save

- 1) Select [RADVD](#) as the address type to make the mesh device assign IPv6 address prefixes to hosts.

Note:

Do not select the [Enable RDNSS](#) and [Enable ULA Prefix](#) check boxes unless required by your ISP. Otherwise you may not be able to access the IPv6 network. For more information about RDNSS and ULA Prefix, contact our technical support.

- 2) Keep [Site Prefix Type](#) as the default setting [Delegated](#). If your ISP has provided a specific IPv6 site prefix, select [Static](#) and enter the prefix.
 - 3) Keep [WAN Connection](#) as the default settings.
4. Click [Save](#) to make the settings effective.

6.2.2. Configure the DHCPv6 Server Address Type

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [Network](#) > [LAN Settings](#).
3. Select [IPv6](#) to configure IPv6 LAN parameters.

DHCP Server IPv4 | IPv6

Group: Default

Address Type: ☐ RADVD ☒ DHCPv6 Server

Starting IPv6 Address: :: 1 (1~FFFE)

Ending IPv6 Address: :: FFFE (1~FFFE)

Address Lease Time: 7200 seconds

Site Prefix Type: ☒ Delegated ☐ Static

WAN Connection: No available interface

Save

- 1) Select **DHCPv6 Server** as the address type to make the mesh device assign IPv6 addresses to hosts.
 - 2) Specify the **Starting/Ending IPv6 Address** for the IPv6 suffixes. The mesh device will generate IPv6 addresses within the specified range.
 - 3) Keep **Address Lease Time** as the default setting.
 - 4) Keep **Site Prefix Type** as the default value **Delegated**. If your ISP has provided a specific IPv6 site prefix, select **Static** and enter the prefix.
 - 5) Keep **WAN Connection** as the default setting.
4. Click **Save** to make the settings effective.

6.3. Set Up a Dynamic DNS Service Account

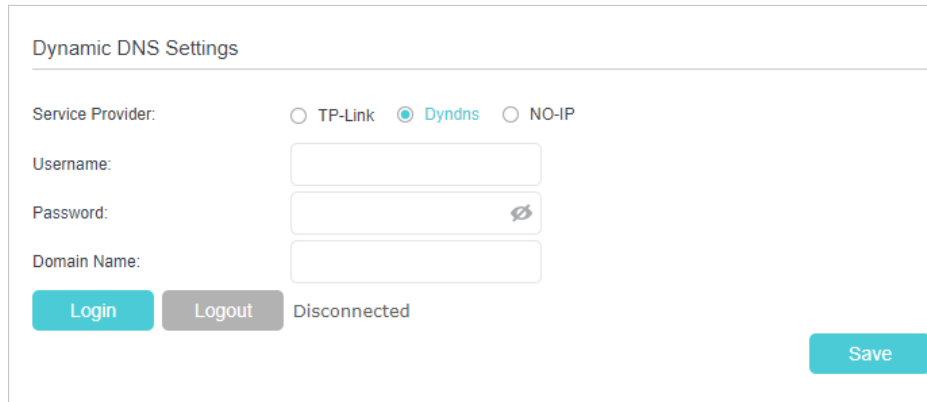
Most ISPs (Internet service providers) assign a dynamic IP address to the mesh device and you can use this IP address to access your mesh device remotely. However, the IP address can change any time and you don't know when it changes. In this case, you might need the DDNS (Dynamic Domain Name Server) feature on the mesh device to allow you and your friends to access your mesh device and local servers (FTP, HTTP, etc.) using domain name, in no need of checking and remembering the IP address.

Note: DDNS does not work if the ISP assigns a private WAN IP address (such as 192.168.1.x) to the mesh device.

To set up DDNS, please follow the instructions below:

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to **Advanced > Network > Dynamic DNS**.
3. Select the **Service Provider** (TP-Link/Dyndns/NO-IP).

4. Log in with your DDNS account, select a service provider. Enter the username, password and domain name of the account (such as lisa.ddns.net).



5. Click [Log in](#) and [Save](#).

 **Tips:** If you want to use a new DDNS account, please log out first, then log in with the new account.

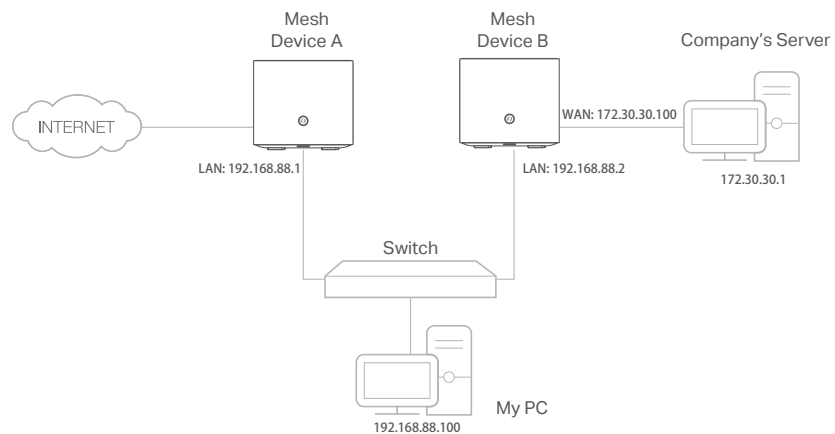
6.4. Create Static Routes

A static route is a pre-determined path that network information must travel to reach a specific host or network. Data from one point to another will always follow the same path regardless of other considerations. Normal internet usage does not require this setting to be configured.

I want to:

Visit multiple networks and multiple servers at the same time.

[For example](#), in a small office, my PC can surf the internet through Mesh Device A, but I also want to visit my company's network. Now I have a switch and another Mesh Device B. I connect the devices as shown in the following image so that the physical connection between my PC and my company's server is established. To surf the internet and visit my company's network at the same time, I need to configure the static routing.



How can I do that?

1. Make sure the mesh devices use different LAN IP addresses on the same subnet. Disable Mesh Device B's DHCP function.
2. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the Mesh Device A.
3. Go to **Advanced > Network > Static Routing**. Select your current **WAN Interface** and click **Save**.

Default Gateway Settings IPv4 | IPv6

Select a WAN interface as the system default gateway:

Select WAN Interface: ipoe_eth_0_2_d Save

Static Routing + Add - Delete

☐	ID	Network Destination	Subnet Mask	Gateway	Status	Modify
☐	--	--	--	--	--	--

4. Click **Add** to add a new static routing entry. Finish the settings according to the following explanations:

Static Routing

+ Add - Delete

☐	ID	Network Destination	Subnet Mask	Gateway	Enable	Modify
--	--	--	--	--	--	--

Network Destination:

Subnet Mask:

Gateway:

Interface:

☒ Enable This Entry

- **Network Destination:** The destination IP address that you want to assign to a static route. This IP address cannot be on the same subnet with the WAN IP or LAN IP of the Mesh Device A. In the example, the IP address of the company network is the destination IP address, so here we enter 172.30.30.1.
 - **Subnet Mask:** Determines the destination network with the destination IP address. If the destination is a single IP address, enter 255.255.255.255; otherwise, enter the subnet mask of the corresponding network IP. In the example, the destination network is a single IP, so here we enter 255.255.255.255.
 - **Gateway:** The IP address of the gateway device to which the data packets will be sent. This IP address must be on the same subnet with the mesh device's IP which sends out the data. In the example, the data packets will be sent to the LAN port of Mesh Device B and then to the Server, so the default gateway should be 192.168.88.2.
 - **Interface:** Determined by the port (WAN/LAN) that sends out the data packets. In the example, the data is sent to the gateway through the LAN port of Mesh Device A, so **LAN** should be selected.
5. Select the **Enable This Entry** check box to enable this entry.
 6. Click **Save** to make the settings effective.

Done!

Open a web browser on your PC. Enter the company server's IP address to visit the company network.

6.5. RIP Settings

To activate RIP for the WAN interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Save' button to start/stop RIP and save the configuration.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
2. Go to [Advanced](#) > [Network](#) > [RIP Settings](#).
3. Configure RIP settings.

RIP Settings

To activate RIP for the WAN interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Save' button to start/stop RIP and save the configuration.

NOTE: RIP cannot be configured on the WAN interface which has NAT enabled.

MD5 Authentication: ☒ [Enable](#)

MD5 Key ID 0:

MD5 Key ID 1:

[Save](#)

Interface	Version	AcceptRA	SendRA	Enabled	RipngEnabled	Modify
--	--	--	--	--	--	--

- [MD5 Authentication](#) - Enable MD5 Authentication to enhance the rip RA packets security.
- [MD5 Key ID 0](#) - Setting the MD5 Key ID 0 value.
- [MD5 Key ID 1](#) - Setting the MD5 Key ID 1 value.
- [Interface](#) - The WAN interface name of the RIP rule table's entry used in.
- [Version](#) - The RIP version (RIPv1/RIPv2) of the RIP rule table's entry used.
- [AcceptRA](#) - Enable it to make the RIP rule entry can accept the mesh device Advertisement.
- [SendRA](#) - Enable it to make the RIP rule entry can send the mesh device Advertisement.
- [Enabled](#) - Enable it to make the RIP rule entry active for IPv4.
- [RipngEnabled](#) - Enable it to make the RIP rule entry active for IPv6, which is also known as Ripng.
- [Modify](#) - Click here to modify the RIP rule entry.

6.6. Specify Wireless Settings

6.6.1. Change Basic Wireless Settings

The mesh device's wireless network name (SSID) and password, and security option are preset in the factory. The preset SSID and password can be found on the product label. You can customize the wireless settings according to your needs.

Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.

➤ **To enable or disable the wireless function:**

1. Go to [Basic](#) > [Wireless](#).
2. The wireless radio is enabled by default. If you want to disable the wireless function of the mesh device, just clear the [Enable](#) check boxes. In this case, all the wireless settings will be invalid.

➤ **To change the wireless network name (SSID) and wireless password:**

1. Go to [Basic](#) > [Wireless](#).
2. Enter a new SSID (32 characters at most) in the [Network Name \(SSID\)](#) field and a new password in the [Password](#) field and click [Save](#). The SSID and password are case-sensitive.

■ **Note:**

If you use a wireless device to change the wireless settings, you will be disconnected after the new settings are effective. Please write down the new SSID and password for future use.

➤ **To hide SSID:**

1. Go to [Basic](#) > [Wireless](#).
2. Select [Hide SSID](#), and your SSID will not be broadcast. Your SSID won't display on your wireless devices when you scan for local wireless networks and you need to manually join the network.

➤ **To change the mode or channel:**

1. Go to [Advanced](#) > [Wireless](#) > [Wireless Settings](#).

Mode: 802.11b/g/n mixed

Channel: Auto

Channel Width: Auto

Transmit Power: ☐ Low ☐ Middle ☒ High

Save

2. Select the wireless network mode or channel and click [Save](#) to make the settings effective.

Mode: Select the desired transmission mode.

- 802.11b/g/n mixed: Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.
- 802.11b/g/n/ax mixed: Select if you are using a mix of 802.11b, 11g, 11n and 11ax wireless clients.
- 802.11a/n/ac mixed: Select if you are using a mix of 802.11a, 11n, and 11ac wireless clients.
- 802.11a/n/ac/ax mixed: Select if you are using a mix of 802.11a, 11n, 11ac and 11ax wireless clients.

Note: When 802.11n only mode is selected, only 802.11n wireless stations can connect to the mesh device. It is strongly recommended that you select 802.11b/g/n mixed (for 2.4GHz) and 802.11a/n/ac/ax mixed (for 5GHz), and all of 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax wireless stations can connect to the mesh device.

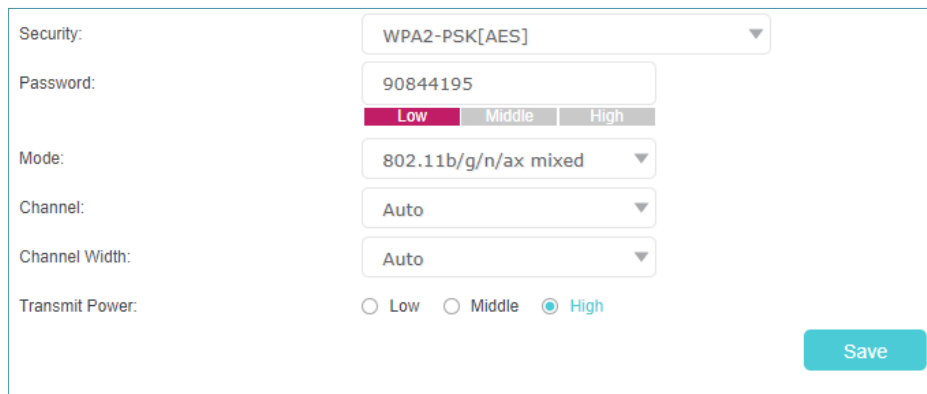
Channel: Select the channel you want to use from the drop-down list. This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

Channel Width: Select the channel width from the drop-down list. The default setting is [Auto](#), which can adjust the channel width for your clients automatically.

Transmit Power: Select Low, Middle, or High to specify the data transmit power. The default and recommended setting is [High](#).

➤ **To change the security option:**

1. Go to [Advanced](#) > [Wireless](#) > [Wireless Settings](#).



The screenshot shows a configuration interface for wireless settings. It includes the following fields and options:

- Security:** A dropdown menu currently set to **WPA2-PSK[AES]**.
- Password:** A text input field containing **90844195**.
- Power Level:** Three radio buttons labeled **Low**, **Middle**, and **High**. The **High** option is selected and highlighted in red.
- Mode:** A dropdown menu currently set to **802.11b/g/n/ax mixed**.
- Channel:** A dropdown menu currently set to **Auto**.
- Channel Width:** A dropdown menu currently set to **Auto**.
- Transmit Power:** Three radio buttons labeled **Low**, **Middle**, and **High**. The **High** option is selected and highlighted in blue.
- Save:** A blue button located at the bottom right of the form.

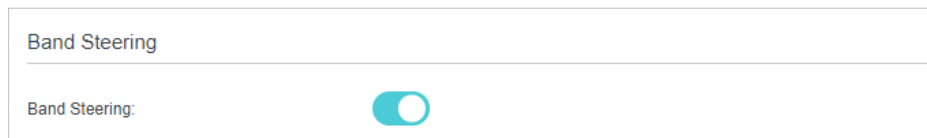
2. Select an option from the [Security](#) drop-down list and configure the related parameters. The mesh device provides four options, No Security, WPA-PSK[TKIP]+WPA2-PSK[AES], WPA2-PSK[AES], WPA2-PSK[AES]+WPA3-Personal. WPA3 uses the newest standard and the security level is the highest. We recommend you don't change the default settings unless necessary.

3. Click [Save](#) to make the settings effective.

➤ **To enable network roaming:**

Network roaming helps devices choose better AP based on actual conditions to balance network demands. (For mesh devices, Band Steering is disabled by default.)

1. Go to [Advanced](#) > [Wireless](#) > [Wireless Settings](#).
2. Locate the [Band Steering](#) section, select the [Enable](#) check box to make the settings effective.



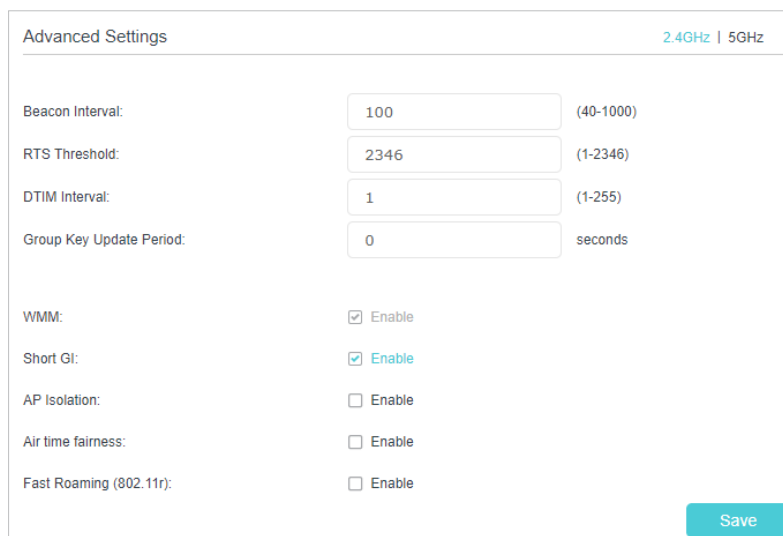
6.6.2. Advanced Wireless Settings

Advanced wireless settings are for those who want more network controls. You can follow the instructions below to configure your mesh device.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for your mesh device.
2. Go to [Advanced](#) > [Wireless](#) > [Advanced Settings](#).

➤ **To change basic advanced settings:**

Locate the [Advanced Settings](#) section and configure the advanced settings according to the explanation below, and then click [Save](#).



- **Beacon Interval:** Enter a value between 40 and 1000 in milliseconds to determine the duration between which beacon packets are broadcast by the mesh device to synchronize the wireless network. The default is 100 milliseconds.

- **RTS Threshold:** Enter a value between 1 and 2347 to determine the packet size of data transmission through the mesh device. By default, the RTS (Request to Send) Threshold size is 2347. If the packet size is greater than the preset threshold, the mesh device sends Request to Send frames to a particular receiving station and negotiates the sending of a data frame, or else the packet will be sent immediately.
- **DTIM Interval:** Enter a value between 1 and 255 to determine the interval of the Delivery Traffic Indication Message (DTIM). 1 indicates the DTIM Interval is the same as **Beacon Interval**.
- **Group Key Update Period:** Enter the number of seconds to control the time interval for the encryption key automatic renewal. The default is 0, indicating no key renewal.
- **WMM:** This feature guarantees the packets with high-priority messages being transmitted preferentially. WMM is enabled compulsively under 802.11n or 802.11ac mode.
- **Short GI:** This feature is enabled by default and recommended to increase the data capacity by reducing the Guard Interval (GI) time.
- **AP Isolation:** Select this check box to enable the AP Isolation feature that allows you to confine and restrict all wireless devices on your network from interacting with each other, but still able to access the internet.
- **Air time fairness:** Select this checkbox to enable the Airtime Fairness(ATF) feature that allows you to optimize the throughput of each flow. The ATF traffic scheduler uses the per-destination airtime targets to balance airtime usage across flow destinations.
- **Fast Roaming (802.11r):** This feature allows a client device to roam quickly in environments implementing the WPA2 Enterprise security, by ensuring that the client device does not need to re-authenticate to the RADIUS server every time it roams from one access point to another. It's recommended that you keep the feature enabled for better roaming experiences.

 Note:

If you are not familiar with the settings mentioned above, it's strongly recommended that you keep the provided default settings; otherwise it may result in lower wireless network performance.

➤ **To enable or disable WPS function:**

WPS (Wi-Fi Protected Setup) provides you with an easier approach to set up a security-protected Wi-Fi connection. This function is enabled by default, but if you do not need this function, clear the WPS **Enable** check box.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for your mesh device.
2. Go to **Advanced > Wireless > WPS**.

The screenshot shows a web interface for configuring a router. It has two main sections: 'Router PIN' and 'WPS Settings'. In the 'Router PIN' section, there is a toggle for 'Enable Router's PIN' which is turned on. Below it, the 'Router's PIN' is displayed as '02824260' in a text box, with 'Generate' and 'Default' buttons to its right. The 'WPS Settings' section has a toggle for 'Enable WPS' which is also turned on; this toggle is highlighted with a red rectangular border. Below the 'Enable WPS' toggle, there is a section titled 'Select a setup method:' with two radio button options: 'Push Button (Recommended)' (which is selected) and 'PIN Number'. Below these options, there is a 'Connect' button and a message 'Failed to add the device!'.

➤ **To create multi-SSID network:**

The mesh device supports additional up to three multi-SSID wireless networks for client access in each wireless band. You can specify the access and security settings to ensure network security and privacy according to your situation.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for your mesh device.
2. Go to [Advanced](#) > [Wireless](#) > [Multi-SSID](#).
 - 1) Locate the [Multi-SSID](#) section, and enable [2.4GHz](#) or [5GHz](#) to open the corresponding setup page.
 - 2) Select the [Enable MSSID 1](#) or [2](#) check box(es) to enable the corresponding multi-SSID network.

Multi-SSID 2.4GHz 5GHz

MSSID1: ☒ Enable

Network Name (SSID): ☐ Hide SSID

Security:

See each other: ☒ Allow guests to see each other

USB Storage Sharing: ☐ Allow guests to access my USB Storage Sharing

MSSID2: ☒ Enable

Network Name (SSID): ☐ Hide SSID

Security:

See each other: ☒ Allow guests to see each other

USB Storage Sharing: ☐ Allow guests to access my USB Storage Sharing

[Save](#)

- 3) Enter a new [Network Name \(SSID\)](#) or use the default name, this field is case sensitive. Don't select [Hide SSID](#) unless you want your guests to manually input the SSID for Wi-Fi access.
- 4) Select the [Security](#) option for the multi-SSID network, [WPA/WPA2 Personal](#) is recommended, and you can set a password for the network.

If you want to allow the clients in your Multi-SSID network to communicate with each other via methods such as Network Neighborhood and Ping, select the [Allow Guests to See Each Other](#) check box.

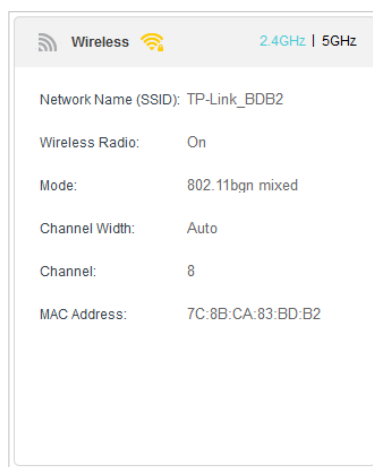
If you want to allow the clients in your Multi-SSID network to access your mesh device's USB storage sharing via methods such as Network Neighborhood and FTP, select the [Allow Guests to Access My USB Storage Sharing](#) check box.

- 5) Repeat step 1) to step 4) to set other wireless networks if needed, and click [Save](#) to make the settings effective.

6.6.3. View Wireless Information

➤ **To view the detailed wireless network settings:**

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [Status](#) page. You will find the [Wireless](#) panel.
3. Click [2.4GHz](#) or [5GHz](#) to view the wireless details.



🔗 **Tips:** You can also see the wireless details by clicking the mesh device icon on [Basic > Network Map](#).

➤ **To view the detailed information of the connected wireless clients:**

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced > Wireless > Statistics](#) page.
3. You can view the detailed information of the wireless clients, including its connection type and security option as well as the packets transmitted.

🔗 **Tips:** You can also see the wireless details by clicking the wireless clients icon on [Basic > Network Map](#).

6.7. Schedule Your Wireless Function

You can automatically turn off your wireless networks when you do not need the wireless connection.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced > Wireless > Wireless Schedule](#).
3. Enable the [Wireless Schedule](#) function.

Wireless Schedule

Wireless Schedule:

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
0:00							
1:00							
2:00							
3:00							
4:00							
5:00							
6:00							
7:00							
8:00							
9:00							
10:00							
11:00							
12:00							
13:00							
14:00							
15:00							
16:00							
17:00							
18:00							
19:00							
20:00							
21:00							
22:00							
23:00							
24:00							

Wi-Fi Off

Restore

Save

4. Click [Add](#) to set the [Wireless Off Time](#), and click [Save](#) to make the settings effective.

Note:

1. Make sure that the time of the mesh device is correct before using this function. For details, refer to [Set System Time](#).
2. The wireless LED will turn off if the corresponding wireless network is disabled.
3. The wireless network will be automatically turned on after the time period you set.

6.8. Use WPS for Wireless Connection

You can use WPS (Wi-Fi Protected Setup) to add a new wireless device to your existing network quickly and easily.

Method 1: Use the WPS button

Use this method if your client device has a WPS button.

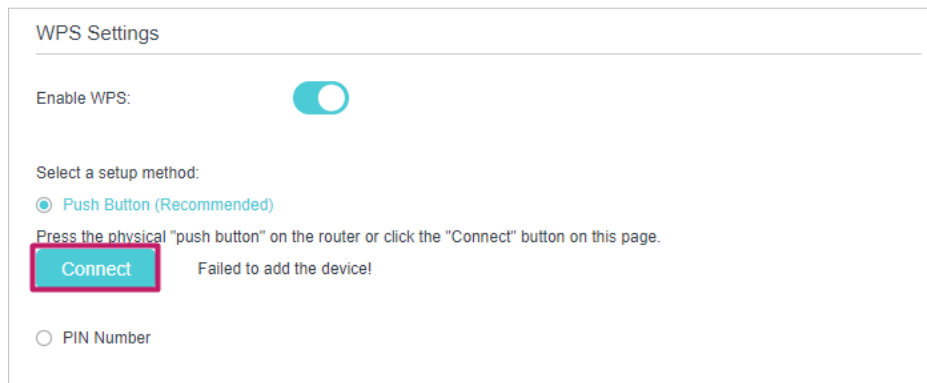
1. Press the WiFi/WPS button of the mesh device.
2. Press the WPS button of the client device directly.
3. The WPS LED flashes for about 2 minutes during the WPS process.

4. When the WPS LED is on, the client device has successfully connected to the mesh device.

Method 2: Use the "Connect" button on the web management page

Use this method if your client device has a WPS button.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [Wireless](#) > [WPS](#) page.



WPS Settings

Enable WPS: ☒

Select a setup method:

☒ Push Button (Recommended)

Press the physical "push button" on the router or click the "Connect" button on this page.

Connect Failed to add the device!

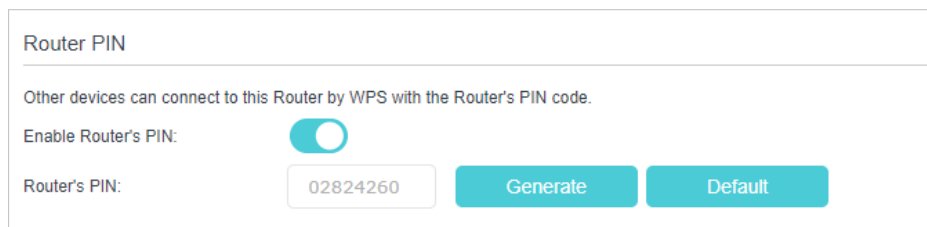
☐ PIN Number

3. Click [Connect](#) on the page.
4. Press the WPS button of the client device directly.
5. The WPS LED of the mesh device flashes for about 2 minutes during the WPS process.
6. When the WPS LED is on, the client device has successfully connected to the mesh device.

Method 3: Enter the mesh device's PIN on your client device

Use this method if your client device asks for the mesh device's PIN.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [Wireless](#) > [WPS](#), and enable [Mesh Device's PIN](#).



Router PIN

Other devices can connect to this Router by WPS with the Router's PIN code.

Enable Router's PIN: ☒

Router's PIN: 02824260 [Generate](#) [Default](#)

3. Take a note of the current PIN of the mesh device. You can also click the [Generate](#) button to get a new PIN.

4. Enter the mesh device's PIN on the client device. (The default PIN is also printed on the label of the mesh device.)
5. The WPS LED flashes for about 2 minutes during the WPS process.
6. When the WPS LED is on, the client device has successfully connected to the mesh device.

Note:

1. The WPS LED on the mesh device will light on for five minutes if the device has been successfully added to the network.
2. The WPS function cannot be configured if the wireless function of the mesh device is disabled. Please make sure the wireless function is enabled before configuring WPS.

Method 4: Enter the client device's PIN on the mesh device

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to **Advanced > Wireless > WPS**, and click **PIN Number**.
3. Enter the **Client's PIN**.



☒ PIN Number

Enter the client's PIN:

Connect

4. Then click the **Connect** button.
5. **Device has been added successfully!** or the similar information will appear on the web page, which means the client device has successfully connected to the mesh device.

Chapter 7

Multi-SSID

Multi-SSID function allows you to provide Wi-Fi access for your visitors without disclosing your main network. When you have guests in your house, apartment, or workplace, you can create a multi-SSID wireless network for them. In addition, you can customize the network settings to ensure your network security and privacy.

➤ **To create a multi-SSID network:**

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Basic > Multi-SSID](#) or [Advanced > Wireless > Multi-SSID](#).
3. Create the multi-SSID network as needed.

The screenshot shows the 'Multi-SSID' configuration page. At the top right, there are tabs for '2.4GHz' and '5GHz'. The page is divided into two sections for 'MSSID1' and 'MSSID2'. Each section contains the following fields:

- MSSID1:**
 - ☒ Enable
 - Network Name (SSID): ☐ Hide SSID
 - Security:
 - See each other: ☒ Allow guests to see each other
- MSSID2:**
 - ☒ Enable
 - Network Name (SSID): ☐ Hide SSID
 - Security:
 - See each other: ☒ Allow guests to see each other

A 'Save' button is located at the bottom right of the form.

- 1) Select the [Enable](#) check box to create the corresponding multi-SSID network. You can create three multi-SSID wireless networks at most.
- 2) Enter a new [Network Name \(SSID\)](#) or use the default name, this field is case-sensitive. Don't select [Hide SSID](#) unless you want your guests to manually input the SSID for Wi-Fi access.
- 3) Select the [Security](#) option for the multi-SSID wireless network, [WPA/WPA2/WPA3 Personal \(Recommended\)](#) is recommended, and you can set a password for the network.
4. Click [Save](#) to make the settings effective. Now your guests can access your multi-SSID wireless network using the SSID and password specified.

Chapter 8

TP-Link Cloud Service

TP-Link Cloud service provides a better way to manage your cloud devices. Log in to your mesh device with a TP-Link ID, and you can easily monitor and manage your home network when you are out and about via the Aginet app. To ensure that your mesh device stays new and gets better over time, the TP-Link Cloud will notify you when an important firmware upgrade is available. Surely you can also manage multiple TP-Link Cloud devices with a single TP-Link ID.

This chapter introduces how to register a new TP-Link ID, bind or unbind TP-Link IDs to manage your mesh device, and the Aginet app with which you can manage your home network no matter where you may find yourself.

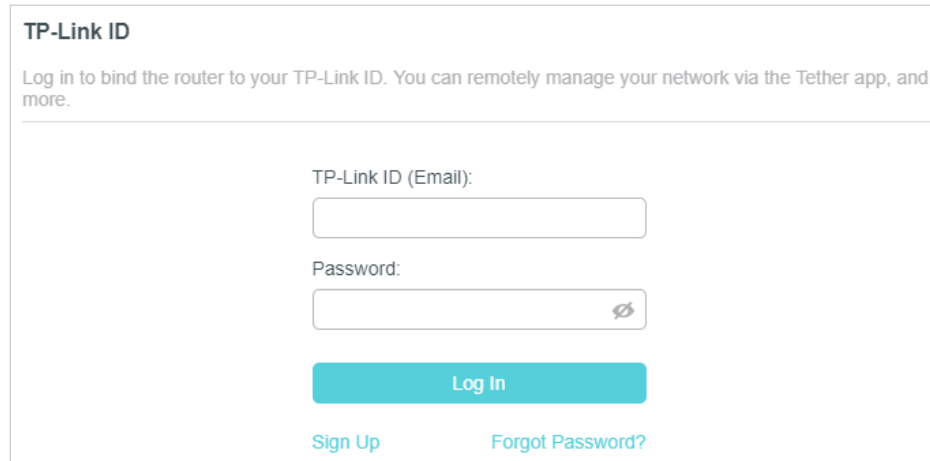
It contains the following sections:

- [Register a TP-Link ID](#)
- [Change Your TP-Link ID Information](#)
- [Manage the User TP-Link IDs](#)
- [Manage the Mesh Device via the TP-Link Aginet App](#)

8.1. Register a TP-Link ID

If you have skipped the registration during the Quick Setup process, you can:

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Basic > TP-Link Cloud](#).
3. Click [Sign Up](#) and follow the instructions to register a TP-Link ID.

The image shows a web form titled "TP-Link ID". Below the title is a subtitle: "Log in to bind the router to your TP-Link ID. You can remotely manage your network via the Tether app, and more." The form contains two input fields: "TP-Link ID (Email):" and "Password:". The "Password:" field has a small eye icon to its right. Below the input fields is a teal "Log In" button. At the bottom of the form are two links: "Sign Up" and "Forgot Password?".

TP-Link ID

Log in to bind the router to your TP-Link ID. You can remotely manage your network via the Tether app, and more.

TP-Link ID (Email):

Password:

Log In

[Sign Up](#) [Forgot Password?](#)

4. After activating your TP-Link ID, come back to the TP-Link Cloud page to log in. The TP-Link ID used to log in to the mesh device for the first time will be automatically bound as an [Admin](#).

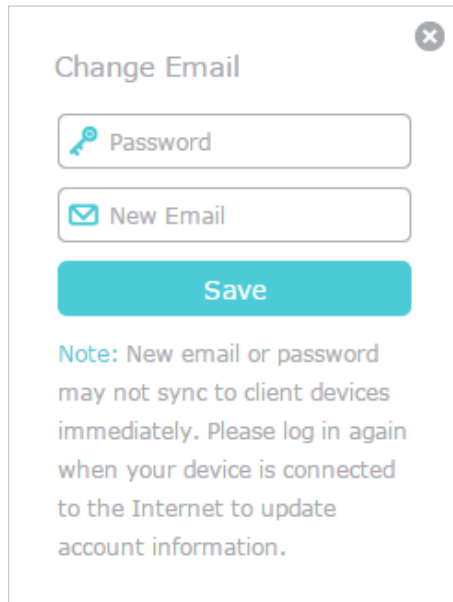
Note:

- To learn more about the [Admin](#) and [User](#) TP-Link ID, refer to [Manage the User TP-Link IDs](#).
- Once you have registered a TP-Link ID on the web management page, you can only register another TP-Link ID via the Aginet APP. Please refer to [Manage the Mesh Device via the TP-Link Aginet App](#) to install the app.
- If you want to unbind the admin TP-Link ID from your mesh device, please go to [Basic > TP-Link Cloud](#), and click [Unbind](#) in the [Device Information](#) section.

8.2. Change Your TP-Link ID Information

Follow the steps below to change your email address and password of your TP-Link ID as needed.

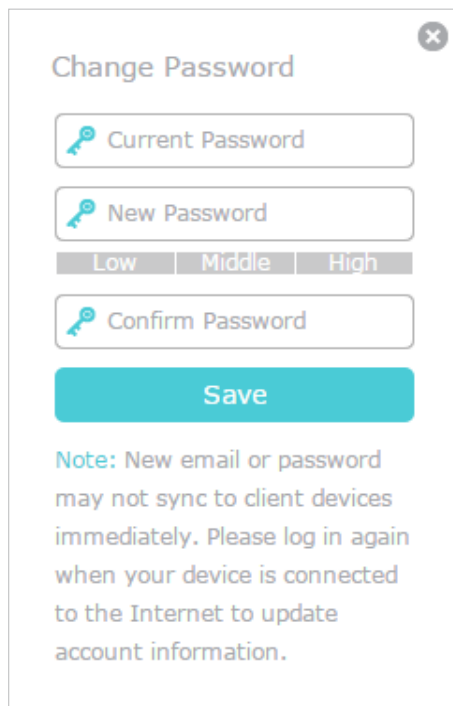
1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID.
2. Go to [Basic > TP-Link Cloud](#), and focus on the [Account Information](#) section.
 - **To change your email address:**
 1. Click  behind the Email.
 2. Enter the password of your TP-Link ID, then a new email address. And click [Save](#).



A dialog box titled "Change Email" with a close button (X) in the top right corner. It contains two input fields: "Password" with a key icon and "New Email" with an envelope icon. Below the fields is a teal "Save" button. A note at the bottom states: "Note: New email or password may not sync to client devices immediately. Please log in again when your device is connected to the Internet to update account information."

- **To change your password:**

1. Click  behind the Password.
2. Enter the current password, then a new password twice. And click [Save](#).



A dialog box titled "Change Password" with a close button (X) in the top right corner. It contains three input fields: "Current Password", "New Password", and "Confirm Password", each with a key icon. Below the "New Password" field are three tabs: "Low", "Middle", and "High". Below the fields is a teal "Save" button. A note at the bottom states: "Note: New email or password may not sync to client devices immediately. Please log in again when your device is connected to the Internet to update account information."

8.3. Manage the User TP-Link IDs

The TP-Link ID used to log in to the mesh device for the first time will be automatically bound as the [Admin](#) account. An admin account can add or remove other TP-Link IDs

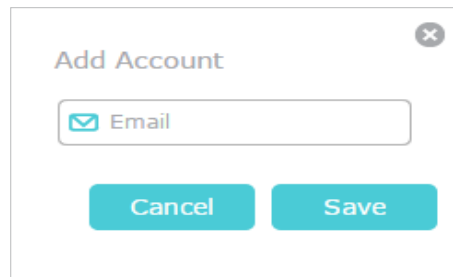
to or from the same mesh device as **Users**. All accounts can monitor and manage the mesh device locally or remotely, but user accounts cannot:

- Reset the mesh device to its factory default settings either on the web management page or in the Aginet app.
- Add/remove other TP-Link IDs to/from the mesh device.

8.3.1. Add TP-Link ID to Manage the Mesh Device

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID.
2. Go to **Basic > TP-Link Cloud**, and focus on the **Bound Accounts** section.
3. Click **+ Bind**, enter another TP-Link ID as needed and click **Save**.

Note: If you need another TP-Link ID, please register a new one via the Aginet app. Refer to [Manage the Mesh Device via the TP-Link Aginet App](#) to install the app and register a new TP-Link ID.



The image shows a modal dialog box titled "Add Account" with a close button (X) in the top right corner. Inside the dialog, there is a text input field with a blue envelope icon and the placeholder text "Email". Below the input field are two buttons: "Cancel" and "Save", both in a teal color.

4. The new TP-Link ID will be displayed in the Bound Accounts table as a **User**.

					+ Bind - Unbind	
☐	ID	Email	Binding Date	Role		
☐	1	dingpin_xiaofen.com	2021/08/04	Admin		
☐	2	dingpin_xiaofen.com	2021/08/04	User		

8.3.2. Remove TP-Link ID(s) from Managing the Mesh Device

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID.
2. Go to **Basic > TP-Link Cloud**, and focus on the **Bound Accounts** section.
3. Tick the checkbox(es) of the TP-Link ID(s) you want to remove and click **Unbind**.

Bound Accounts				
+ Bind - Unbind				
☐	ID	Email	Binding Date	Role
☐	1	thangpvt_123456789@163.com	10/11/2018	Admin
☒	2	thangpvt_123456789@163.com	10/11/2018	User

8.4. Manage the Mesh Device via the TP-Link Aginet App

The Aginet app runs on iOS and Android devices, such as smartphones and tablets.

1. Launch the Apple App Store or Google Play store and search "TP-Link Aginet" or simply scan the QR code to download and install the app.



2. Launch the Aginet app and log in with your TP-Link ID.

Note: If you don't have a TP-Link ID, create one first.

3. Connect your device to the mesh device's wireless network.
4. Go back to the Aginet app, select the model of your mesh device and log in with the password you set for the mesh device.
5. Manage your mesh device as needed.

Note: If you need to remotely access your mesh device from your smart devices, you need to:

- Log in with your TP-Link ID. If you don't have one, refer to [Register a TP-Link ID](#).
- Make sure your smartphone or tablet can access the internet with cellular data or a Wi-Fi network.

Chapter 9

EasyMesh with Seamless Roaming

This chapter introduces the TP-Link EasyMesh feature.

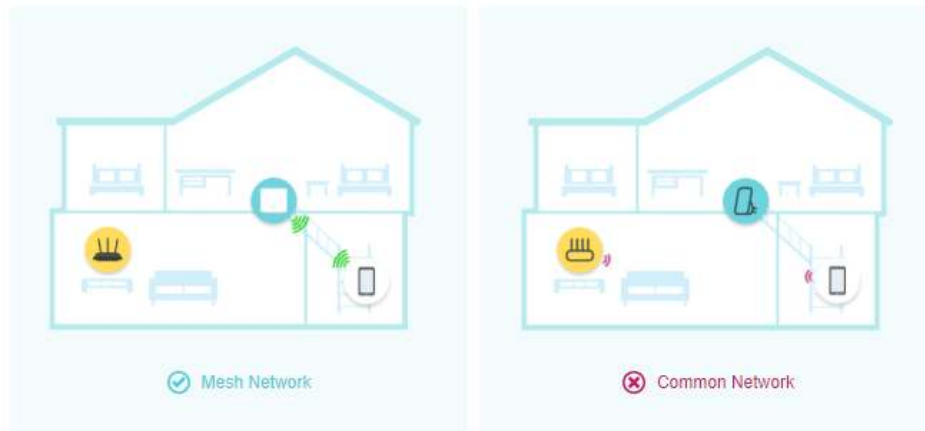
It contains the following sections:

- [Set Up a EasyMesh Network](#)
- [Manage Devices in the EasyMesh Network](#)

TP-Link EasyMesh  Controller and TP-Link EasyMesh  Agent work together to form one unified Wi-Fi network. Walk through your home and stay connected with the fastest possible speeds thanks to EasyMesh's seamless coverage.

 What's EasyMesh?

EasyMesh implements a standards-based approach, combining easy-to-use, self-adapting Wi-Fi with a flexible design, easy setup, and enhanced network intelligence. In an Mesh network, your mobile device will seamlessly switch between the main Router/Gateway(Controller) and Agents, provides the optimal Wi-Fi connection as you move through your home.



Unified Wi-Fi Network

Controller and agents share the same wireless settings, including network name, password, access control settings and more.

Seamless Roaming

Devices automatically switch between your controller and agents as you move through your home for the fastest possible speeds.

Easy Setup and Management

Set up a EasyMesh network with a push of WPS buttons. Manage all network devices on the Aginet app or at your mesh device's web management page.

9. 1. Set Up a EasyMesh Network

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
1. Go to **Basic > Mesh** or **Advanced > Wireless > Mesh**.

EasyMesh

Connect EasyMesh devices to create a mesh network for seamless Wi-Fi coverage and centralized management.

Note: WPA3-Personal and WPA2-Enterprise are unavailable since EasyMesh doesn't support these security types.

2. Connect a EasyMesh agent to this controller by following the setup instructions in the agent’s manual. The agent will be listed on the controller’s Mesh page.
- Note: To check full list of TP-Link EasyMesh devices, visit <https://www.tp-link.com>.
3. If you have set up the agent to join the EasyMesh network, it will be listed on the controller’s EasyMesh page.

Topology

Add Mesh Device

1

EX510_

1

HX220_

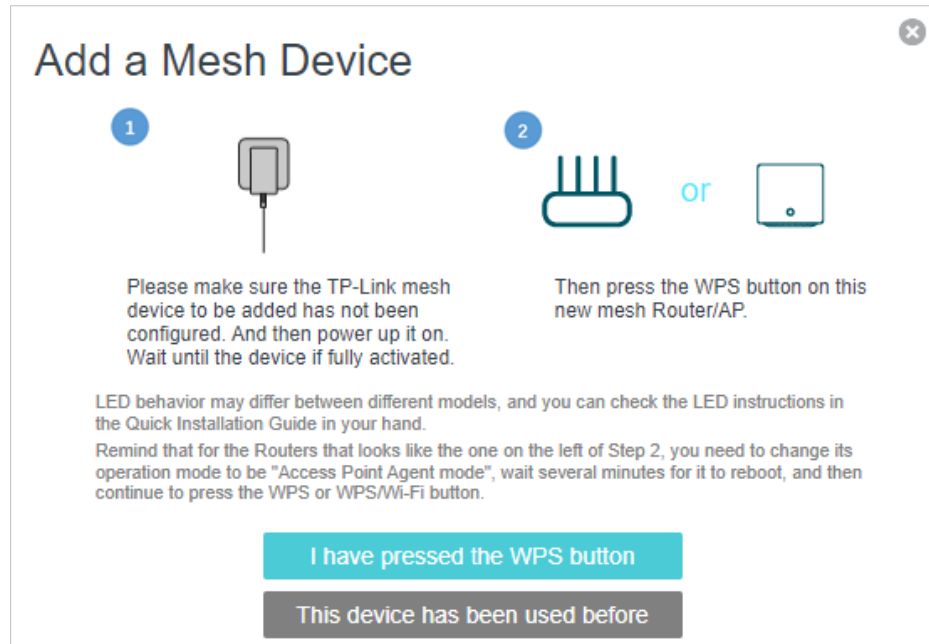
Ethernet

Wireless

Refresh

ID	Device Name	IP Address	MAC Address	Connection Type	Signal Strength	Link Rate	Operation
1				--	--	--	--
2				5GHz_CH 48		1080Mbps	

Otherwise, you need to find it in the Add Mesh Device list and click Add to add it to the EasyMesh network.

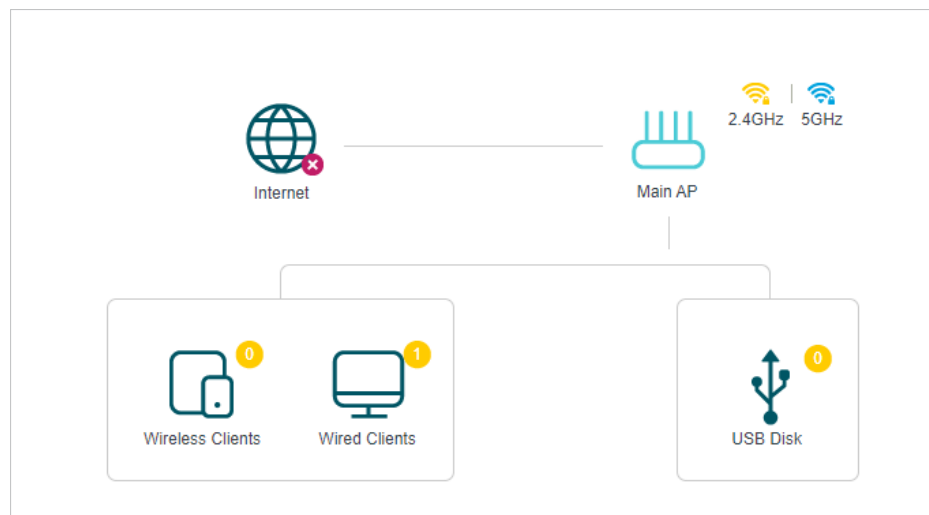


Done! Now your controller and agents successfully form a EasyMesh network!

9.2. Manage Devices in the EasyMesh Network

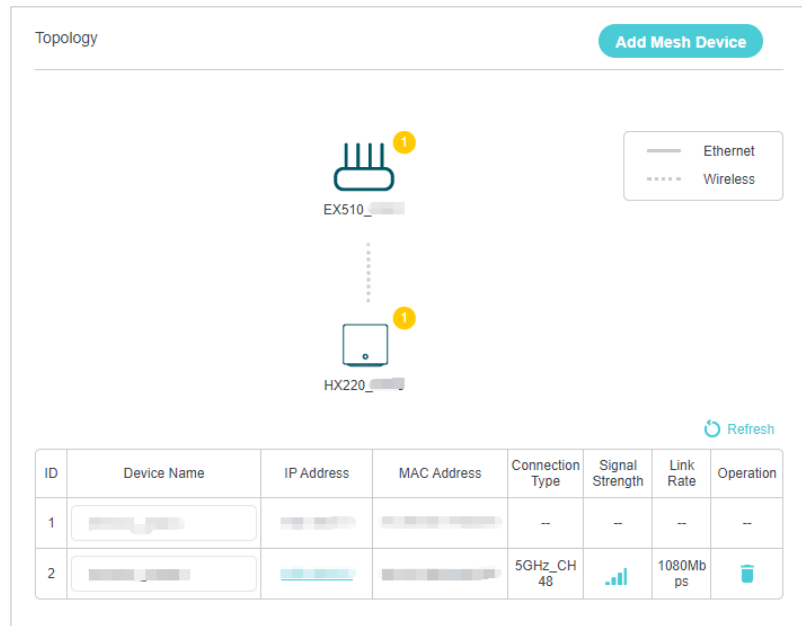
In a EasyMesh network, you can manage all mesh devices and connected clients on your mesh device's web page.

- **To view mesh devices and connected clients in the network:**
 1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
 2. Go to **Basic > Network Map**.
 3. Click  to view all mesh devices, and click   to view all connected clients.

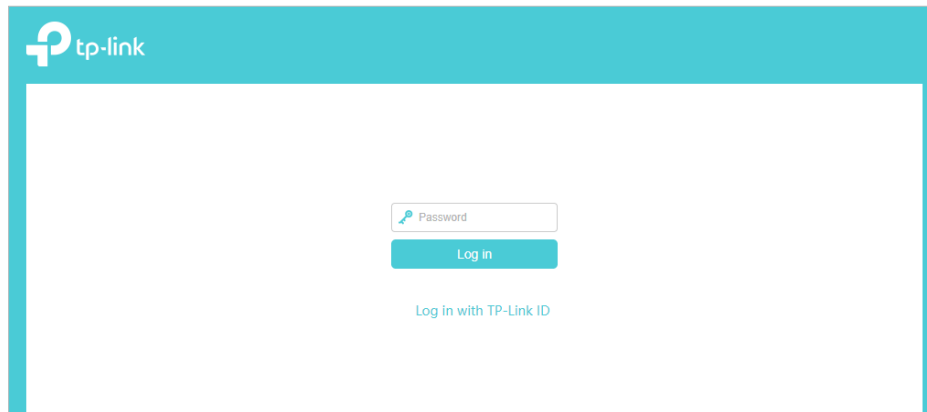


- **To manage a EasyMesh device in the network:**

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
2. Go to **Basic > Network Map**.



3. Click the Mesh device's IP Address to redirect to the web management page of this device and view detailed information.



4. Manage the EasyMesh device as needed. You can:

- Change device information.
- Delete this device from the EasyMesh network.

Chapter 10

Guest Network

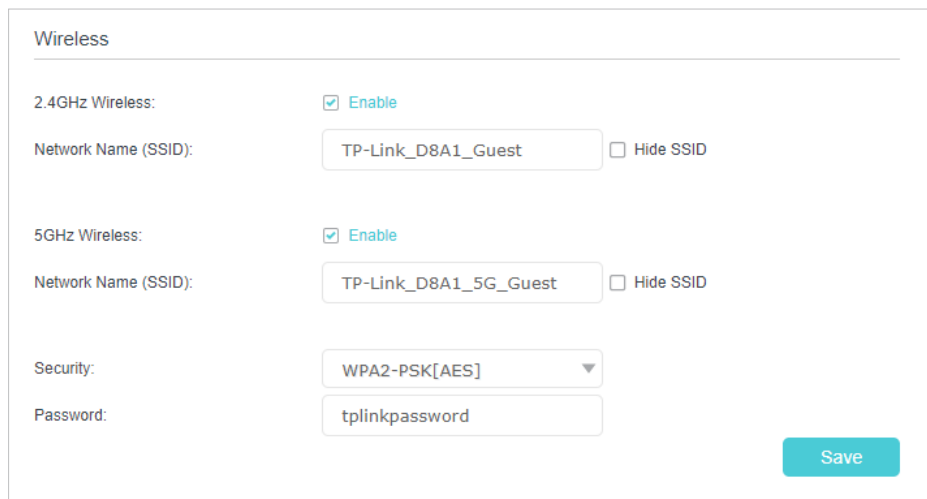
This function allows you to provide Wi-Fi access for guests without disclosing your main network. When you have guests in your house, apartment, or workplace, you can create a guest network for them. In addition, you can customize guest network options to ensure network security and privacy.

It contains the following sections:

- [Create a Network for Guests](#)
- [Customize Guest Network Options](#)

10.1. Create a Network for Guests

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
2. Go to **Advanced** > **Guest Network**. Locate the **Wireless** section.
3. Create a guest network as needed.
 - 1) Tick the Enable checkbox for the 2.4GHz or 5GHz wireless network.
 - 2) Customize the SSID. Don't select **Hide SSID** unless you want your guests to manually input the SSID for guest network access.
 - 3) Select the **Security** type and customize your own password. If **No security** is selected, no password is needed to access your guest network.



The screenshot shows the 'Wireless' configuration page for a guest network. It has two sections for 2.4GHz and 5GHz wireless networks. Both sections have an 'Enable' checkbox checked. The 2.4GHz section has a 'Network Name (SSID)' field with 'TP-Link_D8A1_Guest' and a 'Hide SSID' checkbox. The 5GHz section has a 'Network Name (SSID)' field with 'TP-Link_D8A1_5G_Guest' and a 'Hide SSID' checkbox. Below these is a 'Security' dropdown menu set to 'WPA2-PSK[AES]' and a 'Password' field with 'tplinkpassword'. A 'Save' button is at the bottom right.

Wireless	
2.4GHz Wireless:	☒ Enable
Network Name (SSID):	TP-Link_D8A1_Guest ☐ Hide SSID
5GHz Wireless:	☒ Enable
Network Name (SSID):	TP-Link_D8A1_5G_Guest ☐ Hide SSID
Security:	WPA2-PSK[AES]
Password:	tplinkpassword
Save	

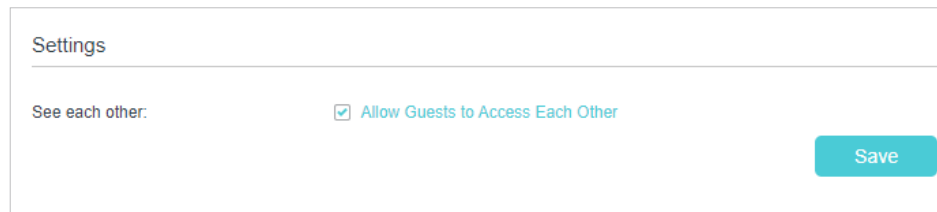
4. Click **Save**. Now your guests can access your guest network using the SSID and password you set!

Tips:

To view guest network information, go to **Network Map** and locate the **Guest Network** section. You can turn on or off the guest network function conveniently.

10.2. Customize Guest Network Options

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
2. Go to **Advanced** > **Guest Network**. Locate the **Settings** section.
3. Customize guest network options according to your needs.



Settings

See each other: ☒ Allow Guests to Access Each Other

Save

- [Allow guests to see each other](#)

Tick this checkbox if you want to allow the wireless clients on your guest network to communicate with each other via methods such as network neighbors and Ping.

4. Click [Save](#). Now you can ensure network security and privacy!

Chapter 11

NAT Forwarding

The mesh device's NAT (Network Address Translation) feature makes devices on the LAN use the same public IP address to communicate with devices on the internet, which protects the local network by hiding IP addresses of the devices. However, it also brings about the problem that an external host cannot initiatively communicate with a specified device on the local network.

With the forwarding feature the mesh device can penetrate the isolation of NAT and allows devices on the internet to initiatively communicate with devices on the local network, thus realizing some special functions.

The TP-Link mesh device supports four forwarding rules. If two or more rules are set, the priority of implementation from high to low is Port Forwarding, Port Triggering, UPnP and DMZ.

It contains the following sections:

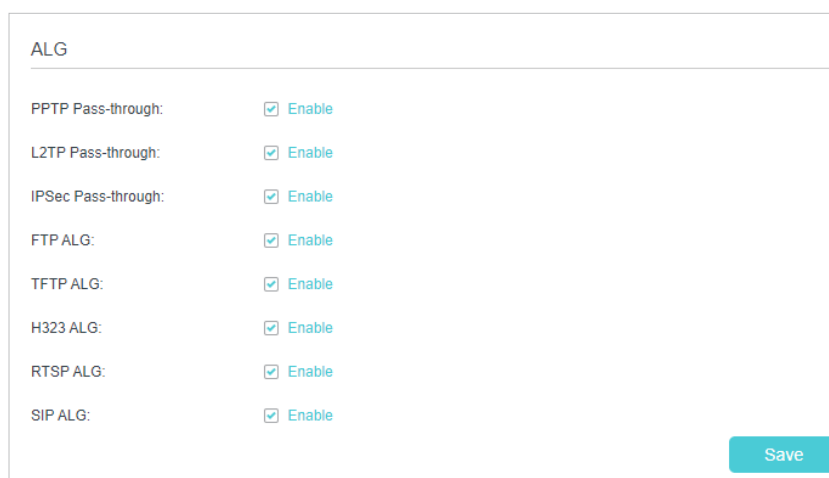
- [ALG](#)
- [Set Up Public Services on The Local Network by Virtual Servers](#)
- [Open Ports Dynamically by Port Triggering](#)
- [Make Applications Free from Port Restriction by DMZ](#)
- [Make Xbox Online Games Run Smoothly by UPnP](#)

11.1. ALG

ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer “control/data” protocols such as FTP, TFTP, H323 etc. It is recommended to keep the default settings.

You may need to disable SIP ALG when you are using voice and video applications to create and accept a call through the mesh device, since some voice and video communication applications do not work well with SIP ALG.

Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device. Go to **Advanced** > **Security** > **ALG**.



ALG	
PPTP Pass-through:	☒ Enable
L2TP Pass-through:	☒ Enable
IPSec Pass-through:	☒ Enable
FTP ALG:	☒ Enable
TFTP ALG:	☒ Enable
H323 ALG:	☒ Enable
RTSP ALG:	☒ Enable
SIP ALG:	☒ Enable

[Save](#)

11.2. Set Up Public Services on The Local Network by Virtual Servers

Virtual Servers are used to set up public services on the local network. A virtual server is defined as an external port, and all requests from the Internet to this external port will be redirected to a designated computer, which must be configured with a static or reserved IP address. When you build up a server on the local network and want to share it on the Internet, Virtual Servers can realize the service and provide it to the Internet users.

The table displays the relevant parameters of the virtual server.

To set up a Virtual Server rule:

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
2. Go to **Advanced** > **NAT Forwarding** > **Virtual Servers** and click  **Add**.
3. Select an interface name from the drop-down list.

Virtual Servers

[+ Add](#) [- Delete](#)

☐	ID	Service Type	External Port	Internal IP	Internal Port	Protocol	Status	Modify
--	--	--	--	--	--	--	--	--

Note: Virtual Server can be configured only when there is an available interface. If the external port is already used for Remote Management or CWMP, Virtual Server will not take effect.

Interface Name:

Service Type: [View Existing Applications](#)

External Port: (XX-XX or XX)

Internal IP: . . .

Internal Port: (XX or Blank, 1-65535)

Protocol:

☒ Enable This Entry

[Cancel](#) [OK](#)

4. Click [View Existing Applications](#) to select a service from the list to automatically populate the appropriate port number in the [External Port](#) and [Internal Port](#) fields. If the service is not listed, enter the External Port number (e.g. 21) or a range of ports (e.g. 21-25). Leave the Internal Port blank if it is the same as the External Port or enter a specific port number (e.g. 21) if the External Port is a single port. The following picture takes application [FTP](#) as an example.

Virtual Servers

[+ Add](#) [- Delete](#)

☐	ID	Service Type	External Port	Internal IP	Internal Port	Protocol	Status	Modify
--	--	--	--	--	--	--	--	--

Note: Virtual Server can be configured only when there is an available interface. If the external port is already used for Remote Management or CWMP, Virtual Server will not take effect.

Interface Name:

Service Type: [View Existing Applications](#)

External Port: (XX-XX or XX)

Internal IP: . . .

Internal Port: (XX or Blank, 1-65535)

Protocol:

☒ Enable This Entry

[Cancel](#) [OK](#)

5. Enter the IP address of the computer running the service application in the Internal IP field.
6. Select a protocol for the service application: TCP, UDP, or All from the Protocol drop-down list.
7. Select Enable This Entry.
8. Click **OK**.

 Tips:

- If you want to disable this entry, click the Bulb icon.
- It is recommended to keep the default settings of Internal Port and Protocol if you are not clear about which port or protocol to use.
- If the local host device is hosting more than one type of available services, you need to create a rule for each service. Please note that the External Port should NOT be overlapped.

11.3. Open Ports Dynamically by Port Triggering

Port Triggering can specify a triggering port and its corresponding external ports. When a host on the local network initiates a connection to the triggering port, all the external ports will be opened for subsequent connections. The mesh device can record the IP address of the host. When the data from the internet return to the external ports, the mesh device can forward them to the corresponding host. Port Triggering is mainly applied to online games, VoIPs, video players and common applications including MSN Gaming Zone, Dialpad and Quick Time 4 players, etc.

Follow the steps below to configure the Port Triggering rules:

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
2. Go to **Advanced > NAT Forwarding > Port Triggering** and click  **Add**.

Port Triggering

+ Add - Delete

☐	ID	Application	Triggering Port	Triggering Protocol	External Port	External Protocol	Status	Modify
--	--	--	--	--	--	--	--	--

Interface Name:

Application: [View Existing Applications](#)

Triggering Port: (XX, 1-65535)

Triggering Protocol:

External Port: (XX or XX-XX, 1-65535, at most 5 pairs)

External Protocol:

☒ Enable This Entry

[Cancel](#) [OK](#)

3. Click [View Existing Applications](#), and select the desired application. The [Triggering Port](#), [Triggering Protocol](#) and [External Port](#) will be automatically filled in. The following picture takes application [MSN Gaming Zone](#) as an example.

Port Triggering

+ Add - Delete

☐	ID	Application	Triggering Port	Triggering Protocol	External Port	External Protocol	Status	Modify
--	--	--	--	--	--	--	--	--

Interface Name:

Application: [View Existing Applications](#)

Triggering Port: (XX, 1-65535)

Triggering Protocol:

External Port: (XX or XX-XX, 1-65535, at most 5 pairs)

External Protocol:

☒ Enable This Entry

[Cancel](#) [OK](#)

4. Click [OK](#).

Port Triggering								
 Add  Delete								
☐	ID	Application	Triggering Port	Triggering Protocol	External Port	External Protocol	Status	Modify
☐	1	MSN Gaming Zone	47624	TCP or UDP	2300-2400, 28800-29000	TCP or UDP		 

 Tips:

- You can add multiple port triggering rules according to your network need.
- The triggering ports can not be overlapped.
- If the application you need is not listed in the Existing Applications list, please enter the parameters manually. You should verify the external ports the application uses first and enter them into [External Port](#) field according to the format the page displays.

11.4. Make Applications Free from Port Restriction by DMZ

When a PC is set to be a DMZ (Demilitarized Zone) host on the local network, it is totally exposed to the internet, which can realize the unlimited bidirectional communication between internal hosts and external hosts. The DMZ host becomes a virtual server with all ports opened. When you are not clear about which ports to open in some special applications, such as IP camera and database software, you can set the PC to be a DMZ host.

 Note:

When DMZ is enabled, the DMZ host is totally exposed to the internet, which may bring some potential safety hazards. If DMZ is not in use, please disable it in time.

I want to:

Make the home PC join the internet online game without port restriction.

[For example](#), due to some port restriction, when playing the online games, you can log in normally but cannot join a team with other players. To solve this problem, set your PC as a DMZ host with all ports open.

How can I do that?

1. Assign a static IP address to your PC, for example 192.168.88.100.
2. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
1. Go to [Advanced](#) > [NAT Forwarding](#) > [DMZ](#) and tick to enable DMZ.
3. Enter the PC's IP address 192.168.88.100 manually in the [DMZ Host IP Address](#) field.

DMZ

DMZ: ☒ Enable

DMZ Host IP Address:

Save

2. Click **SAVE**.

Done!

The configuration is completed. You've set your PC to a DMZ host and now you can make a team to game with other players.

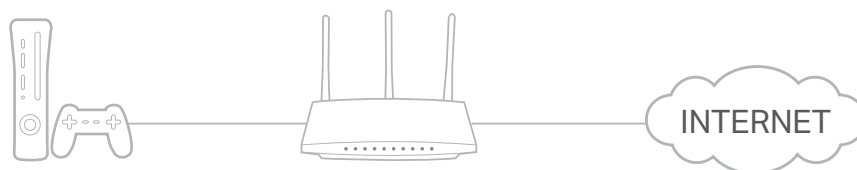
11.5. Make Xbox Online Games Run Smoothly by UPnP

The UPnP (Universal Plug and Play) protocol allows applications or host devices to automatically find the front-end NAT device and send request to it to open the corresponding ports. With UPnP enabled, the applications or host devices on the local network and the internet can freely communicate with each other thus realizing the seamless connection of the network. You may need to enable the UPnP if you want to use applications for multiplayer gaming, peer-to-peer connections, real-time communication (such as VoIP or telephone conference) or remote assistance, etc.

Tips:

- UPnP is enabled by default in this mesh device.
- Only the application supporting UPnP protocol can use this feature.
- UPnP feature needs the support of operating system (e.g. Windows Vista/ Windows 7/ Windows 8, etc. Some of operating system need to install the UPnP components).

For example, when you connect your Xbox to the mesh device which has connected to the internet to play online games, UPnP will send request to the mesh device to open the corresponding ports allowing the following data penetrating the NAT to transmit. Therefore, you can play Xbox online games without a hitch.



If necessary, you can follow the steps to change the status of UPnP.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.

2. Go to [Advanced](#) > [NAT Forwarding](#) > [UPnP](#) and toggle on or off according to your needs.

UPnP

UPnP:

UPnP Service List

Total Clients: 0

Refresh

ID	Service Description	External Port	Protocol	Internal IP Address	Internal Port
--	--	--	--	--	--

Chapter 12

Parental Controls

This function allows you to block inappropriate, explicit and malicious websites, and control access to specified websites at specified time.

I want to:

Control what types of websites my children or other home network users can visit and the time of day they are allowed to access the internet.

For example, I want to allow my children's devices (e.g. a computer or a tablet) to access only www.tp-link.com and Wikipedia.org from 18:00 (6 PM) to 22:00 (10 PM) on the weekdays and not other time.

How can I do that?

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Basic > Parental Controls](#) or [Advanced > Parental Controls](#).

Parental Controls

+ Add

Name	Filter Level	Time Limits	Devices	Insights	Internet Access	Modify
--	--	--	--	--	--	--

3. Click [Add](#), and then enter the [Name](#) manually. Click [Add](#) and specify the devices belonging to the family member. Click [Next](#).

Parental Controls

+ Add

Name	Filter Level	Time Limits	Devices	Insights	Internet Access	Modify
--	--	--	--	--	--	--

Filter Level

Basic Info ————— Time Controls

Name:

Devices List:

+

Add

4. Select a filter level based on the age of the family member. Blocked content will then be displayed in the Filter Content list. Click [Next](#).

Parental Controls

+ Add

Name	Filter Level	Time Limits	Devices	Insights	Internet Access	Modify
--	--	--	--	--	--	--

Filter Level

Basic Info
Time Controls

Child (0-7)

Pre-Teen (8-12)

Teen (13-17)

Adult (>17)

Based on the selected filter level, Adult Content, Social Networking have already been filtered for 123. You can block more from Available Categories or by adding a new keyword.

Filter Content

+ Add a New Keyword

Available Categories:

Adult Content

Social Networking

Games

Media

Online Communication

Pay to Surf

Downloads

Cancel
Back
Next

- (Optional) Delete items from the Filter Content list, add items from the Available Categories list, or click Add a New Keyword to add a filter keyword (for example, "Facebook") or URL.
- Enable Time Limits for Mon to Fri and Sat & Sun, then set the daily internet time allowed. Enable BedTime on School Nights (Sunday to Thursday) and Weekend (Friday and Saturday), then set the time period during devices in the profile cannot access the internet.

Parental Controls

Add

Name	Filter Level	Time Limits	Devices	Insights	Internet Access	Modify
--	--	--	--	--	--	--

Filter Level

Basic Info

Time Controls

Weekdays

☒ Mon

☒ Tues

☒ Wed

☒ Thur

☒ Fri

☐ Sat

☐ Sun

Time Limits

Set daily time limits for the total time spent online.

Weekdays

☒ Enable

2h

30min

8h

Weekends

☒ Enable

2h

30min

8h

Bed Time

Set a time period while this profile cannot access the internet.

Weekdays

☒ Enable

From

10 : 00 PM

To

06 : 00 AM

Weekends

☒ Enable

From

10 : 00 PM

To

06 : 00 AM

Cancel

Back

Save

7. Click [Save](#).

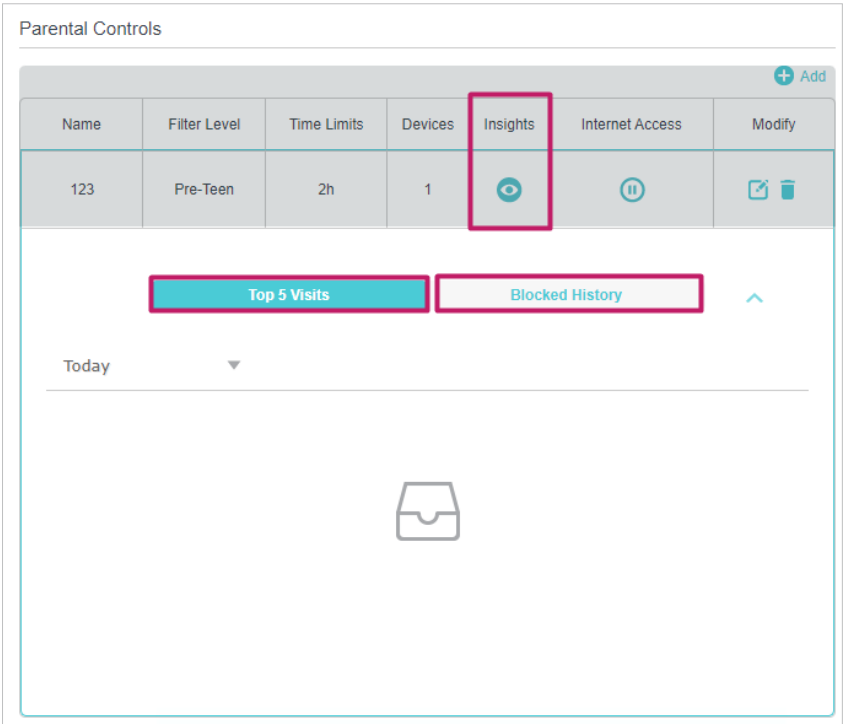
Done!

Now you can control your children’s internet access as needed.

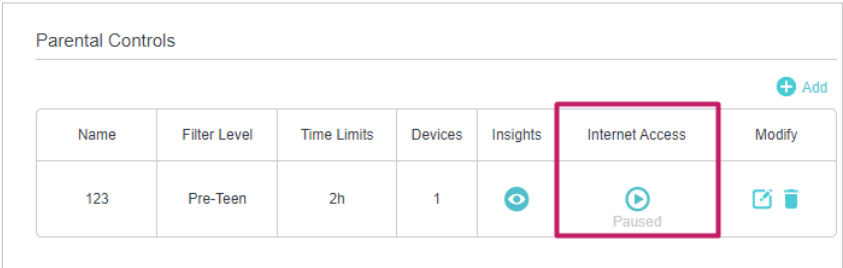
 **Tips:**

- To monitor internet usage of a family member:
 1. Find the profile of the family member, then click the **Insights** icon.
 2. On the **Top 5 Visits** page, select a day of the last 7 days to check the time spent online and top visited websites. You can block the websites if needed.
 3. On the **Blocked History** page, select a day of the last 7 days to check the blocked website history. You can **unblock websites** if needed, and click Unblocked Websites to view them.

95



- To pause or resume internet access of a family member:
Find the profile of the family member, then click the **Pause/Play** icon.



Chapter 13

Quality of Service

This function allows you to specify the priority of traffic and minimizes the impact of network congestion.

The mesh device allows you to configure the quality of service (QoS) for optimal throughput and performance when handling differentiated wireless traffic, such as Voiceover-IP (VoIP), other types of audio, video, streaming media, and traditional IP data.

To configure QoS on the mesh devices, you should set parameters on the transmission queues for different types of wireless traffic. In normal use, we recommend that you keep the default values for the mesh devices.

To set up QoS for the network:

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [QoS](#).
3. Enable [QoS](#).

QoS

QoS: ☒ Enable

Upload Bandwidth: 0 Mb...

Download Bandwidth: 0 Mb...

IPTV QoS: ☐ Enable

Advanced

High: 60%

Middle: 30%

Low: 10%

Save

4. Enter the upload and download bandwidths provided by your ISP.

The screenshot shows the 'QoS' configuration page. At the top, the title 'QoS' is displayed. Below it, the 'QoS:' section has a checked 'Enable' checkbox. Underneath, 'Upload Bandwidth:' and 'Download Bandwidth:' are both set to '0' with a unit dropdown menu showing 'Mb...'. The 'IPTV QoS:' section has an unchecked 'Enable' checkbox. Below this is an 'Advanced' section with a circular arrow icon. It contains three sliders: 'High:' set to 60%, 'Middle:' set to 30%, and 'Low:' set to 10%. A 'Save' button is located at the bottom right.

5. (Optional) Enable [IPTV QoS](#), then set the priority and reserved bandwidth of IPTV traffic.

This screenshot is similar to the previous one, but the 'IPTV QoS:' section now has a checked 'Enable' checkbox, which is highlighted with a red rectangle. The 'Advanced' section and sliders remain the same. The 'Save' button is still at the bottom right.

6. (Optional) Click [Advanced](#) and arrange the sliders to set the bandwidth percentage of each priority.

QoS

QoS: ☒ Enable

Upload Bandwidth: Mb... ▼

Download Bandwidth: Mb... ▼

IPTV QoS: ☒ Enable

Advanced

High: 60%

Middle: 30%

Low: 10%

Save

7. Click [Save](#) to make the settings effective.

To set up QoS for a specific device:

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [QoS](#).
3. In the [QoS Rule List](#) table, choose a priority section and click [Add](#).

QoS Rule List

High Priority: 60%	Middle Priority: 30%	Low Priority: 10%
Add	Add	Add

4. In the QoS Rule window, click scan and click  to choose a device, then click OK to add it to the rule.

QoS Rule

Type:

☒ By Device

Device Name:

Unknown

scan

MAC Address:

Cancel

OK

ID	Device Name	IP Address	MAC Address	Operation
1	Unknown			+

Chapter 14

Network Security

This chapter guides you on how to protect your home network from unauthorized users by implementing network security functions. You can block or allow specific client devices to access your wireless network using MAC Filtering, or using Access Control for wired and wireless networks, or you can prevent ARP spoofing and ARP attacks by using IP & MAC Binding.

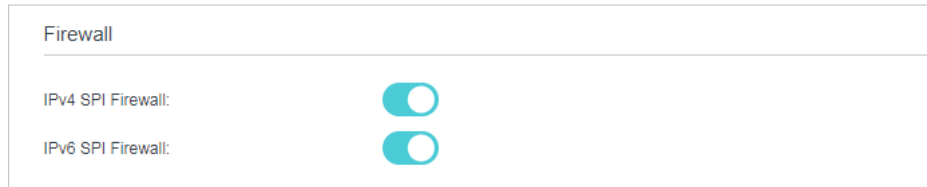
This chapter contains the following sections:

- [Firewall & DoS Protection](#)
- [Service Filtering](#)
- [Access Control](#)
- [IP & MAC Binding](#)
- [IPv6 Firewall](#)

14.1. Firewall & DoS Protection

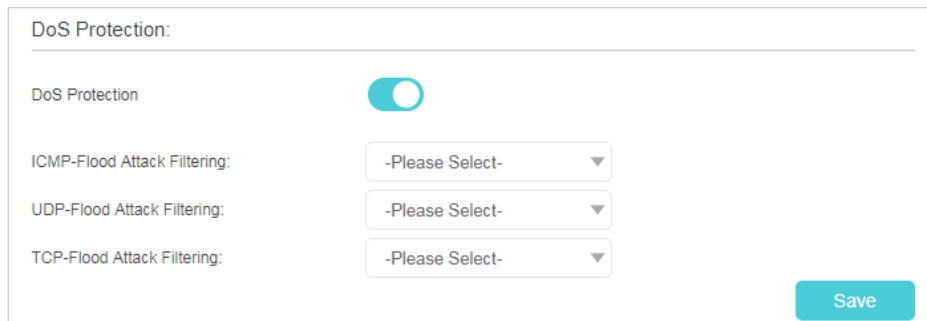
The SPI (Stateful Packet Inspection) Firewall and DoS (Denial of Service) Protection protect the mesh device from cyber attacks.

The SPI Firewall can prevent cyber attacks and validate the traffic that is passing through the mesh device based on the protocol. This function is enabled by default, and it is recommended to keep the default settings.



DoS Protection can protect your home network against DoS attacks from flooding your network with server requests. Follow the steps below to configure DoS Protection.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [Security](#) > [Firewall & DoS Protection](#).



3. Enable [DoS Protection](#).
4. Set the protection level ([Low](#), [Middle](#) or [High](#)) for [ICMP-Flood Attack Filtering](#), [UDP-Flood Attack Filtering](#) and [TCP-Flood Attack Filtering](#).
 - [ICMP-Flood Attack Filtering](#) - Enable to prevent the ICMP (Internet Control Message Protocol) flood attack.
 - [UDP-Flood Attack Filtering](#) - Enable to prevent the UDP (User Datagram Protocol) flood attack.
 - [TCP-Flood Attack Filtering](#) - Enable to prevent the TCP (Transmission Control Protocol) flood attack.
5. Click [Save](#).

Tips:

1. The level of protection is based on the number of traffic packets. You can specify the level under [DoS Protection Level Settings](#).

Dos Protection Level Settings

ICMP-Flood Protection Level:	Low:	1200	(5-3600) packets/sec
	Middle:	2400	(5-3600) packets/sec
	High:	3600	(5-3600) packets/sec
UDP-Flood Protection Level:	Low:	1200	(5-3600) packets/sec
	Middle:	2400	(5-3600) packets/sec
	High:	3600	(5-3600) packets/sec
TCP-SYN-Flood Protection Level:	Low:	1200	(5-3600) packets/sec
	Middle:	2400	(5-3600) packets/sec
	High:	3600	(5-3600) packets/sec

Save

- The protection will be triggered immediately when the number of packets exceeds the preset threshold value, and the vicious host will be displayed in the [Blocked DoS Host List](#).

Blocked DoS Host List

Host Number: 0 Refresh Delete

☐	ID	IP Address	MAC Address
--	--	--	--

14.2. Service Filtering

With Service Filtering, you can prevent certain users from accessing the specified service, and even block internet access completely.

- Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
- Go to [Advanced](#) > [Security](#) > [Service Filtering](#), and enable [Service Filtering](#).

Service Filtering

Service Filtering: ☒

- Click [Add](#).

Filtering List

Refresh + Add - Delete

☐	ID	Service Type	Port	IP Address	Status	Modify
--	--	--	--	--	--	--

Service Type:

Protocol:

Starting Port: (1-65535)

Ending Port: (1-65535)

Service Type:

Filter Service For: ☐ Single IP Address ☐ IP Address Range ☒ All IP Addresses

Cancel Save

4. Select a **Service Type** from the drop-down list and the following four fields will be automatically filled in. Select **Custom** when your desired service type is not listed, and enter the information manually.
5. Specify the IP address(es) that this filtering rule will apply to.
6. Click **Save** to make the settings effective.

Note: If you want to disable an entry, click the  icon.

14.3. Access Control

Access Control is used to block or allow specific client devices to access your network (via wired or wireless) based on a list of blocked devices (Blacklist) or a list of allowed devices (Whitelist).

I want to: Block or allow specific client devices to access my network (via wired or wireless).

How can I do that?

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to **Advanced > Security > Access Control** and enable **Access Control**.

Access Control

Access Control: ☒

3. Select the access mode to either block (recommended) or allow the device(s) to access your network.

To block specific device(s):

- 1) Select **Blacklist** and click **Save**.

Access Mode

Access Mode:
☒ Blacklist
☐ Whitelist

Save

- 2) Select the device(s) to be blocked in the **Online Devices** table (or click the **Add** under the **Devices in Blacklist** and enter the **Device Name** and **MAC Address** manually).
- 3) Click **Block** above the **Online Devices** table. The selected devices will be added to **Devices in Blacklist** automatically.

Devices in Blacklist

+ Add
- Delete

☐	ID	Device Name	MAC Address	Modify
☐	--	--	--	--

Online Devices

Refresh
Block

☐	ID	Device Name	IP Address	MAC Address	Connection Type
☐	1	DESKTOP-XXXXXX	192.168.0.100	9C-8C-4B-1D-8D-A8	Wired

To allow specific device(s):

- 1) Select **Whitelist** and click **Save**.

Access Mode

Access Mode:
☐ Blacklist
☒ Whitelist

Save

- 2) Click **Add** in the **Devices in Whitelist** section.

The screenshot shows a web interface titled "Devices in Whitelist". At the top right, there are "Add" (green plus icon) and "Delete" (red minus icon) buttons. Below this is a table with the following structure:

☐	ID	Device Name	MAC Address	Modify
☐	---	---	---	---

Below the table, there are two input fields: "Device Name:" and "MAC Address:". The "MAC Address" field has a placeholder showing five dashes. At the bottom right, there are "Cancel" and "Save" buttons.

- 3) Enter the [Device Name](#) and [MAC Address](#). (You can copy and paste the information from [Online Devices](#) table if the device is connected to your network.)
- 4) Click [Save](#).

Done!

Now you can block or allow specific client devices to access your network (via wired or wireless) by [Blacklist](#) or [Whitelist](#).

14. 4. IP & MAC Binding

IP & MAC Binding, namely, ARP (Address Resolution Protocol) Binding, is used to bind a network device's IP address to its MAC address. This will prevent ARP spoofing and other ARP attacks by denying network access to a device with a matching IP address in the Binding list, but an unrecognized MAC address.

I want to:

Prevent ARP spoofing and ARP attacks.

How can I do that?

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [Security](#) > [IP & MAC Binding](#), and enable [IP & MAC Binding](#).

IP & MAC Binding

IP & MAC Binding: ☒

Binding List

[+ Add](#) [- Delete](#)

☐	ID	MAC Address	IP Address	Status	Enable	Modify
☐	--	--	--	--	--	--

ARP List

[Refresh](#) [Bind](#)

☐	ID	MAC Address	IP Address	Bound	Modify
☐	1	84-16-F9-03-E2-D3	192.168.0.100	Unloaded	

3. Bind your device(s) according to your needs.

To bind the connected device(s):

- 1) Select the device(s) to be bound in the [ARP List](#).
- 2) Click [Bind](#) to add to the [Binding List](#).

To bind the unconnected device:

- 1) Click [Add](#) in the [Binding List](#) section.

Binding List

[+ Add](#) [- Delete](#)

☐	ID	MAC Address	IP Address	Status	Enable	Modify
☐	--	--	--	--	--	--

MAC Address:

IP Address:

☒ [Enable This Entry](#)

[Cancel](#) [OK](#)

- 2) Enter the [MAC address](#) and [IP address](#) that you want to bind.
- 3) Select the [Enable This Entry](#) check box to enable the entry and click [Save](#).

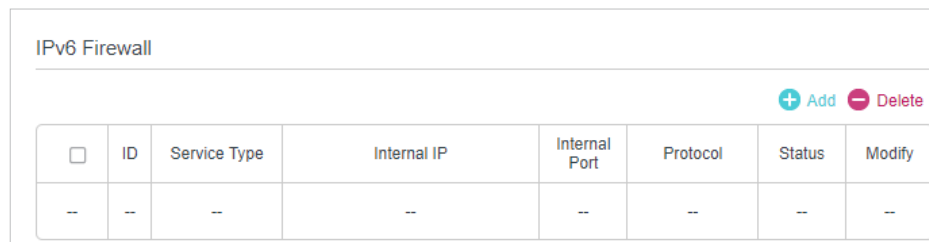
Done!

Enjoy the internet without worrying about ARP spoofing and ARP attacks.

14.5. IPv6 Firewall

IPv6 Firewall protects your IPv6 network by preventing access from the internet. However, when you are hosting a service, such as a file sharing server in your local network, you can choose to allow access to the server from the internet by adding entries on this page. This feature is available only when you've set up an IPv6 connection.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [Security](#) > [IPv6 Firewall](#).

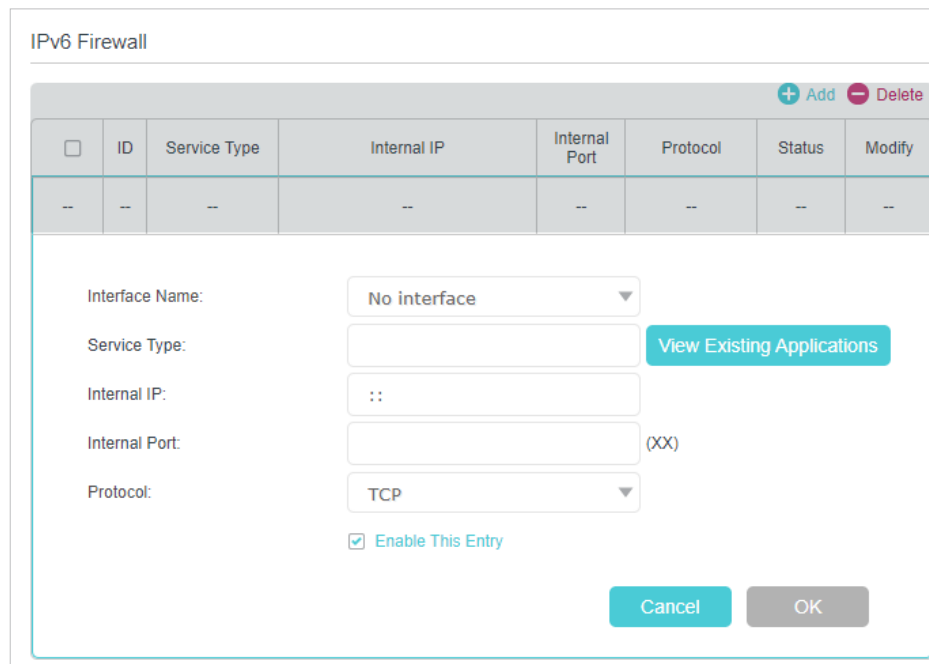


IPv6 Firewall

+ Add - Delete

☐	ID	Service Type	Internal IP	Internal Port	Protocol	Status	Modify
--	--	--	--	--	--	--	--

3. Click [Add](#).



IPv6 Firewall

+ Add - Delete

☐	ID	Service Type	Internal IP	Internal Port	Protocol	Status	Modify
--	--	--	--	--	--	--	--

Interface Name: No interface ▼

Service Type: View Existing Applications

Internal IP: ::

Internal Port: (XX)

Protocol: TCP ▼

☒ Enable This Entry

Cancel
OK

4. Select an interface name from the drop-down list. Interface names are names of the internet connections you have set up.
5. Click [View Existing Applications](#) to select a service from the list to automatically populate the Port field with an appropriate port number. It is recommended to keep the default Port if you are unsure about which one to use. If the service is not listed, manually enter the Service Type and the Port number (e.g., 21 or 21-25). The following picture takes application [FTP](#) as an example.

IPv6 Firewall

+ Add - Delete

☐	ID	Service Type	Internal IP	Internal Port	Protocol	Status	Modify
--	--	--	--	--	--	--	--

Interface Name:

Service Type: [View Existing Applications](#)

Internal IP:

Internal Port: (XX)

Protocol:

☒ Enable This Entry

Cancel OK

6. Select the local host device running the service. Enter its global IPv6 address in the Global IPv6 Address field.
7. Select a protocol for the service from the drop-down list.
8. Select Enable This Entry.
9. Click OK.

 Tips:

- If you want to disable this entry, click the Bulb icon.
- If the local host device hosts more than one type of available service, you need to create a rule for each service. Please note that ports should NOT be used by multiple services.

Chapter 15

VPN Server&Client

The mesh device offers several ways to set up VPN connections:

VPN Server allows remote devices to access your home network in a secured way through the internet. The mesh device supports three types of VPN Server:

OpenVPN is somewhat complex but with higher security and more stability, suitable for restricted environments such as campus network and company intranet.

PPTP VPN is easy to use with the built-in VPN software of computers and mobile devices, but it is vulnerable and may be blocked by some ISPs.

IPSec VPN is more secure but slower than PPTP VPN, and may have trouble getting around firewalls.

VPN Client allows devices in your home network to access remote VPN servers, without the need to install VPN software on each device.

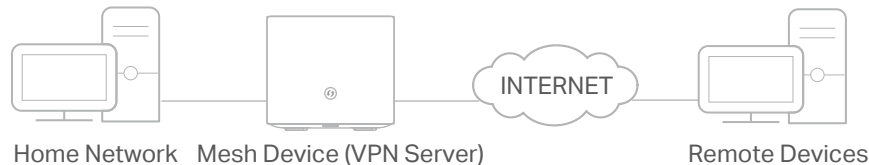
This chapter contains the following sections:

- [Use OpenVPN to Access Your Home Network](#)
- [Use PPTP VPN to Access Your Home Network](#)
- [Use IPSec VPN to Access Your Home Network](#)
- [VPN Connections](#)

15.1. Use OpenVPN to Access Your Home Network

OpenVPN Server is used to create an OpenVPN connection for remote devices to access your home network.

To use the VPN feature, you need to enable OpenVPN Server on your mesh device, and install and run VPN client software on remote devices. Please follow the steps below to set up an OpenVPN connection.



Step1. Set up OpenVPN Server on Your Mesh Device

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
2. Go to **Advanced > VPN > OpenVPN**, and tick the box of **Enable VPN Server**.

OpenVPN

Note: No certificate currently, please **Generate** one before enabling VPN Server.

☒ **Enable VPN Server**

Service Type: ☒ **UDP** ☐ **TCP**

Service Port:

VPN Subnet/Netmask:

Client Access: ☒ **Home Network Only** ☐ **Internet and Home Network**

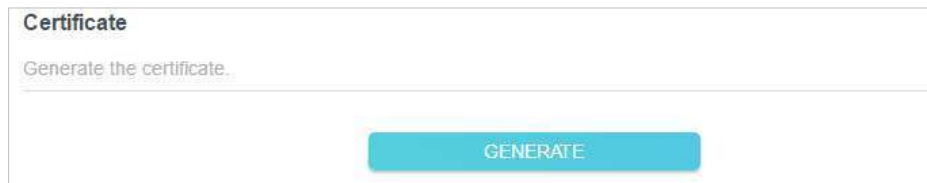
Save

Note:

- Before you enable VPN Server, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for mesh device's WAN port and synchronize your System Time with internet.
- The first time you configure the OpenVPN Server, you may need to generate a certificate before you enable the VPN Server.

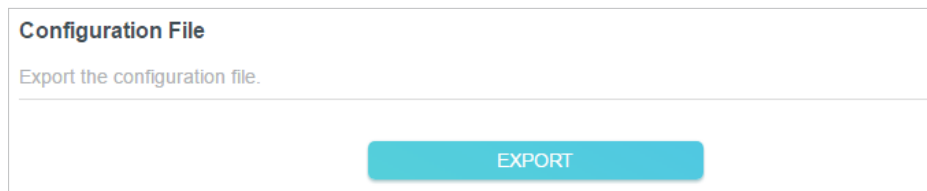
3. Select the **Service Type** (communication protocol) for OpenVPN Server: UDP, TCP.
4. Enter a VPN **Service Port** to which a VPN device connects, and the port number should be between 1024 and 65535.
5. In the **VPN Subnet/Netmask** fields, enter the range of IP addresses that can be leased to the device by the OpenVPN server.
6. Select your **Client Access** type. Select **Home Network Only** if you only want the remote device to access your home network; select **Internet and Home Network** if you also want the remote device to access internet through the VPN Server.

7. Click **SAVE**.
8. Click **GENERATE** to get a new certificate.

A screenshot of a web interface for generating a certificate. It has a title 'Certificate' and a text input field with the placeholder 'Generate the certificate.'. Below the input field is a blue button labeled 'GENERATE'.

■ **Note:** If you have already generated one, please skip this step, or click **GENERATE** to update the certificate.

9. Click **EXPORT** to save the OpenVPN configuration file which will be used by the remote device to access your mesh device.

A screenshot of a web interface for exporting a configuration file. It has a title 'Configuration File' and a text input field with the placeholder 'Export the configuration file.'. Below the input field is a blue button labeled 'EXPORT'.

Step 2. Configure OpenVPN Connection on Your Remote Device

1. Visit <http://openvpn.net/index.php/download/community-downloads.html> to download the OpenVPN software, and install it on your device where you want to run the OpenVPN client utility.

■ **Note:** You need to install the **OpenVPN** client utility on each device that you plan to apply the VPN function to access your mesh device. Mobile devices should download a third-party app from Google Play or Apple App Store.

2. After the installation, copy the file exported from your mesh device to the OpenVPN client utility's "config" folder (for example, **C:\Program Files\OpenVPN\config** on Windows). The path depends on where the OpenVPN client utility is installed.
3. Run the OpenVPN client utility and connect it to OpenVPN Server.

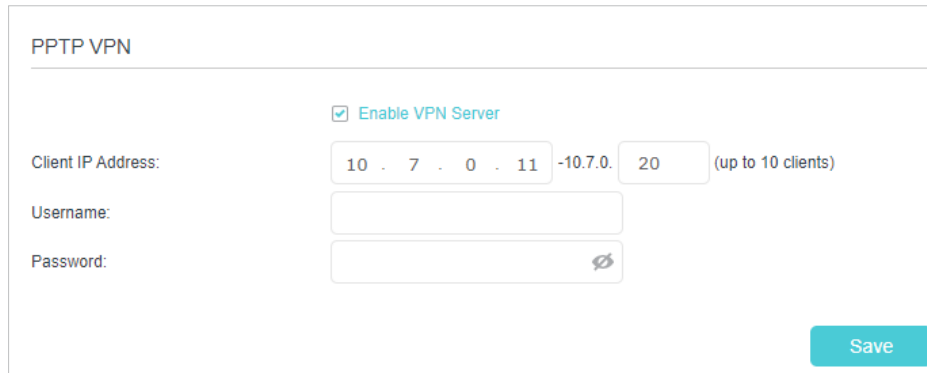
15.2. Use PPTP VPN to Access Your Home Network

PPTP VPN Server is used to create a PPTP VPN connection for remote devices to access your home network.

To use the VPN feature, you need to set up PPTP VPN Server on your mesh device, and configure the PPTP connection on remote devices. Please follow the steps below to set up a PPTP VPN connection.

Step 1. Set up PPTP VPN Server on Your Mesh Device

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
2. Go to **Advanced > VPN > PPTP VPN**, and tick the box of **Enable VPN Server**.



PPTP VPN

☒ Enable VPN Server

Client IP Address: 10 . 7 . 0 . 11 -10.7.0. 20 (up to 10 clients)

Username:

Password: 

Save

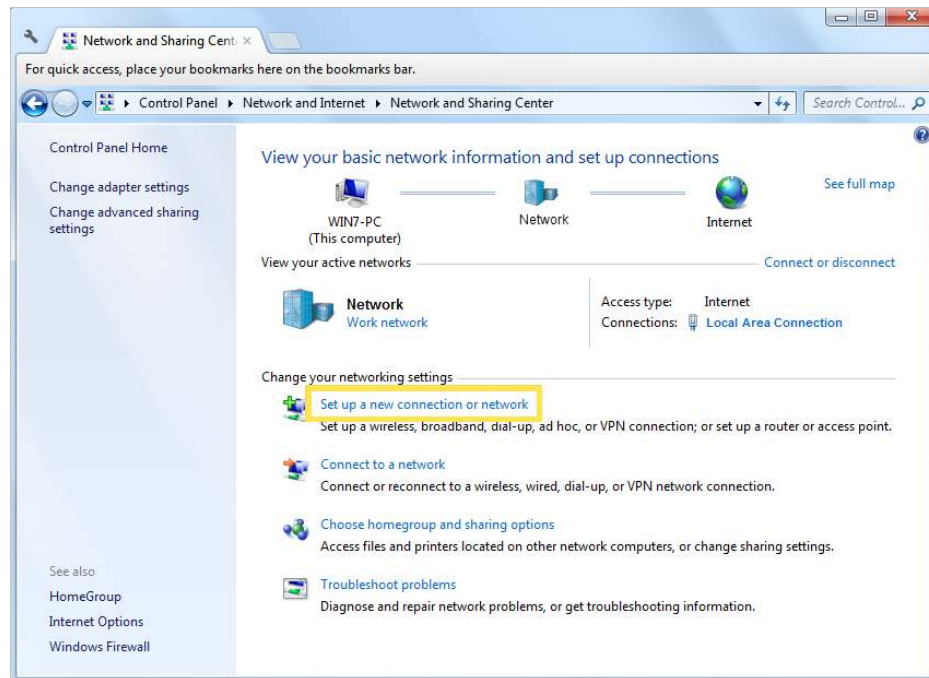
■ **Note:** Before you enable [VPN Server](#), we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for mesh device's WAN port and synchronize your [System Time](#) with internet.

3. In the [Client IP Address](#) field, enter the range of IP addresses (up to 10) that can be leased to the devices by the PPTP VPN server.
4. Enter the [Username](#) and [Password](#) to authenticate clients to the PPTP VPN server.
5. Click [SAVE](#).
6. On the client devices, create a PPTP VPN connection. The official supported platforms include Windows, Mac OSX, Linux, iOS, and Android.
7. Launch the PPTP VPN program, add a new connection and enter the domain name of the registered DDNS service or the static IP address that is assigned to the WAN port, to connect the client device to the PPTP VPN server.

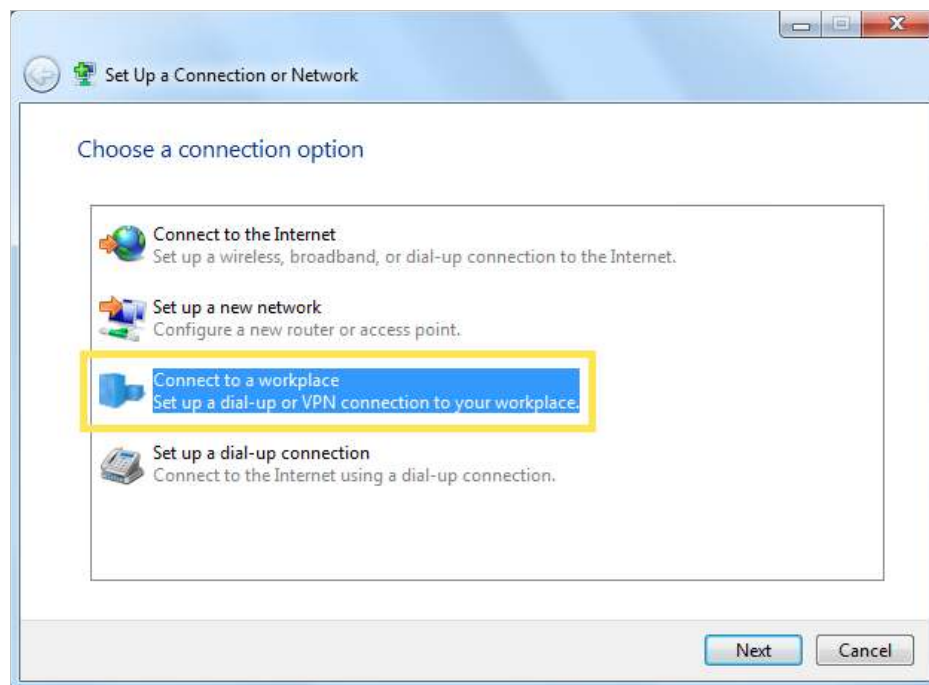
Step 2. Configure PPTP VPN Connection on Your Remote Device

The remote device can use the Windows built-in PPTP software or a third-party PPTP software to connect to PPTP Server. Here we use the [Windows built-in PPTP software](#) as an example.

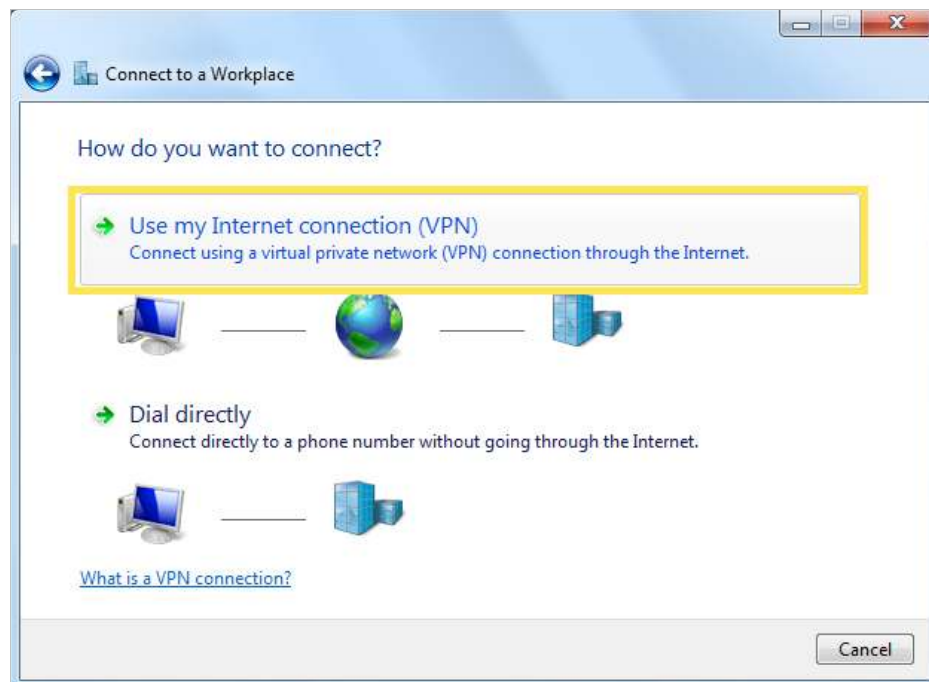
1. Go to [Start > Control Panel > Network and Internet > Network and Sharing Center](#).
2. Select [Set up a new connection or network](#).



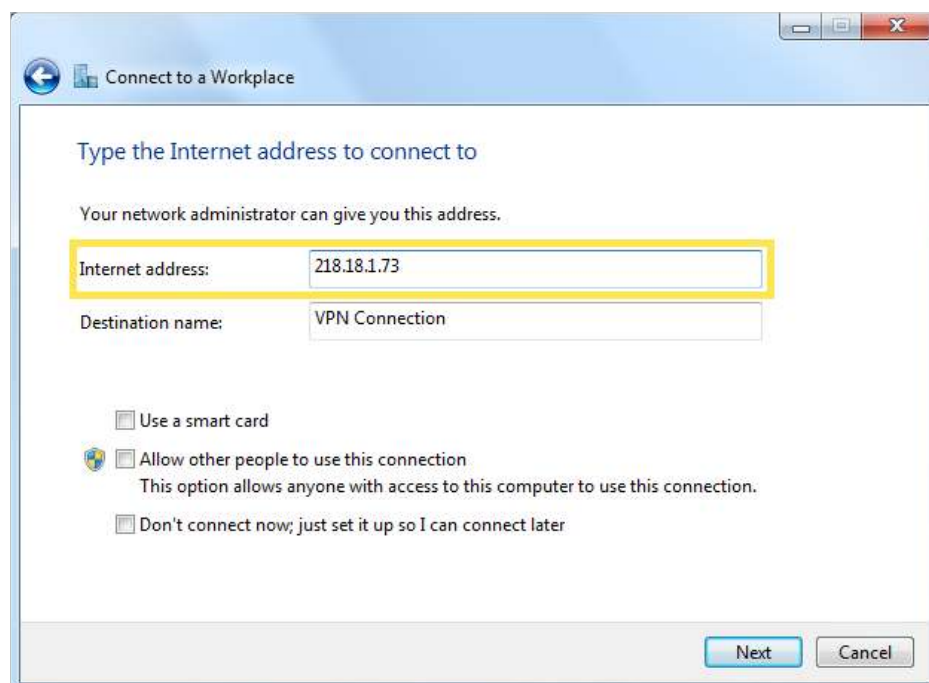
3. Select [Connect to a workplace](#) and click [Next](#).



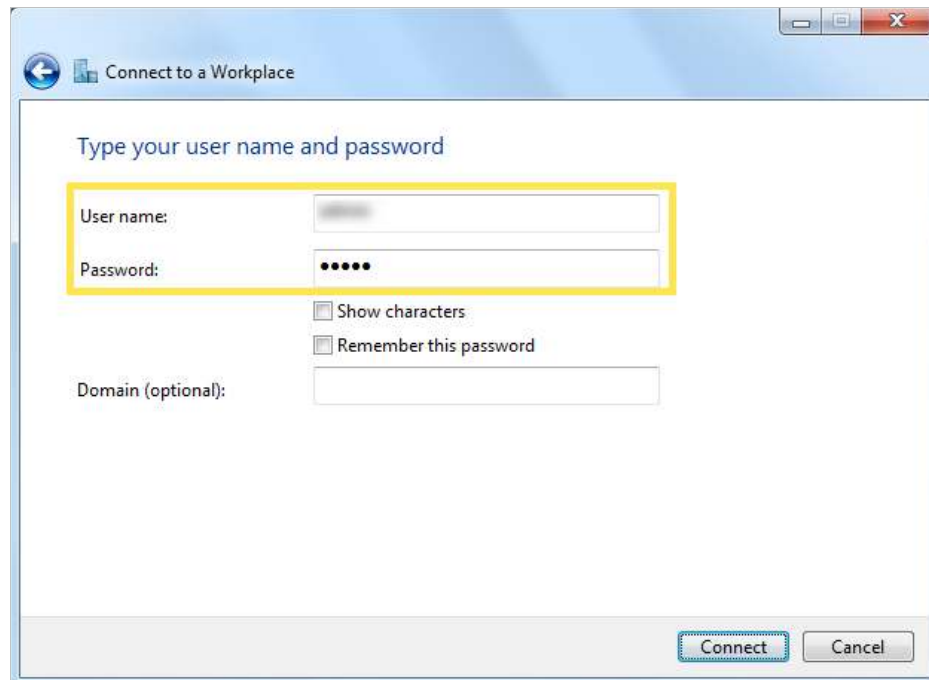
4. Select [Use my Internet connection \(VPN\)](#).



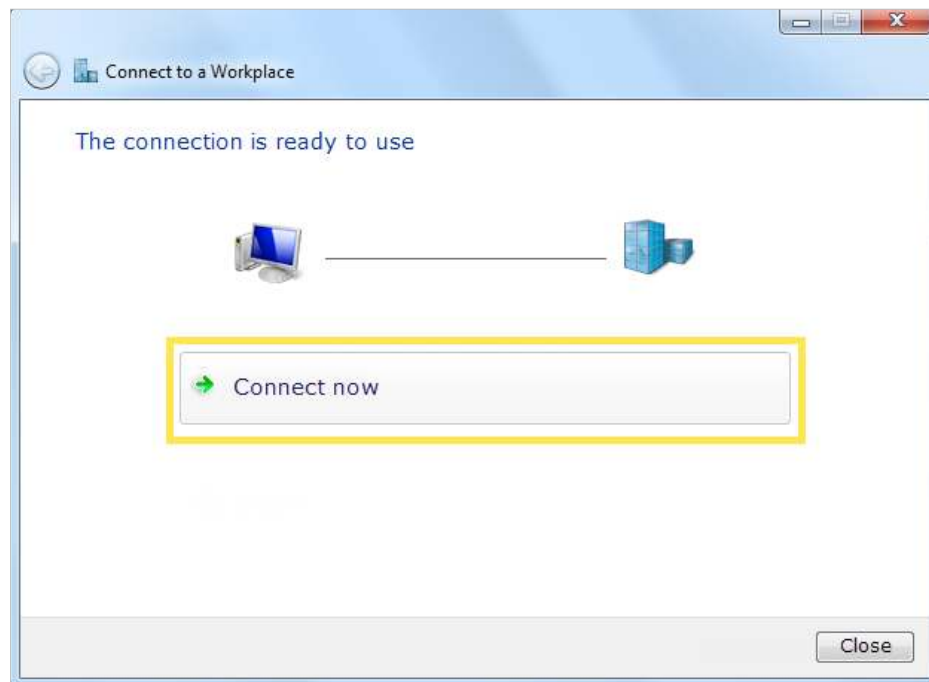
5. Enter the internet IP address of the mesh device (for example: 218.18.1.73) in the **Internet address** field. Click **Next**.



6. Enter the **User name** and **Password** you have set for the PPTP VPN server on your mesh device, and click **Connect**.



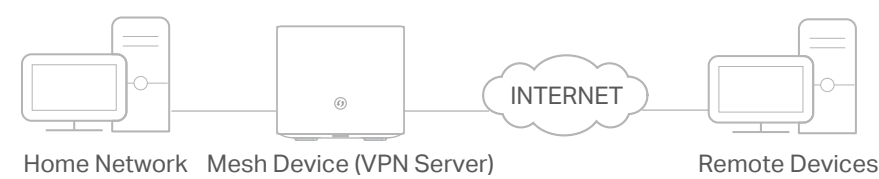
7. Click [Connect Now](#) when the VPN connection is ready to use.



15.3. Use IPsec VPN to Access Your Home Network

IPsec VPN Server is used to create a IPsec VPN connection for remote devices to access your home network.

To use the VPN feature, you need to set up IPsec VPN Server on your mesh device, and configure the IPsec connection on remote devices. Please follow the steps below to set up the IPsec VPN connection.



Step 1. Set up IPsec VPN Server on Your Mesh Device

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
2. Go to [Advanced > VPN > IPsec VPN](#), and enable [Dead Peer Detection](#).

- Note:**
- Firmware update may be required to support IPsec VPN Server.
 - Before you enable [Dead Peer Detection](#), we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for mesh device’s WAN port and synchronize your [System Time](#) with internet.

IPsec VPN

Dead Peer Detection:

+

Add

−

Delete

☐	Connection Name	Remote Gateway	Local Address	Remote Address	Status	Enable	Modify
☐	--	--	--	--	--	--	--

3. Click [Add](#).
4. Configure the IPsec VPN server parameters.

Dead Peer Detection:
☒

+ Add
- Delete

☐	Connection Name	Remote Gateway	Local Address	Remote Address	Status	Enable	Modify
--	--	--	--	--	--	--	--

IPSec Connection Name:
Name

Remote IPSec Gateway (URL):
0.0.0.0

Tunnel access from local IP addresses:
Subnet Address

IP Address for VPN:
0 . 0 . 0 . 0

Subnet Mask:
255 . 255 . 255 . 0

Tunnel access from remote IP addresses:
Subnet Address

IP Address for VPN:
0 . 0 . 0 . 0

Subnet Mask:
255 . 255 . 255 . 0

Key Exchange Method:
Auto (IKE)

Authentication Method:
Pre-Shared Key

Pre-Shared Key:
psk_key

Perfect Forward Secrecy:
Enable

Advanced

Cancel
OK

- Configure the advanced settings according to the following explanation. We recommend that you keep the default settings. If you want to change these settings, make sure that both VPN server endpoints use the same Encryption Algorithm, Integrity Algorithm, Diffie-Hellman Group and Key Lifetime in both phase1 and phase2.

The screenshot shows a configuration window titled "Advanced" with a sub-header "Advanced". It is divided into two sections: "Phase 1" and "Phase 2".

Phase 1 Settings:

- Mode: Main (dropdown)
- Local Identifier Type: Local Wan IP (dropdown)
- Local Identifier: (text input)
- Remote Identifier Type: Remote Wan IP (dropdown)
- Remote Identifier: (text input)
- Encryption Algorithm: 3DES (dropdown)
- Integrity Algorithm: MD5 (dropdown)
- Diffie-Hellman Group for Key Exchange: 1024bit (dropdown)
- Key Life Time(Seconds): 3600 (text input)

Phase 2 Settings:

- Encryption Algorithm: 3DES (dropdown)
- Integrity Algorithm: MD5 (dropdown)
- Diffie-Hellman Group for Key Exchange: 1024bit (dropdown)
- Key Life Time(Seconds): 3600 (text input)

At the bottom right, there are "Cancel" and "OK" buttons.

6. Click **OK**.

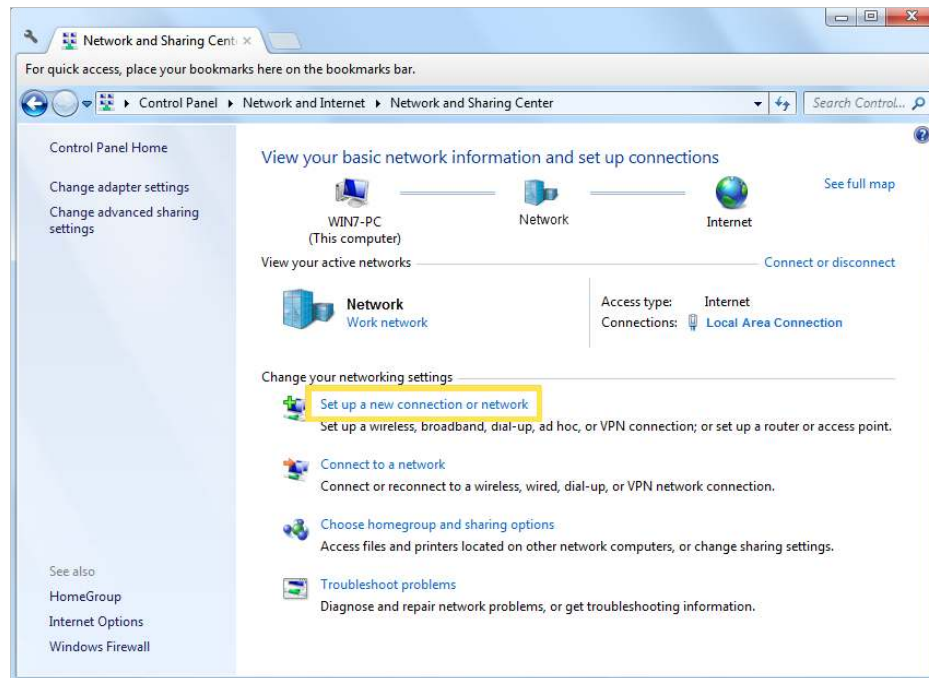
Note:

- For the comprehensive guide, please refer to the User Guide on the product's support page.

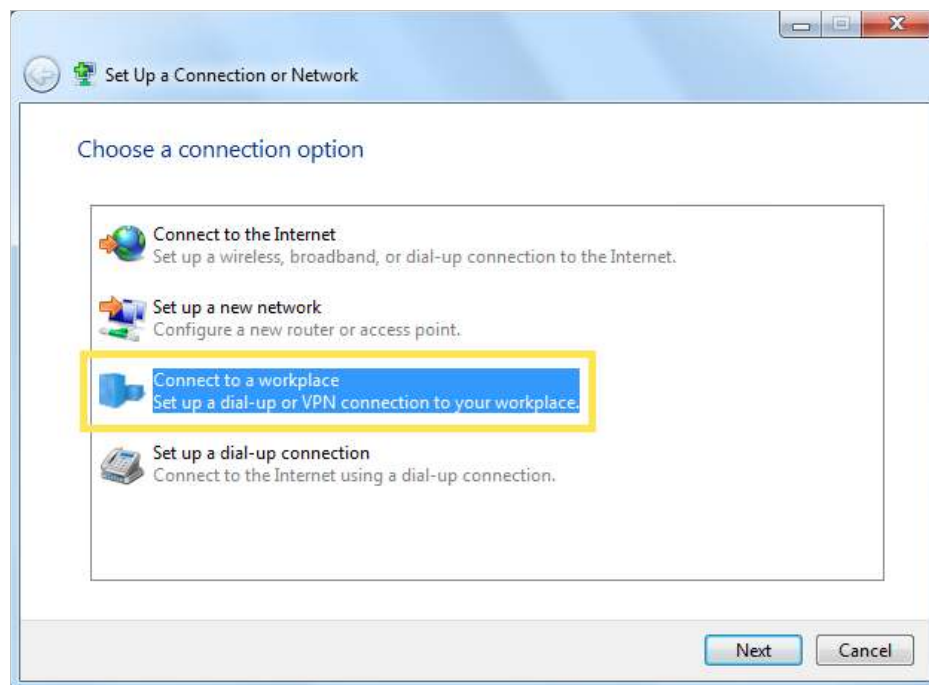
Step 2. Configure IPSec VPN Connection on Your Remote Device

The remote device can use the Windows or Mac OS built-in IPSec software or a third-party IPSec software to connect to IPSec Server. Here we use the [Windows built-in IPSec software](#) as an example.

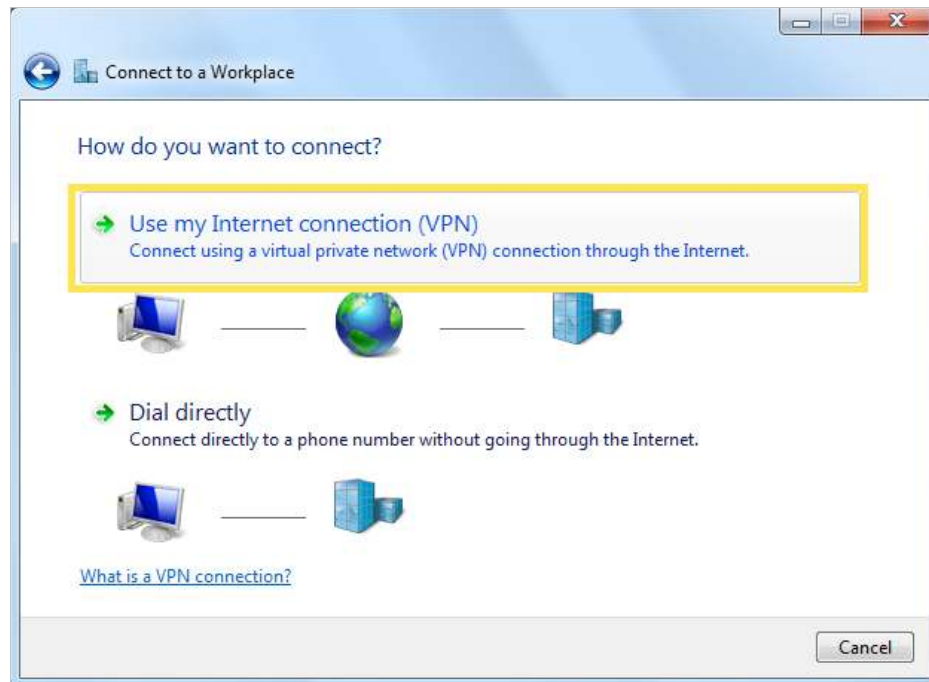
1. Go to [Start > Control Panel > Network and Internet > Network and Sharing Center](#).
2. Select [Set up a new connection or network](#).



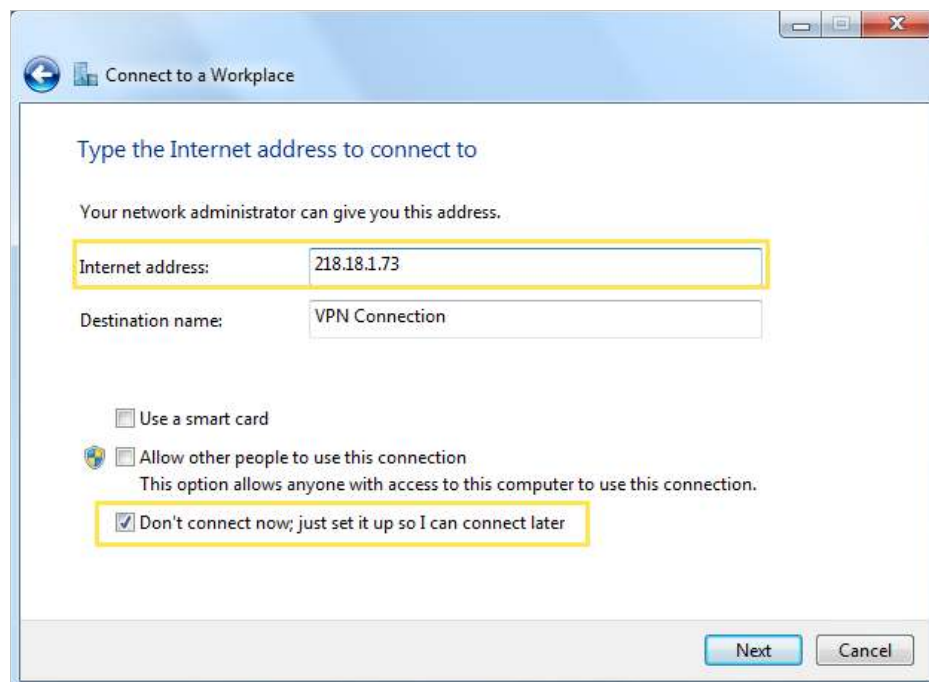
3. Select [Connect to a workplace](#) and click [Next](#).



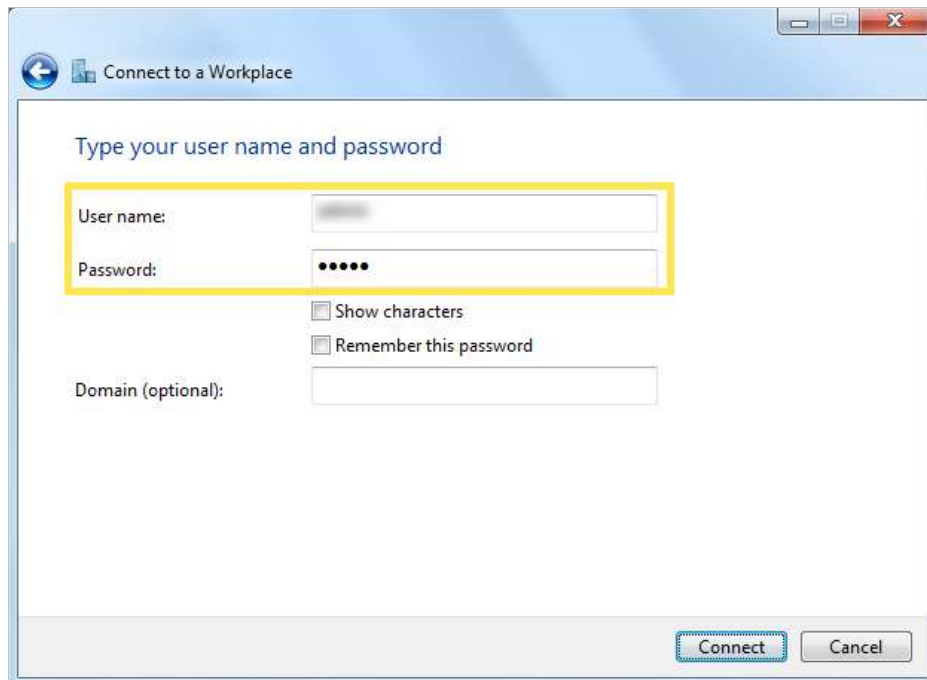
4. Select [Use my Internet connection \(VPN\)](#).



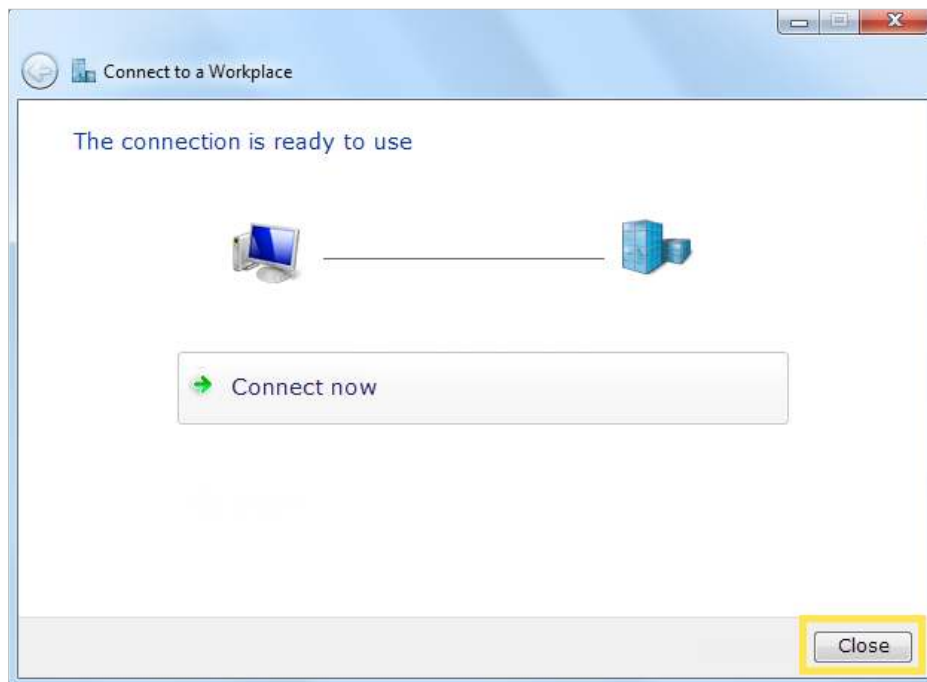
5. Enter the internet IP address of the mesh device (for example: 218.18.1.73) in the **Internet address** field, and select the checkbox **Don't connect now; just set it up so I can connect later**. Click **Next**.



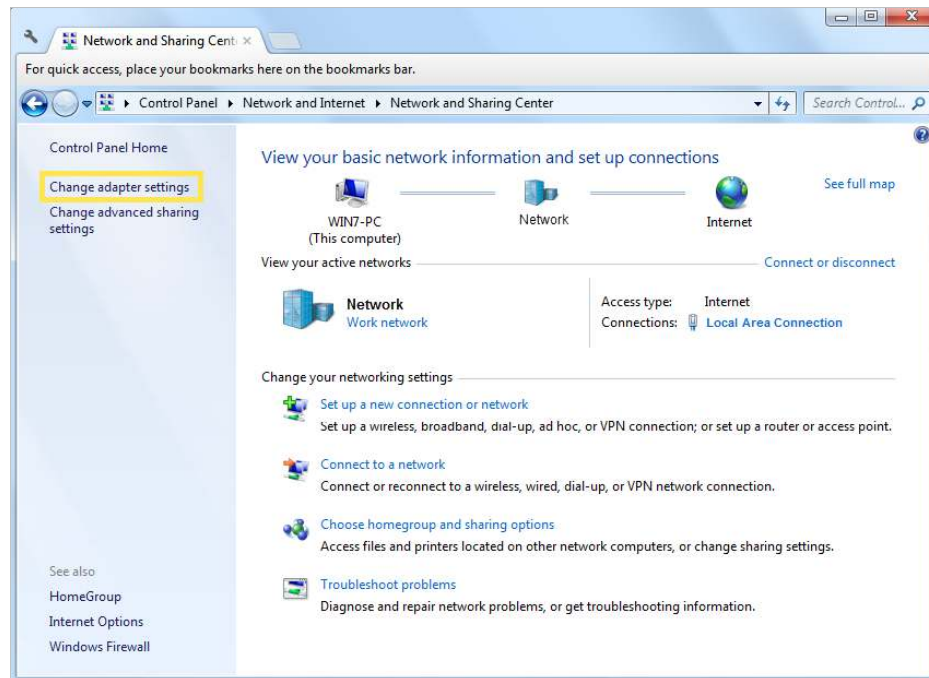
6. Enter the **User name** and **Password** you have set for the IPSec VPN server on your mesh device, and click **Connect**.



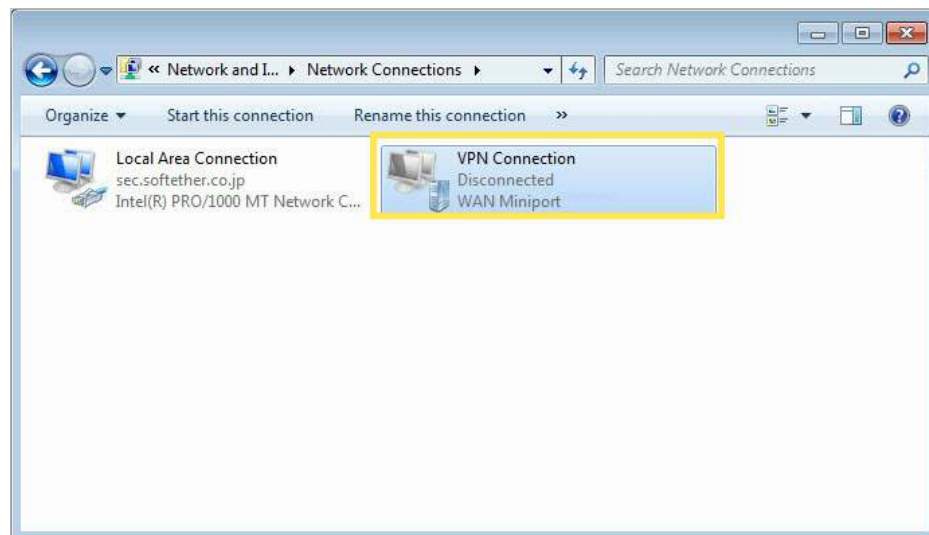
7. Click [Close](#) when the VPN connection is ready to use



8. Go to [Network and Sharing Center](#) and click [Change adapter settings](#).



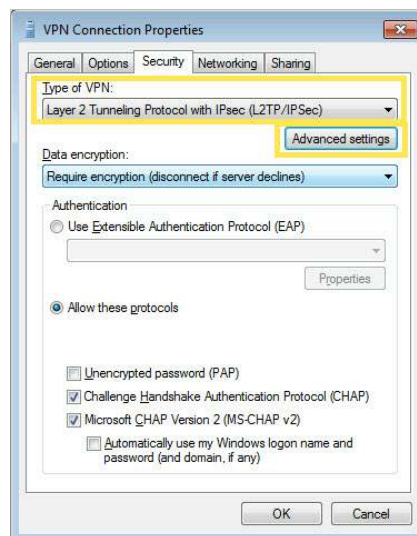
9. Find the VPN connection you created, then double-click it.



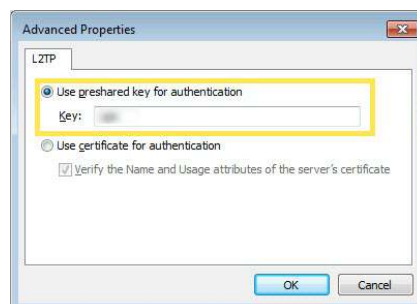
10. Enter the **User name** and **Password** you have set for the IPSec VPN server on your mesh device, and click **Properties**.



11. Switch to the **Security** tab, select **Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)** and click **Advanced settings**.



12. Select **Use preshared key for authentication** and enter the IPsec Pre-Shared Key you have set for the IPsec VPN server on your mesh device. Then click **OK**.



Done! Click **Connect** to start VPN connection.



15. 4. VPN Connections

VPN Connections page displays the clients that are currently connected to the OpenVPN servers, PPTP VPN servers and IPSec VPN hosted on the mesh device.

- 1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
- 2. Go to **Advanced > VPN > VPN connections**.

VPN Connections

OpenVPN Connection

ID	Client IP Address	Modify
--	--	--

PPTP VPN Connection

ID	Client IP Address	Modify
--	--	--

IPSec VPN Connection

☐	Connection Name	Remote Gateway	Local Address	Remote Address	Status	Enable	Modify
--	--	--	--	--	--	--	--

Chapter 16

Manage Your Mesh Device

This chapter introduces how to change the system settings and administrate your mesh device's network.

This chapter contains the following sections:

- [Set System Time](#)
- [Control the LED](#)
- [Test Internet Connectivity](#)
- [Update the Firmware](#)
- [Back Up and Restore Configuration Settings](#)
- [Reboot the Mesh Device](#)
- [Administration Management](#)
- [System Log](#)
- [CWMP Settings](#)
- [SNMP Settings](#)
- [Monitor the Internet Traffic Statistics](#)
- [Port Mirror](#)

16.1. Set System Time

System time is the time displayed while the mesh device is running. The system time you configure here will be used for other time-based functions like Parental Controls and Wireless Schedule. You can manually set how to get the system time.

Follow the steps below to set your system time.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [System Tools](#) > [Time Settings](#) page.

System Time

Time Zone: (GMT-08:00) Pacific Time (US & Canada); Tijuana

Date: 1/7/2016 (MM/DD/YY)

Time: 23 : 59 : 13

NTP: ☒ Enable

NTP Server I: 0.0.0.0 (Optional)

NTP Server II: 0.0.0.0 (Optional)

Get from PC Get from the Internet Save

3. Configure the system time using the following methods:
[Get from PC](#): Click this button if you want to use the current time of your PC.
[Get from the Internet](#): Click this button if you want to get time from the internet. Make sure your mesh device can access the internet before you select this way to get system time.
4. Click [Save](#).
5. After setting the system time, you can set [Daylight Saving Time](#) according to your needs. Enable [Daylight Saving Time](#), and set the start and end time and then click [Save](#) to make the settings effective.

Daylight Saving Time

☐ Enable Daylight Saving Time

Start: 2016 Jan M Last W Tue T 00:00

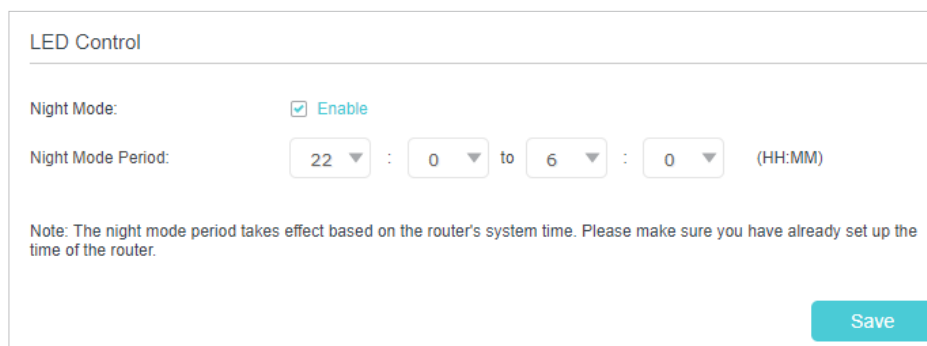
End: 2016 Oct M Last W Sun T 03:00

Save

16.2. Control the LED

The LED of the mesh device indicates its activities and status. You can enable the Night Mode feature to specify a time period during which the LED is off.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
2. Go to [Advanced](#) > [System](#) > [LED Control](#).
3. Enable [Night Mode](#).
4. Specify the LED off time, and the LED will be off during this period every day.
5. Click [SAVE](#).



LED Control

Night Mode: ☒ [Enable](#)

Night Mode Period: 22 : 0 to 6 : 0 (HH:MM)

Note: The night mode period takes effect based on the router's system time. Please make sure you have already set up the time of the router.

[Save](#)

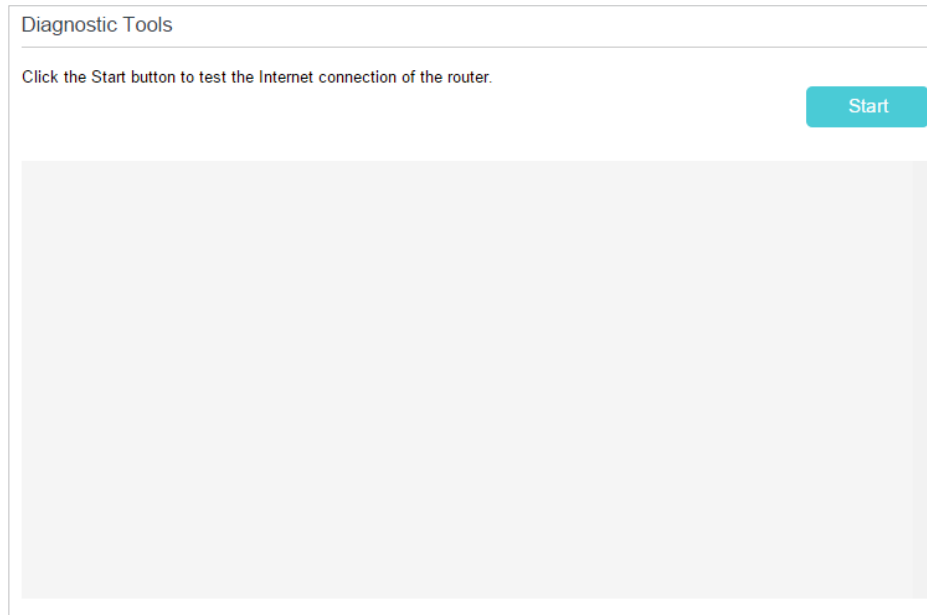
16.3. Test Internet Connectivity

Diagnostics function is used to test the connectivity between the mesh device and the host or other network devices.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [System Tools](#) > [Diagnostics](#) page.

➤ **To test the internet connection of the mesh device:**

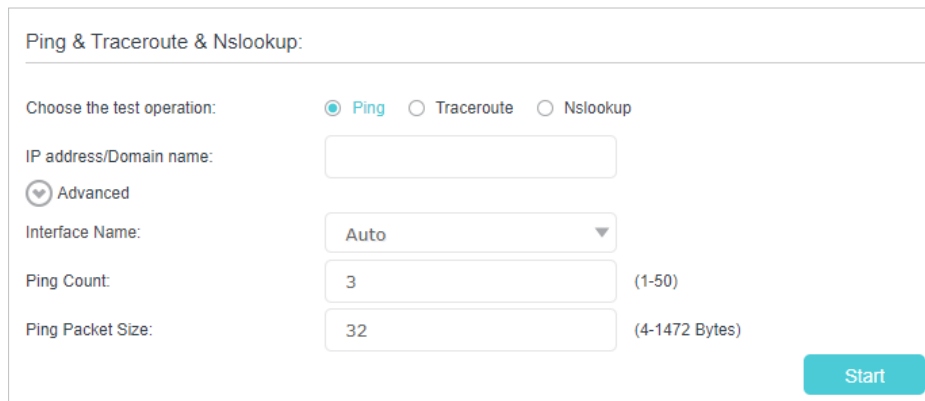
Locate the [Diagnostic Tools](#) section, and click the [Start](#) to test the internet connectivity and you will find the test results in the gray box.



The screenshot shows a web interface titled "Diagnostic Tools". Below the title, there is a text instruction: "Click the Start button to test the Internet connection of the router." To the right of this text is a teal "Start" button. Below the instruction is a large, empty light gray rectangular area, likely a placeholder for test results.

➤ **To run ping and traceroute tools:**

- 1) Locate the [Diagnostic Tools](#) section.



The screenshot shows a configuration form titled "Ping & Traceroute & Nslookup:". It contains several fields and options:

- Choose the test operation:** Three radio buttons are present: "Ping" (selected), "Traceroute", and "Nslookup".
- IP address/Domain name:** A text input field.
- Advanced:** A dropdown menu currently showing "Advanced".
- Interface Name:** A dropdown menu currently showing "Auto".
- Ping Count:** A text input field with the value "3". To its right, the range "(1-50)" is displayed.
- Ping Packet Size:** A text input field with the value "32". To its right, the range "(4-1472 Bytes)" is displayed.
- A teal "Start" button is located at the bottom right of the form.

- 2) Select [Ping](#) or [Traceroute](#) or [Nslookup](#) as the diagnostic tool to test the connectivity.
 - [Ping](#) is used to test the connectivity between the mesh device and the tested host, and measure the round-trip time.
 - [Traceroute](#) is used to display the route (path) your mesh device has passed to reach the tested host, and measure transit delays of packets across an internet Protocol network.
 - [Nslookup](#) is used to queries the Domain Name System (DNS) to obtain the mapping between a domain name and IP address, or other DNS records.
- 3) Enter the [Target IP Address/Domain Name](#) of the tested host. You can change the default test options if necessary.

- 4) Click [Start](#) to begin the diagnostics, and you will find the test results in the gray box.

16.4. Update the Firmware

TP-Link is dedicated to improving product features, giving you a better network experience.

We will inform you through the web management page if there's any update firmware available for your mesh device. The latest firmware can also be downloaded from the [Support](#) page of our website www.tp-link.com for free.

Note:

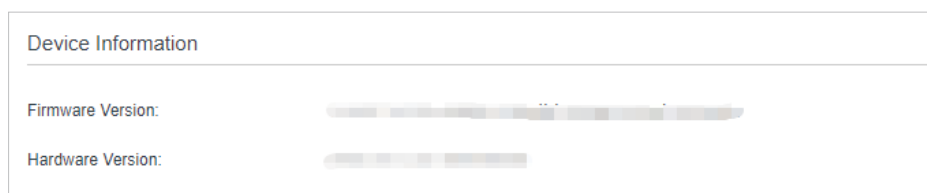
1. Make sure that you have a stable connection between the mesh device and your computer. It is NOT recommended to upgrade the firmware wirelessly.
2. Back up your mesh device configuration before upgrading the firmware.
3. DO NOT turn off the mesh device during the firmware upgrade.

➤ **Follow the steps below to upgrade the firmware online:**

1. Click Check for Upgrades.
2. If a new firmware is displayed, click Upgrade and click Yes when prompted, then the mesh device will automatically download the latest firmware file and upgrade.

➤ **Follow the steps below to manually update the firmware:**

1. Download the latest firmware file for the mesh device from our website www.tp-link.com.
2. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
3. Go to [Advanced](#) > [System Tools](#) > [Firmware Upgrade](#).
4. Focus on the [Device Information](#) section. Make sure the downloaded firmware file matches with the [Hardware Version](#).



5. Focus on the [Local Upgrade](#) section. Click [Browse](#) to locate the downloaded new firmware file, and click [Upgrade](#).

Local Upgrade

-	ID	Device Name	Model Name	MAC Address	Firmware Version
☒	1	living_room	HX220		

New firmware file:

6. Wait a few minutes for the upgrading and rebooting.

16.5. Back Up and Restore Configuration Settings

The configuration settings are stored as a configuration file in the mesh device. You can back up the configuration file to your computer for future use and restore the mesh device to a previous settings from the backup file when needed. Moreover, if needed you can erase the current settings and reset the mesh device to its default factory settings.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [System Tools](#) > [Backup & Restore](#).

➤ **To back up configuration settings:**

Click [Backup](#) to save a copy of the current settings to your local computer. A conf.bin file will be stored to your computer.

Backup

Save a copy of your current settings.

➤ **To restore configuration settings:**

- 1) Click [Browse](#) to locate the previous backup configuration file, and click [Restore](#).

Restore

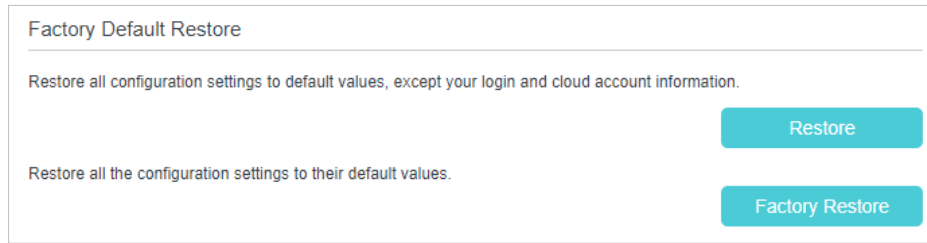
Restore previous settings from a saved file.

File:

- 2) Wait a few minutes for the restoring and rebooting.

➤ **To reset the mesh device to factory default settings:**

- 1) Locate the [Factory Default Restore](#) section, and click [Factory Restore](#) to reset the mesh device.



The screenshot shows a web interface titled "Factory Default Restore". Below the title is a horizontal line. Underneath the line, there is a paragraph: "Restore all configuration settings to default values, except your login and cloud account information." To the right of this paragraph is a blue button labeled "Restore". Below this paragraph is another paragraph: "Restore all the configuration settings to their default values." To the right of this paragraph is a blue button labeled "Factory Restore".

- 2) Wait a few minutes for the resetting and rebooting.

Note:

1. During the resetting process, do not turn off the mesh device.
2. We strongly recommend you back up the current configuration settings before resetting the mesh device.

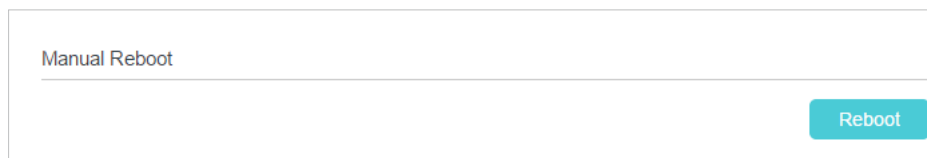
16.6. Reboot the Mesh Device

The Reboot feature cleans the cache to enhance the running performance of the mesh device. You can reboot the mesh device manually or set it to reboot regularly.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [System Tools](#) > [Reboot Schedule](#), and you can restart your mesh device.

➤ **To reboot the mesh device manually:**

Click [Reboot](#), and wait a few minutes for the mesh device to rebooting.



The screenshot shows a web interface titled "Manual Reboot". Below the title is a horizontal line. To the right of the line is a blue button labeled "Reboot".

➤ **To schedule the mesh device to reboot at a specific time:**

- 1) Enable [Auto Reboot](#).
- 2) Specify the [Time](#) when the mesh device reboots.

Reboot Schedule

Note: Before enabling Reboot Schedule, please make sure your router is connected to the internet. Then go to [Time Settings](#) and choose **Get from the Internet** to get the correct network time.

Current Time: 01/08/2016 00:10:57

Reboot Schedule: ☐ Enable

Repeat: Every day

Reboot Time: 3 : 0

[Save](#)

3) Click [Save](#) to make the settings effective.

Some settings of the mesh device may take effect only after rebooting, including:

- Change the LAN IP Address (system will reboot automatically).
- Change the Operation Mode (system will reboot automatically).
- Upgrade the firmware of the mesh device (system will reboot automatically).
- Restore the mesh device to its factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically).

Note:

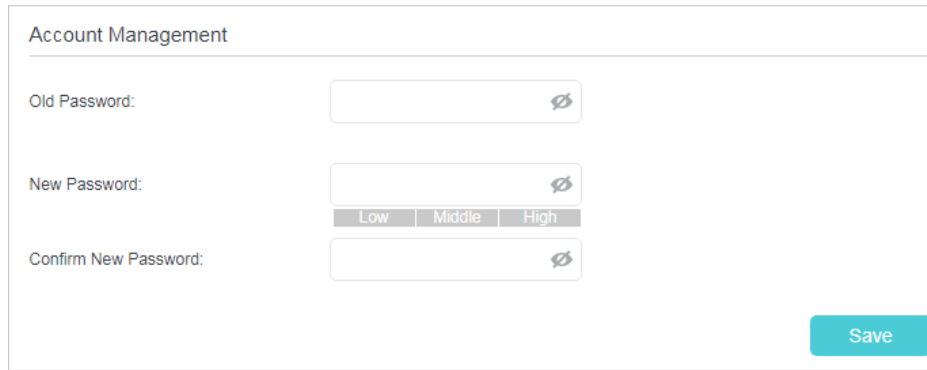
The Auto Reboot feature takes effect based on the mesh device's system time. Please make sure you have already set up the time of the mesh device.

16.7. Administration Management

16.7.1. Change the Login Password

A login password is required to log in to the mesh device's web management page. You are asked to set a login password at first login. You can change it with the account management feature.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [System Tools](#) > [Administration](#), and locate the [Account Management](#) section.



The screenshot shows the 'Account Management' section of a web interface. It contains three password input fields: 'Old Password:', 'New Password:', and 'Confirm New Password:'. Each field has a toggle icon to its right. Below the 'New Password:' field, there are three tabs labeled 'Low', 'Middle', and 'High'. A teal 'Save' button is located at the bottom right of the form.

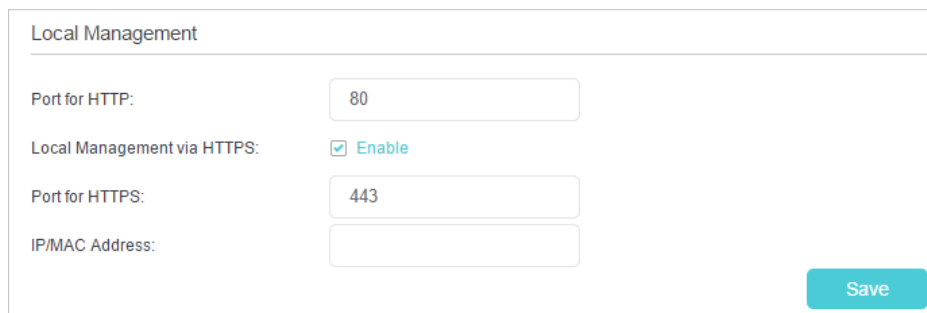
3. Enter the old password and a new password twice (both case-sensitive).
4. Click [Save](#) to make the settings effective.

16.7.2. Local Management

You can control the local devices' authority to manage the mesh device via Local Management feature. By default all local connected devices are allowed to manage the mesh device. You can also specify one device to manage the mesh device and enable local management over a more secure way, HTTPS.

Follow the steps below to allow only the specific device to manage the mesh device via the local management over HTTPS.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [System Tools](#) > [Administration](#), and locate the [Local Management](#) section.
3. Enable [Local Management over HTTPS](#) and keep the [Port for HTTP](#) and [Port for HTTPS](#) as the default settings. Enter the [IP address](#) or [MAC address](#) of the local device to manage the mesh device.



The screenshot shows the 'Local Management' section of a web interface. It contains four settings: 'Port for HTTP:' with a value of '80', 'Local Management via HTTPS:' with a checked checkbox and the text 'Enable', 'Port for HTTPS:' with a value of '443', and 'IP/MAC Address:' with an empty input field. A teal 'Save' button is located at the bottom right of the form.

4. Click [Save](#).

Now, you can manage the mesh device over both HTTP (<http://tplinkwifi.net>) and HTTPS (<https://tplinkwifi.net>).

Note:

If you want all local devices can manage the mesh device, just leave the [IP/MAC Address](#) field blank.

16.7.3. Remote Management

By default, the remote devices are not allowed to manage the mesh device from the internet. You can enable remote management over HTTP and/or HTTPS if needed. HTTPS is a more secure way to access the mesh device.

Note:

If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), you cannot use the remote management feature because private addresses are not routed on the internet.

Follow the steps below to allow remote devices to manage the mesh device over HTTPS.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [System Tools](#) > [Administration](#), and locate the [Remote Management](#) section.

The screenshot shows the 'Remote Management' configuration page. It includes the following fields and options:

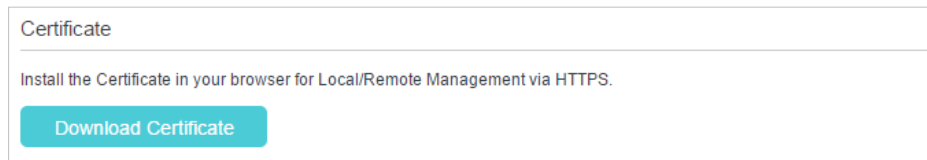
- Remote Management:** A checkbox labeled 'Enable' which is currently unchecked.
- Port for HTTP:** A text input field containing the value '80'.
- Remote Management via HTTPS:** A checkbox labeled 'Enable' which is currently unchecked.
- Port for HTTPS:** A text input field containing the value '443'.
- Manage This Router via the Address:** A text input field containing the message 'Your router is not connected to the Internet.'
- Client Device Allowed for Remote Management:** A section with two radio button options:
 - ☒ Only the Following IP Addresses
 - ☐ All
- Add a new IP:** A sub-section under the 'Only the Following IP Addresses' option, featuring a blue plus icon, a text input field, a dropdown menu showing '32', and a red minus icon.
- Save:** A blue button located at the bottom right of the form.

3. Enable [Remote Management](#) and [Remote Management via HTTPS](#) to allow for HTTPS connection. Keep the [Port](#) as the default setting.
4. Set the client device allowed for remote management. Select [All](#) to allow all remote devices to manage the mesh device. If you just want to allow a specific device to manage the mesh device, select [Only the Following IP/MAC Address](#) and enter the IP/MAC address of the remote device.
5. Click [Save](#).

All devices or the specific device on the internet can log in to your mesh device using the address displayed on the [Manage This Mesh Device via the Address](#) field to manage the mesh device.

 Tips:

1. If you were warned about the certificate when visiting the web management page remotely, click [Trust](#) (or a similar option) to continue. To avoid this warning, you can download and install the certificate on the mesh device's web management page at [Advanced > System Tools > Administration](#).

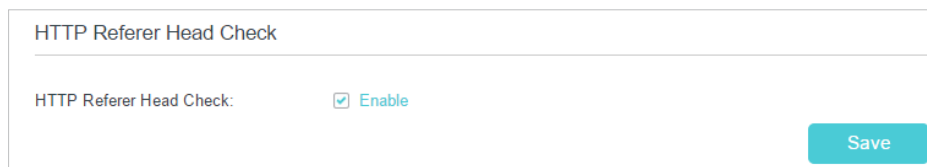


2. The mesh device's WAN IP is usually a dynamic IP. Please refer to [Configure IPv6 LAN Settings](#) if you want to log in to the mesh device through a domain name.

16.7.4. HTTP Referer Head Check

HTTP referer header check function can protect your networks against CSRF attacks. This function is enabled by default. You can disable this function if needed.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced > System Tools > Administration](#), and locate the [HTTP Referer Head Check](#) section.
3. Clear the [Enable](#) check box and click [Save](#) if you want to disable this function.

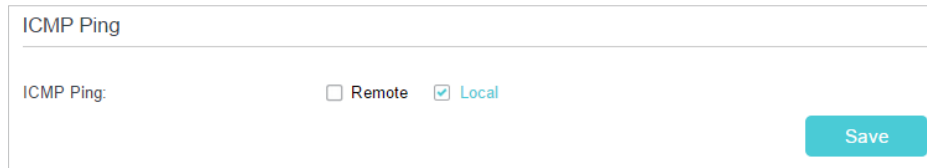


16.7.5. ICMP Ping

ICMP (Internet Control Message Protocol) Ping is used to diagnose the network by sending ICMP echo request packets to the target remote or local host and waiting for an ICMP response.

You can control the mesh device's replies to ICMP Ping requests.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced > System Tools > Administration](#), and locate the [ICMP Ping](#) section.

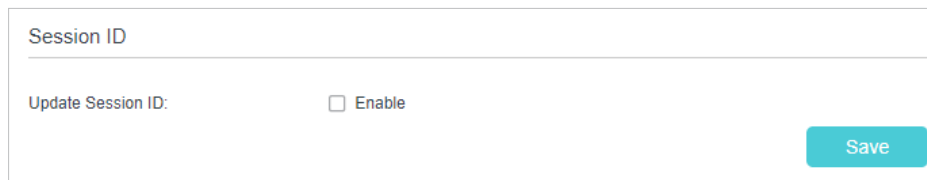


3. Specify the ICMP Ping reply options.
 - **Remote:** Select it if you want the computers on a public network to ping the mesh device's WAN IP address.
 - **Local:** Enabled by default, if enabled, the computers on a private network can ping the mesh device's LAN IP address.
4. Click **Save** to make the settings effective.

16.7.6. Session ID

When Session ID function is enabled, it will be saved into Flash every time the PPP connection is updated. This can prevent some problems of PPPoE/L2TP/PPTP connection being rejected to reconnect to servers when the device is powered off or the network disconnect accidentally.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to **Advanced > System Tools > Administration**, and locate the **Session ID** section.



3. Enable the **Update Session ID** and Click **Save** to make the settings effective.

16.8. System Log

System Log can help you know what happened to your mesh device, facilitating you to locate the malfunctions. For example when your mesh device does not work properly, you may need to save the system log and send it to the technical support for troubleshooting.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to **Advanced > System Tools > System Log** page.

System Log

Type: ALL
Level: Notice

Refresh Delete All

ID	Time	Type	Level	Log Content
1	2016-01-01 02:43:34	HTTPD	Notice	Clear log.

Log Settings Save Log

➤ **To view the system logs:**

You can view specific system logs by selecting the log type and level.

Click [Refresh](#) to refresh the log list.

➤ **To save the system logs:**

You can save the system logs to your local computer or a remote server.

Click [Save Log](#) to save the logs in a txt file to your computer.

Click [Log Settings](#) to set the storage path of logs.

Log Settings

☒ Save Locally

Minimum Level: Information

☒ Save Remotely

Minimum Level: Warning

Server IP: 192.168.1.100

Server Port: 514

Local Facility Name: User

Back Save

- **Save Locally:** Select this option to cache the system log to the mesh device's local memory, select the minimum level of system log to be saved from the drop-down list. The logs will be shown in the table in descending order on the System Log page.
- **Save Remotely:** Select this option to send the system log to a remote server, select the minimum level of system log to be saved from the drop-down list and enter the information of the remote server. If the remote server has a log viewer client or a sniffer tool implemented, you can view and analyze the system log remotely in real-time.

16.9. CWMP Settings

The mesh device supports CWMP (CPE WAN Management Protocol), also called TR-069. This collects information, performs diagnostics and configures the devices automatically via ACS (Auto-Configuration Server).

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [System Tools](#) > [CWMP Settings](#) page.

CWMP Settings

CPE WAN Management Protocol (also called TR-069) allows Auto-Configuration Server (ACS) to perform auto-configuration, provision, connection, and diagnostics to this device. You may configure this function under your ISP's instructions.

CWMP: ☒

Inform: ☒

Inform DataModel with TR098: ☐

Inform Interval:

ACS URL:

ACS Username:

ACS Password:

Interface used by TR-069 client:

CPE ID: ☒ SN ☐ LAN MAC ☐ WAN MAC

☒ Connection Request Authentication

Username:

Password:

Path: ☒ Manual ☐ Random

Port:

URL:

☐ Simple Traversal of UDP over NATs:

Save

- **CWMP:** Enable or disable the CWMP (CPE WAN Management Protocol) function.
- **Inform:** Enable or disable the function of sending an inform message to the ACS (Auto Configuration Server) periodically.
- **Inform Interval:** Set the time interval in seconds when the Inform message will be sent to the ACS.
- **ACS URL:** Enter the web address of the ACS which is provided by your ISP.

- **ACS Username/Password:** Enter the username/password to log in to the ACS server.
- **Interface used by TR-069 client:** Select which interface to be used by the TR-069 client.
- **Display SOAP messages on serial console:** Enable or disable this function.
- **Connection Request Authentication:** Select this check box to enable authentication for the connection request.
- **Username/Password:** Enter the username/password for the ACS server to log in to the mesh device.
- **Path:** Enter the path for the ACS server to log in to the mesh device.
- **Port:** Enter the port that connects to the ACS server.
- **URL:** Enter the URL that connects to the ACS server.
- **Simple Traversal of UDP over NATs:** Select this check box to enable STUN for the connection request and set the STUN maximum and minimum keep alive period, server address and port.

Click **Save** to make the settings effective.

16. 10. SNMP Settings

SNMP (Simple Network Management Protocol) is widely used in network management for network monitoring. It allows management applications to retrieve status updates and statistics from the SNMP agent within this device. In this way, network administrators can easily search and modify the information on any node on the network. Meanwhile, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating.

The **SNMP Agent** is an application running on the mesh device that performs the operational role of receiving and processing SNMP messages, sending responses to the SNMP manager, and sending traps when an event occurs. So a mesh device contains SNMP "agent" software can be monitored and/or controlled by SNMP Manager using SNMP messages.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to **Advanced > System Tools > SNMP Settings** page.

SNMP Settings

Simple Network Management Protocol (SNMP) allows management applications to retrieve status updates and statistics from the SNMP agent within this device.

Enable SNMP Agent: ☒

SNMP Agent for WAN: ☐

Read-only Community:

Write Community:

System Name:

System Description:

System Location:

System Contact:

Trap Manager IP:

[Save](#)

- **SNMP Agent/SNMP Agent for WAN:** Turn on to enable the built-in SNMP agent that allows the mesh device to operate as the operational role in receiving and processing of SNMP messages, sending responses to the SNMP manager, and triggering SNMP traps when an event occurs.
- **Read-only Community:** Displays the default public community string that protects the mesh device from unauthorized access.
- **Write Community:** Displays the default write community string that protects the mesh device from unauthorized changes.
- **System Name:** Displays the administratively-assigned name for this managed device.
- **System Description:** Displays the textual description of the managed device. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software.
- **System Location:** Displays the physical location of this device (for example, the telephone closet, 3rd floor).
- **System Contact:** Displays the textual identification of the contact person for this managed device, together with information on how to contact this person.
- **Trap Manager IP:** Displays the IP address of the host to receive the traps.

You are suggested to keep the default settings. Click [Save](#) to make the settings effective.

16. 11. Monitor the Internet Traffic Statistics

The traffic statistics function allows you to monitor the volume of internet traffic statistics. You can view the network traffic of the LAN, WAN and WLAN sent and received packets.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [System Tools](#) > [Traffic Statistics](#).
3. Turn on [Enable Traffic Statistics](#) to enable traffic statistics function, you can view the total number of packets and bytes received and transmitted by the mesh device within the selected [Statistics Interval](#). This function is disabled by default.

Traffic Statistics

Enable Traffic Statistics: ☒

Traffic Statistics and NAT Boost cannot be enabled at the same time.

Statistics Interval: 10 seconds

Save

4. You can refer to [Traffic Statistics List](#) for the detailed information about the traffic usage of all devices.

Traffic Statistics List

[Refresh](#) [Reset All](#) [Delete All](#)

IP Address/ MAC Address	Total Packets	Total Bytes	Current Packets	Current Bytes	Current ICMP Tx	Current UDP Tx	Current SYN Tx	Modify
--	--	--	--	--	--	--	--	--

16. 12. Port Mirror

This feature copies network packets of the WAN port to a specific LAN port for data analysis and network monitoring.

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [System Tools](#) > [Port Mirror](#)

Port Mirror

Enable: ☒ Enable

Lan Interface: LAN1 ▼

Timeout: 0 (seconds)

Save

3. Enable Port Mirroring.
4. Select a LAN port to mirror network packets of the WAN port.
5. Set a Timeout duration after which Port Mirroring will disable automatically. If you set Timeout to 0 seconds, Port Mirroring will not disable automatically.
6. Save the settings.

FAQ

Q1. What should I do if I forget my wireless password?

The default wireless password is printed on the label of the mesh device. If the password has been altered:

1. Connect your computer to the mesh device using an Ethernet cable.
2. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
3. Go to [Wireless](#) to retrieve or reset your wireless password.

Q2. What should I do if I forget my web management password?

- If you are using a TP-Link ID to log in, or you have enabled the Password Recovery feature of the mesh device, click [Forgot password](#) on the login page and then follow the instructions to reset it.
- Alternatively, press and hold the [Reset](#) button of the mesh device until the Power LED blinks to restore factory default settings, and then visit <http://tplinkwifi.net> or <http://192.168.88.1> to create a new login password.

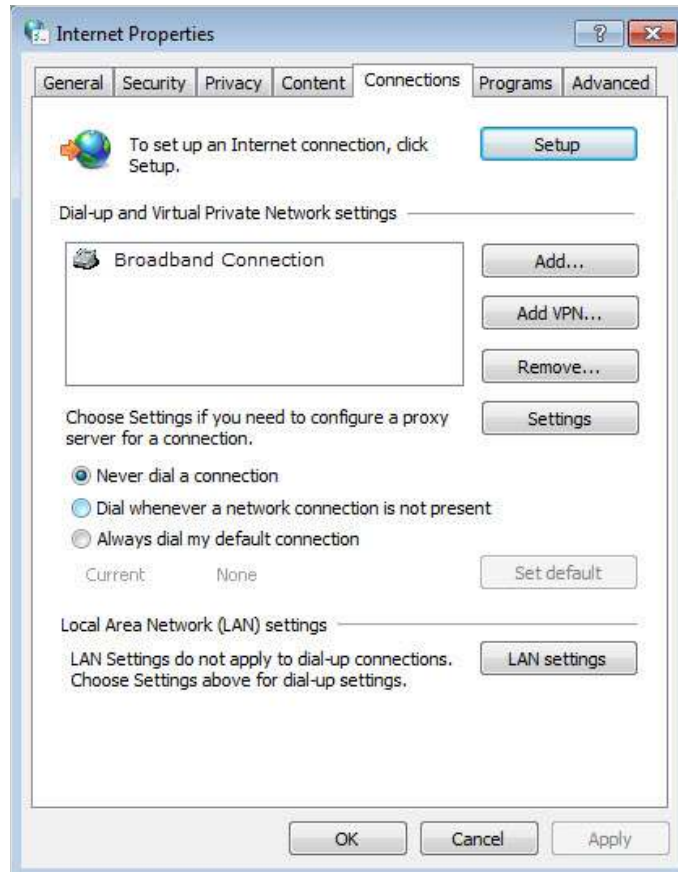
Note:

- You'll need to reconfigure the mesh device to surf the internet once the mesh device is reset, and please mark down your new password for future use.

Q3. What should I do if I can't log in to the mesh device's web management page?

This can happen for a variety of reasons. Please try the methods below to log in again.

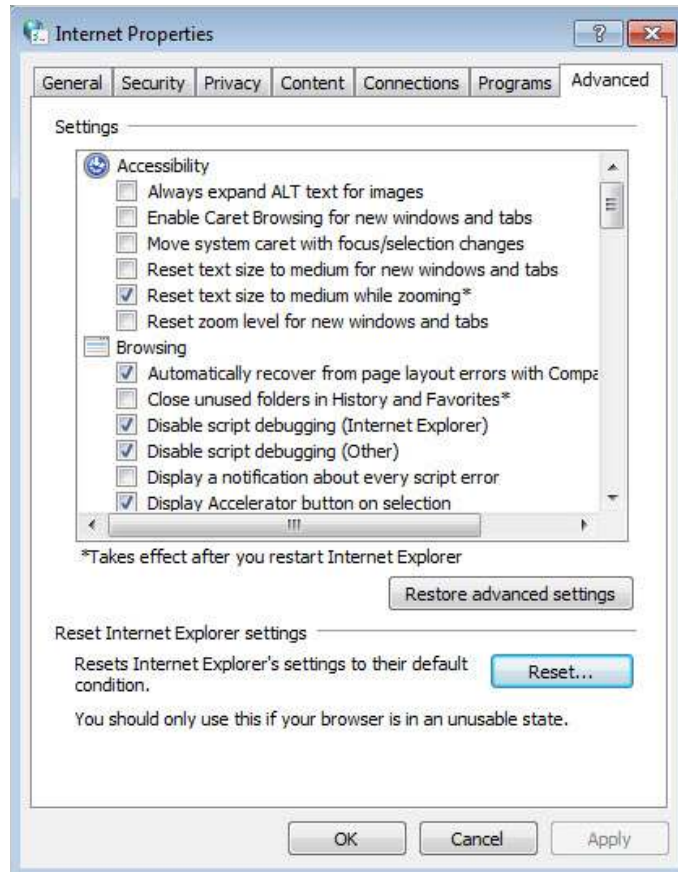
- Make sure your computer is connected to the mesh device correctly and the corresponding LED indicator(s) light up.
- Make sure the IP address of your computer is configured as [Obtain an IP address automatically](#) and [Obtain DNS server address automatically](#).
- Make sure <http://tplinkwifi.net> or <http://192.168.88.1> is correctly entered.
- Check your computer's settings:
 - 1) Go to [Start](#) > [Control Panel](#) > [Network and Internet](#), and click [View network status and tasks](#).
 - 2) Click [Internet Options](#) on the bottom left.
 - 3) Click [Connections](#) and select [Never dial a connection](#).



4) Click [LAN settings](#) and deselect the following three options and click [OK](#).



5) Go to [Advanced](#) > [Restore advanced settings](#), click [OK](#) to save the settings.



- Use another web browser or computer to log in again.
- Reset the mesh device to factory default settings and try again. If login still fails, please contact the technical support.

Note: You'll need to reconfigure the mesh device to surf the internet once the mesh device is reset.

Q4.What should I do if I can't access the internet even though the configuration is finished?

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
2. Go to **Advanced > Network > Status** to check internet status:

If IP Address is a valid one, please try the methods below and try again:

- Your computer might not recognize any DNS server addresses. Please manually configure the DNS server.
 - 1) Go to **Advanced > Network > LAN Settings > DHCP Server**.
 - 2) Enter 8.8.8.8 as Primary DNS, click **SAVE**.

Tips: 8.8.8.8 is a safe and public DNS server operated by Google.

☒ DHCP Server ☐ DHCP Relay

IP Address Pool:	192 . 168 . 88 . 2 - 192 . 168 . 88 . 249
Address Lease Time:	120 minutes. (1-2880. The default value is 1440.)
Default Gateway:	192 . 168 . 88 . 1 (Optional)
Default Domain:	(Optional)
Primary DNS:	8 . 8 . 8 . 8 (Optional)
Secondary DNS:	0 . 0 . 0 . 0 (Optional)

Save

- Restart the modem and the mesh device.
 - 1) Power off your modem and mesh device, and leave them off for 1 minute.
 - 2) Power on your modem first, and wait about 2 minutes until it gets a solid cable or Internet light.
 - 3) Power on the mesh device.
 - 4) Wait another 1 or 2 minutes and check the internet access.
- Reset the mesh device to factory default settings and reconfigure the mesh device.
- Upgrade the firmware of the mesh device.
- Check the TCP/IP settings on the particular device if all other devices can get internet from the mesh device.

As the picture below shows, if the IP Address is 0.0.0.0, please try the methods below and try again:

Status

Internet status overview is displayed on this page.

Internet

Status: WAN port is unplugged

Internet Connection Type: Dynamic IP

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

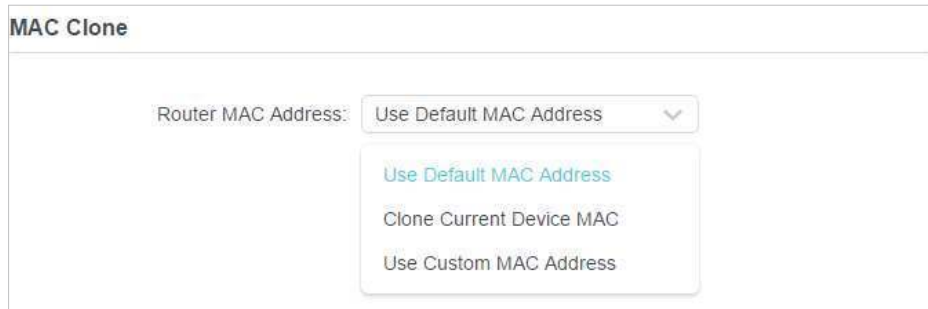
Default Gateway: 0.0.0.0

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0

- Make sure the physical connection between the mesh device and the modem is proper.
- Clone the MAC address of your computer.

- 1) Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
- 2) Go to [Internet](#) or [Advanced](#) > [Network](#) > [Internet](#) and focus on the [MAC Clone](#) section.
- 3) Choose an option as needed (enter the MAC address if [Use Custom MAC Address](#) is selected), and click [SAVE](#).



 Tips:

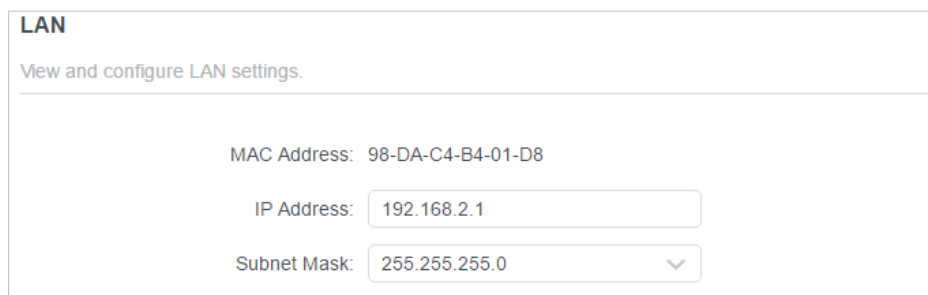
- Some ISP will register the MAC address of your computer when you access the internet for the first time through their Cable modem, if you add a mesh device into your network to share your internet connection, the ISP will not accept it as the MAC address is changed, so we need to clone your computer's MAC address to the mesh device.
- The MAC addresses of a computer in wired connection and wireless connection are different.

- **Modify the LAN IP address of the mesh device.**

 Note:

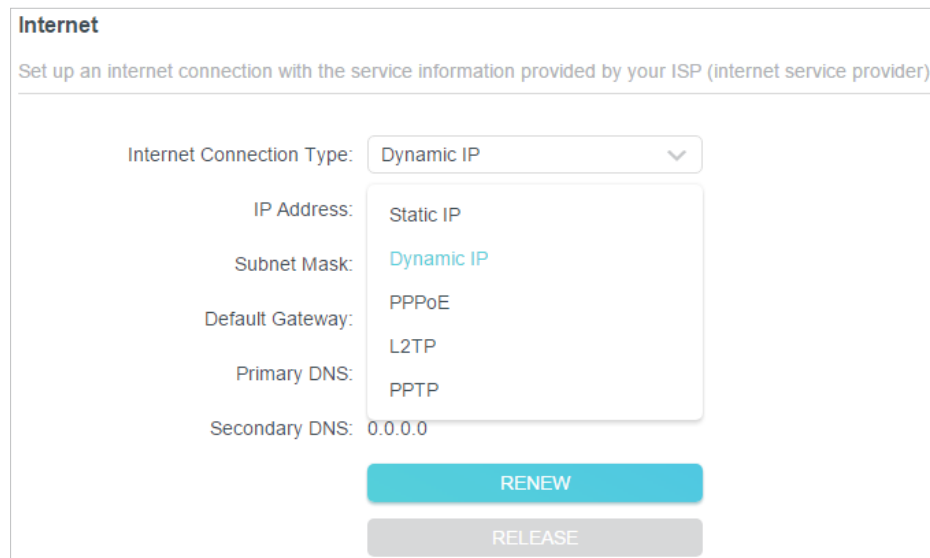
Most TP-Link mesh devices use 192.168.88.1 as their default LAN IP address, which may conflict with the IP range of your existing ADSL modem/router. If so, the mesh device is not able to communicate with your modem and you can't access the internet. To resolve this problem, we need to change the LAN IP address of the mesh device to avoid such conflict, for example, 192.168.2.1.

- 1) Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
- 2) Go to [Advanced](#) > [Network](#) > [LAN](#).
- 3) Modify the LAN IP address as the follow picture shows. Here we take 192.168.2.1 as an example.
- 4) Click [Save](#).



- Restart the modem and the mesh device.

- 1) Power off your modem and mesh device, and leave them off for 1 minute.
 - 2) Power on your modem first, and wait about 2 minutes until it get a solid cable or Internet light.
 - 3) Power on the mesh device.
 - 4) Wait another 1 or 2 minutes and check the internet access.
- Double check the internet connection type.
 - 1) Confirm your internet connection type, which can be learned from the ISP.
 - 2) Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
 - 3) Go to [Advanced](#) > [Network](#) > [Internet](#).
 - 4) Select your [Internet Connection Type](#) and fill in other parameters.
 - 5) Click [Save](#).



Internet

Set up an internet connection with the service information provided by your ISP (internet service provider).

Internet Connection Type: Dynamic IP

IP Address: Static IP

Subnet Mask: Dynamic IP

Default Gateway: PPPoE

Primary DNS: L2TP

Secondary DNS: PPTP

0.0.0.0

[RENEW](#)

[RELEASE](#)

- 6) Restart the modem and the mesh device again.
- Please upgrade the firmware of the mesh device.
- If you've tried every method above but still cannot access the internet, please contact the technical support.

Q5.What should I do if I can't find my wireless network or I cannot connect the wireless network?

If you fail to find any wireless network, please follow the steps below:

- Make sure the wireless function of your device is enabled if you're using a laptop with built-in wireless adapter. You can refer to the relevant document or contact the laptop manufacturer.

- Make sure the wireless adapter driver is installed successfully and the wireless adapter is enabled.

- **On Windows 7**

- 1) If you see the message [No connections are available](#), it is usually because the wireless function is disabled or blocked somehow.
- 2) Click [Troubleshoot](#) and windows might be able to fix the problem by itself.

- **On Windows XP**

- 1) If you see the message [Windows cannot configure this wireless connection](#), this is usually because windows configuration utility is disabled or you are running another wireless configuration tool to connect the wireless.
- 2) Exit the wireless configuration tool (the TP-Link Utility, for example).
- 3) Select and right click on [My Computer](#) on desktop, select [Manage](#) to open Computer Management window.
- 4) Expand [Services and Applications](#) > [Services](#), find and locate [Wireless Zero Configuration](#) in the Services list on the right side.
- 5) Right click [Wireless Zero Configuration](#), and then select [Properties](#).
- 6) Change [Startup type](#) to [Automatic](#), click on Start button and make sure the Service status is [Started](#). And then click [OK](#).

If you can find other wireless network except your own, please follow the steps below:

- Check the WLAN LED indicator on your mesh device/modem.
- Make sure your computer/device is still in the range of your mesh device/modem. Move it closer if it is currently too far away.
- Go to [Wireless](#) or [Advanced](#) > [Wireless](#) > [Wireless Settings](#), and check the wireless settings. Double check your wireless Network Name and SSID is not hided.

If you can find your wireless network but fail to connect, please follow the steps below:

- **Authenticating problem/password mismatch:**

- 1) Sometimes you will be asked to type in a PIN number when you connect to the wireless network for the first time. This PIN number is different from the Wireless Password/Network Security Key, usually you can only find it on the label of your mesh device.



2) If you cannot find the PIN or PIN failed, you may choose [Connecting using a security key instead](#), and then type in the [Wireless Password/Network Security Key](#).

3) If it continues to show note of [Network Security Key Mismatch](#), it is suggested to confirm the wireless password of your mesh device.

■ **Note:** Wireless Password/Network Security Key is case sensitive.

- **Windows unable to connect to XXXX / Can not join this network / Taking longer than usual to connect to this network:**
 - Check the wireless signal strength of your network. If it is weak (1~3 bars), please move the mesh device closer and try again.
 - Change the wireless Channel of the mesh device to 1, 6 or 11 to reduce interference from other networks.
 - Re-install or update the driver for your wireless adapter of the computer.

FCC compliance information statement



Product Name: BBA Mesh

Model Number: BBA Mesh

Component Name	Model
I.T.E. Power	T120200-2B1

Responsible party:

TP-Link USA Corporation

Address: 10 Mauchly, Irvine, CA 92618

Website: <http://www.tp-link.com/us/>

Tel: +1 626 333 0234

Fax: +1 909 527 6804

E-mail: sales.usa@tp-link.com

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 23 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

We, **TP-Link USA Corporation**, has determined that the equipment shown as above has been shown to comply with the applicable technical standards, FCC part 15. There is no unauthorized change is made in the equipment and the equipment is properly maintained and operated.

Issue Date: 2022.09.06

FCC compliance information statement

Product Name: I.T.E. Power Supply

Model Number: T120200-2B1

Responsible party:

TP-Link USA Corporation

Address: 10 Mauchly, Irvine, CA 92618

Website: <http://www.tp-link.com/us/>

Tel: +1 626 333 0234

Fax: +1 909 527 6804

E-mail: sales.usa@tp-link.com

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

We, **TP-Link USA Corporation**, has determined that the equipment shown as above has been shown to comply with the applicable technical standards, FCC part 15. There is no unauthorized change is made in the equipment and the equipment is properly maintained and operated.

Issue Date: 2022.09.06

Canadian Compliance Statement

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. l'appareil ne doit pas produire de brouillage;
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement

Caution:

The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

DFS (Dynamic Frequency Selection) products that operate in the bands 5250-5350 MHz, 5470-5600MHz, and 5650-5725MHz.

Avertissement:

Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

Les produits utilisant la technique d'atténuation DFS (sélection dynamique des fréquences) sur les bandes 5250- 5350 MHz, 5470-5600MHz et 5650-5725MHz.

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Industry Canada Statement

CAN ICES-3 (B)/NMB-3(B)

NCC Notice & BSMI Notice:

注意！

取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前述合法通信，指依電信管理法規定作業之無線電通信。

低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

應避免影響附近雷達系統之操作。

高增益指向性天線只得應用於固定式點對點系統。

安全諮詢及注意事項

- 安全諮詢及注意事項
- 請使用原裝電源供應器或只能按照本產品注明的電源類型使用本產品。
- 清潔本產品之前請先拔掉電源線。請勿使用液體、噴霧清潔劑或濕布進行清潔。
- 注意防潮，請勿將水或其他液體潑灑到本產品上。
- 插槽與開口供通風使用，以確保本產品的操作可靠並防止過熱，請勿堵塞或覆蓋開口。
- 請勿將本產品置放於靠近熱源的地方。除非有正常的通風，否則不可放在密閉位置中。
- 不要私自拆開機殼或自行維修，如產品有故障請與原廠或代理商聯繫。

限用物質含有情況標示聲明書

設備名稱：Whole Home Mesh Wi-Fi AP Equipment name				型號（型式）：HX510/HX220/... Type designation (Type)		
單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛 Lead (Pb)	汞 Mercury (Hg)	鎘 Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr ⁺⁶)	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
PCB	○	○	○	○	○	○
外殼	○	○	○	○	○	○
電源供應器	—	○	○	○	○	○

天線	○	○	○	○	○	○
備考1. “超出0.1 wt %” 及 “超出0.01 wt %” 係指限用物質之百分比含量超出百分比含量基準值 Note 1: “Exceeding 0.1 wt %” and “exceeding 0.01 wt %” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition. 備考2. “○” 係指該項限用物質之百分比含量未超出百分比含量基準值。 Note 2: “○” indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence. 備考3. “—” 係指該項限用物質為排除項目。 Note 3: The “—” indicates that the restricted substance corresponds to the exemption.						

Safety Information

- Keep the device away from water, fire, humidity or hot environments.
- Do not attempt to disassemble, repair, or modify the device. If you need service, please contact us.
- Do not use damaged charger or USB cable to charge the device.
- Do not use any other chargers than those recommended
- Do not use the device where wireless devices are not allowed.
- Adapter shall be installed near the equipment and shall be easily accessible.
- Use only power supplies which are provided by manufacturer and in the original packing of this product. If you have any questions, please don't hesitate to contact us.
- This product uses radios and other components that emit electromagnetic fields. Electromagnetic fields and magnets may interfere with pacemakers and other implanted medical devices. Always keep the product and its power adapter more than 15 cm (6 inches) away from any pacemakers or other implanted medical devices. If you suspect your product is interfering with your pacemaker or any other implanted medical device, turn off your product and consult your physician for information specific to your medical device.
- Operating Temperature: 0℃~40℃

Please read and follow the above safety information when operating the device. We cannot guarantee that no accidents or damage will occur due to improper use of the device. Please use this product with care and operate at your own risk.

Explanations of the symbols on the product label

Symbol	Explanation
	DC voltage
	AC voltage
	Class II equipment

Symbol	Explanation
	Polarity of output terminals
	Energy efficiency Marking
	Indoor use only
	Caution
	Operator's manual
	RECYCLING This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/ EU in order to be recycled or dismantled to minimize its impact on the environment. User has the choice to give his product to a competent recycling organization or to the retailer when he buys a new electrical or electronic equipment.