



User Guide

BE19000 Tri-Band Wi-Fi 7 Gaming Router
Archer GE800

Contents

About This Guide	1
Chapter 1. Get to Know About Your Router	3
1. 1. Product Overview.....	4
1. 2. Appearance	4
1. 2. 1.Front Panel.....	4
1. 2. 2.Back Panel and Side Panel.....	5
Chapter 2. Connect the Hardware	7
2. 1. Position Your Router	8
2. 2. Connect Your Router.....	8
Chapter 3. Log In to Your Router.....	10
Chapter 4. Set Up Internet Connection	12
4. 1. Use Quick Setup Wizard	13
4. 2. Quick Setup Via TP-Link Tether App.....	13
4. 3. Manually Set Up Your Internet Connection	14
4. 4. Set Up the Router as an Access Point	17
4. 5. Set Up an IPv6 Internet Connection	17
4. 5. 1.Set up IPv6 Firewall Rules	20
Chapter 5. TP-Link Cloud Service	22
5. 1. Register a TP-Link ID.....	23
5. 2. Change Your TP-Link ID Information.....	23
5. 3. Manage the User TP-Link IDs	25
5. 3. 1.Add TP-Link ID to Manage the Router.....	25
5. 3. 2.Remove TP-Link ID(s) from Managing the Router.....	26
5. 4. Manage the Router via the TP-Link Tether App	26
Chapter 6. Network Map	28
Chapter 7. Wireless Settings	32
7. 1. Specify Wireless Settings	33
7. 2. Schedule Your Wireless Function	35

7.3.	Use WPS for Wireless Connection	36
7.3.1.	Connect via the Client's PIN	36
7.3.2.	Connect via the Router's PIN	37
7.3.3.	Push the WPS Button.....	37
7.4.	Advanced Wireless Settings	38
Chapter 8. Guest Network.....		40
8.1.	Create a Network for Guests	41
8.2.	Customize Guest Network Options.....	42
Chapter 9. IoT Network		43
Chapter 10.USB Settings.....		45
10.1.	Access the USB Storage Device	46
10.1.1.	Access the USB Device Locally	46
10.1.2.	Access the USB Device Remotely	47
10.1.3.	Customize the Access Settings	49
10.2.	Media Sharing	51
10.3.	Time Machine	52
Chapter 11.HomeShield		54
11.1.	Network Check	55
11.2.	Parental Controls	56
11.3.	QoS	58
11.4.	More Features	59
Chapter 12.EasyMesh with Seamless Roaming.....		61
12.1.	Add a Router as a Satellite Device.....	62
12.2.	Add a Range Extender as a Satellite Device	64
12.3.	Manage Devices in the EasyMesh Network.....	65
Chapter 13.Network Security		67
13.1.	Protect the Network from Cyber Attacks	68
13.2.	Access Control	68
13.3.	IP & MAC Binding	71
13.4.	ALG	72
13.5.	Device Isolation.....	73
Chapter 14.NAT Forwarding.....		74

14. 1.	Share Local Resources on the Internet by Port Forwarding	75
14. 2.	Open Ports Dynamically by Port Triggering	77
14. 3.	Make Applications Free from Port Restriction by DMZ	78
14. 4.	Make Xbox Online Games Run Smoothly by UPnP	79

Chapter 15.VPN Server&Client..... 81

15. 1.	Use OpenVPN to Access Your Home Network.....	82
15. 2.	Use PPTP VPN to Access Your Home Network	83
15. 3.	Use L2TP/IPSec VPN to Access Your Home Network	88
15. 4.	Use WireGuard VPN to Access Your Home Network	95
15. 5.	Use VPN Client to Access a Remote VPN Server	97

Chapter 16.Customize Your Network Settings..... 102

16. 1.	Change the Internet Settings	103
16. 2.	Change the LAN Settings	105
16. 3.	Set Up Link Aggregation	106
16. 4.	Flow Controller	106
16. 5.	Configure to Support IPTV Service.....	107
16. 6.	Specify DHCP Server Settings	108
16. 7.	Set Up a Dynamic DNS Service Account	110
16. 8.	Create Static Routes.....	112

Chapter 17.Manage the Router 115

17. 1.	Update the Firmware.....	116
17. 1. 1.	Auto Update	116
17. 1. 2.	Online Update	116
17. 1. 3.	Local Update	117
17. 1. 4.	EasyMesh Satellite Update.....	117
17. 2.	Backup and Restore Configuration Settings.....	118
17. 3.	Change the Login Password	119
17. 4.	Password Recovery.....	120
17. 5.	Local Management	121
17. 6.	Remote Management.....	122
17. 7.	System Log.....	124
17. 8.	Test the Network Connectivity	126
17. 9.	Set System Time and Language	128
17. 10.	Set the Router to Reboot Regularly.....	130
17. 11.	Control the LED.....	131

Chapter 18.Game Center 133

18. 1. Check Key Parameters on Game Panel	134
18. 2. Game Acceleration	136
18. 2. 1. QoS.....	137
18. 2. 2.Game Server Acceleration	137
18. 2. 3.Gear Acceleration.....	140
18. 3. Game Port Forwarding.....	141
18. 4. Game Statictics.....	142
18. 5. Game Detector	143
18. 6. Game Diagnostics	144
FAQ.....	146






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.

Features available in the router may vary by model and software version. Router 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 Router 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 > System > Firmware Update means the Firmware Update page is under the System 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	<ul style="list-style-type: none"> Click to edit the corresponding entry. Click to delete 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 router.

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 7 (802.11be), Wi-Fi 6 (802.11ax), and features including Multi-Link Operation (MLO), 320 MHz Bandwidth, 4K-QAM, Multi-RUs, OFDMA, and MU-MIMO requires clients to also support the corresponding features.

* HomeShield includes the Free Basic Plan. Fees apply for more advanced features. Visit tp-link.com/homeshield for more information.

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

* This router may not support all the mandatory features as ratified in the IEEE 802.11be specification.

* Further software upgrades for feature availability may be required.

* Actual network speed may be limited by the rate of the product's Ethernet WAN or LAN port, the rate supported by the network cable, Internet service provider factors and other environmental conditions.

Chapter 1

Get to Know About Your Router

This chapter introduces what the router can do and shows its appearance.

It chapter contains the following sections:

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

1.1. Product Overview

TP-Link Wi-Fi 7 router, with the 802.11be Wi-Fi technology and the brand-new 6 GHz band, achieves Wi-Fi performance at its ultimate level. The new features of Wi-Fi 7 and 4k QAM dramatically improve throughput and increase capacity and efficiency of the whole network. Access to the 6 GHz band brings more bandwidth, faster speeds, and lower latency, opening up resources for future innovations.

Moreover, it is simple and convenient to set up and use the TP-Link router due to its intuitive Tether app and powerful web interface.





1.2. Appearance

1.2.1. Front Panel



The physical buttons are located on the front of the router.

Button Description

Button		Indication
	WPS Button	Press this button, and immediately press the WPS button on your client device to start the WPS process.
	Wi-Fi Button	Press and hold this button for about 2 seconds to turn on or off the wireless function of your router.
	Acceleration Button	Press this button to turn on Game Mode. Press and hold this button for about 2 seconds to turn off the Game Mode.
	LED Button	Press this button to turn the router's LED on or off. Press and hold this button for about 2 seconds to switch RGB effects.

1. 2. 2. Back Panel and Side Panel



The following parts are located on the back panel.

Item	Description
Power On/Off Button	Press this button to power on or off the router.
POWER Port	For connecting the router to a power socket via the provided power adapter.
USB 3.0 Port	For connecting your USB storage devices to the router.
Gaming Port	For connecting your game device to prioritizes the game device traffic.
10Gbps WAN/LAN Combo Port	The combo port pairs a RJ45 port with an SFP+ port. Only one port in the pair can be used at a time. RJ45 port: For connecting to your modem, the Ethernet outlet or other internet devices. Used as the WAN or LAN port. SFP+ port: For connecting to your PON Stick.
10Gbps WAN/LAN Port	For connecting to your modem, the Ethernet outlet or other internet devices. Used as the WAN or LAN port.
2.5Gbps LAN Port (1-3)	For connecting your PC or other wired devices to the router.
Reset Button	Press and hold the Reset button until the LED blinks blue to restore factory default settings.

Note:

10Gbps WAN/LAN Combo port and 10Gbps WAN/LAN port cannot be used as the WAN port at the same time. If you choose one of the ports as the WAN port for internet service, the other ports will be used as LAN port by default. It's recommended to use the RJ45 port in the 10Gbps WAN/LAN Combo pair as the WAN port.

LED Description

Check the router's working status by following the LEDs.

LED Status	Description
Alternating Red & Blue	The router is starting up.

LED Status	Description
Selected RGB Effect (Default: Fire effect)	The router is working properly.
Blinking Red	No internet connection.
Blinking Orange	The Wi-Fi is off.
Blinking Yellow	The Wi-Fi is off and there is no internet connection.
Blinking Blue	The router is upgrading firmware, establishing WPS connection, or resetting to factory default settings.

Chapter 2

Connect the Hardware

This chapter contains the following sections:

- [Position Your Router](#)
- [Connect Your Router](#)

2.1. Position Your Router

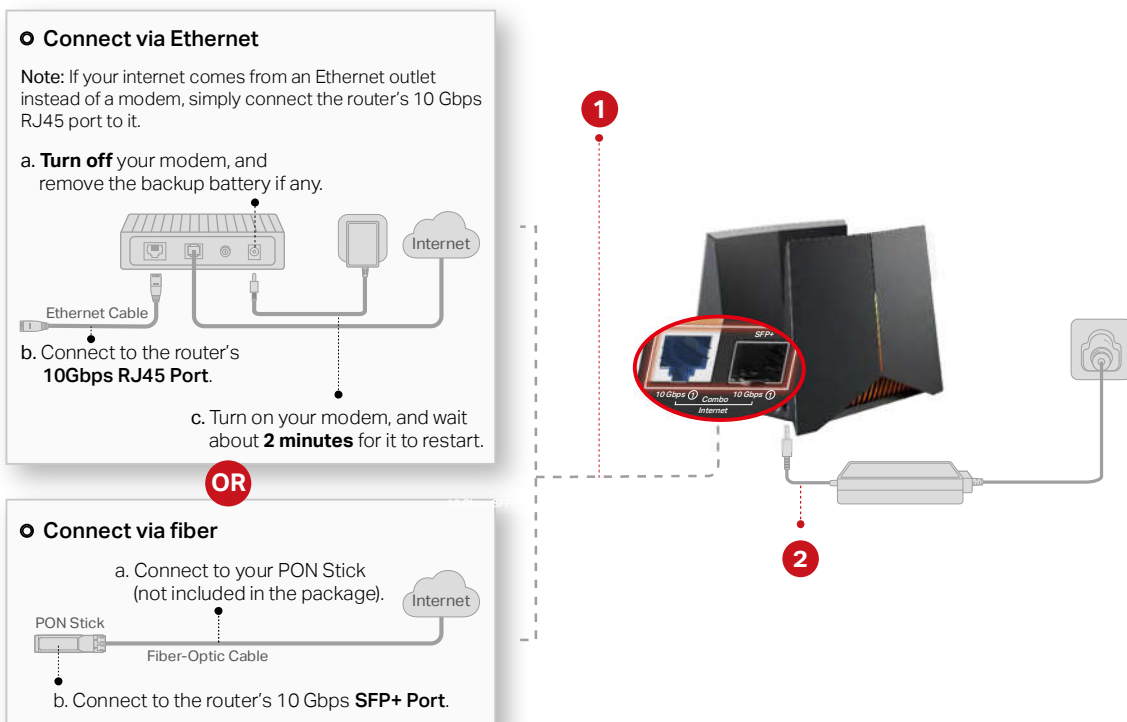
- The product should not be located in a place where it will be exposed to moisture or excessive heat.
- Place the router in a location where it can be connected to multiple devices as well as to a power source.
- Make sure the cables and power cord are safely placed out of the way so they do not create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

2.2. Connect Your Router

1. Connect the router's **10Gbps Combo port** to the internet via Ethernet or fiber network.

Note:

Note: If you want to change the WAN port for internet service, go to the Tether app or web management page to configure it.



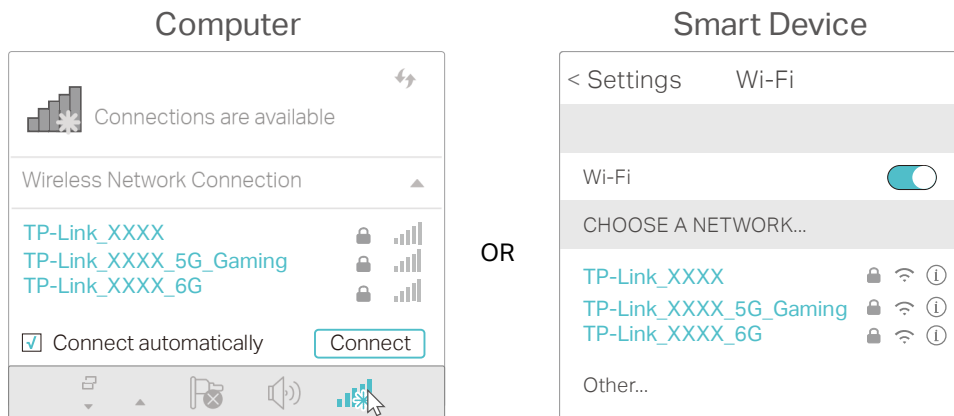
2. Connect the power adapter to the router and press the Power button to turn on the router.
3. Wait until the LED of the router **blinks red** or until the **Fire RGB effect activates** before moving on.
4. Connect your computer to the router.

- **Method 1: Wired**

Turn off the Wi-Fi on your computer and connect the devices to the LAN port of your router.

- **Method 2: Wirelessly**

- 1) Find the SSIDs (Network Names) and Wireless Password printed on the label at the bottom of the router.
- 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

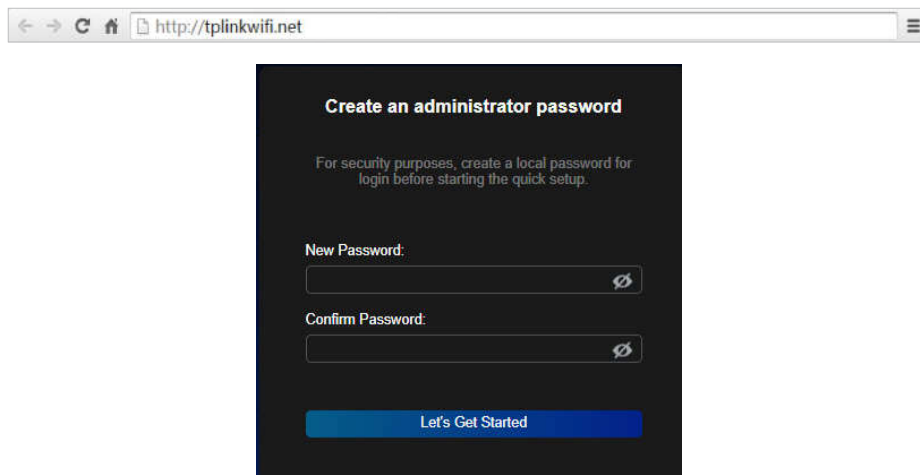
Log In to Your Router

With a web-based utility, it is easy to configure and manage the router. The web-based utility can be used on any Windows, Mac OS or UNIX OS with a Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari.

Follow the steps below to log in to your router.

1. Set up the TCP/IP Protocol in [Obtain an IP address automatically](#) mode on your computer.
2. Visit <http://tplinkwifi.net>, and create a login password for secure management purposes. Then click [Let's Get Started](#) to log in.

Note: 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 router to the internet. The router 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 Tether App](#)
- [Manually Set Up Your Internet Connection](#)
- [Set Up the Router as an Access Point](#)
- [Set Up an IPv6 Internet Connection](#)

4.1. Use Quick Setup Wizard

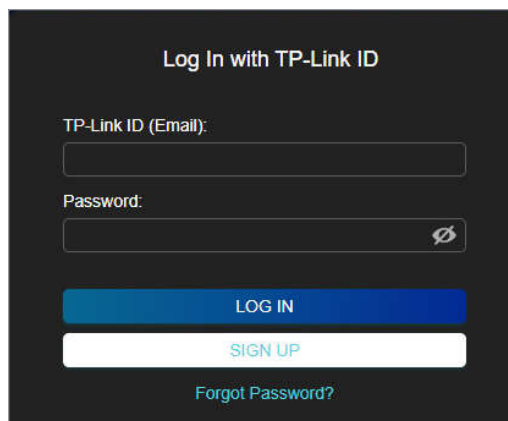
The Quick Setup Wizard will guide you to set up your router.

🔗 **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 router.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Follow the step-by-step instructions to complete Quick Setup configuration or go to **Advanced > Quick Setup** for configuration to connect your router to the internet. Then follow the step-by-step instructions to connect your router 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. Then follow the instructions to bind the cloud router to your TP-Link ID.



📌 **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 router.

4.2. Quick Setup Via TP-Link Tether App

The Tether 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 Tether” or simply scan the QR code to download and install the app.



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

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

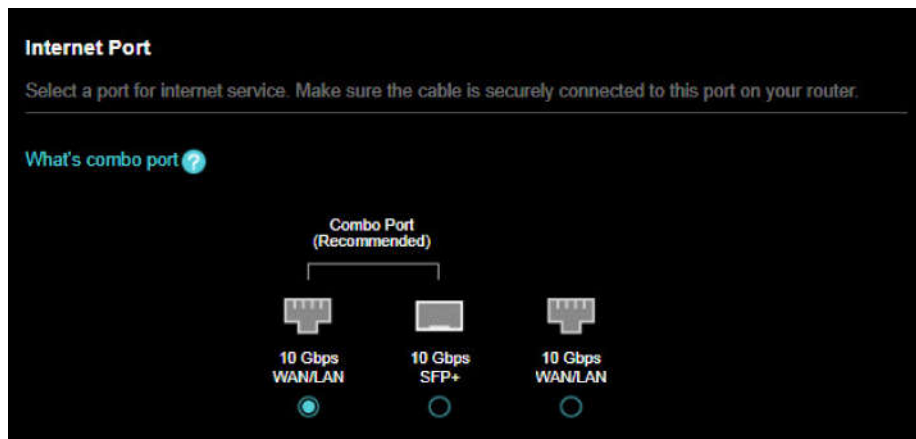
3. Tap the **+** button and select **Gaming Router > Archer GE800**. Then follow the steps to complete the setup and connect to the internet.
4. Connect your devices to the router's wireless network and enjoy the internet!

4.3. Manually Set Up Your Internet Connection

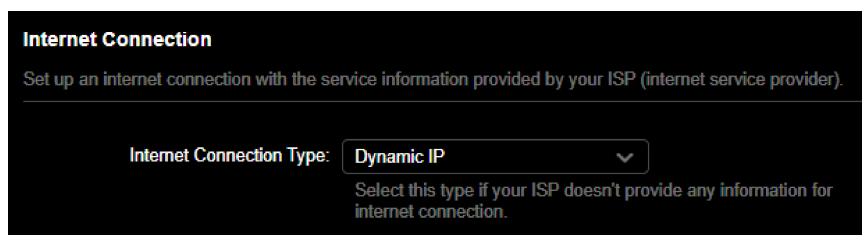
In this part, you can check your current internet connection settings. You can also modify the settings according to the service information provided by your ISP.

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

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Internet**.
3. Select a port for internet service. Make sure the cable is securely connected to this port on your router.



4. Select your internet connection type from the drop-down list.



5. Follow the instructions on the page to continue the configuration. Parameters on the figures are just used for demonstration.
 - 1) If you choose **Dynamic IP**, you need to select whether to clone the MAC address. Dynamic IP users are usually equipped with a cable TV or fiber cable.

Internet Connection

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

Internet Connection Type: ▼
 Select this type if your ISP doesn't provide any information for internet connection.

MAC Clone

Set the MAC address of your router. Use the default address unless your ISP allows internet access from only a specific MAC address.

Router MAC Address: ▼

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

Internet Connection

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

Internet Connection Type: ▼
 Select this type if your ISP provides specific IP parameters.

IP Address:

Subnet Mask:

Default Gateway:

Primary DNS:

Secondary DNS: (Optional)

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

Internet Connection

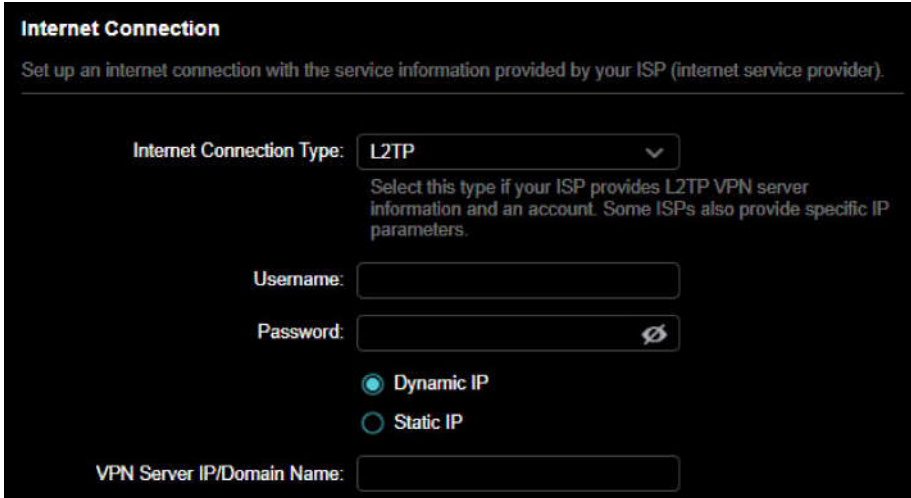
Set up an internet connection with the service information provided by your ISP (internet service provider).

Internet Connection Type: ▼
 Select this type if your ISP only provides a username and password.

Username:

Password:

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

Internet Connection Type: **L2TP** ▼
Select this type if your ISP provides L2TP VPN server information and an account. Some ISPs also provide specific IP parameters.

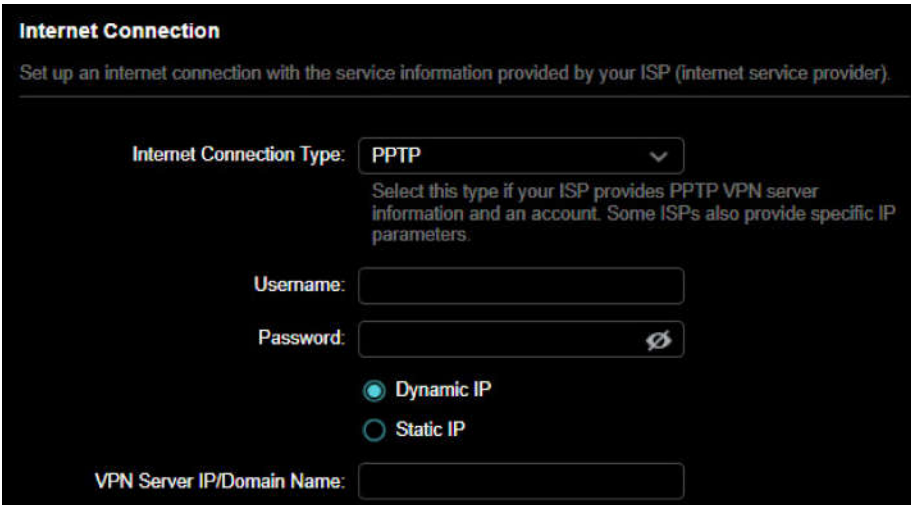
Username:

Password:

Dynamic IP
 Static IP

VPN Server IP/Domain Name:

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

Internet Connection Type: **PPTP** ▼
Select this type if your ISP provides PPTP VPN server information and an account. Some ISPs also provide specific IP parameters.

Username:

Password:

Dynamic IP
 Static IP

VPN Server IP/Domain Name:

6. Click **SAVE**.

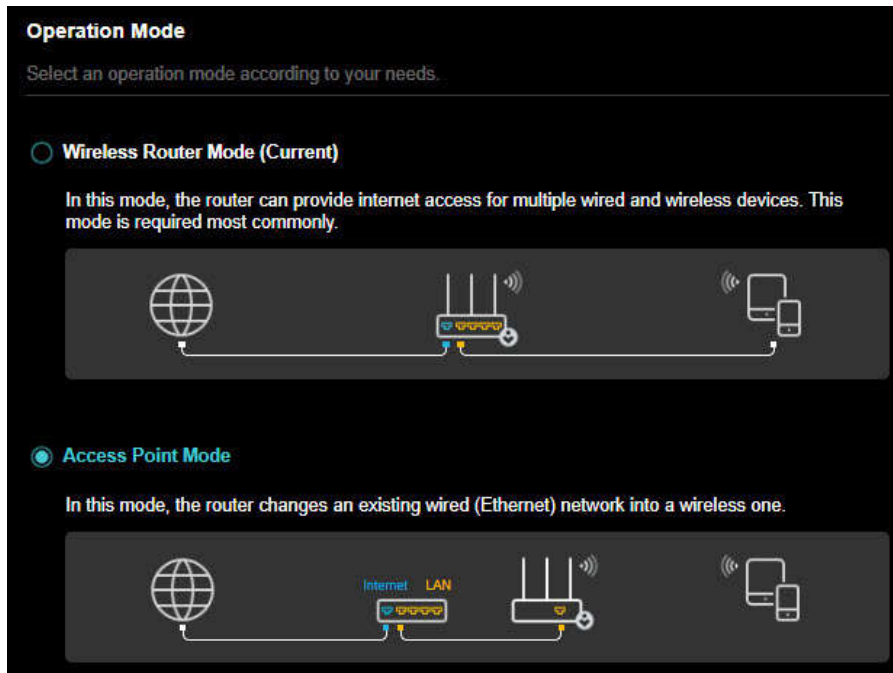
 **Tips:**

- 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 Router as an Access Point

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

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > System > Operation Mode**, select **Access Point Mode** and click **SAVE**. The router will reboot and switch to Access Point mode.



3. After rebooting, connect the router to your existing wired router via an Ethernet cable.
4. Log in again to the web management page <http://tplinkwifi.net>, and go to **Advanced > 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, NAT Forwarding, and game acceleration features 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, Dynamic IP(SLAAC/DHCPv6), Static IP, 6to4 tunnel, Pass-Through (Bridge).

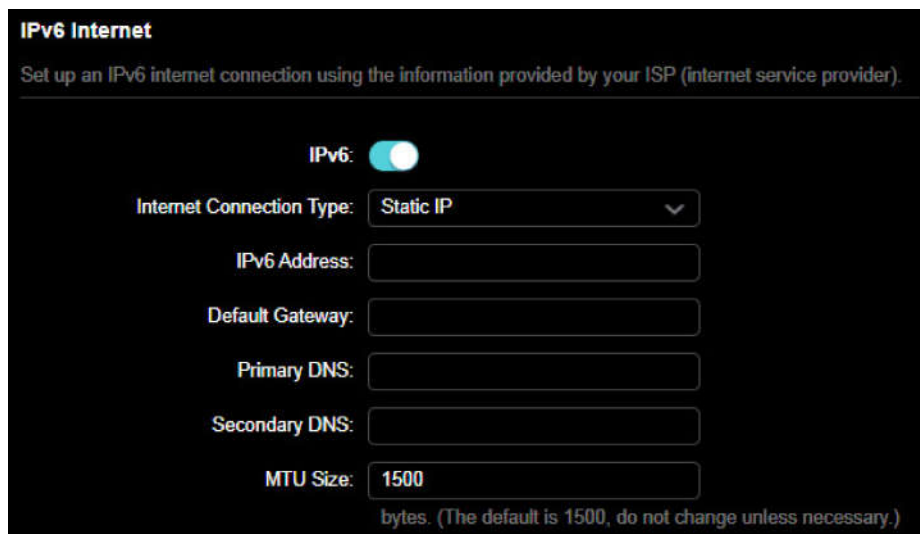
1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced > IPv6](#).
3. Enable IPv6 and select the internet connection type provided by your ISP.

☞ 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 **SAVE**.



IPv6 Internet
Set up an IPv6 internet connection using the information provided by your ISP (internet service provider).

IPv6:

Internet Connection Type:

IPv6 Address:

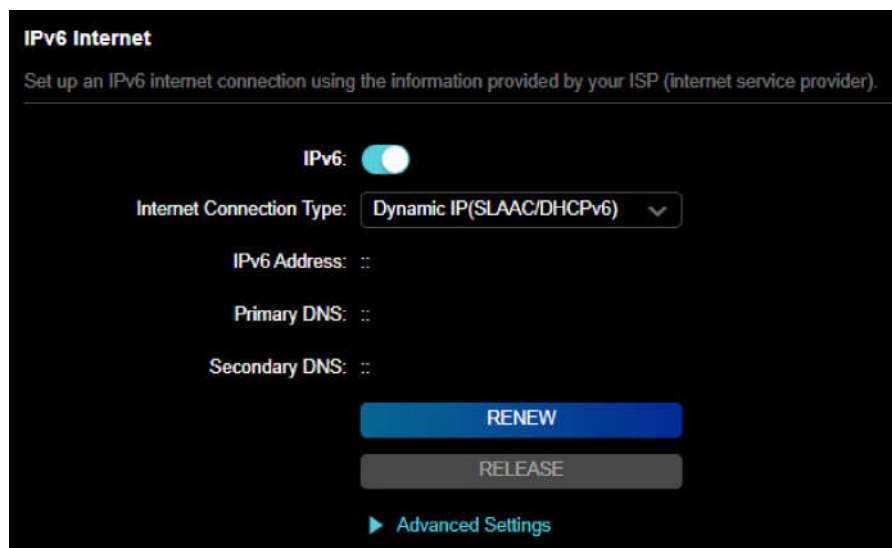
Default Gateway:

Primary DNS:

Secondary DNS:

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

- 2) **Dynamic IP(SLAAC/DHCPv6):** Click **Advanced Settings** to input further information if your ISP requires. Click **SAVE** and then click **Renew**.



IPv6 Internet
Set up an IPv6 internet connection using the information provided by your ISP (internet service provider).

IPv6:

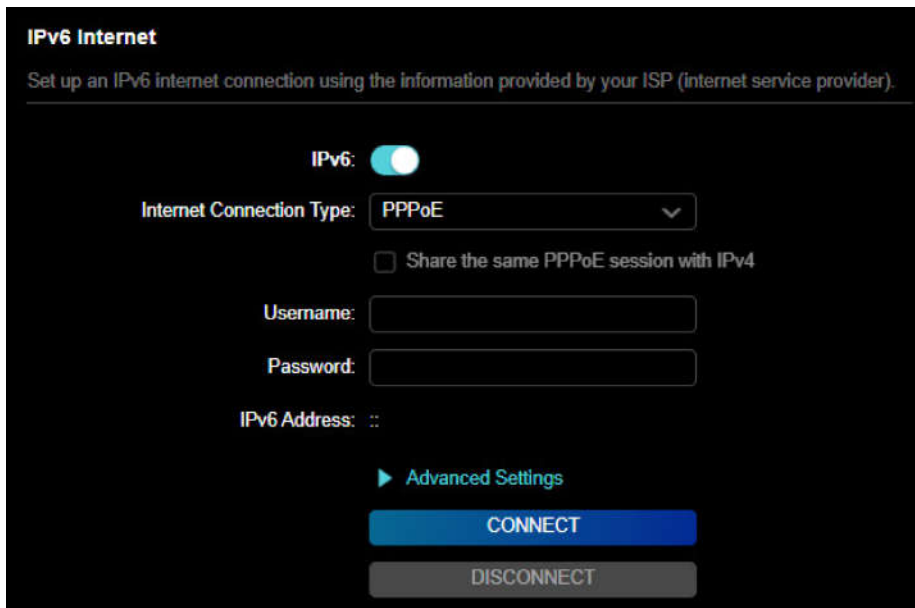
Internet Connection Type:

IPv6 Address:

Primary DNS:

Secondary DNS:

- 3) **PPPoE:** By default, the router uses the IPv4 account to connect to the IPv6 server. Click [Advanced](#) to input further information if your ISP requires. Click [SAVE](#) and then click [Connect](#).



IPv6 Internet
Set up an IPv6 internet connection using the information provided by your ISP (internet service provider).

IPv6:

Internet Connection Type: **PPPoE**

Share the same PPPoE session with IPv4

Username:

Password:

IPv6 Address: ::

[▶ Advanced Settings](#)

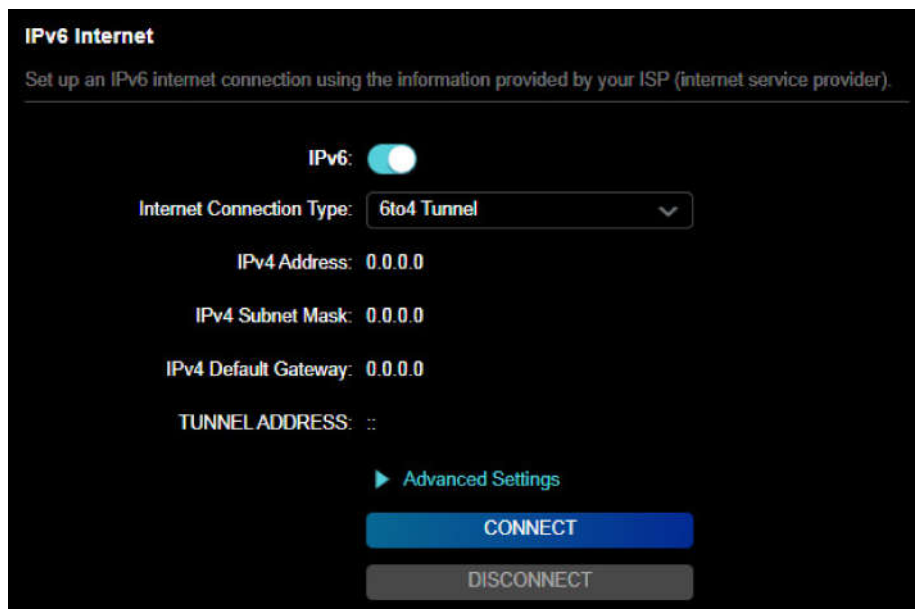
CONNECT

DISCONNECT

Note:

If your ISP provides two separate accounts for the IPv4 and IPv6 connections, manually enter the username and password for the IPv6 connection.

- 4) **6to4 Tunnel:** An IPv4 internet connection type is a prerequisite for this connection type ([Manually Set Up Your Internet Connection](#)). Click [Advanced](#) to input further information if your ISP requires. Click [SAVE](#) and then click [Connect](#).



IPv6 Internet
Set up an IPv6 internet connection using the information provided by your ISP (internet service provider).

IPv6:

Internet Connection Type: **6to4 Tunnel**

IPv4 Address: 0.0.0.0

IPv4 Subnet Mask: 0.0.0.0

IPv4 Default Gateway: 0.0.0.0

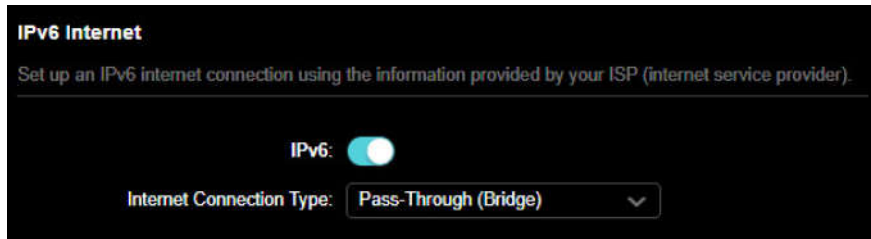
TUNNEL ADDRESS: ::

[▶ Advanced Settings](#)

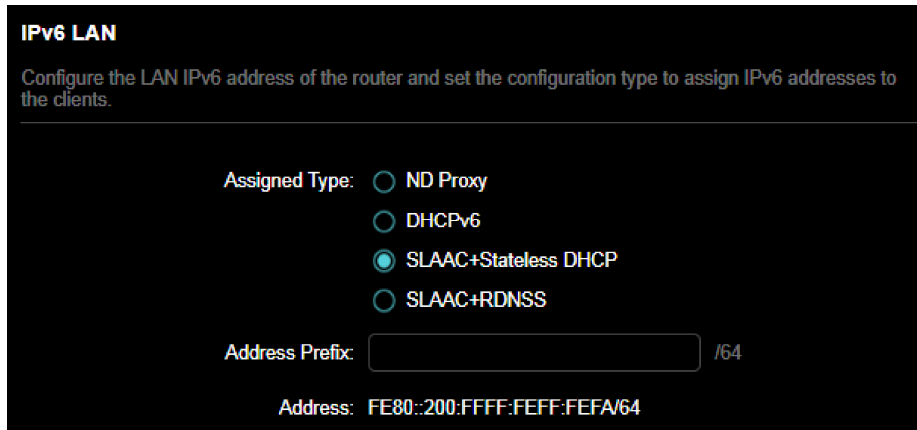
CONNECT

DISCONNECT

- 5) **Pass-Through (Bridge):** Click [SAVE](#) and skip to Step 6.



5. Configure LAN ports. Windows users are recommended to choose from the first two types. Fill in [Address Prefix](#) provided by your ISP, and click [SAVE](#).



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

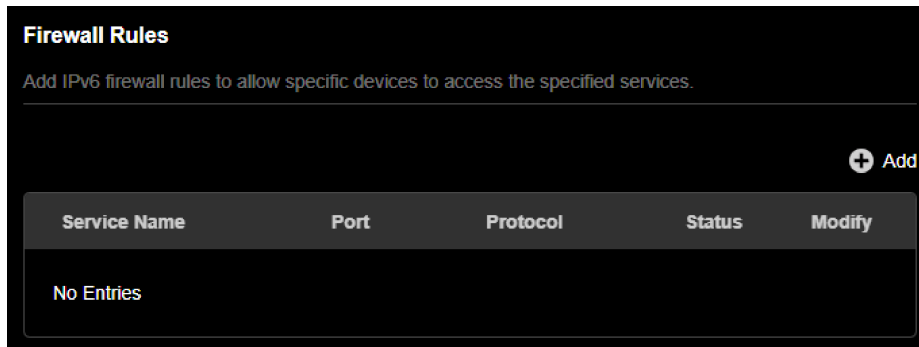
 **Tips:**

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

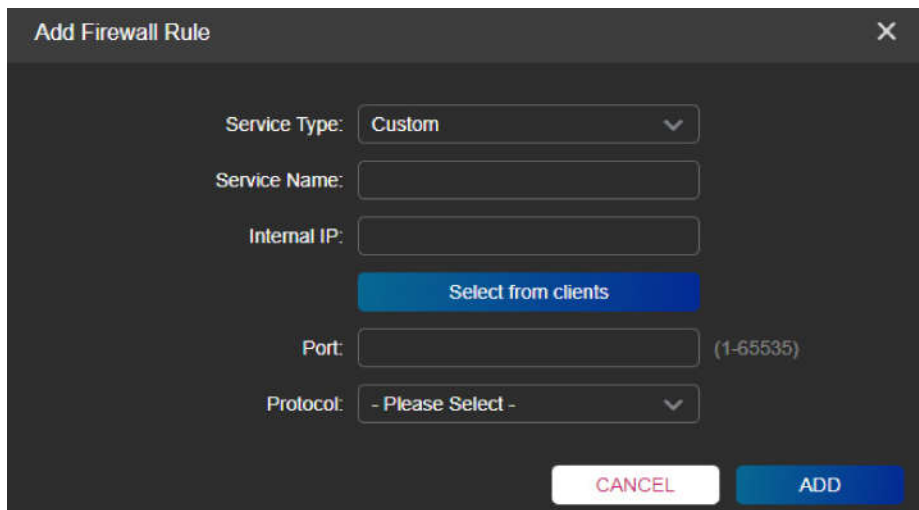
4. 5. 1. Set up IPv6 Firewall Rules

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>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [IPv6](#), and locate the **Firewall Rules** section.
3. Click [Add](#).



4. Select a service from the drop-down list of [Service Type](#). The Port and Protocol will be automatically filled in. It is recommended to keep the default Port and Protocol if you are unsure about which to use. If the service is not listed, please manually enter the Service Type, and specify the [Port](#) and [Protocol](#).



5. Specify a [Service Name](#) for the rule.
6. In the [Internal IP](#) field, enter a valid IPv6 address to run the service. You can click [Select from clients](#), choose a local host device, and its IPv6 address will be automatically filled in as the Internal IP.
7. Click [SAVE](#).

Chapter 5

TP-Link Cloud Service

TP-Link Cloud service provides a better way to manage your cloud devices. Log in to your router with a TP-Link ID, and you can easily monitor and manage your home network when you are out and about via the Tether app. To ensure that your router 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 router, and the Tether app with which you can manage your home network no matter where you may find yourself.

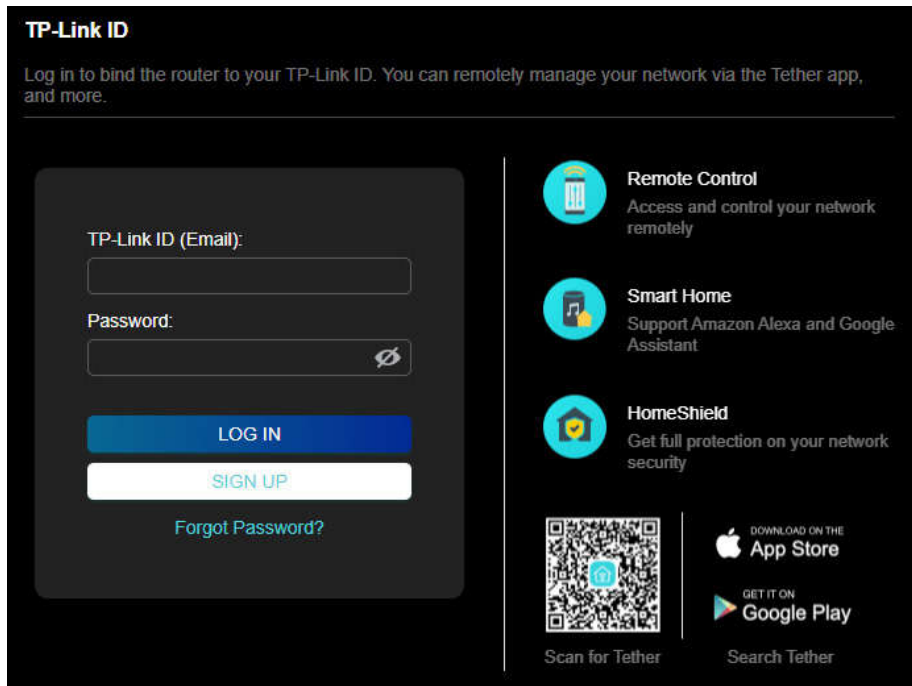
It contains the following sections:

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

5.1. Register a TP-Link ID

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced > TP-Link ID](#).
3. Click [SIGN UP](#) and follow the instructions to register a TP-Link ID.



4. After activating your TP-Link ID, come back to the TP-Link ID page to log in. The TP-Link ID used to log in to the router for the first time will be automatically bound as an **Owner**.

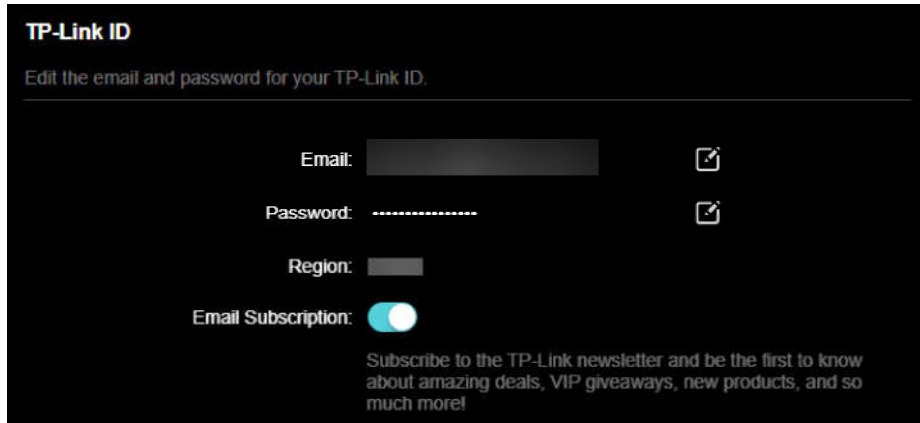
Note:

- To learn more about the **Owner** 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 Tether APP. Please refer to [Manage the Router via the TP-Link Tether App](#) to install the app.
- If you want to unbind the admin TP-Link ID from your router, please go to [Advanced > TP-Link ID](#), and click **Unbind** in the [Device Information](#) section.

5.2. 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>, and log in with your TP-Link ID.
2. Go to [Advanced > TP-Link ID](#), and focus on the [TP-Link ID](#) section.



TP-Link ID

Edit the email and password for your TP-Link ID.

Email: 


Password: 

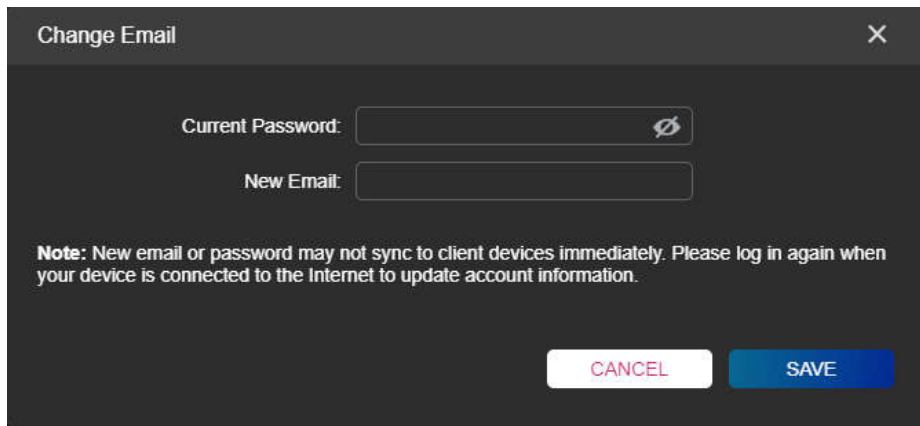
Region:

Email Subscription:


Subscribe to the TP-Link newsletter and be the first to know about amazing deals, VIP giveaways, new products, and so much more!

- **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](#).



Change Email ✕


Current Password: 

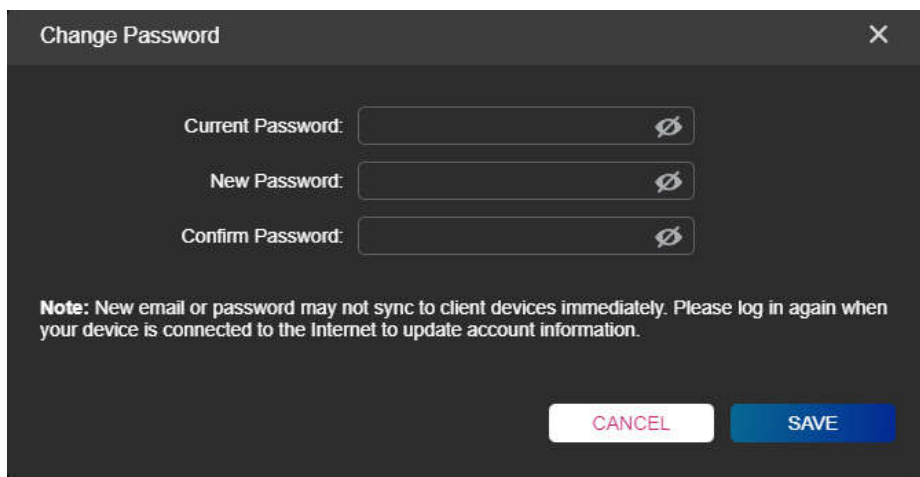
New Email:

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.


[CANCEL](#) [SAVE](#)


- **To change your password:**


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



Change Password ✕

Current Password: 

New Password: 

Confirm Password: 

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.


[CANCEL](#) [SAVE](#)

5.3. Manage the User TP-Link IDs

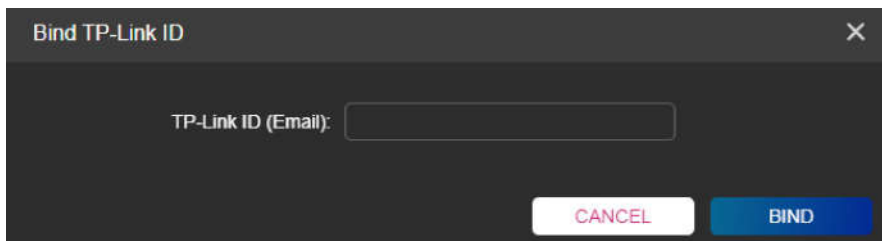
The TP-Link ID used to log in to the router for the first time will be automatically bound as the **Owner** account. An admin account can add or remove other TP-Link IDs to or from the same router as **Users**. All accounts can monitor and manage the router locally or remotely, but user accounts cannot:

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

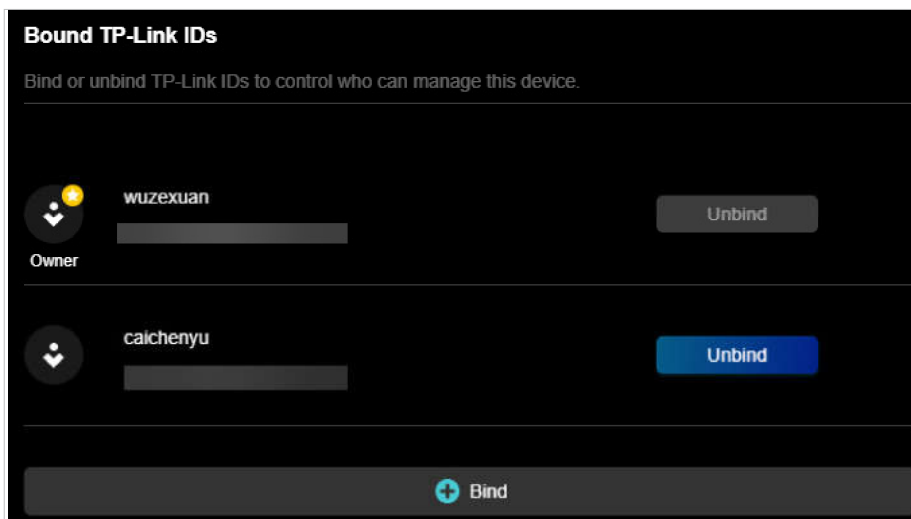
5.3.1. Add TP-Link ID to Manage the Router

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID.
2. Go to **Advanced > TP-Link ID**, and focus on the **Bound TP-Link IDs** section.
3. Click  **Bind**, enter another TP-Link ID as needed and click **BIND**.

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

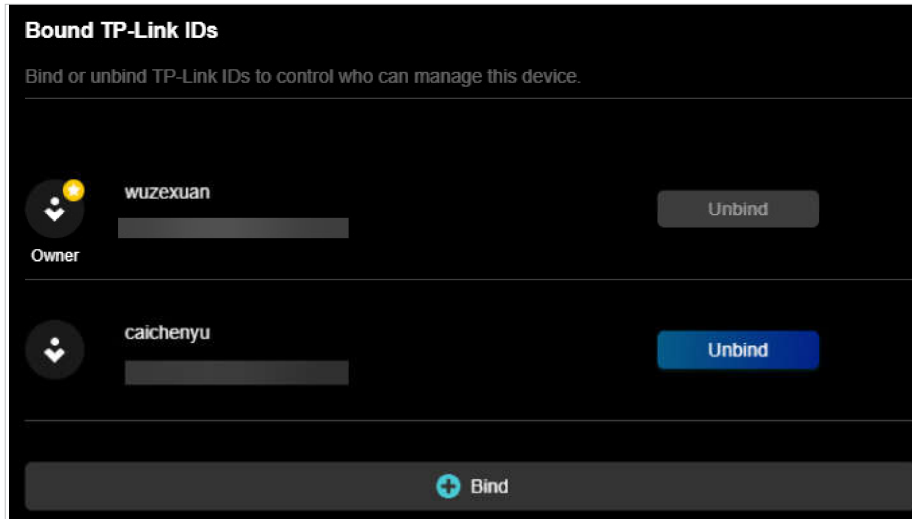


4. The new TP-Link IDs will be displayed. Only the TP-Link ID used to log in to the router for the first time will be automatically bound as the **Owner** account.



5.3.2. Remove TP-Link ID(s) from Managing the Router

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID.
2. Go to **Advanced > TP-Link ID**, and focus on the **Bound TP-Link IDs** section.
3. Select the TP-Link ID(s) you want to remove and click **Unbind**.



4. Confirm by clicking **UNBIND**.



5.4. Manage the Router via the TP-Link Tether App

The Tether 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 Tether" or simply scan the QR code to download and install the app.



2. Launch the Tether 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 router's wireless network.
4. Go back to the Tether app, select the model of your router and log in with the password you set for the router.

5. Manage your router as needed.

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

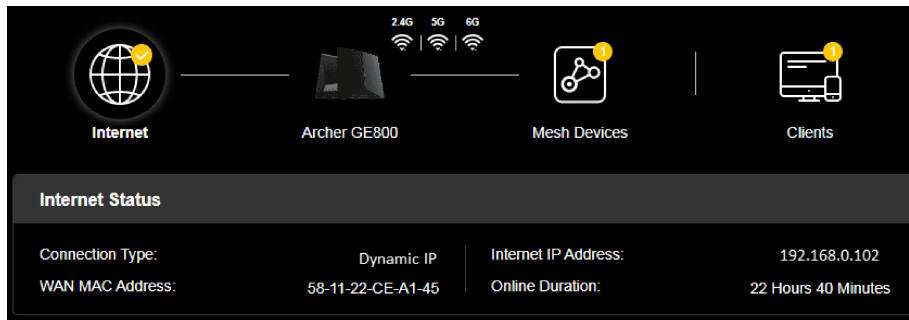
- Log in with your TP-Link ID. If you don't have one, refer to [Register a TP-Link ID](#).
- Make sure your smartphone or tablet can access the internet with cellular data or a Wi-Fi network.

Chapter 6

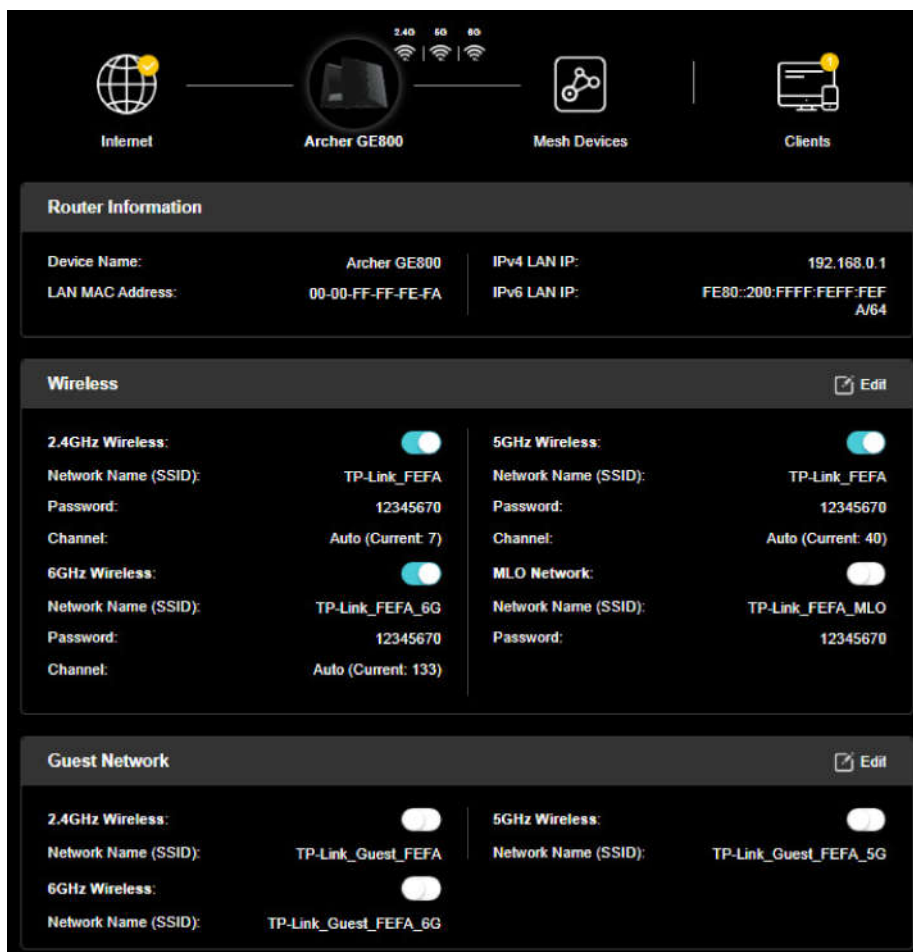
Network Map

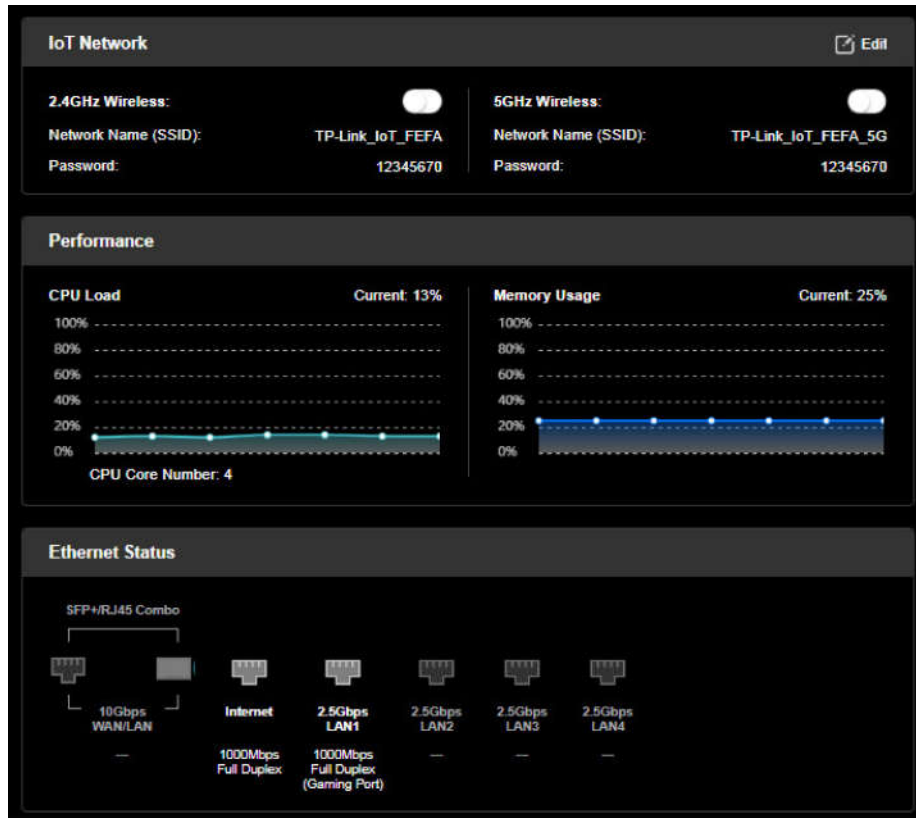
Network Map outlines device connectivity of your network visually and helps you manage general settings of the network.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Network Map](#).
3. Click each network device icon to check and manage general network settings.
 - Click [Internet](#) to check internet status.

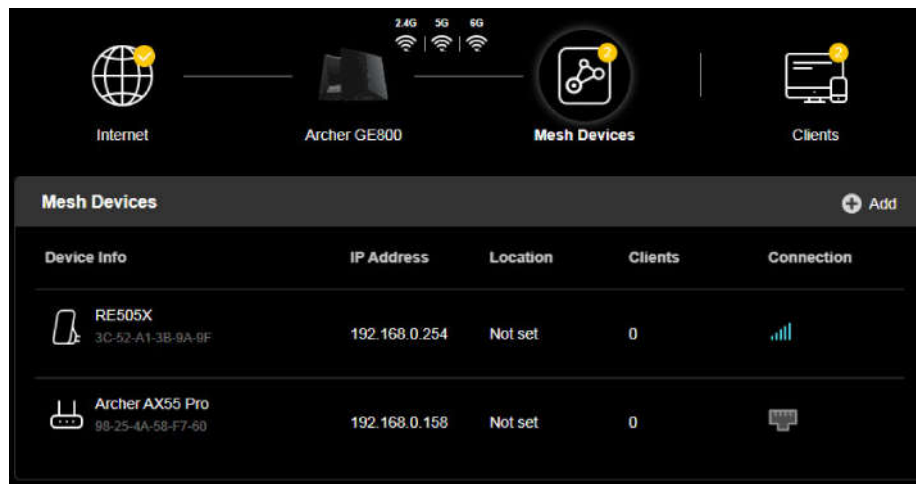


- Click the router to check device status and network settings. You can turn on or off the wireless network or guest network, or click [Edit](#) to change related settings.

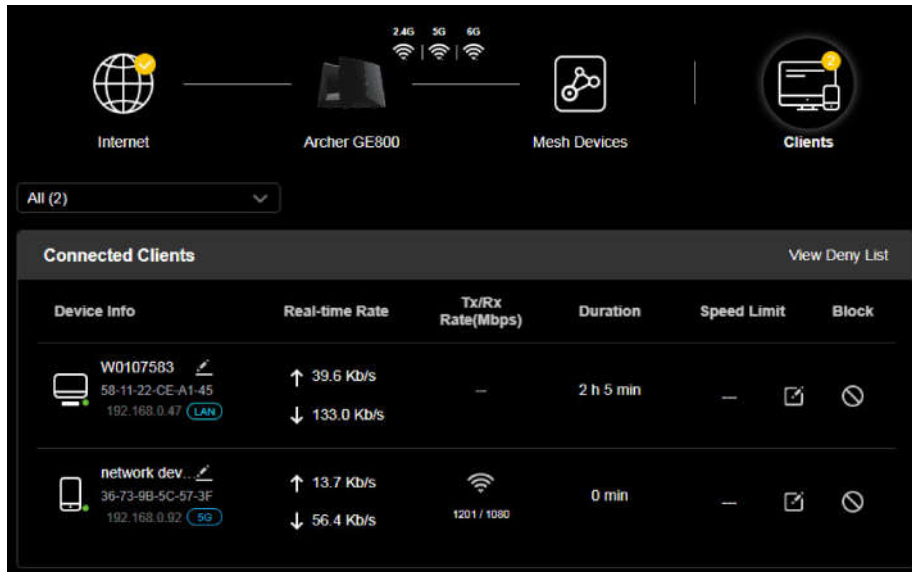





- Click [Mesh Devices](#) to view the devices that form a mesh network with the router.

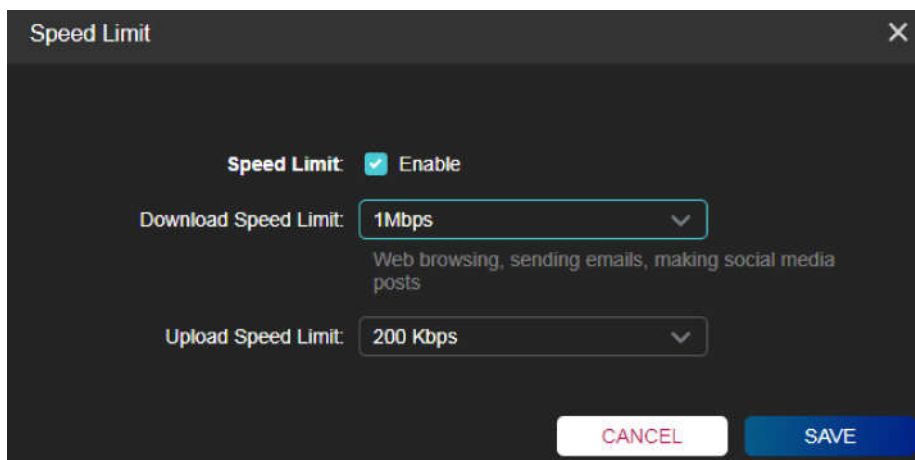


- Click [Clients](#) to view the client devices in your network. You can block devices so they cannot access your network, or set [Speed Limit](#) to limit their upload and download speeds.



To limit the speeds of a device:

1. Click  in the **Speed Limit** column.
2. Enable **Speed Limit**.
3. Set the download and upload speed limit according to your needs.
4. Click **SAVE**. The speeds of the device will be limited.



Chapter 7

Wireless Settings

This chapter guides you on how to configure the wireless settings.

It contains the following sections:

- [Specify Wireless Settings](#)
- [Schedule Your Wireless Function](#)
- [Use WPS for Wireless Connection](#)
- [Advanced Wireless Settings](#)

7.1. Specify Wireless Settings

The router's wireless network names (SSIDs), password, and security option are preset in the factory. The preset SSIDs and password can be found on the label of the router. You can customize the wireless settings according to your needs.

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

Wireless Settings

Personalize settings for each band or enable Smart Connect to configure the same settings for 2.4GHz and 5GHz bands.

TWT: Enable ?

OFDMA/MU-MIMO:

Smart Connect: Enable ?

2.4GHz/5GHz: Enable Share Network

Network Name (SSID): Hide SSID

Security:

Password:

2.4GHz Channel Width:

2.4GHz Channel:

5GHz Channel Width:

5GHz Channel:

The channel width and channel you've selected will overlap with DFS channels. This will require some waiting time to meet regulatory radar detection requirements.

6GHz: Enable Share Network

Network Name (SSID): Hide SSID

Security:

Password:

Channel Width:

Channel: Enable PSC ?

Mode:

- **To enable or disable TWT:**

TWT (Target Wake Time) allows 802.11ax routers and clients to negotiate their periods to transmit and receive data packets. Clients only wake up at TWT sessions and remain in sleep mode for the rest of the time, which significantly extend their battery life. It is disabled by default.

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

- **To enable or disable OFDMA:**

OFDMA enables multiple users to transmit data simultaneously, and thus greatly improves speed and efficiency. Noted that only when your clients also support OFDMA, can you fully enjoy the benefits. It is disabled by default.

1. Go to [Advanced](#) > [Wireless](#) > [Wireless Settings](#).
2. Enable [OFDMA+MU-MIMO](#) or [OFDMA only](#).

- **To use the Smart Connect function:**

Smart Connect combines the 2.4 GHz and 5 GHz bands and assigns your devices between them to balance network demands, while leaving the brand-new 6 GHz band exclusive for your Wi-Fi 6E devices to unleash the most out of the latest Wi-Fi.

1. Go to [Advanced](#) > [Wireless](#) > [Wireless Settings](#).
2. Enable [Smart Connect](#).



3. Keep the default values or set a new SSID and password, and click [SAVE](#). This SSID and password will be applied for the 2.4 GHz and 5 GHz wireless networks. If you want to configure the wireless settings separately for each band, deselect the checkbox to disable this feature.

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

1. Go to [Wireless](#) or [Advanced](#) > [Wireless](#) > [Wireless Settings](#).
2. The wireless bands are enabled by default. If you want to disable a wireless band, just deselect its [Enable](#) checkbox.

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

1. Go to [Wireless](#) or [Advanced](#) > [Wireless](#) > [Wireless Settings](#).
2. Create a new SSID in [Network Name \(SSID\)](#) and customize the password for the network in [Password](#). The value is case-sensitive.

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

- **To hide SSID:**
 1. Go to [Wireless](#) or [Advanced > Wireless > Wireless Settings](#).
 2. Select [Hide SSID](#), and your SSID won't display when you scan for local wireless networks on your wireless device and you need to manually join the network.
- **To change the security option:**
 1. Go to [Advanced > Wireless > Wireless Settings](#).
 2. Select an option from the [Security](#) drop-down list. We recommend you don't change the default settings unless necessary.
- **To change channel settings:**
 1. Go to [Advanced > Wireless > Wireless Settings](#).
 2. Select a [Channel Width](#) (bandwidth) for the wireless network. It is recommended to just leave it as default.
 3. Select an operating [Channel](#) for the wireless network. It is recommended to leave the channel to [Auto](#) if you are not experiencing the intermittent wireless connection issue.

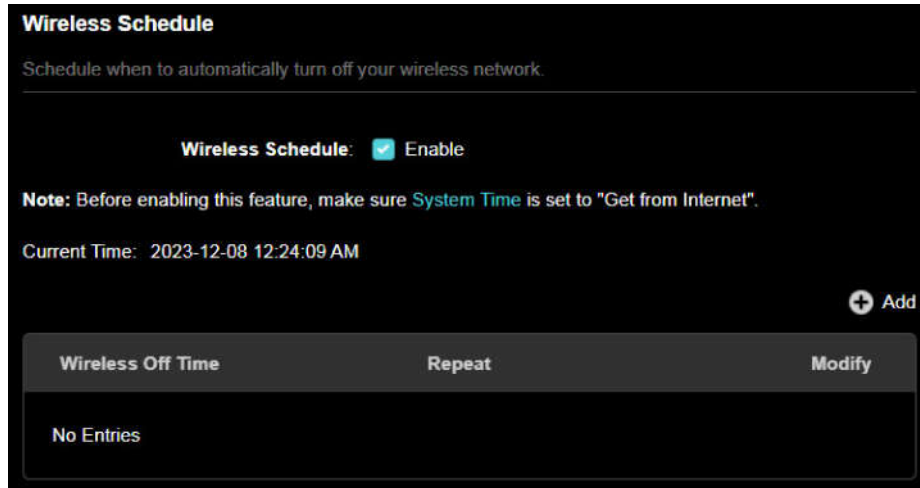
For the 6 GHz network, you can select the [Enable PSC](#) checkbox. When PSC (Preferred Scanning Channel) is enabled, only channels with higher connectivity will be reserved to ensure 6 GHz device connections.
- **To change the transmission mode:**
 1. Go to [Advanced > Wireless > Wireless Settings](#).
 2. For the 2.4 GHz and 5 GHz networks, disable [Smart Connect](#), then select a transmission [Mode](#) according to your wireless client devices. It is recommended to just leave it as default.

The 6 GHz network only supports 802.11ax mode, which cannot be changed.

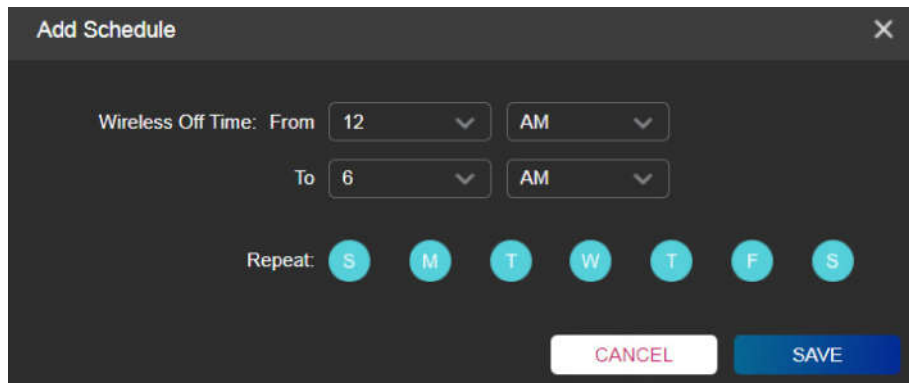
7.2. Schedule Your Wireless Function

The wireless network can be automatically off at a specific time when you do not need the wireless connection.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced > Wireless > Wireless Schedule](#).
3. Enable the [Wireless Schedule](#) feature.



4. Click [Add](#) to specify a wireless off period during which you need the wireless off automatically, and click [SAVE](#).



Note:

- The Effective Time Schedule is based on the time of the router. You can go to [Advanced > System > Time & Language](#) to modify the time.
- The wireless network will remain on for the rest of the time.

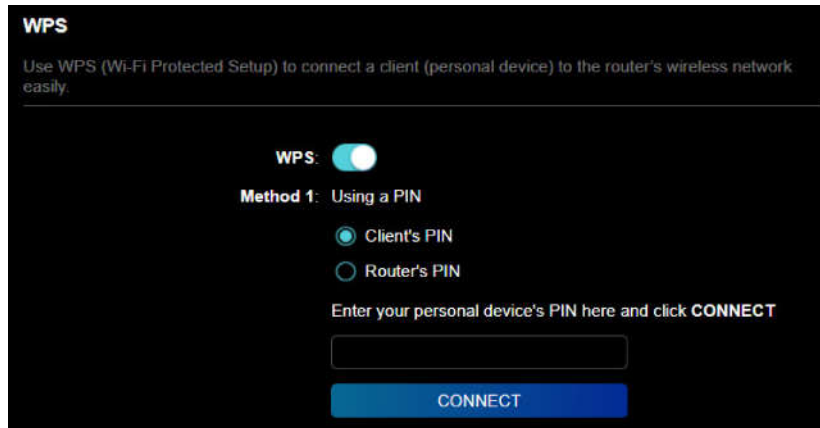
7.3. Use WPS for Wireless Connection

Wi-Fi Protected Setup (WPS) provides an easier approach to set up a security-protected Wi-Fi connection.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Make sure the Wi-Fi of your router is on and go to [Advanced > Wireless > WPS](#).

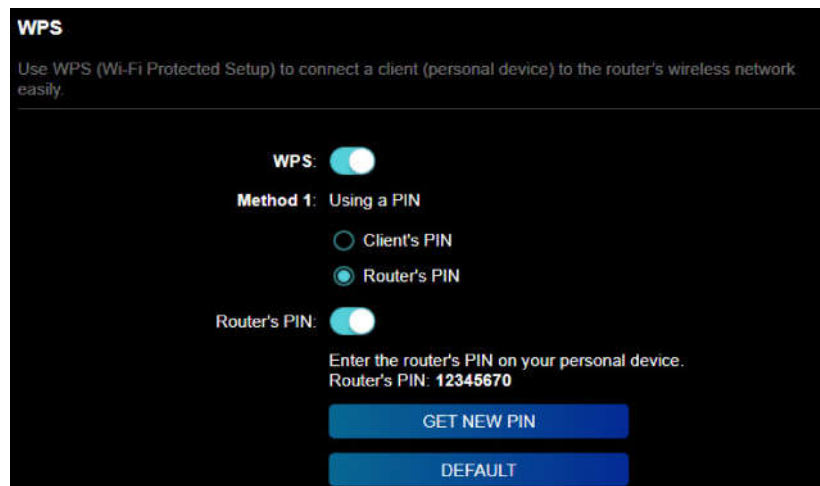
7.3.1. Connect via the Client's PIN

Enter the PIN of your device and click [Connect](#). Then your device will get connected to the router.



7.3.2. Connect via the Router's PIN

Select **Router's PIN** in **Method 1** to enable **Router's PIN**. You can use the default PIN or generate a new one.

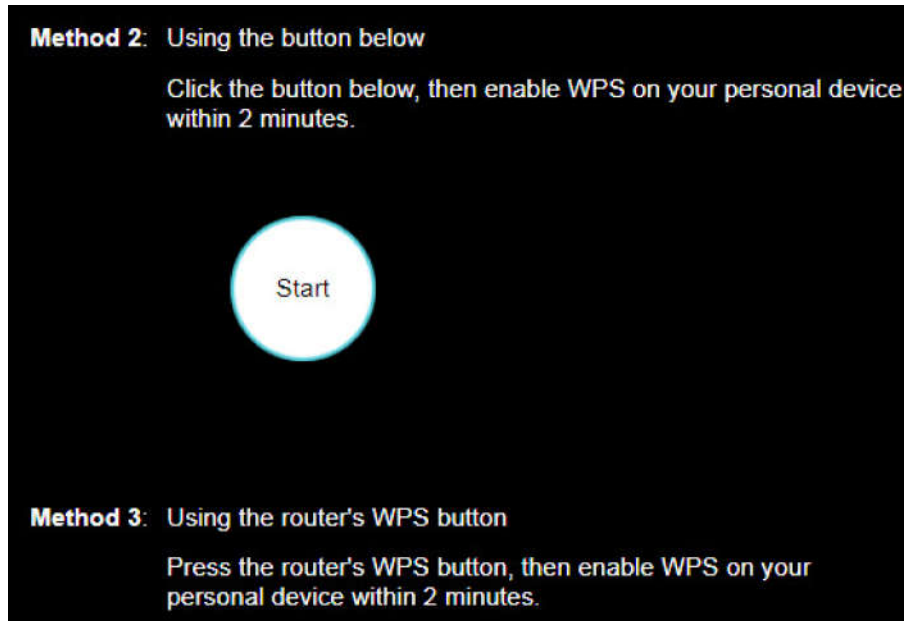


Note:

PIN (Personal Identification Number) is an eight-character identification number preset to each router. WPS supported devices can connect to your router with the PIN. The default PIN is printed on the label of the router.

7.3.3. Push the WPS Button

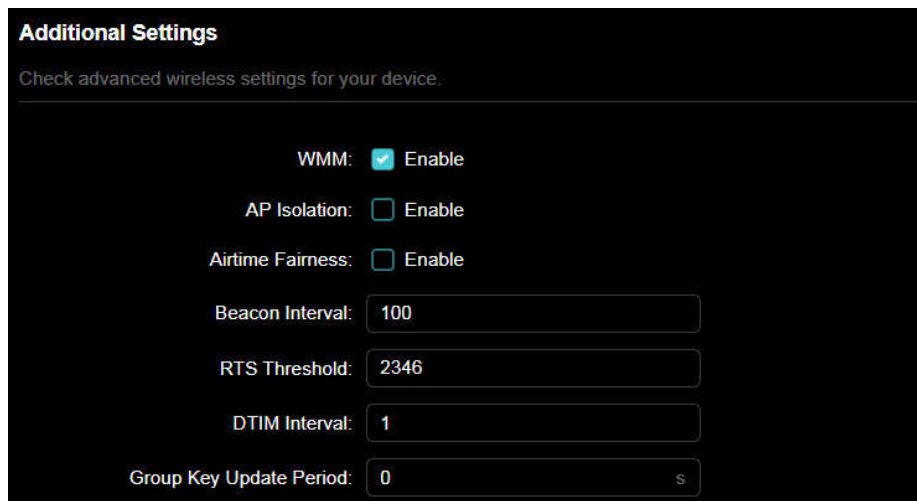
Click **Start** on the screen or directly press the router's WPS button. Within two minutes, enable WPS on your personal device. **Success** will appear on the screen and the WPS LED of the router should change from blinking blue to your selected RGB effect (default: Fire effect), indicating successful WPS connection.



7.4. Advanced Wireless Settings

Check advanced wireless settings for your device.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > Wireless > Additional Settings**.
3. Configure advanced wireless settings.



- **WMM** - WMM function can guarantee the packets with high-priority messages being transmitted preferentially.
- **AP Isolation** - This function isolates all connected wireless stations so that wireless stations cannot access each other through WLAN.

- **Airtime Fairness** - This function can improve the overall network performance by sacrificing a little bit of network time on your slow devices.
- **Beacon Interval** - Enter a value between 40 and 1000 in milliseconds to determine the duration between beacon packets that are broadcasted by the router to synchronize the wireless network. The default value is 100 milliseconds.
- **RTS Threshold**- Enter a value between 1 and 2346 to determine the packet size of data transmission through the router. By default, the RTS (Request to Send) Threshold size is 2346. If the packet size is greater than the preset threshold, the router will send RTS frames to a particular receiving station and negotiate the sending of a data frame.
- **DTIM Interval** - The value determines the interval of DTIM (Delivery Traffic Indication Message). Enter a value between 1 and 15 intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Group Key Update Period** - Enter a number of seconds (minimum 30) to control the time interval for the encryption key automatic renewal. The default value is 0, meaning no key renewal.

Chapter 8

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](#)

8.1. Create a Network for Guests

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > Wireless > Guest Network** or click **Wireless** on the top page. Locate the **Guest Network** section.
3. Create a guest network as needed.
 - 1) Tick the Enable checkbox for the 2.4GHz, 5 GHz, or 6GHz 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) Enable **Bandwidth Control** if you want to limit the network speed of your guests. Then enter the limited bandwidth value.
 - 4) Set the **Effective Time** for how long the Guest Network turns on.
 - 5) Select the **Security** type and customize your own password. If **No security** is selected, no password is needed to access your guest network.

Guest Network

Enable the wireless bands you want your guests to use and complete the related information.

2.4GHz: Enable [Share Network](#)

Network Name (SSID): Hide SSID

Bandwidth Control: Enable

Download Bandwidth: Mbps

Upload Bandwidth: Mbps

5GHz: Enable [Share Network](#)

Network Name (SSID): Hide SSID

Bandwidth Control: Enable

6GHz: Enable [Share Network](#)

Network Name (SSID): Hide SSID

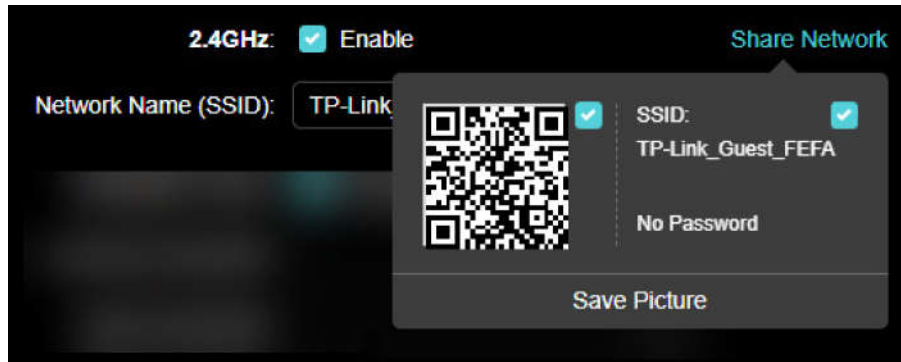
Bandwidth Control: Enable

Effective Time: ▼

Security: ▼

This security type is not considered secure. Consider selecting a more secure encryption.

- Click **SAVE**. Now your guests can access your guest network using the SSID and password you set!
- You can also click **Share Network** to share the SSID and password to your guests.

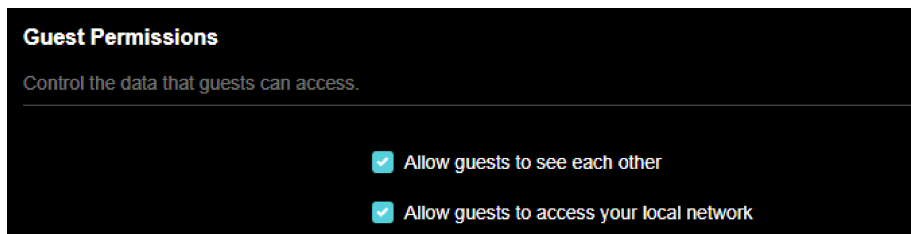


 **Tips:**

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.

8.2. Customize Guest Network Options

- Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
- Go to **Advanced > Wireless > Guest Network**. Locate the **Guest Permissions** section.
- Customize guest network options according to your needs.



- **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.

- **Allow guests to access your local network**

Tick this checkbox if you want to allow the wireless clients on your guest network to communicate with the devices connected to your router's LAN ports or main network via methods such as network neighbors and Ping.

- Click **SAVE**. Now you can ensure network security and privacy!

Chapter 9

IoT Network

This feature further secures your home network by allowing you to create a dedicated wireless network to manage your IoT devices together, such as smart lights and cameras.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced > Wireless > IoT Network](#).
3. Create an IoT network as needed.
4. Tick the [Enable](#) checkbox for the 2.4GHz, or 5 GHz wireless network. For the 5 GHz network, make sure your IoT devices can connect to a 5 GHz network.
 - 1) Customize the SSID. Don't select [Hide SSID](#) unless you want your IoT devices to manually input the SSID for network access.
 - 2) Select the [Security](#) type and customize your own password. If [No security](#) is selected, no password is needed to access the IoT network.

5. Click [SAVE](#). Now you can connect your IoT devices to the dedicated IoT network.
6. You can also click [Sharing Network](#) to share the SSID and password to others.

Chapter 10

USB Settings

This chapter describes how to use the USB ports to share files and media from the USB storage devices over your home network locally, or remotely through the internet.

The router supports USB external flash drives and hard drives.

It contains the following sections:

- [Access the USB Storage Device](#)
- [Media Sharing](#)
- [Time Machine](#)

10. 1. Access the USB Storage Device

Insert your USB storage device into the router's USB port and then access files stored there locally or remotely.

🔗 Tips:

- If you use USB hubs, make sure no more than 4 devices are connected to the router.
- If the USB storage device requires using bundled external power, make sure the external power has been connected.
- If you use a USB hard drive, make sure its file system is FAT32, exFat, NTFS or HFS+.
- Before you physically disconnect a USB device from the router, safely remove it to avoid data damage: Go to [Advanced > USB > USB Storage Device](#) and click [Remove](#).

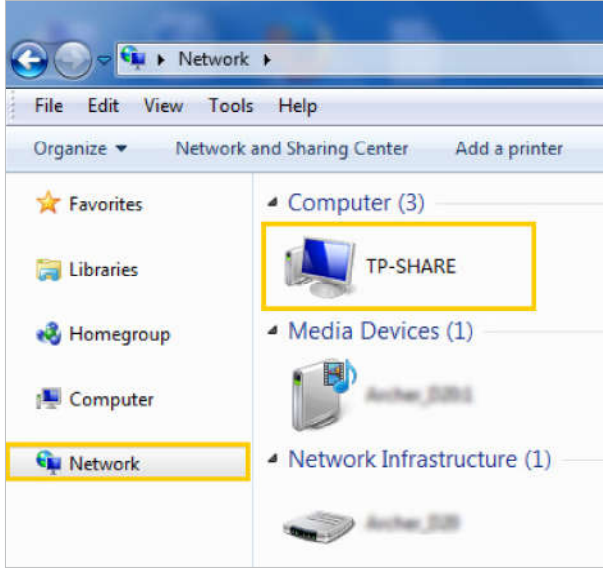
10. 1. 1. Access the USB Device Locally

Insert your USB storage device into the router's USB port and then refer to the following table to access files stored on your USB storage device.

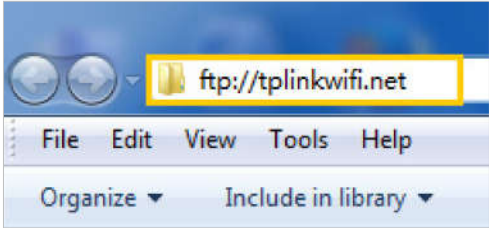
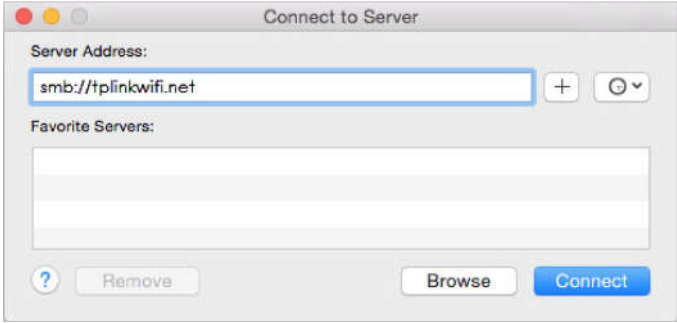
Windows computer

- **Method 1:**
Go to [Computer > Network](#), then click the Network Server Name ([TP-SHARE](#) by default) in the [Computer](#) section.

📌 **Note:**
Operations in different systems are similar. Here we take Windows 7 as an example.



The screenshot shows a Windows 7 'Network' window. The address bar shows 'Network'. The left sidebar has 'Network' selected. The main pane shows three categories: 'Computer (3)', 'Media Devices (1)', and 'Network Infrastructure (1)'. Under 'Computer (3)', the 'TP-SHARE' icon is highlighted with a yellow box.

<p>Windows computer</p>	<ul style="list-style-type: none"> • Method 2: <p>Open the Windows Explorer (or go to Computer) and type the server address \\tplinkwifi.net or ftp://tplinkwifi.net in the address bar, then press Enter.</p> 
<p>Mac</p>	<ol style="list-style-type: none"> 1) Select Go > Connect to Server. 2) Type the server address smb://tplinkwifi.net. 3) Click Connect.  <ol style="list-style-type: none"> 4) When prompted, select the Guest radio box. (If you have set up a username and a password to deny anonymous access to the USB disks, you should select the Registered User radio box. To learn how to set up an account for the access, refer to To Set Up Authentication for Data Security.)
<p>Tablet</p>	<p>Use a third-party app for network files management.</p>

 **Tips:**

You can also access your USB storage device by using your Network/Media Server Name as the server address. Refer to [To Customize the Address of the USB Storage Device](#) to learn more.

10. 1. 2. Access the USB Device Remotely

You can access your USB disk outside the local area network. For example, you can:

- Share photos and other large files with your friends without logging in to (and paying for) a photo-sharing site or email system.
- Get a safe backup for the materials for a presentation.
- Remove the files on your camera's memory card from time to time during the journey.

Note:

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

Follow the steps below to configure remote access settings.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > USB > USB Storage Device**.
3. Tick the **Internet FTP** checkbox, and then click **SAVE**.

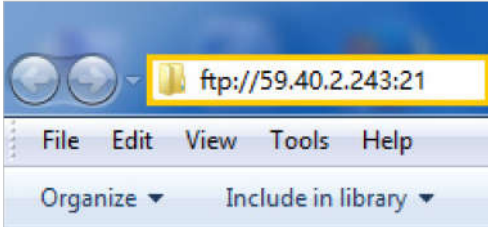
Access Method

Select the method for accessing your USB storage device. The device can then be reached via the access address.

Network/Media Server Name:

Enable	Access Method	Address	Port
<input checked="" type="checkbox"/>	Samba for Windows Samba for macOS/Linux	\\192.168.0.1 smb://192.168.0.1	---
<input checked="" type="checkbox"/>	Local FTP	ftp://192.168.0.1:21	21
<input checked="" type="checkbox"/>	Internet FTP	ftp://172.31.53.225:21 Set DDNS	<input type="text" value="21"/>

4. Refer to the following table to access your USB disk remotely.

Computer	<ol style="list-style-type: none"> 1) Open the Windows Explorer (or go to Computer, only for Windows users) or open a web browser. 2) Type the server address in the address bar: Type in ftp://<WAN IP address of the router>:<port number> (such as ftp://59.40.2.243:21). If you have specified the domain name of the router, you can also type in ftp://<domain name>:<port number> (such as ftp://MyDomainName:21) <div data-bbox="644 526 1134 752" style="text-align: center;">  </div> <ol style="list-style-type: none"> 3) Press Enter on the keyboard. 4) Access with the username and password you set in To Set Up Authentication for Data Security. <p><small>📌 Tips:</small> You can also access the USB disk via a third-party app for network files management, which can resume broken file transfers.</p>
	Tablet

📌 Tips:

Click [Set Up a Dynamic DNS Service Account](#) to learn how to set up a domain name for you router.

10. 1. 3. Customize the Access Settings

By default, all the network clients can access all folders on your USB disk. You can customize your sharing settings by setting a sharing account, sharing specific contents and setting a new sharing address on the router's web management page.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [USB](#) > [USB Storage Device](#).

- **To Customize the Address of the USB Storage Device**

You can customize the server name and use the name to access your USB storage device.

1. In the [Access Method](#) session, make sure [Samba for Windows](#) is ticked, and enter a [Network/Media Server Name](#) as you like, such as [MyShare](#), then click [SAVE](#).

Access Method

Select the method for accessing your USB storage device. The device can then be reached via the access address.

Network/Media Server Name:

Enable	Access Method	Address	Port
<input checked="" type="checkbox"/>	Samba for Windows Samba for macOS/Linux	\\192.168.0.1 smb://192.168.0.1	—
<input checked="" type="checkbox"/>	Local FTP	ftp://192.168.0.1:21	21
<input type="checkbox"/>	Internet FTP	ftp://172.31.53.225:21 Set DDNS	<input type="text" value="21"/>

2. Now you can access the USB storage device by visiting `\\MyShare` (for Windows) or `smb://MyShare` (for Mac).

- **To Only Share Specific Content**

Focus on the [File Sharing](#) section. Specify sharing folders that you want to share and click [SAVE](#).

File Sharing

Share files with devices in your home or office network.

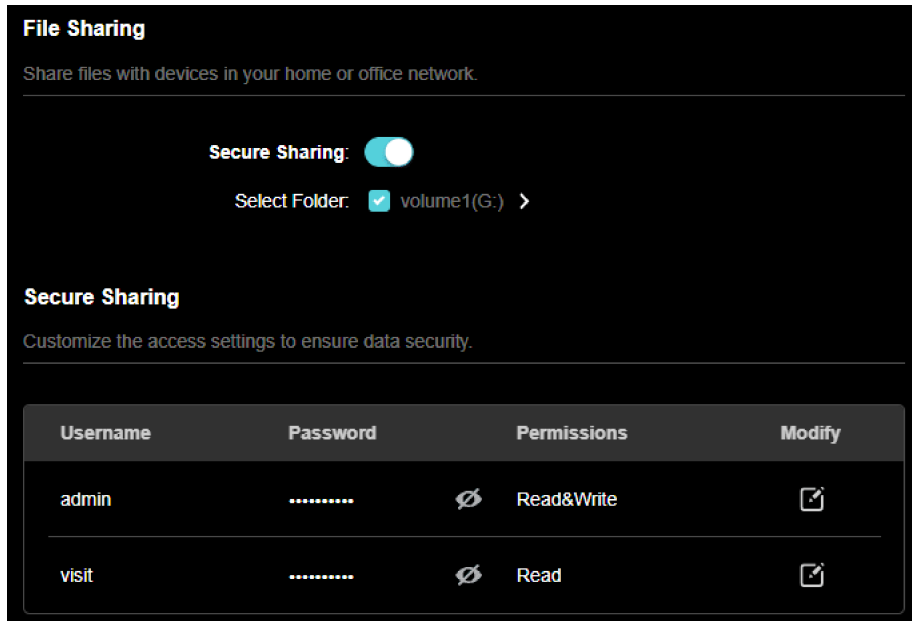
Secure Sharing:

Select Folder: volume1(G:) >

- **To Set Up Authentication for Data Security**

You can set up authentication for your USB storage device so that network clients will be required to enter username and password when accessing the USB storage device.

1. In the [File Sharing](#) section, enable [Secure Sharing](#).



2. Click to modify the access account. The username and password are both **admin** for default administrator account, and both **visit** for default visitor account. Accessing as an administrator can read and modify the shared folders while visitors can only read the shared folders.

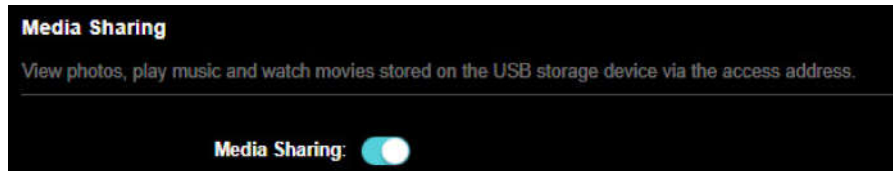
Note:

1. For Windows users, do not set the sharing username the same as the Windows username. Otherwise, Windows credential mechanism may cause the following problems:
 - If the sharing password is also the same as the Windows password, authentication will not work since the Windows will automatically use its account information for USB access.
 - If the sharing password is different from the Windows password, the Windows will be unable to remember your credentials and you will always be required to enter the sharing password for USB access.
2. Due to Windows credential mechanism, you might be unable to access the USB disk after changing Authentication settings. Please log out from the Windows and try to access again. Or you can change the address of the USB disk by referring to [To Customize the Address of the USB Storage Device](#).

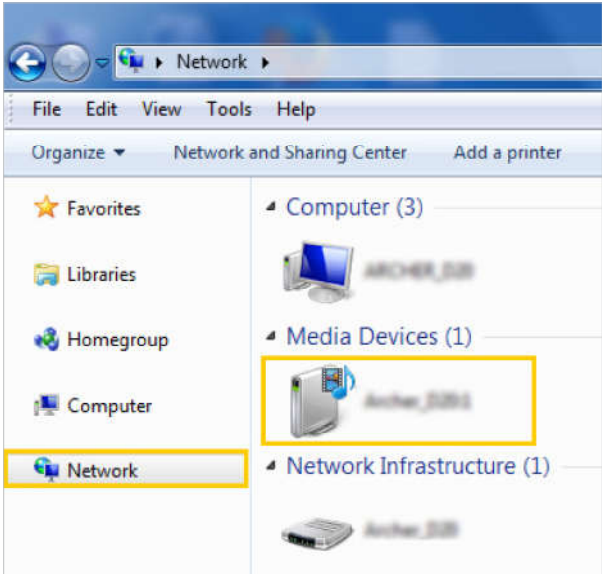
10.2. Media Sharing

The feature of **Media Sharing** allows you to view photos, play music and watch movies stored on the USB storage device directly from DLNA-supported devices, such as your computer, tablet and PS2/3/4.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > USB > USB Storage Device**.
3. Enable **Media Sharing**.



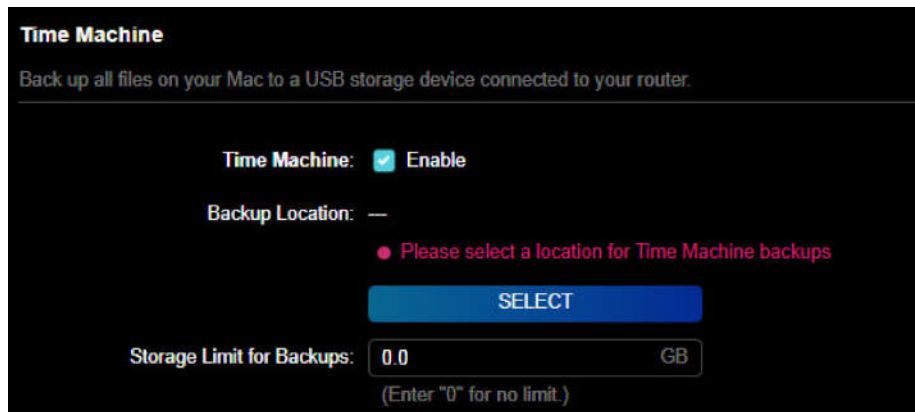
4. When your USB storage device is inserted into the router, your DLNA-supported devices (such as your computer and pad) connected to the router can detect and play the media files on the USB storage devices.
5. Refer to the following table for detailed instructions.

Windows Computer	<ul style="list-style-type: none"> • Go to Computer > Network, then click the Media Server Name (Model number-share by default) in the Media Devices section. <p>■ Note: Here we take Windows 7 as an example.</p> 
Tablet	<ul style="list-style-type: none"> • Use a third-party DLNA-supported player.

10.3. Time Machine

Time Machine backs up all files on your Mac computer to a USB storage device connected to your router.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [USB](#) > [Time Machine](#).



3. Tick the checkbox to enable [Time Machine](#).
4. Click [SELECT](#) to select a location for Time Machine backups.
5. Set the [Storage Limit for Backups](#).
Note: 0 means no limit for the space.
6. Click [SAVE](#).

Chapter 11

HomeShield

Customize your home network with enhanced security using a kit of features built in TP-Link HomeShield. Whether protecting your sensitive data or limiting the access of kids and guests, TP-Link HomeShield provides you the tools you need to fully manage your network.

It contains the following sections:

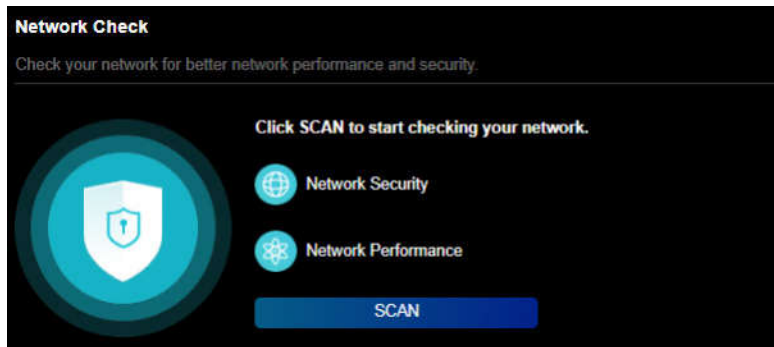
- [Network Check](#)
- [Parental Controls](#)
- [QoS](#)
- [More Features](#)

*For an easier way to check your home network protection system, you can download the Tether app to enjoy full Homeshield features.

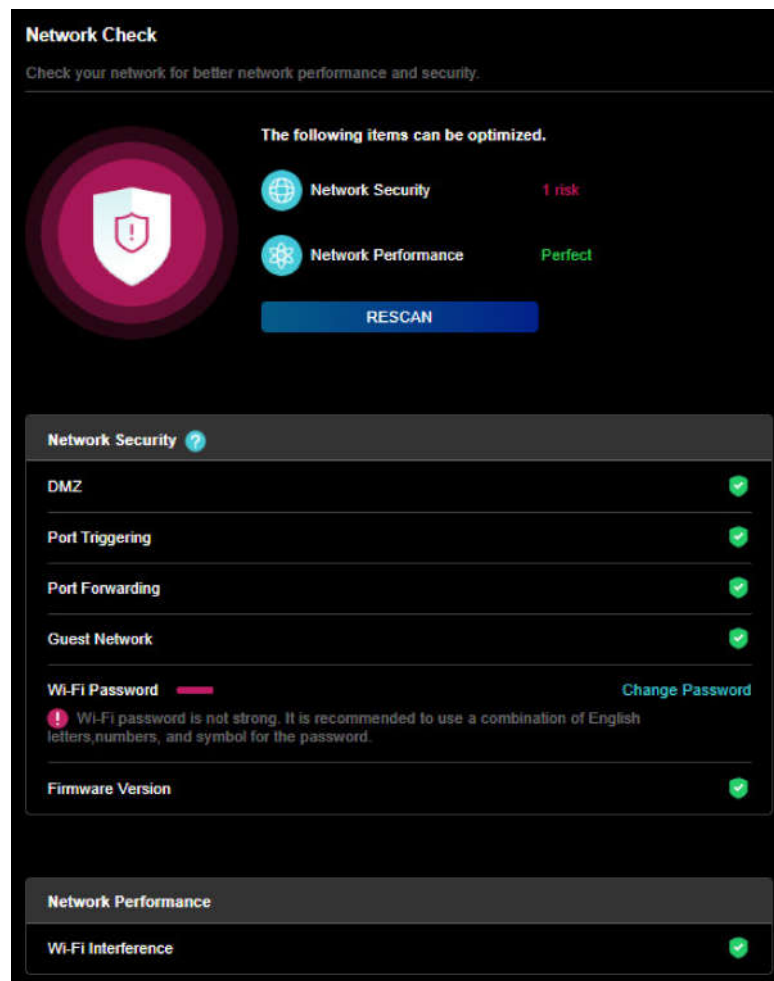
11.1. Network Check

Scan your whole network to help analyze and optimize your network.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced > HomeShield > Network Check](#).
3. Click **SCAN**.



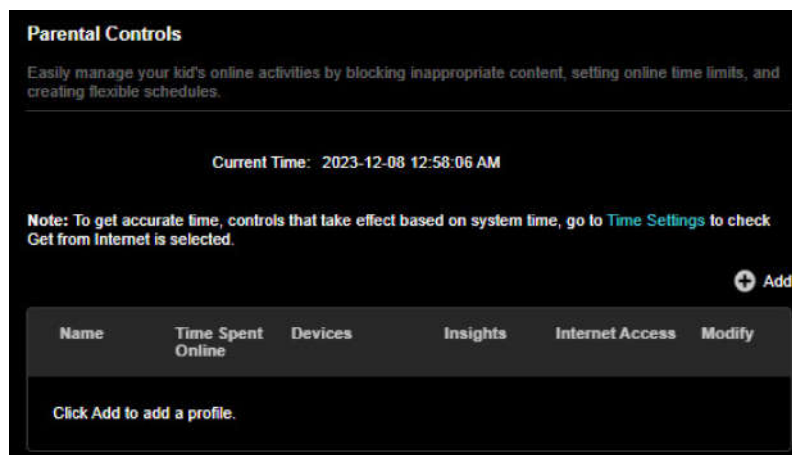
4. Optimize your network according to the tips.



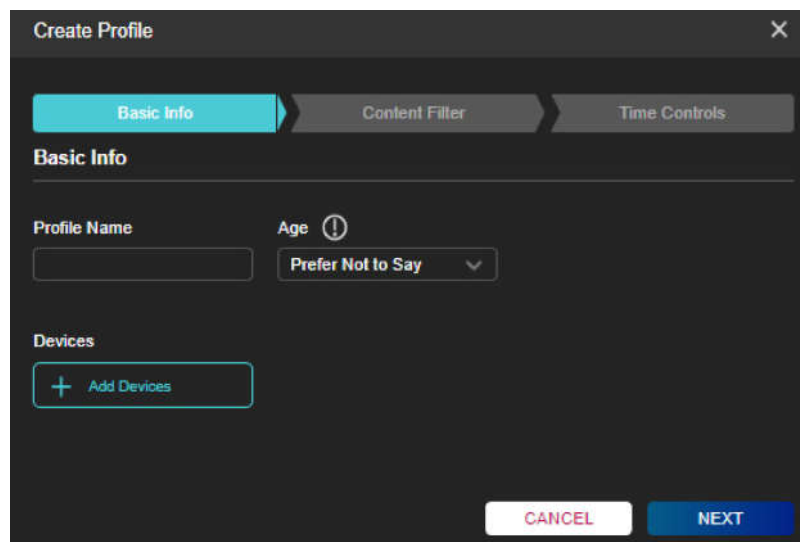
11.2. Parental Controls

Parental Controls allows you to set up unique restrictions on internet access for each member of your family. You can block inappropriate content, set daily limits for the total time spent online and restrict internet access to certain times of the day.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [HomeShield](#) > [Parental Controls](#).
3. Click + [Add](#) to create a profile for a family member.



4. Add basic profile information.

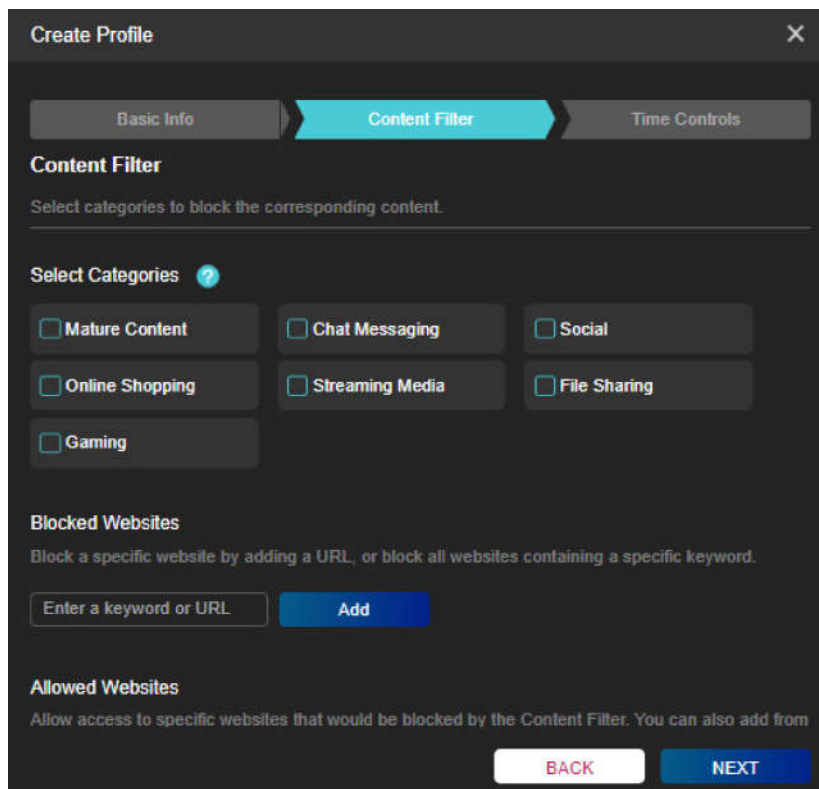


- 1) Enter a [Name](#) for the profile to make it easier to identify. Set the [Age](#) to get the corresponding filter level.
- 2) Under [Devices](#), add devices that belong to this family member. Access restrictions will be applied to these devices.

Note: Only devices that have previously been connected to your router's network are listed here. If you are unable to find the device you want to add, connect it to your network and then try again.

3) Click [NEXT](#)

5. Block content for this profile.

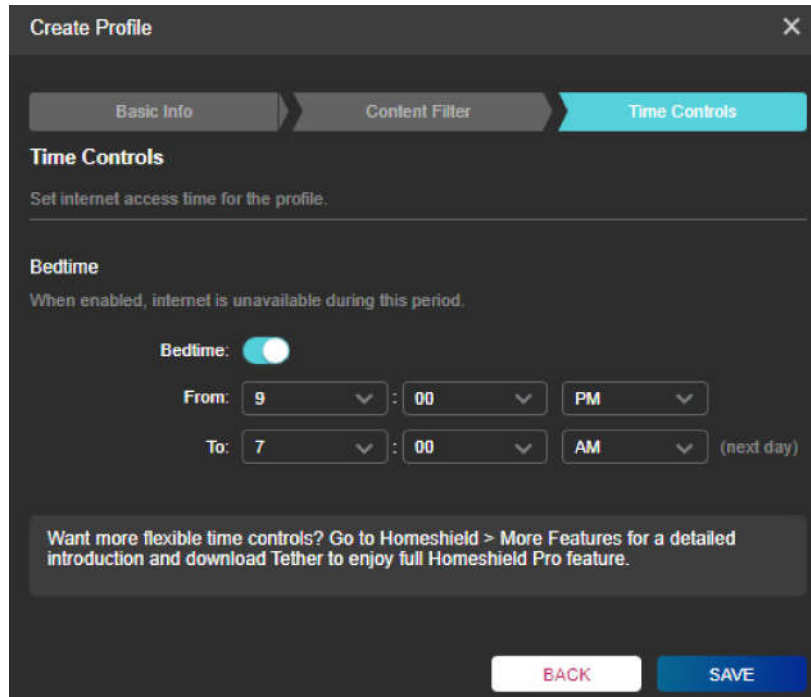



1) Select the content categories to block in the [Content Filter](#) list.





2) You can also block a specific website. Enter a keyword (for example, "Facebook") or a URL (for example, "www.facebook.com"), then click [Add](#).

3) Click [NEXT](#).

6. Set time restrictions on internet access.



- 4) Enable **Bedtime** and use the up/down arrows or enter times in the fields. Devices under this profile will be unable to access the internet during this time period.
- 5) Click **SAVE**.
- 6) After adding a profile, you can click the Insight icon to check the detailed visited history, and click  to pause the network for this profile anytime.

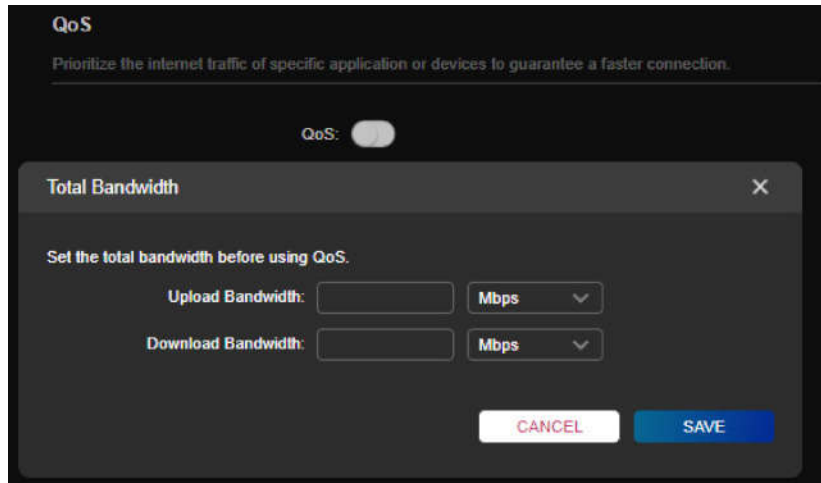
Name	Time Spent Online	Devices	Insights	Internet Access	Modify
Tony	0	0			 

Note: You can go to [Advanced > HomeShield > More Features](#) for a detailed introduction and download Tether to enjoy full HomeShield premium features.

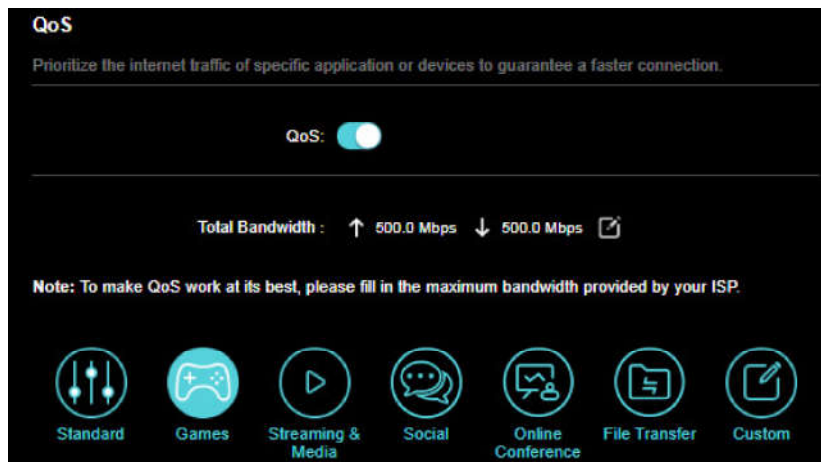
11.3. QoS

QoS (Quality of Service) allows you to prioritize connection of specific devices for a set duration. Devices set as high priority will be allocated more bandwidth and so continue to run smoothly even when there is heavy traffic on the network.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced > HomeShield > QoS](#).
3. Enable **QoS** to set the total bandwidth. Then click **SAVE**.



4. Select an activity to prioritize the internet traffic of the specific applications to guarantee a faster connection.



11.4. More Features

Download the Tether app and subscribe to enjoy the full features of HomeShield.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > HomeShield > More Features**.
3. Follow the web instructions to get full features of HomeShield.



More Features

Download the Tether app and subscribe to enjoy the full features of HomeShield.

Start your 30-day free trial on Tether
[Compare Basic and Pro Features](#)

DOWNLOAD ON THE
App Store

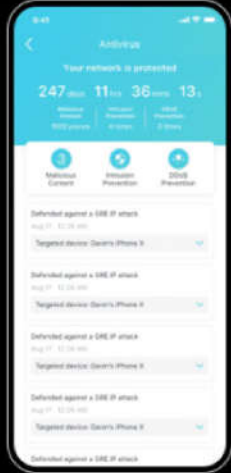
GET IT ON
Google Play



Real-Time Protection **Parental Controls** **Usage Analysis**

Detect and identify cyber threats to keep your privacy and connected devices protected.

- IoT Protection**
Get real-time security for your Internet of Things
- Intrusion Prevention System**
Identifies and block network intruders
- Malicious Content Filter**
Block malicious content
- DDoS Protection**
Protects your home network from DDoS attacks



The screenshot shows the Tether app interface. At the top, it says "Your network is protected" with statistics: 247 apps, 11 on, 36 apps, 13. Below this are three toggle switches for Malicious Content, Intrusion Prevention, and DDoS Protection. A list of detected DDoS attacks is shown, each with a timestamp and a dropdown menu for the targeted device (e.g., "Targeted device: Samsung iPhone 8").

Chapter 12

EasyMesh with Seamless Roaming

This product is compatible with EasyMesh. This chapter introduces the EasyMesh feature.

It contains the following sections:

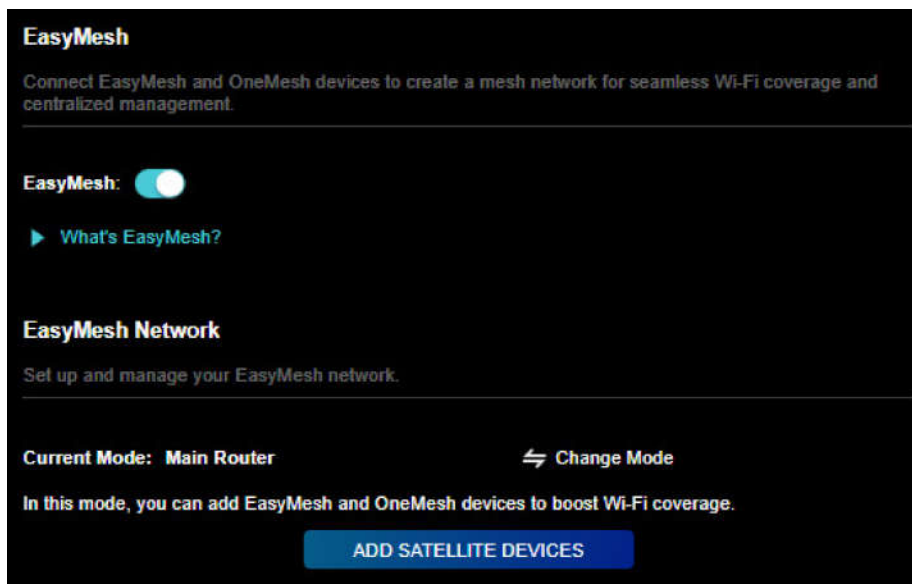
- [Add a Router as a Satellite Device](#)
- [Add a Range Extender as a Satellite Device](#)
- [Manage Devices in the EasyMesh Network](#)

EasyMesh routers and extenders 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.

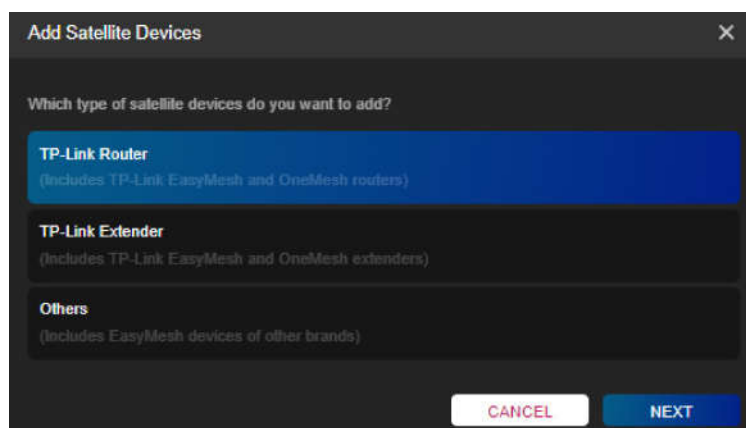
Note: Routers and range extenders must be compatible with EasyMesh or OneMesh™. Firmware upgrades may be required.

12.1. Add a Router as a Satellite Device

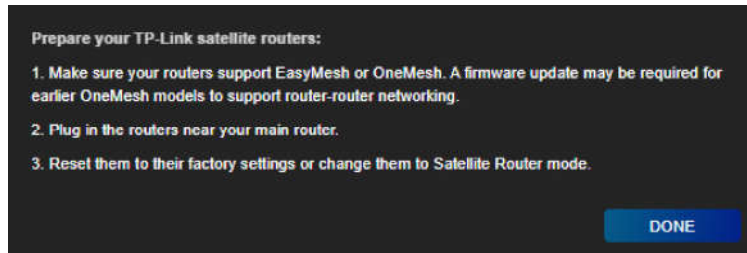
1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > EasyMesh**, and enable **EasyMesh**.



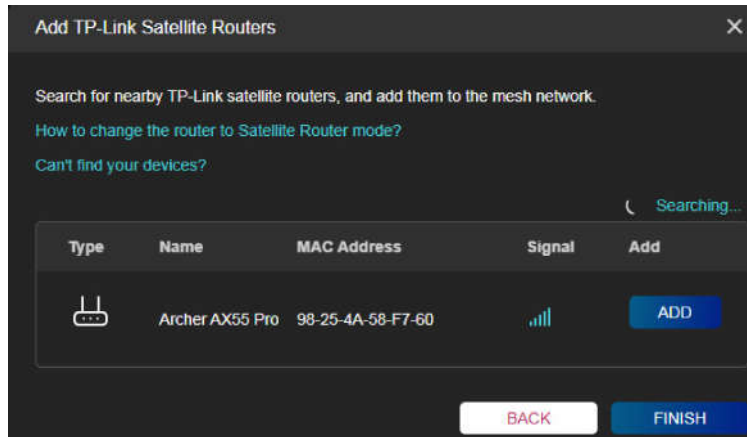
3. Click **ADD SATELLITE DEVICES**, select **TP-Link Router**, then click **NEXT**.



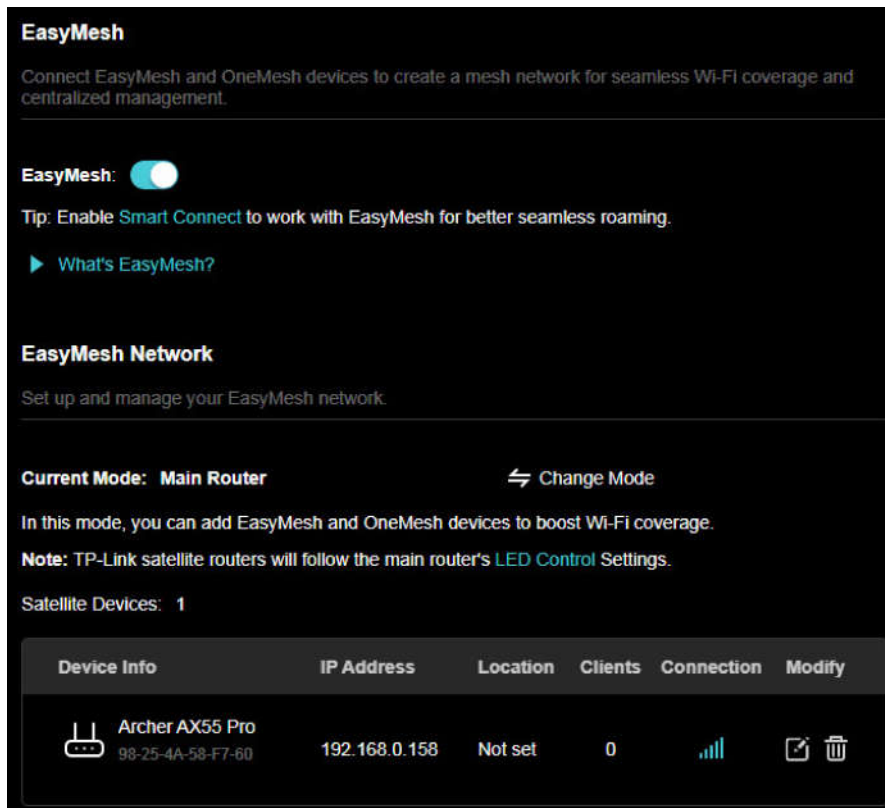
4. Follow the page instructions to prepare your satellite router, then click **DONE**.



5. Click **ADD**. When prompted “This device has been added successfully”, click **OK**, then click **FINISH**.

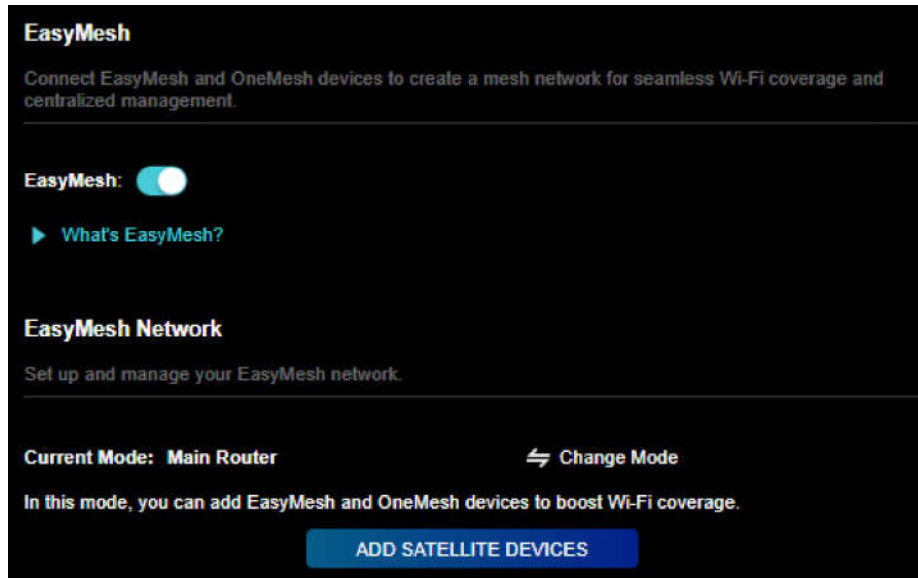


6. Done! The satellite router will also appear on the list.

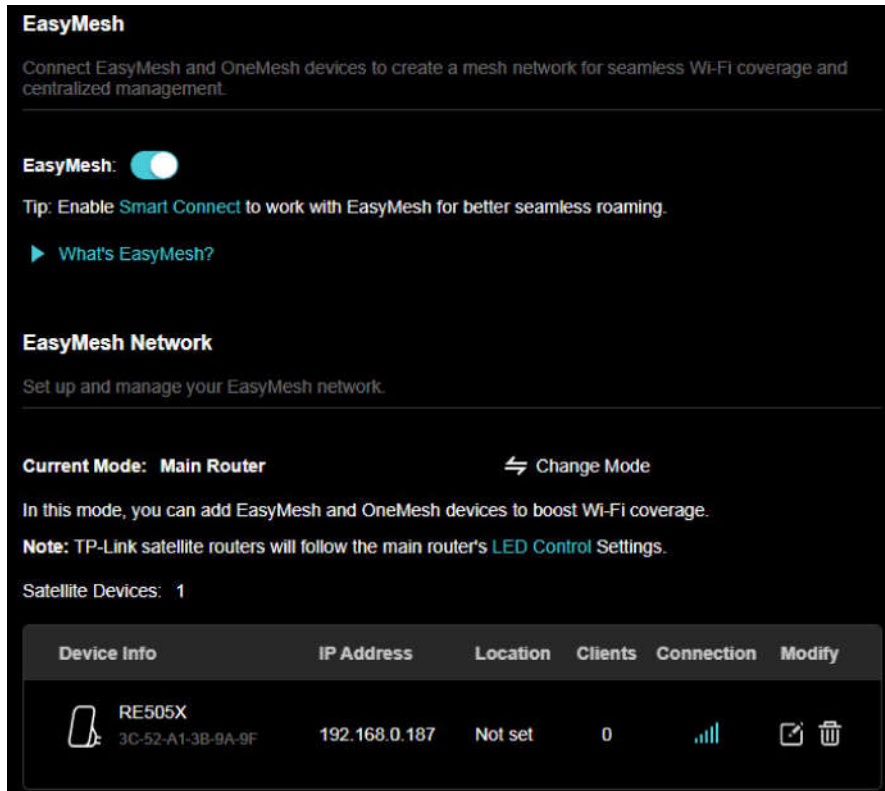


12.2. Add a Range Extender as a Satellite Device

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced** > **EasyMesh**, and enable **EasyMesh**.



3. Plug in the extender next to the main router.
4. Within 2 minutes, press the WPS button on main router and on the extender. Wait until the WPS process is complete.
5. Done! You can check the mesh device on the router's web page too.



12.3. Manage Devices in the EasyMesh Network

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

- **To view mesh devices and connected clients in the network:**

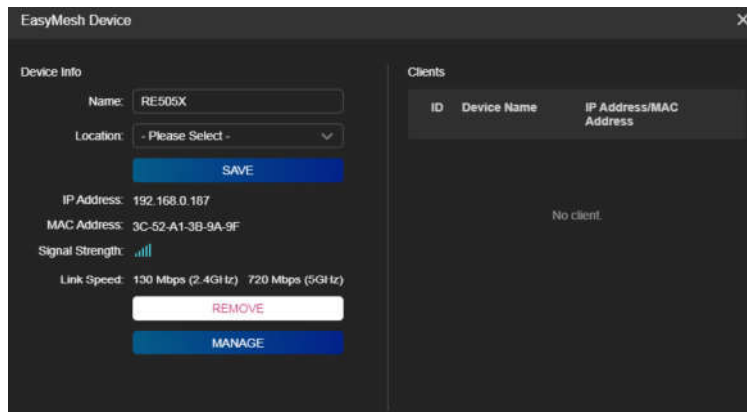
1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Network Map](#).
3. Click [Mesh Devices](#) to view all mesh devices, and click [Clients](#) to view all connected clients.

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

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [EasyMesh](#).

Device Info	IP Address	Location	Clients	Connection	Modify
RE505X 3C-52-A1-3B-9A-9F	192.168.0.187	Not set	0		

3. Click the Modify button  to view detailed information and change its settings.



- Change device information.
- Click **MANAGE** to redirect to the web management page of this device.
- Click **REMOVE** to delete this device from the EasyMesh network.

Chapter 13

Network Security

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

It contains the following sections:

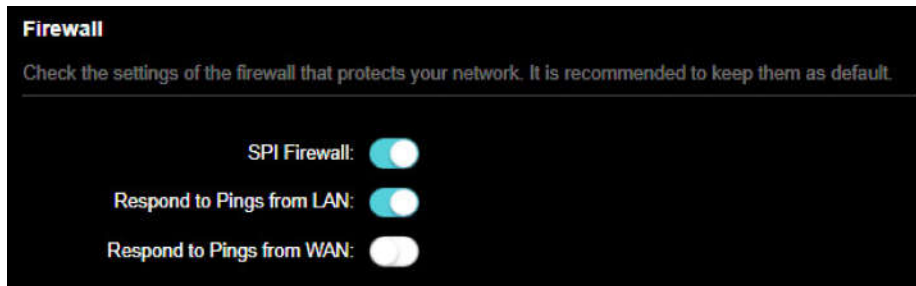
- [Protect the Network from Cyber Attacks](#)
- [Access Control](#)
- [IP & MAC Binding](#)
- [ALG](#)
- [Device Isolation](#)

*For a more comprehensive home network protection system, refer to the [HomeShield](#) chapter.

13. 1. Protect the Network from Cyber Attacks

The SPI (Stateful Packet Inspection) Firewall protects the router from cyber attacks and validate the traffic that is passing through the router based on the protocol. This function is enabled by default.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > Security > Firewall**. It's recommended to keep the default settings.



13. 2. 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 (Deny List) or a list of allowed devices (Allow List).

I want to:

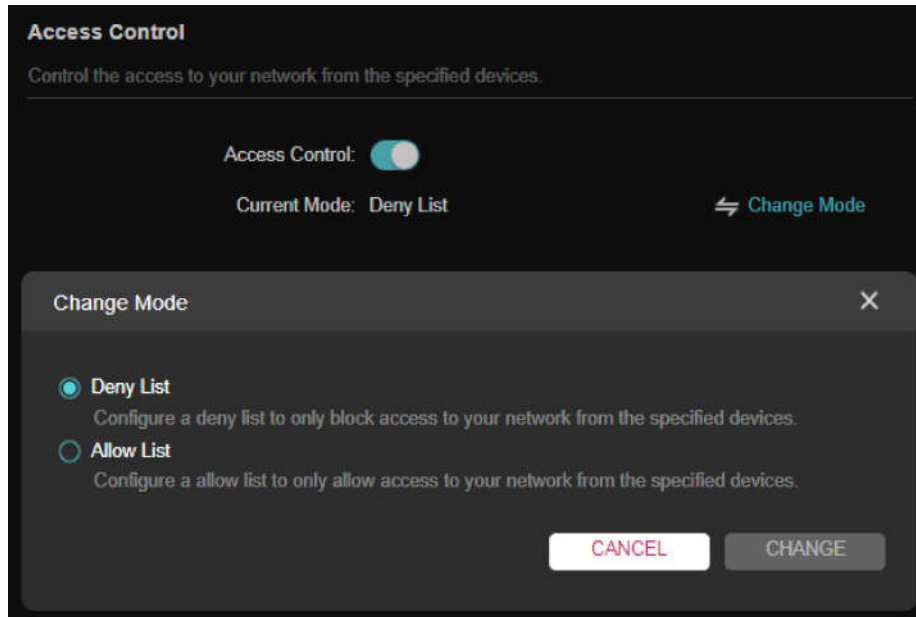
Block or allow specific client devices to access my network (via wired or wireless).

How can I do that?

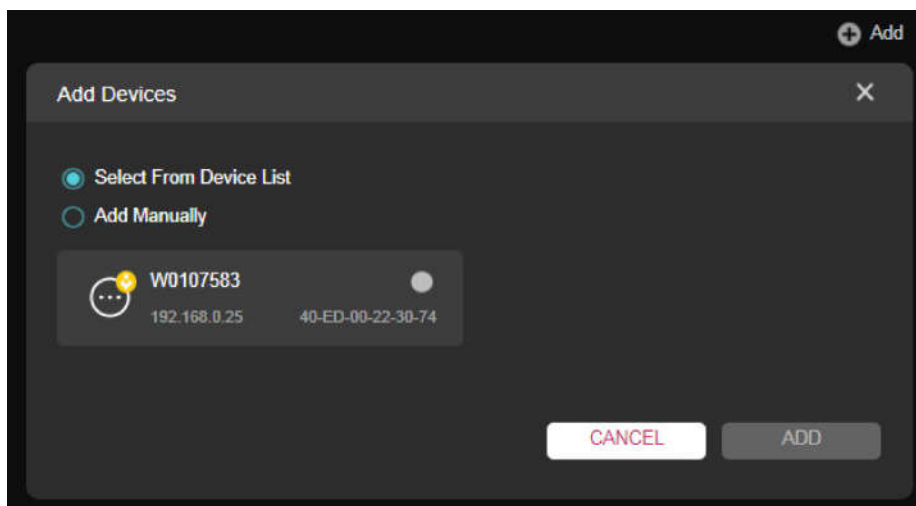
1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > Security > Access Control**.
3. Toggle on to enable **Access Control**.
3. Click **Change Mode** and select the access mode to either block (recommended) or allow the device(s) in the list.

To block specific device(s):



- 1) Select **Deny List**.



2) Click **+ Add** and select devices you want to be blocked and Click **ADD**.

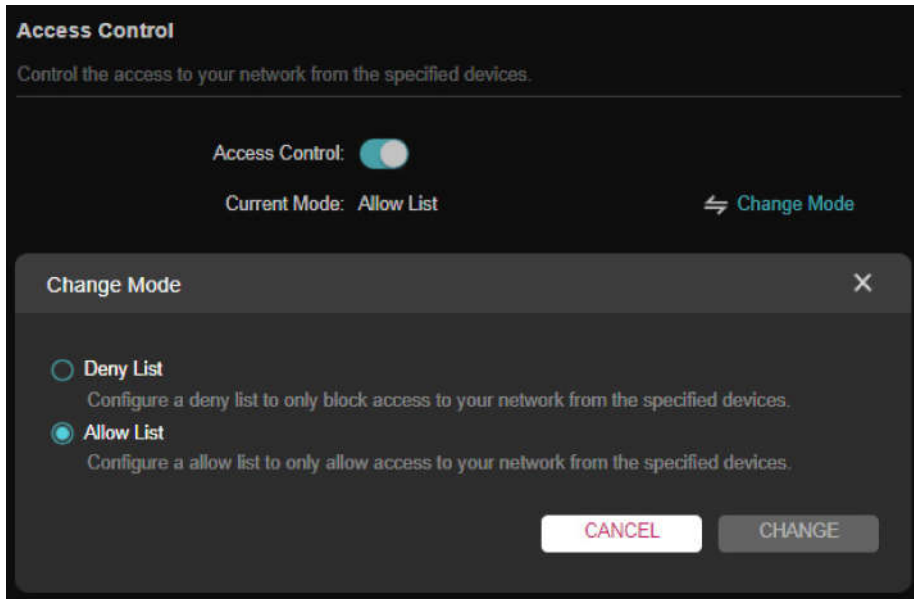


3) The **Operation Succeeded** message will appear on the screen, which means the selected devices have been successfully added to the Deny List.

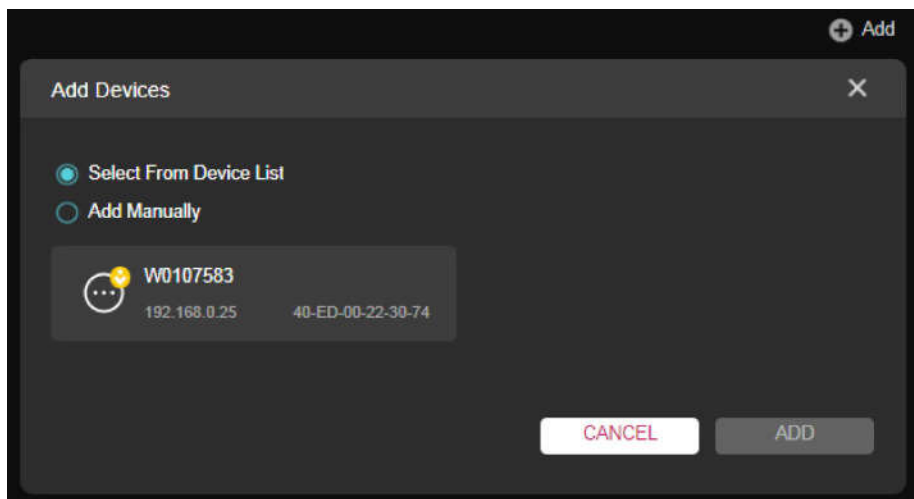
Device Type	Device Name	MAC Address	Modify
	qqq	EE-56-58-76-68-67	

To allow specific device(s):

1) Select **Allow List** and click **SAVE**.



- 2) Your own device is in the Allow List by default and cannot be deleted. Click **+Add** to add other devices to the Allow List.



- 3) The **Operation Succeeded** message will appear on the screen, which means the selected devices have been successfully added to the Allow List.

Device Type	Device Name	MAC Address	Modify
	ttt	E6-67-58-79-D5-78	
	W0107583	40-ED-00-22-30-74	

Done!

Now you can block or allow specific client devices to access your network (via wired or wireless) using the [Allow List](#) or [Deny List](#).

13.3. IP & MAC Binding

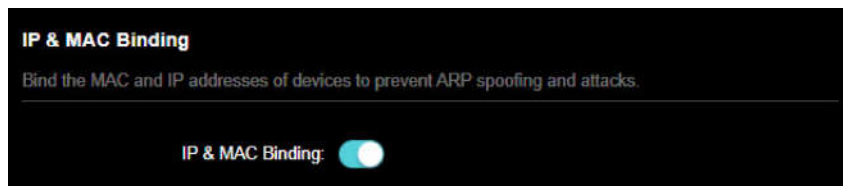
IP & MAC Binding, namely, ARP (Address Resolution Protocol) Binding, is used to bind network device's IP address to its MAC address. This will prevent ARP Spoofing and other ARP attacks by denying network access to an device with matching IP address in the Binding list, but unrecognized MAC address.

I want to:

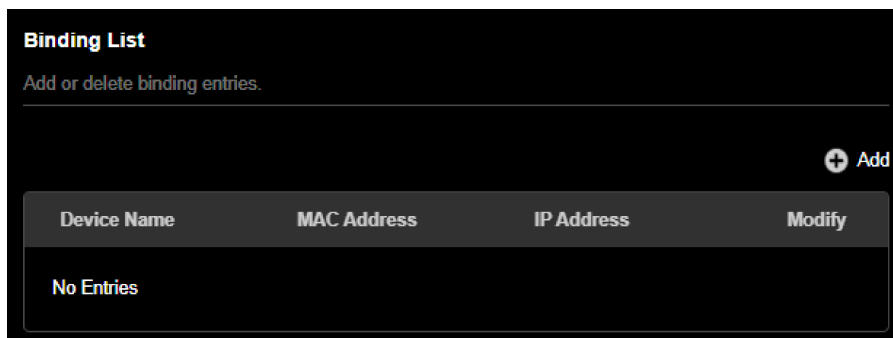
Prevent ARP spoofing and ARP attacks.

How can I do that?

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [Security](#) > [IP & MAC Binding](#).
3. Enable [IP & MAC Binding](#).



4. Bind your device(s) according to your need.
 - 1) Click [+ Add](#) in the [Binding List](#) section.



- 2) To bind the connected devices, click [VIEW CONNECTED DEVICES](#) and select the device you want to bind. The [MAC Address](#) and [IP Address](#) fields will be automatically filled in. To bind the unconnected devices, enter the [MAC Address](#) and [IP Address](#) that you want to bind.

The screenshot shows a dark-themed dialog box titled "Add Binding Entry" with a close button (X) in the top right corner. Inside the dialog, there is a "MAC Address:" label followed by a text input field containing five dashes. Below this is a blue button labeled "VIEW CONNECTED DEVICES". Underneath is an "IP Address:" label followed by an empty text input field. At the bottom right, there are two buttons: a white "CANCEL" button and a blue "SAVE" button.

3) Click **SAVE**.

Done!

Now you don't need to worry about ARP spoofing and ARP attacks!

13.4. ALG

ALG allows customized 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 router, since some voice and video communication applications do not work well with SIP ALG.

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

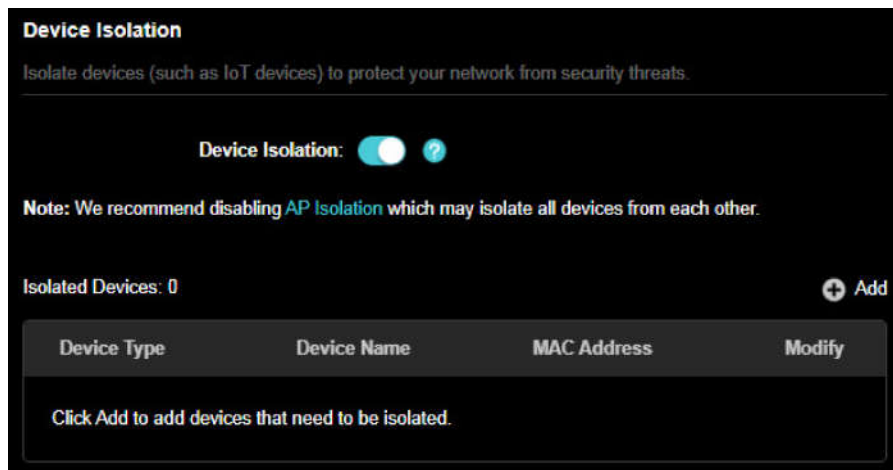
The screenshot displays the "ALG" configuration page. At the top, it says "ALG" and "Check the ALG (Application Layer Gateway) settings. It is recommended to keep them as default." Below this, there is a list of settings, each with a toggle switch that is currently turned on (indicated by a blue circle):

- PPTP Passthrough:
- L2TP Passthrough:
- IPSec Passthrough:
- FTP ALG:
- TFTP ALG:
- RTSP ALG:
- H323 ALG:
- SIP ALG:

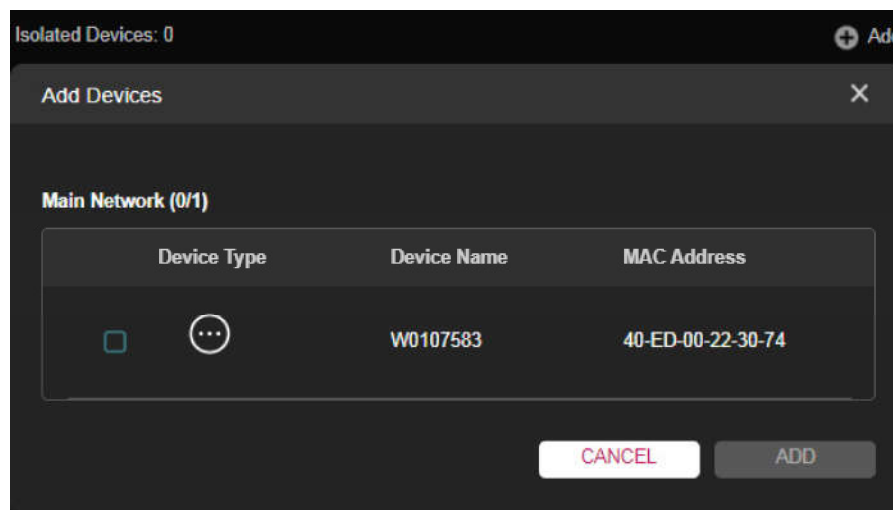
13.5. Device Isolation

Some devices, such as IoT devices, are vulnerable to security threats. To keep your important devices and data safe, you can isolate these devices to protect your network from being infected.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > Security > Device Isolation**. Enable **Device Isolation**.



3. Click **+Add** to add your IoT devices.



Done!

While isolated, isolated devices (these devices) can still access the internet and communicate with other isolated devices. However, isolated devices (these devices) cannot transfer data with devices on your home, including managing gateway devices, accessing USB devices, etc.

Chapter 14

NAT Forwarding

The router'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 router 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 router 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:

- [Share Local Resources on the Internet by Port Forwarding](#)
- [Open Ports Dynamically by Port Triggering](#)
- [Make Applications Free from Port Restriction by DMZ](#)
- [Make Xbox Online Games Run Smoothly by UPnP](#)

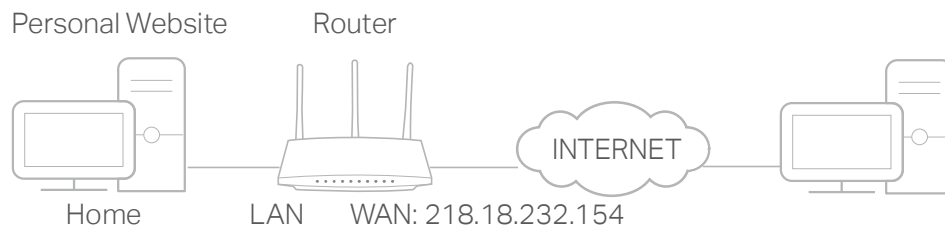
14. 1. Share Local Resources on the Internet by Port Forwarding

When you build up a server on the local network and want to share it on the internet, Port Forwarding can realize the service and provide it to internet users. At the same time Port Forwarding can keep the local network safe as other services are still invisible from the internet.

Port Forwarding can be used for setting up public services on your local network, such as HTTP, FTP, DNS, POP3/SMTP and Telnet. Different services use different service ports. Port 80 is used in HTTP service, port 21 in FTP service, port 25 in SMTP service and port 110 in POP3 service. Please verify the service port number before the configuration.

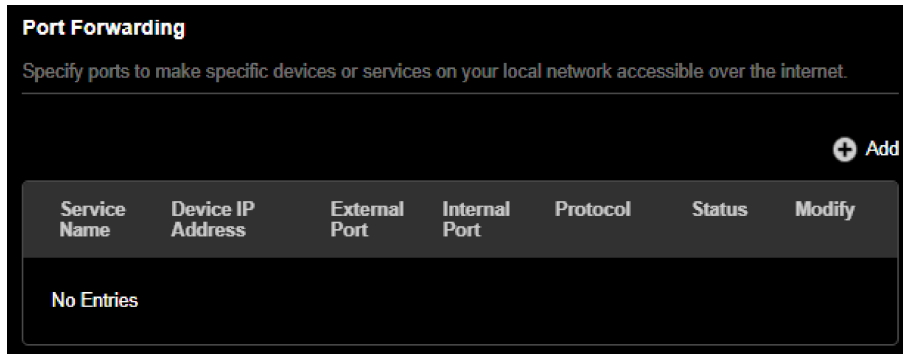
I want to:

Share my personal website I've built in local network with my friends through the internet. **For example**, the personal website has been built on my home PC (192.168.0.100). I hope that my friends on the internet can visit my website in some way. The PC is connected to the router with the WAN IP address 218.18.232.154.



How can I do that?

1. Assign a static IP address to your PC, for example 192.168.0.100.
2. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
3. Go to **Advanced > NAT Forwarding > Port Forwarding**.
 1. Click **+Add**.



4. Click [VIEW COMMON SERVICES](#) and select **HTTP**. The **External Port**, **Internal Port** and **Protocol** will be automatically filled in.
5. Click [VIEW CONNECTED DEVICES](#) and select your home PC. The **Device IP Address** will be automatically filled in. Or enter the PC's IP address 192.168.0.100 manually in the **Device IP Address** field.
6. Click [SAVE](#).

Tips:

- It is recommended to keep the default settings of **Internal Port** and **Protocol** if you are not clear about which port and protocol to use.
- If the service you want to use is not in the common services list, you can enter the corresponding parameters manually. You should verify the port number that the service needs.

- You can add multiple port forwarding rules if you want to provide several services in a router. Please note that the [External Port](#) should not be overlapped.

Done!

Users on the internet can enter [http:// WAN IP](#) (in this example: [http:// 218.18.232.154](#)) to visit your personal website.

Tips:

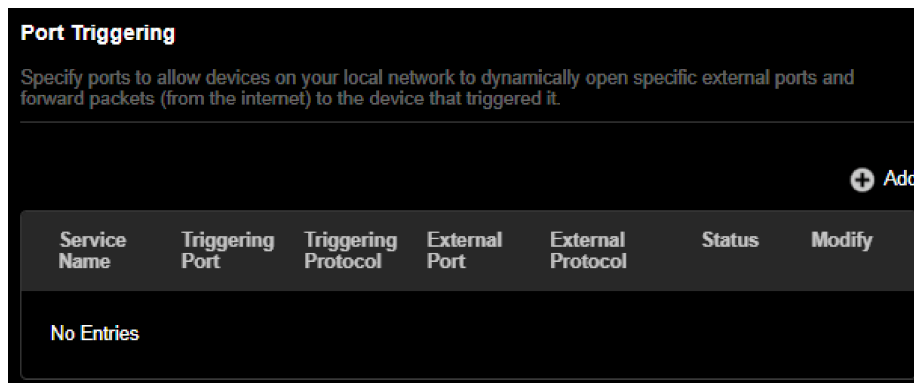
- The WAN IP should be a public IP address. For the WAN IP is assigned dynamically by the ISP, it is recommended to apply and register a domain name for the WAN referring to [Set Up a Dynamic DNS Service Account](#). Then users on the internet can use [http:// domain name](#) to visit the website.
- If you have changed the default [External Port](#), you should use [http:// WAN IP: External Port](#) or [http:// domain name: External Port](#) to visit the website.

14. 2. 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 router can record the IP address of the host. When the data from the internet return to the external ports, the router 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:

- Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
- Go to [Advanced > NAT Forwarding > Port Triggering](#) and click [+Add](#).



- Click [VIEW COMMON SERVICES](#), 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.

4. Click **SAVE**.

📌 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.

14.3. 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.

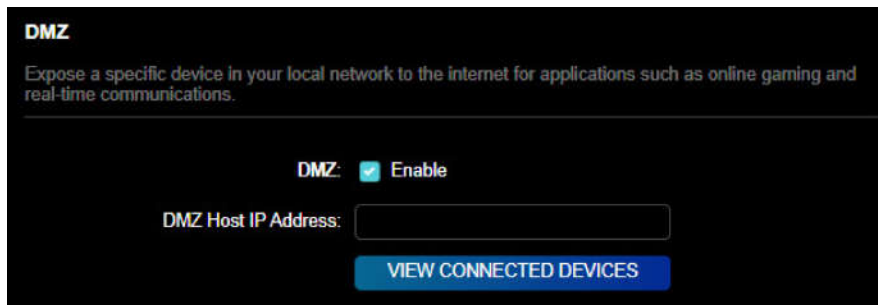
I want to:

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 192.168.0.100.
2. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
3. Go to [Advanced](#) > [NAT Forwarding](#) > [DMZ](#) and tick to enable DMZ.
4. Click [VIEW CONNECTED DEVICES](#) and select your PC. The [Device IP Address](#) will be automatically filled in. Or enter the PC's IP address 192.168.0.100 manually in the [DMZ Host IP Address](#) field.



5. 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.

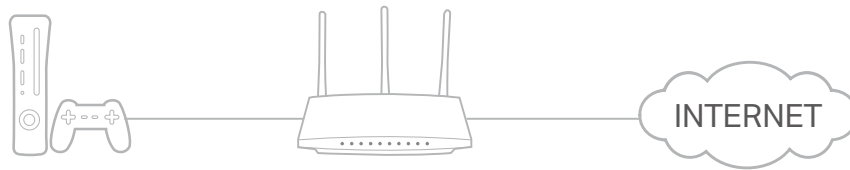
14.4. Make Xbox Online Games Run Smoothly by UPnP

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:

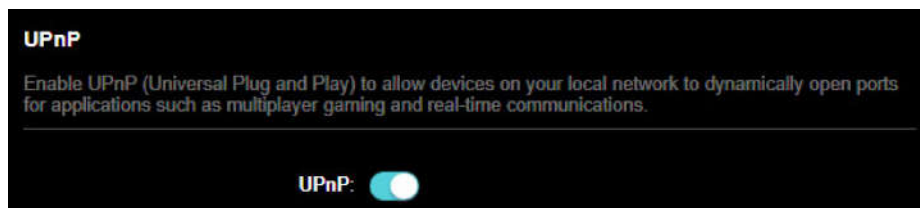
- UPnP is enabled by default in this router.
- Only the application supporting UPnP protocol can use this feature.
- UPnP feature needs the support of operating system (e.g. Windows Vista/ Windows 7/ Windows 8, etc. Some of operating system need to install the UPnP components).

[For example](#), when you connect your Xbox to the router which has connected to the internet to play online games, UPnP will send request to the router 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>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced** > **NAT Forwarding** > **UPnP** and toggle on or off according to your needs.



Chapter 15

VPN Server&Client

The router 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 router 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.

L2TP/IPSec VPN is more secure but slower than PPTP VPN, and may have trouble getting around firewalls.

WireGuard VPN is a secure, fast and modern VPN protocol. It is based on the UDP protocol and uses modern encryption algorithms to improve work efficiency.

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

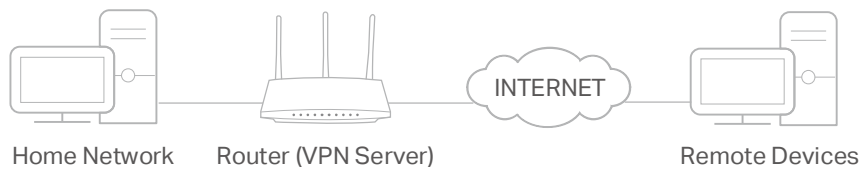
This chapter contains the following sections:

- [Use OpenVPN to Access Your Home Network](#)
- [Use PPTP VPN to Access Your Home Network](#)
- [Use L2TP/IPSec VPN to Access Your Home Network](#)
- [Use WireGuard VPN to Access Your Home Network](#)
- [Use VPN Client to Access a Remote VPN Server](#)

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 router, 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 Router

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

OpenVPN
Set up an OpenVPN for secure, remote access to your network.

Note: No certificate has been created. Generate one below before enabling OpenVPN.

OpenVPN: Enable

Service Type: UDP TCP

Service Port:

VPN Subnet:

Netmask:

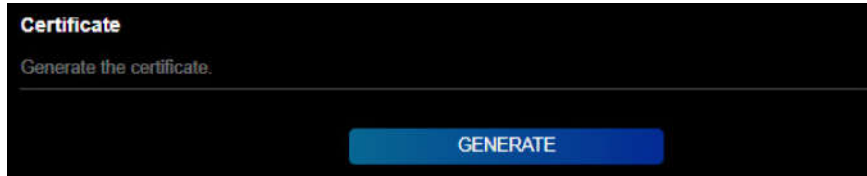
Client Access: ▼

Note:

- Before you enable VPN Server, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router'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.

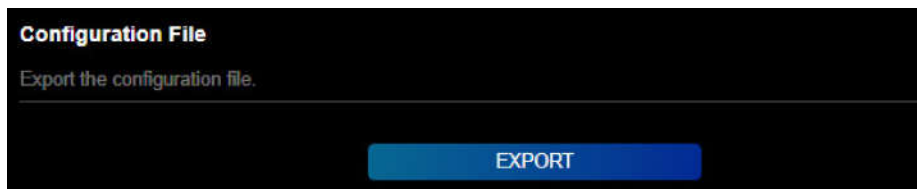
3. Select the **Service Type** (communication protocol) for OpenVPN Server: UDP, TCP.
4. Enter a VPN **Service Port** to which a VPN device connects, and the port number should be between 1024 and 65535.
5. In the **VPN Subnet/Netmask** fields, enter the range of IP addresses that can be leased to the 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.



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 router.



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 router. 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 router 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 router, 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 Router

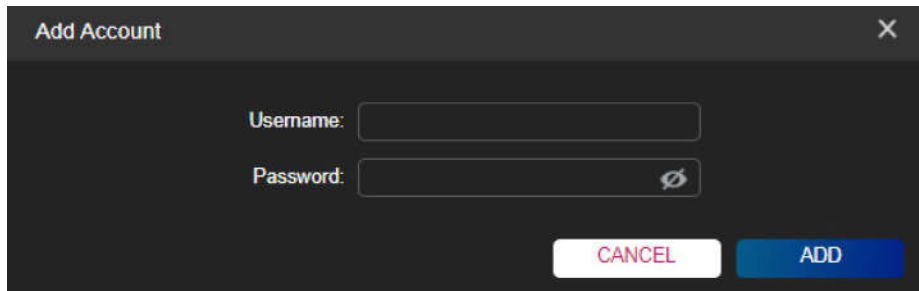
1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > VPN Server > PPTP**, and tick the **Enable** box of **PPTP**.

Note: Before you enable **VPN Server**, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router'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. Set the PPTP connection permission according to your needs.
 - Select **Allow Samba (Network Place) access** to allow your VPN device to access your local Samba server.
 - Select **Allow NetBIOS passthrough** to allow your VPN device to access your Samba server using NetBIOS name.
 - Select **Allow Unencrypted connections** to allow unencrypted connections to your VPN server.
5. Click **SAVE**.
6. Configure the PPTP VPN connection account for the remote device. You can create up to 16 accounts.

Username	Password	Modify
No Entries		

- 1) Click **Add**.
- 2) Enter the **Username** and **Password** to authenticate devices to the PPTP VPN Server.

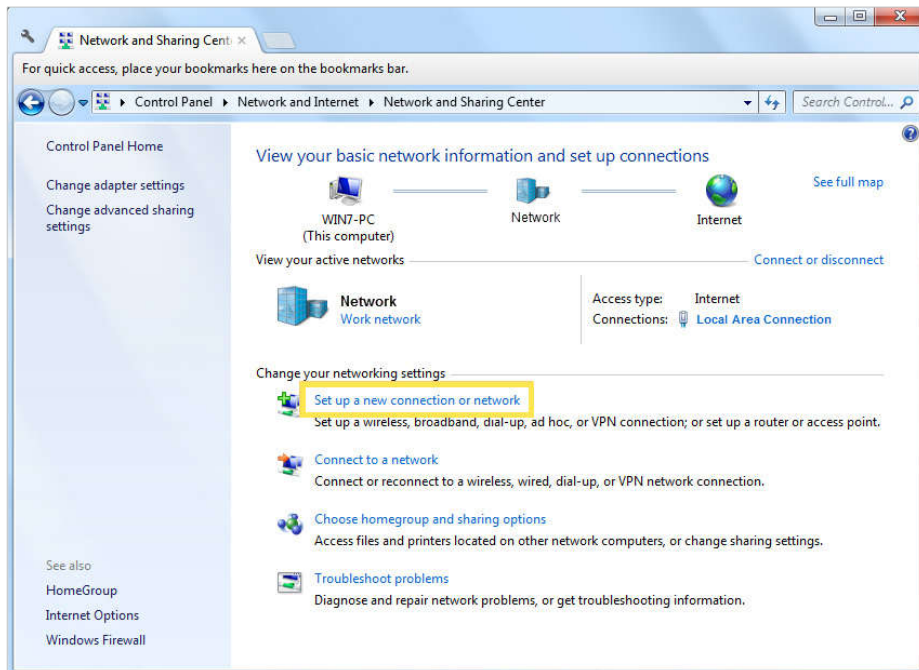


3) Click [ADD](#).

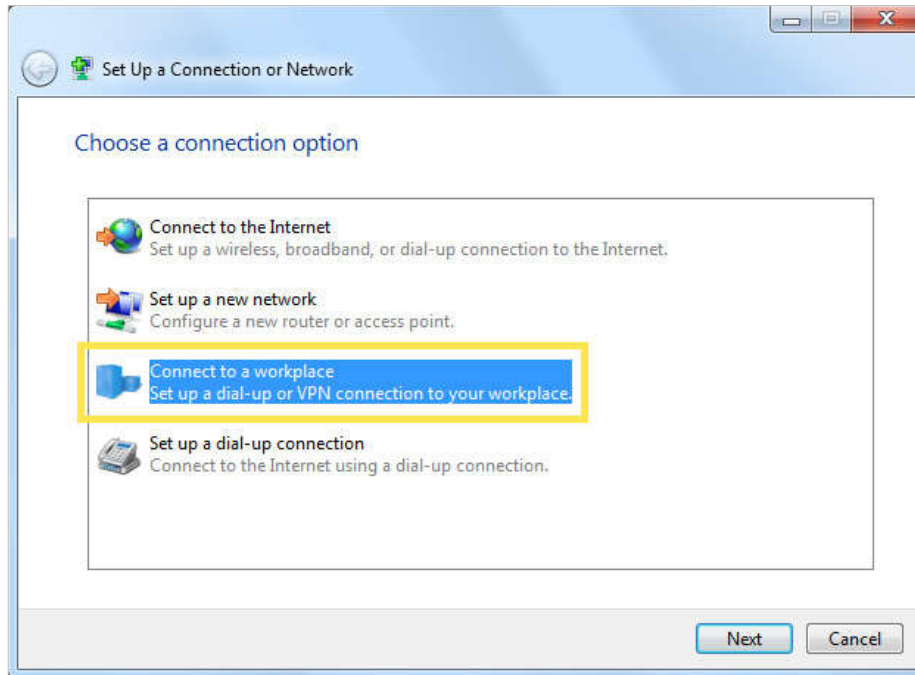
Step 2. Configure PPTP VPN Connection on Your Remote Device

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.

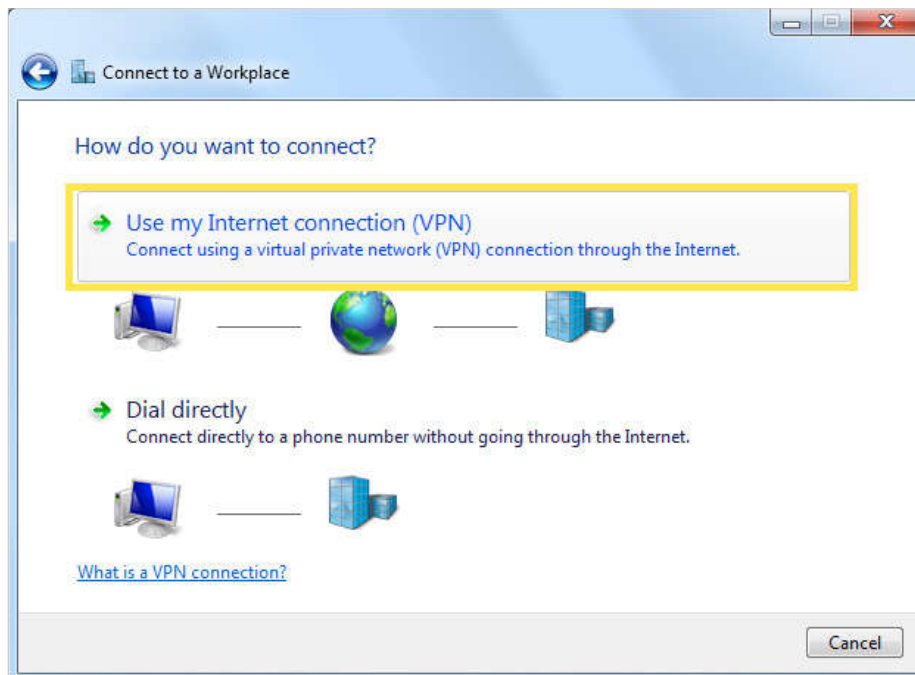
1. Go to [Start > Control Panel > Network and Internet > Network and Sharing Center](#).
2. Select [Set up a new connection or network](#).



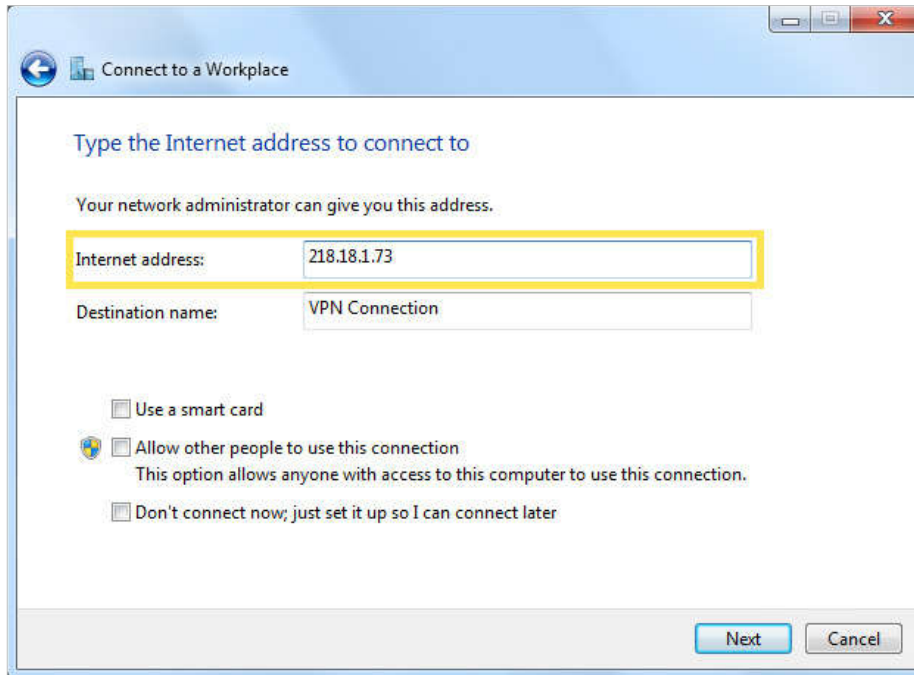
3. Select [Connect to a workplace](#) and click [Next](#).



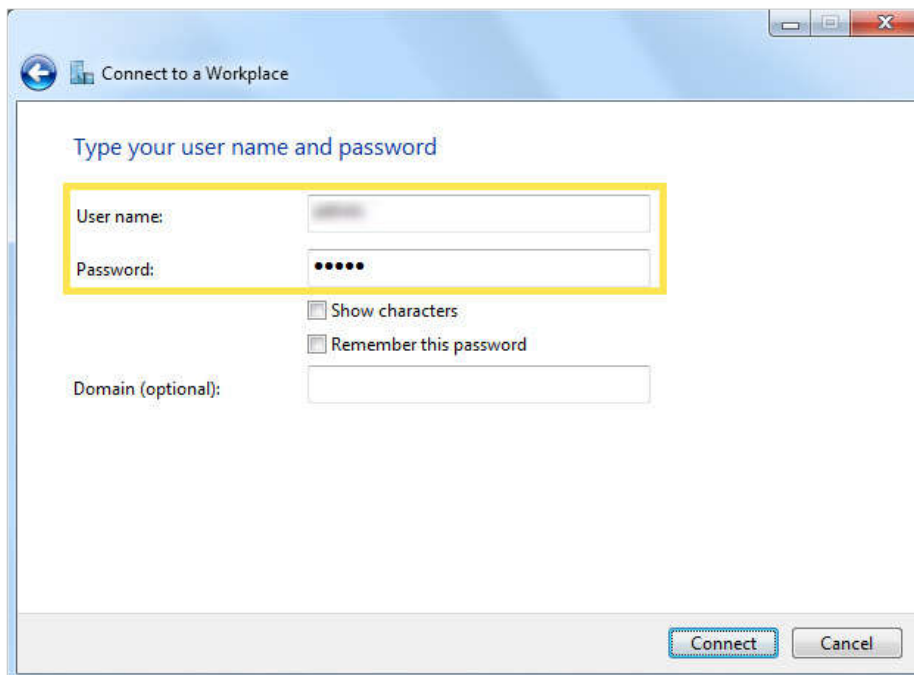
4. Select Use my Internet connection (VPN).



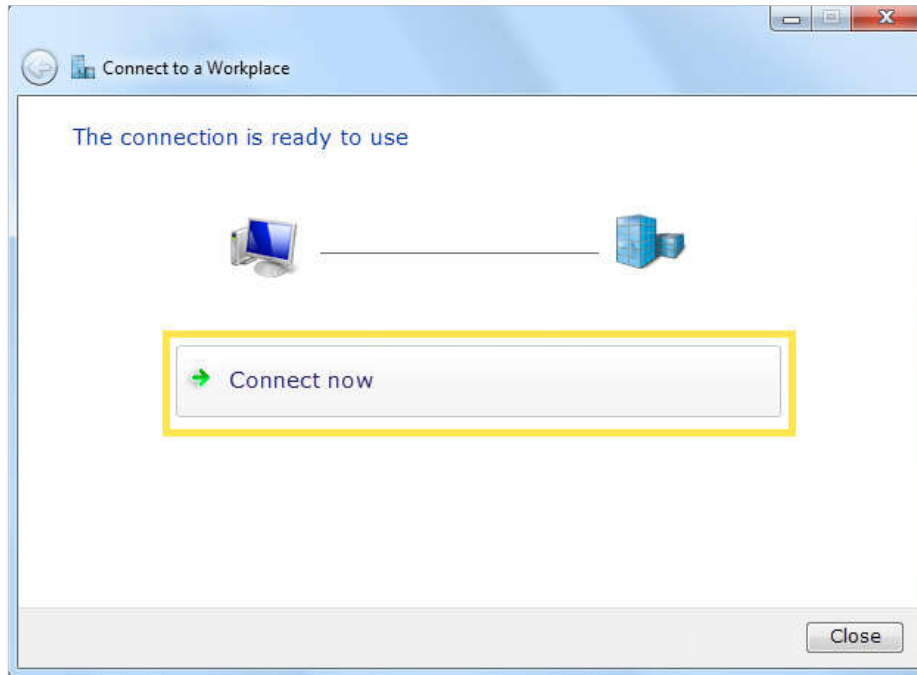
5. Enter the internet IP address of the router (for example: 218.18.1.73) in the Internet address field. Click Next.



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



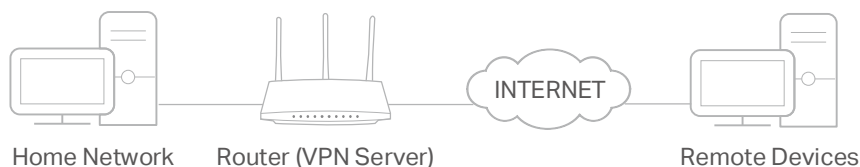
7. Click **Connect Now** when the VPN connection is ready to use.



15.3. Use L2TP/IPSec VPN to Access Your Home Network

L2TP/IPSec VPN Server is used to create a L2TP/IPSec VPN connection for remote devices to access your home network.

To use the VPN feature, you need to set up L2TP/IPSec VPN Server on your router, and configure the L2TP/IPSec connection on remote devices. Please follow the steps below to set up the L2TP/IPSec VPN connection.



Step 1. Set up L2TP/IPSec VPN Server on Your Router

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > VPN Server > L2TP/IPSec**, and enable **L2TP/IPSec**.

Note:

- Firmware update may be required to support L2TP/IPSec VPN Server.
- Before you enable **VPN Server**, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router's WAN port and synchronize your **System Time** with internet.

L2TP/IPSec
Set up a L2TP/IPSec VPN and accounts for quick, remote access to your network.

L2TP/IPSec: Enable

Client IP Address: -
(up to 10 clients)

IPSec Encryption:

IPSec Pre-Shared Key:

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 L2TP/IPSec VPN server.
4. Keep **IPSec Encryption** as **Encrypted** and create an **IPSec Pre-Shared Key**.
5. Click **SAVE**.
6. Configure the L2TP/IPSec VPN connection account for the remote device. You can create up to 16 accounts.

Account List
Configure accounts (up to 16) that can be used by remote clients to connect to the VPN server.

[+ Add](#)

Username	Password	Modify
No Entries		

- 4) Click **Add**.
- 5) Enter the **Username** and **Password** to authenticate devices to the L2TP/IPSec VPN Server.

Add Account ✕

Username:

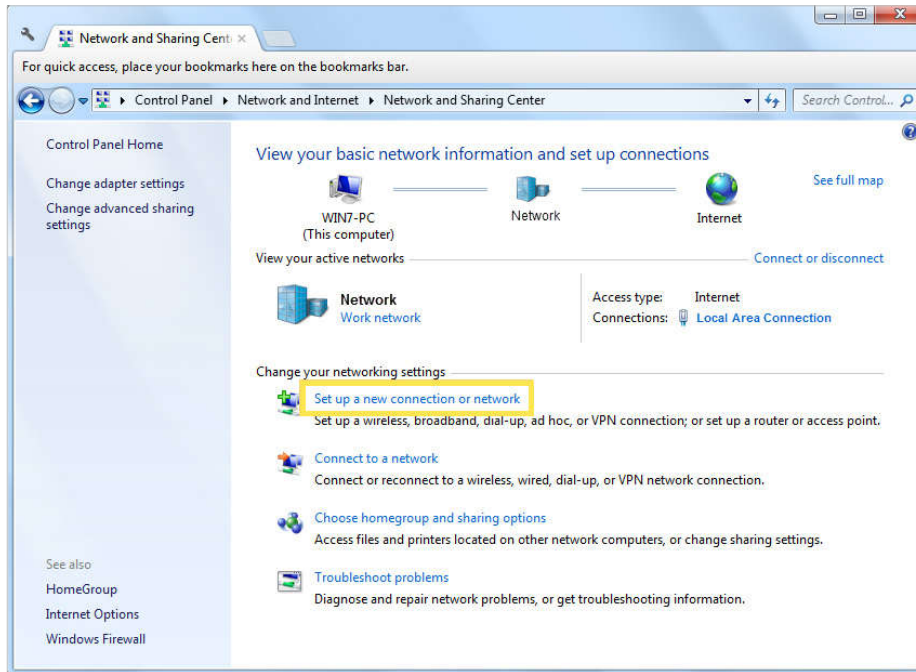
Password:

- 6) Click **ADD**.

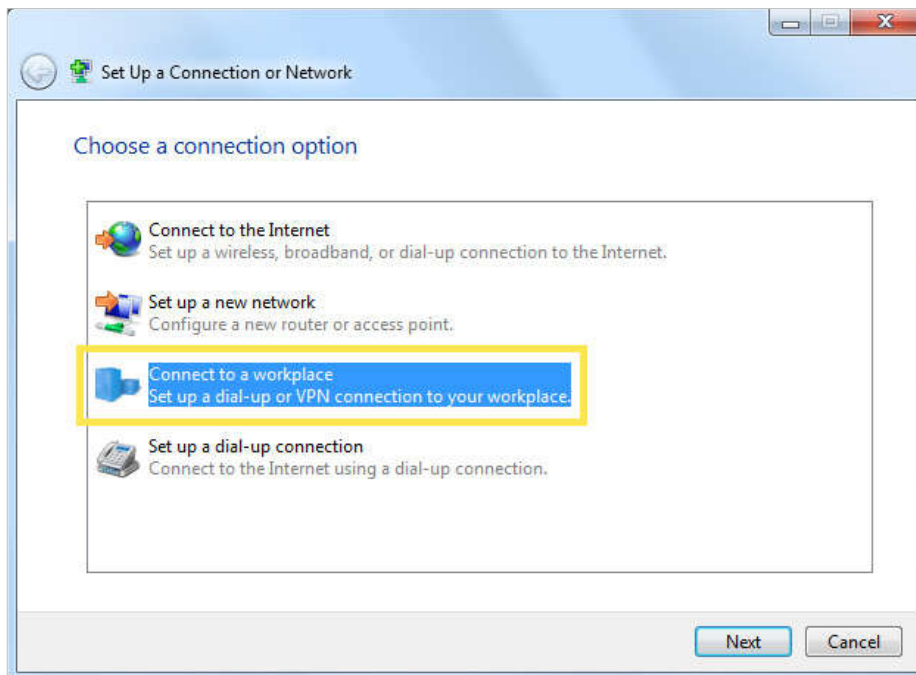
Step 2. Configure L2TP/IPSec VPN Connection on Your Remote Device

The remote device can use the Windows or Mac OS built-in L2TP/IPSec software or a third-party L2TP/IPSec software to connect to L2TP/IPSec Server. Here we use the [Windows built-in L2TP/IPSec software](#) as an example.

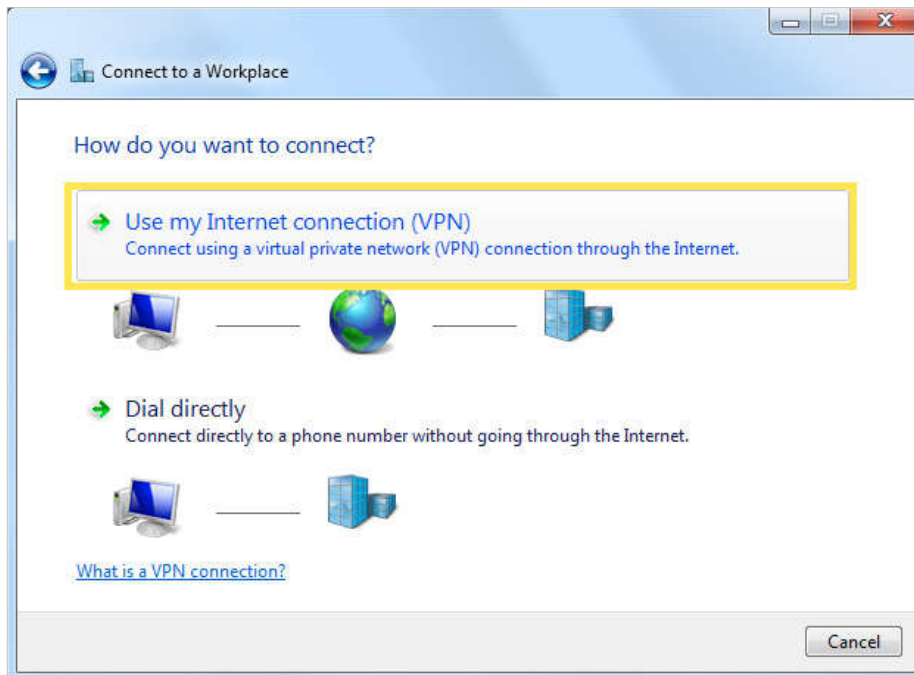
1. Go to [Start > Control Panel > Network and Internet > Network and Sharing Center](#).
2. Select [Set up a new connection or network](#).



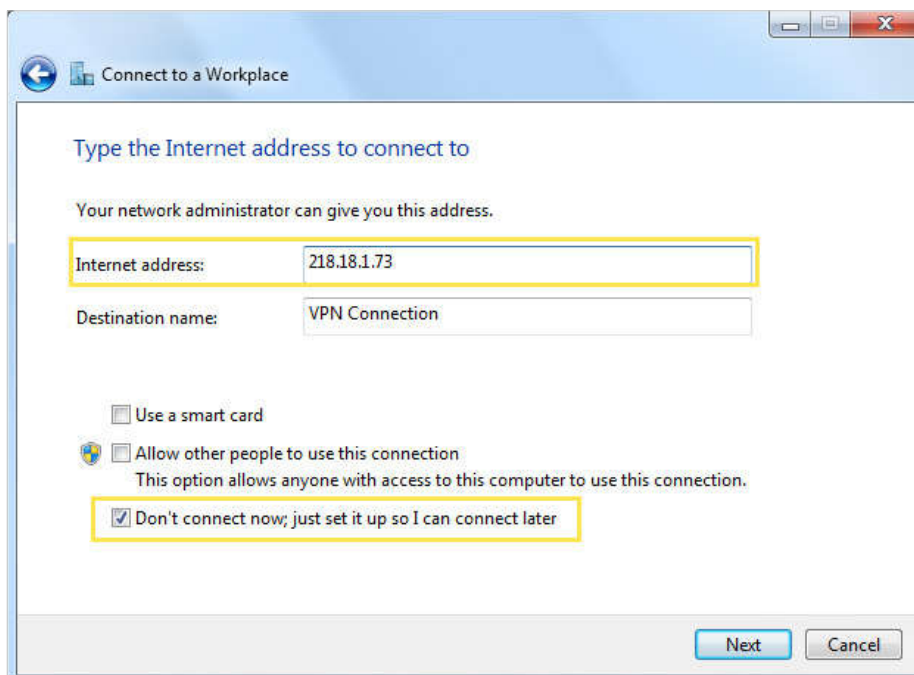
3. Select [Connect to a workplace](#) and click [Next](#).



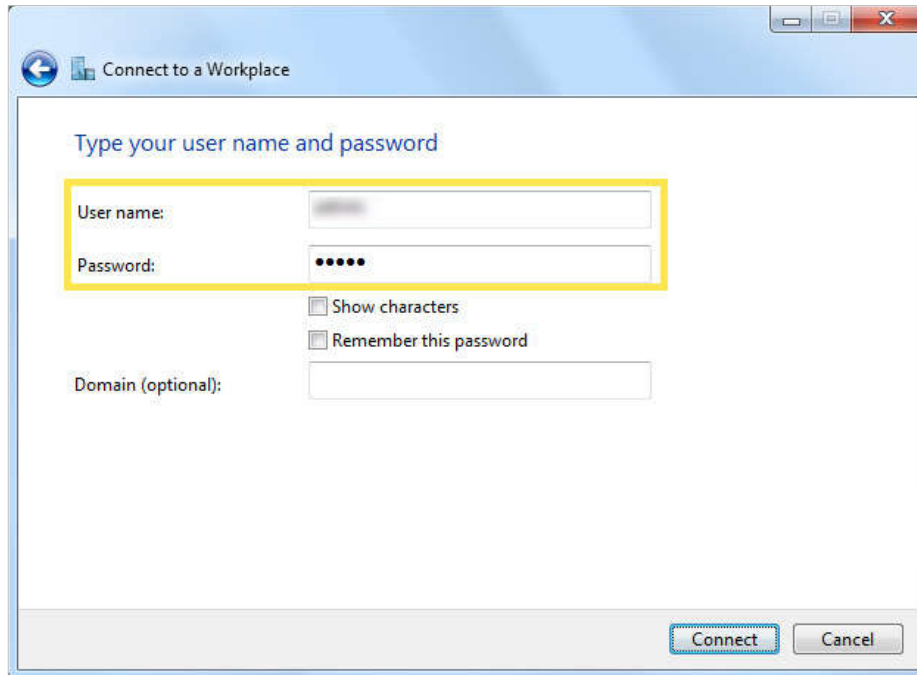
4. Select **Use my Internet connection (VPN)**.



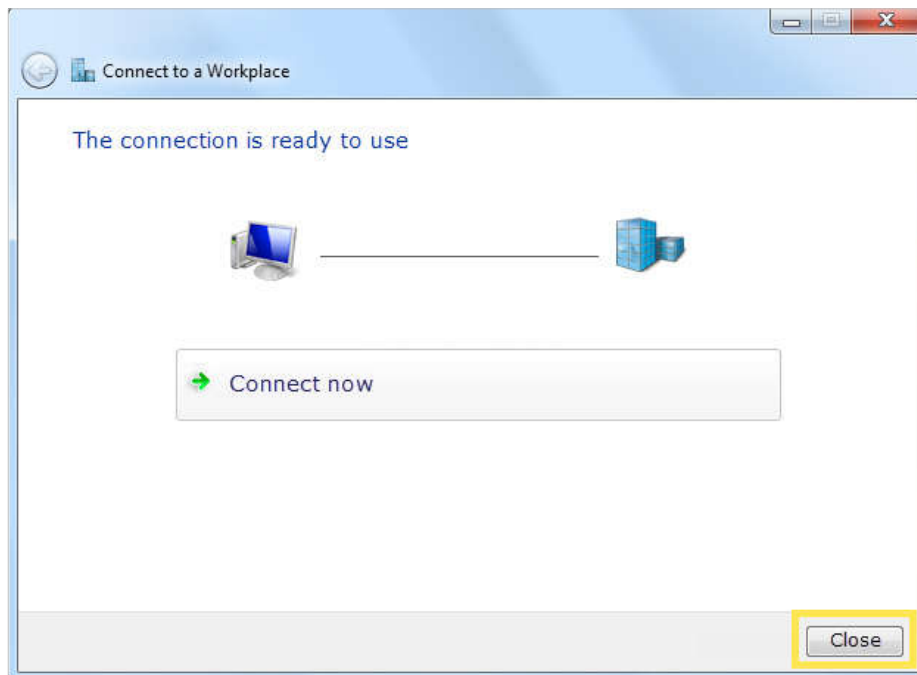
5. Enter the internet IP address of the router (for example: 218.18.1.73) in the **Internet address** field, and select the checkbox **Don't connect now; just set it up so I can connect later**. Click **Next**.



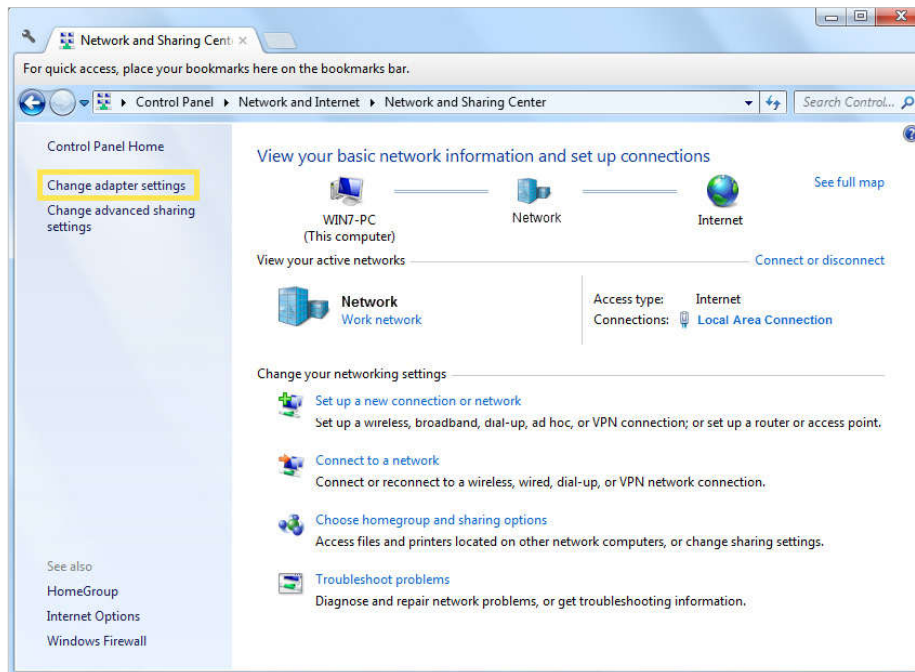
6. Enter the **User name** and **Password** you have set for the L2TP/IPSec VPN server on your router, and click **Connect**.



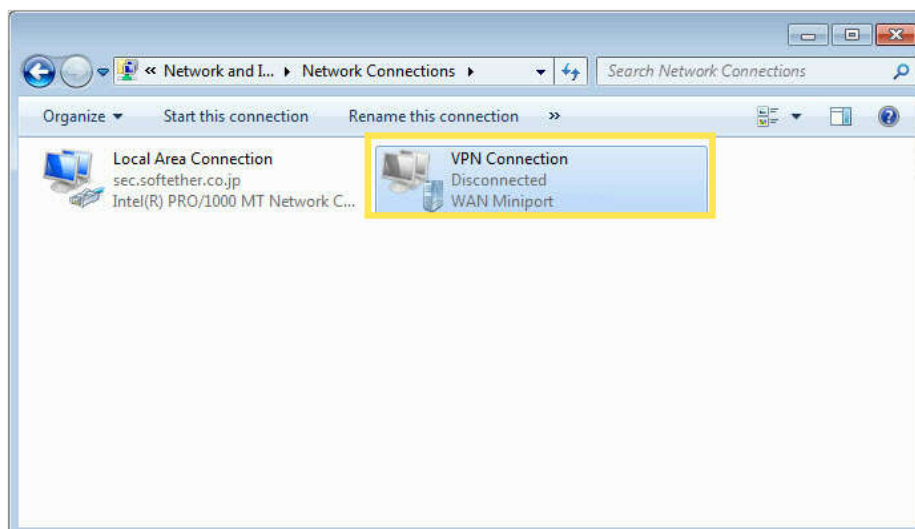
7. Click [Close](#) when the VPN connection is ready to use



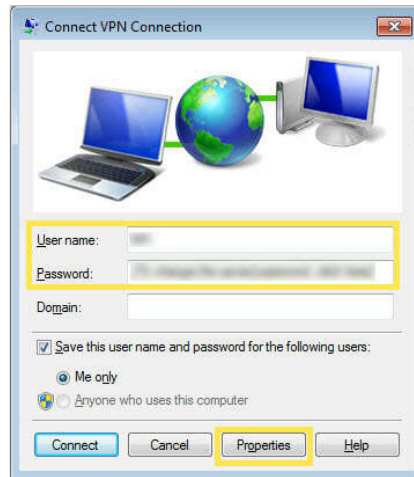
8. Go to [Network and Sharing Center](#) and click [Change adapter settings](#).



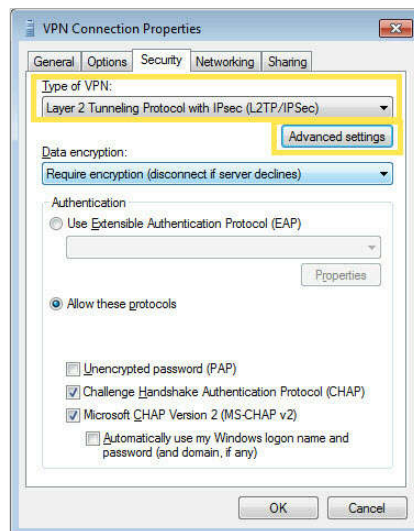
9. Find the VPN connection you created, then double-click it.



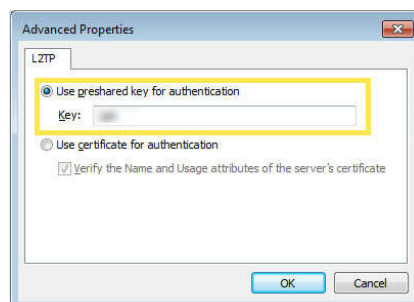
10. Enter the **User name** and **Password** you have set for the L2TP/IPSec VPN server on your router, and click **Properties**.



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 L2TP/IPSec VPN server on your router. Then click **OK**.



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



15.4. Use WireGuard VPN to Access Your Home Network

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

Step 1. Set up WireGuard VPN Server on Your Router

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

WireGuard

Set up a WireGuard VPN and accounts for quick, remote and secure access to your network.

WireGuard: **Enable**

Tunnel IP Address:

Listen Port:
(1024-65535)

Client Access: ▼

▼ **Advanced Settings**

DNS: **Enable**

Persistent Keepalive:

Private Key: S1aWc23zG4PgqzrE3GG3WJnXjeQ2HPfKG1WYbFV5Eo=

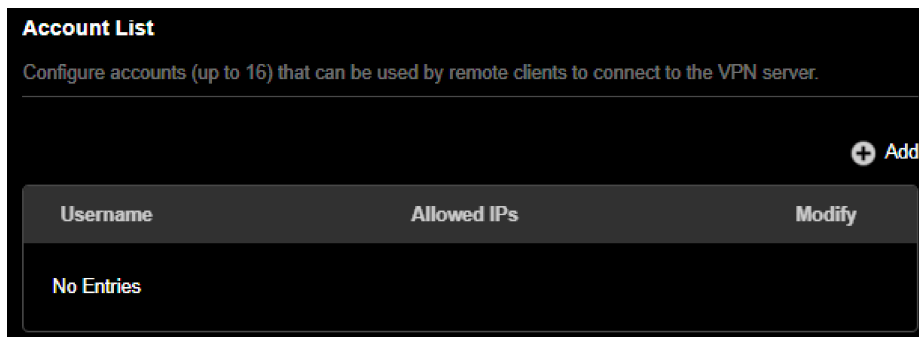
Public Key: WLhXkYSdE7PBS57WbimwfDG8tTu3o2zR1cqbQcYX3Y=

[RENEW KEY](#)

3. Set the [Tunnel IP Address](#) and [Listen Port](#). Do NOT change it unless necessary.
4. 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.
5. (Optional) Click [Advanced Settings](#) to display more settings. If [DNS](#) is turned on, the router will become the DNS server of the VPN client that establishes a connection with it. Change the [Persistent Keepalive](#) time (25 seconds by default) to send out heartbeat regularly, you can also click [RENEW KEY](#) to update the private key and public key.

Step 2. Create accounts that can be used by remote clients to connect to the VPN server.

1. Locate the [Account List](#) section. Click [Add](#) to create an account.



2. Give a name to this account.
3. Enter the address of the virtual interface assigned to this account. Do NOT change it unless necessary.
4. Traffic sent from the WireGuard VPN client to the allowed IPs (client) will be transmitted through the tunnel. By default, all network traffic from clients will be transmitted through the tunnel. Do NOT change it unless necessary.

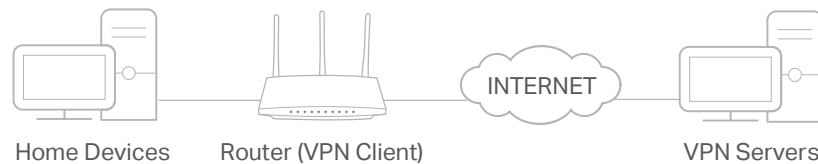
5. Traffic sent from the WireGuard VPN server to the allowed IPs (server) will be transmitted through the tunnel. Do NOT change it unless necessary.
6. Enable or disable pre-shared key.
7. Click **SAVE**.

Note: One account can only be used by one WireGuard VPN client at the same time to connect to the WireGuard VPN server.

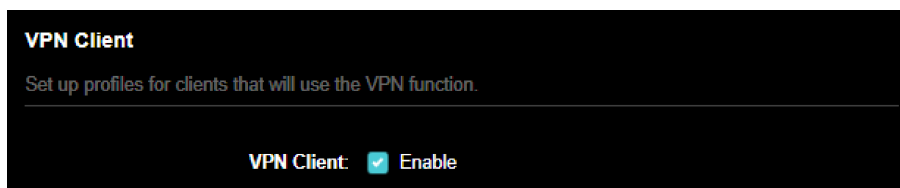
15.5. Use VPN Client to Access a Remote VPN Server

VPN Client is used to create VPN connections for devices in your home network to access a remote VPN server.

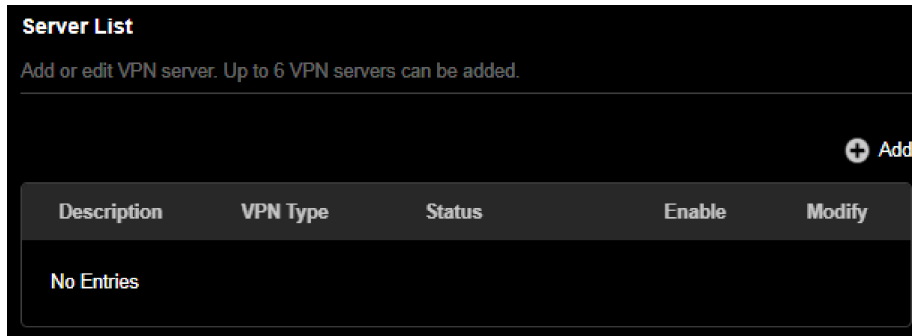
To use the VPN feature, simply configure a VPN connection and choose your desired devices on your router, then these devices can access the remote VPN server. Please follow the steps below:



1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
 2. Go to **Advanced > VPN Client**.
- Note:** Firmware update may be required to support VPN Client.
3. Enable **VPN Client**, then save the settings.



4. Add VPN servers, and enable the one you need.
 - 1) In the **Server List** section, click **Add**.
 - 2) Specify a description for the VPN, and choose the VPN type.

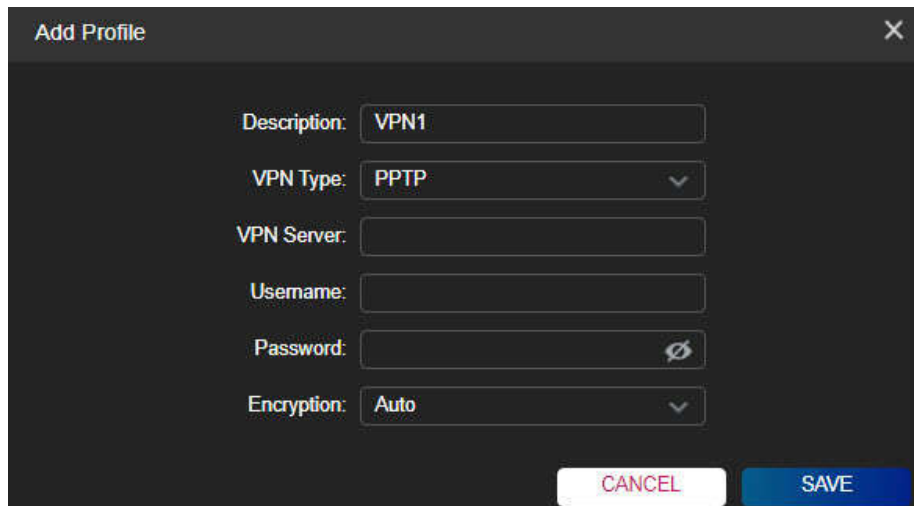


3) Enter the VPN information provided by your VPN provider.

- **OpenVPN:** Enter the VPN username and password if required by your VPN provider, otherwise simply leave them empty. Then import the configuration file provided by your VPN provider.

Note: You can also check the box of **Import the CA file or edit the .ovpn file manually**, then upload the CA file or manually configure the settings.

- **PPTP:** Enter the VPN server address (for example: 218.18.1.73) and the VPN username and password provided by your VPN provider.

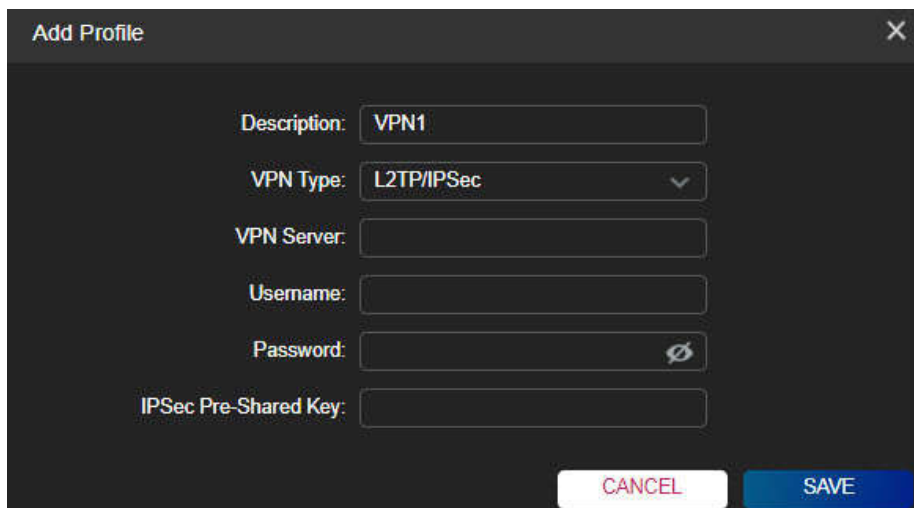


The screenshot shows a dark-themed 'Add Profile' dialog box with a close button (X) in the top right corner. The form contains the following fields:

- Description:
- VPN Type: (dropdown menu)
- VPN Server:
- Username:
- Password: (with an eye icon for visibility toggle)
- Encryption: (dropdown menu)

At the bottom right, there are two buttons: a white 'CANCEL' button and a blue 'SAVE' button.

- **L2TP/IPSec VPN:** Enter the VPN server address (for example: 218.18.1.73), VPN username and password, and IPSec pre-shared key provided by your VPN provider.



The screenshot shows a dark-themed 'Add Profile' dialog box with a close button (X) in the top right corner. The form contains the following fields:

- Description:
- VPN Type: (dropdown menu)
- VPN Server:
- Username:
- Password: (with an eye icon for visibility toggle)
- IPSec Pre-Shared Key:

At the bottom right, there are two buttons: a white 'CANCEL' button and a blue 'SAVE' button.

- **WireGuard VPN:** Give a description, and click **BROWSE** to import the WireGuard VPN server configuration. Then you will see the detailed parameters. Do NOT change the parameters unless necessary.

Add Profile
✕

Description:

VPN Type:

Import from Config File:

BROWSE

NAT: Enable

▼ Interface

Private Key:

Address:

DNS Server 1: (Optional)

DNS Server 2: (Optional)

MTU Size: bytes (Optional)

▼ Peer

Public Key:

Pre-Shared Key: (Optional)

Allowed IPs:

Endpoint Address:

Endpoint Port:

Persistent Keepalive: (Optional)

CANCEL
SAVE

- 4) Save the settings.
5. Add and manage the devices that will use the VPN function.
 - 1) In the [Device List](#) section, click [Add](#).

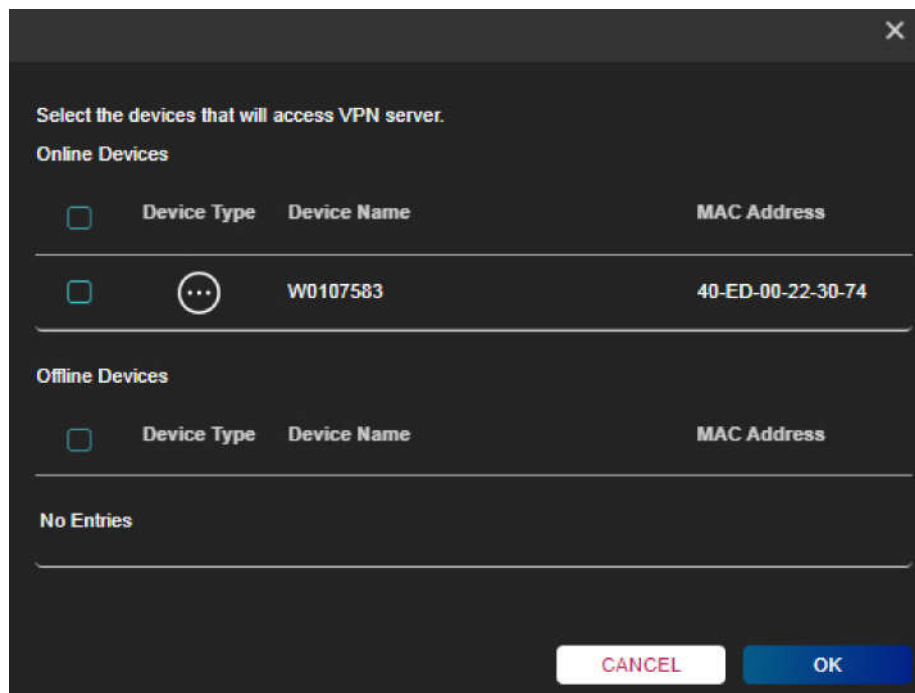
Device List

Manage devices that will use the VPN function.

+ Add

Type	Device Name	MAC Address	VPN Access	Modify
No Entries				

2) Choose and add the devices that will access the VPN server you have configured.



6. Save the settings.

Done! Now the devices you specified can access the VPN server you enabled.

Chapter 16

Customize Your Network Settings

This chapter guides you on how to configure advanced network features.

It contains the following sections:

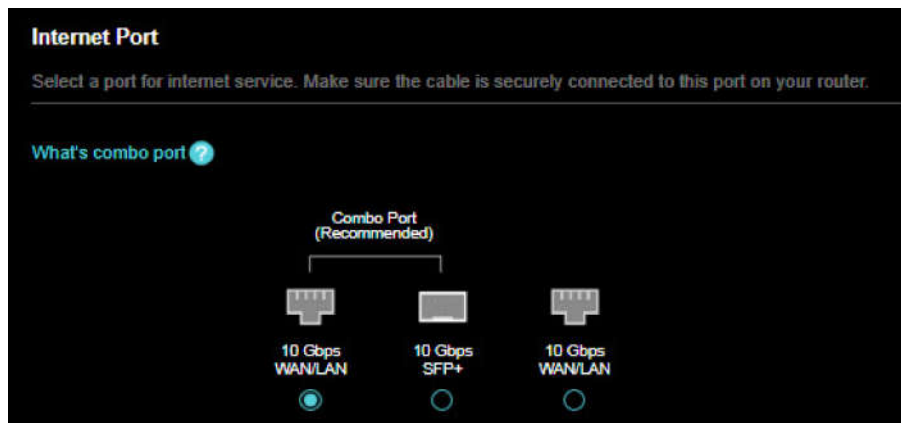
- [Change the Internet Settings](#)
- [Change the LAN Settings](#)
- [Configure to Support IPTV Service](#)
- [Specify DHCP Server Settings](#)
- [Set Up a Dynamic DNS Service Account](#)
- [Create Static Routes](#)

16.1. Change the Internet Settings

After setting up your internet, you can also easily change the internet settings if needed in the future.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [Network](#) > [Internet](#).

- **To change the internet port:**



1. Select the desired internet port. Make sure the cable is securely connected to this port on your router.
2. Click [SAVE](#).

- **To change the internet connection settings:**

Internet Connection

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

Internet Connection Type:

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

▼ Advanced Settings

DNS Address:

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0

MTU Size: bytes
(Do not change unless necessary.)

Host Name:

Get IP using Unicast DHCP

1. Select the internet connection type and configure the settings according to the information provided by your ISP.
2. Optional. Reveal the advanced settings and change the settings if needed. It's recommended to keep the default settings.
3. Click [SAVE](#).

- **To change the MAC address of the router:**

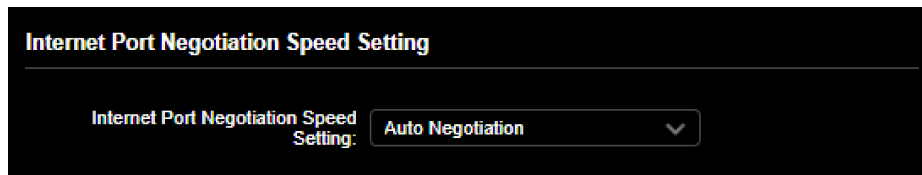
MAC Clone

Router MAC Address:

00 - 00 - ff - ff - fe - fb

You have three options, [Use Default MAC Address](#), [Clone Current Device MAC](#), [Use Custom MAC Address](#).

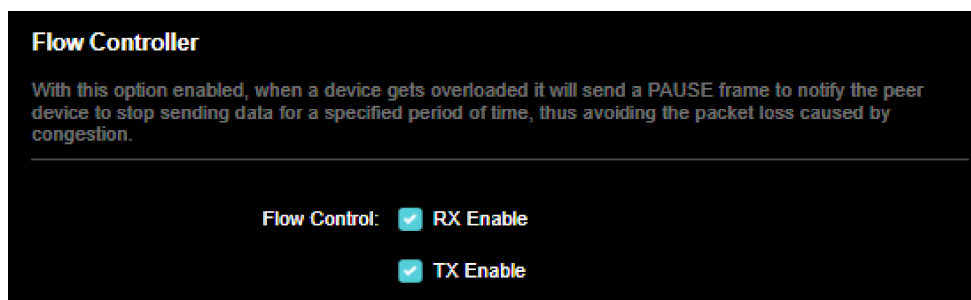
- **To change the Internet Port Negotiation Speed Setting**



You can change the internet port speed mode. [Auto Negotiation](#) is recommended.

- **To enable Flow Controller**

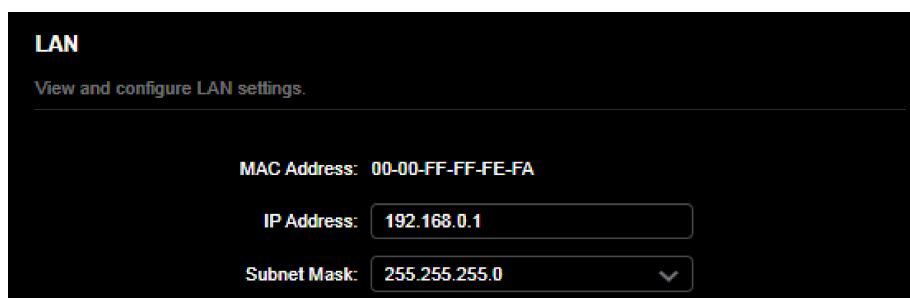
With [Flow Controller](#) enabled, when a device gets overloaded it will send a PAUSE frame to notify the peer device to stop sending data for a specified period of time, thus avoiding the packet loss caused by congestion. [Flow Controller](#) is enabled by default.



16.2. Change the LAN Settings

The router is preset with a default LAN IP 192.168.0.1, 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 on your local network or your network requires a specific IP subnet, you can change it.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [Network](#) > [LAN](#).
3. Type in a new IP Address appropriate to your needs. And leave the [Subnet Mask](#) as the default settings.



4. Click **SAVE**.

Note: If you have set the Port Forwarding, DMZ or DHCP address reservation, and the new LAN IP address is not in the same subnet with the old one, then you should reconfigure these features.

16.3. Set Up Link Aggregation

The Link Aggregation feature combines two ports together to make a single highbandwidth data path, thus sustaining a higher-speed and more stable wired network.

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

2. Go to **Advanced > Network > LAN**, and locate the **Link Aggregation** section.

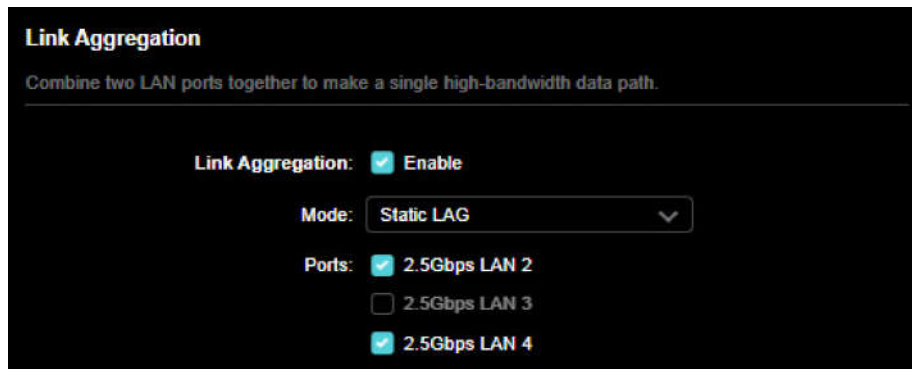
3. Enable **Link Aggregation**.

Note: To avoid LAN port conflicts, Link Aggregation and IPTV/VLAN cannot be enabled at the same time.

4. Select the **Mode** according to your need. It's recommended that you select the same link aggregation mode for both ends of the link.

- **Static LAG:** The member ports are manually added to the LAG. It is recommended for a simple home network.
- **LACP:** The router uses LACP to implement dynamic link aggregation and disaggregation by exchanging LACP packets with its peer device. LACP extends the flexibility of the LAG configuration. It is recommended for a complex network.

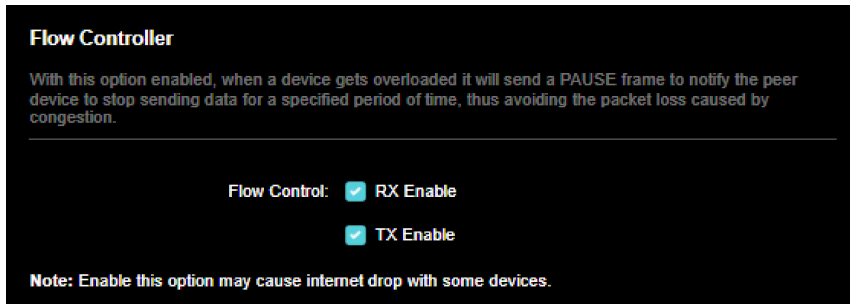
5. Select the **Ports** that Link Aggregation will take effect, and click **SAVE**.



16.4. Flow Controller

With **Flow Controller** enabled, when a device gets overloaded it will send a PAUSE frame to notify the peer device to stop sending data for a specified period of time, thus avoiding the packet loss caused by congestion.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > Network > LAN**, and locate the **Flow Controller** section.
3. **Flow Controller** is enabled by default. Please note that enable **Flow Controller** may cause internet drop with some devices.



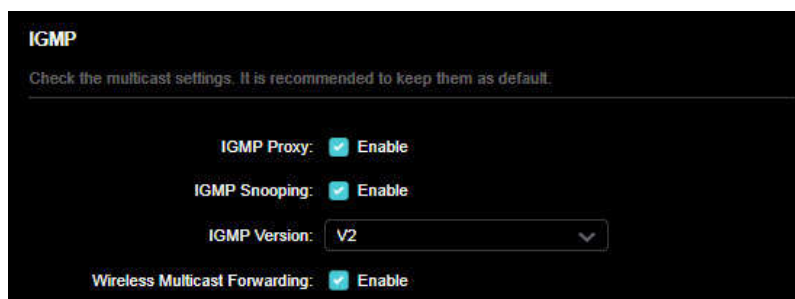
16.5. Configure to Support IPTV Service

I want to:

Configure IPTV setup to enable Internet/IPTV/Phone service provided by my internet service provider (ISP).

How can I do that?

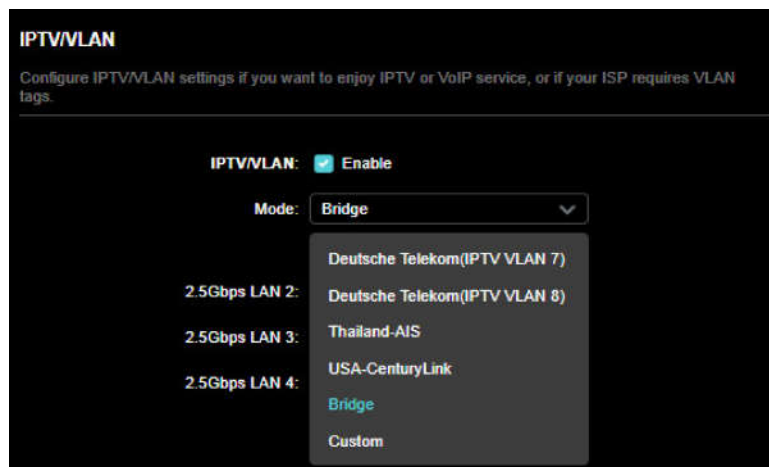
1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > Network > IPTV/VLAN**.
3. **If your ISP provides the networking service based on IGMP technology, e.g., British Telecom(BT) and Talk Talk in UK:**
 - 1) Tick the **IGMP Proxy** and **IGMP Snooping** checkbox, then select the **IGMP Version**, either V2 or V3, as required by your ISP.



- 2) Check the [Wireless Multicast Forwarding](#) status. When enabled, the multicast packets will be forwarded automatically. You are recommended to keep it as default.
- 3) Click [SAVE](#).
- 4) After configuring IGMP proxy, IPTV can work behind your router now. You can connect your set-top box to any of the router's Ethernet port.

If IGMP is not the technology your ISP applies to provide IPTV service:

- 1) Tick [Enable IPTV/VLAN](#).
- 2) Select the appropriate [Mode](#) according to your ISP.
 - Select [Bridge](#) if your ISP is not listed and no other parameters are required.
 - Select [Custom](#) if your ISP is not listed but provides necessary parameters.



- 3) After you have selected a mode, the necessary parameters, including the LAN port for IPTV connection, are predetermined. If not, select the LAN type to determine which port is used to support IPTV service.
- 4) Click [SAVE](#).
- 5) Connect the set-top box to the corresponding LAN port which is predetermined or you have specified in Step 3.

Done!

Your IPTV setup is done now! You may need to configure your set-top box before enjoying your TV.

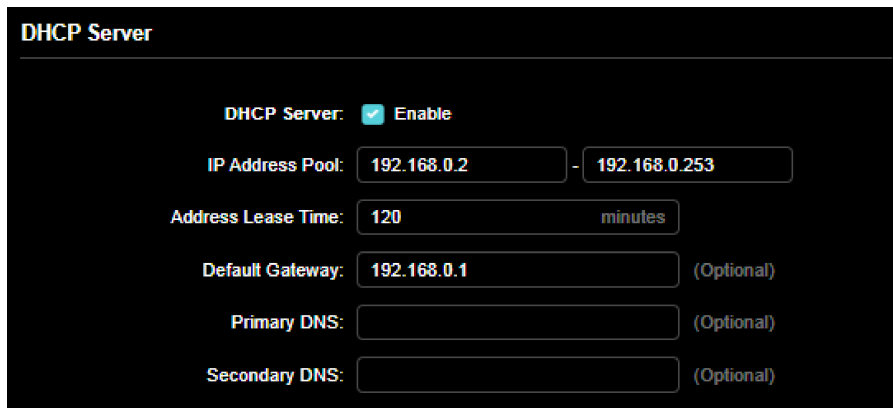
16.6. Specify DHCP Server Settings

By default, the DHCP (Dynamic Host Configuration Protocol) Server is enabled and the router acts as a DHCP server; it dynamically assigns TCP/IP parameters to client

devices from the IP Address Pool. You can change the settings of the DHCP Server if necessary, and you can reserve LAN IP addresses for specified client devices.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [Network](#) > [DHCP Server](#).

- **To specify the IP address that the router assigns:**



DHCP Server

DHCP Server: Enable

IP Address Pool: -

Address Lease Time: minutes

Default Gateway: (Optional)

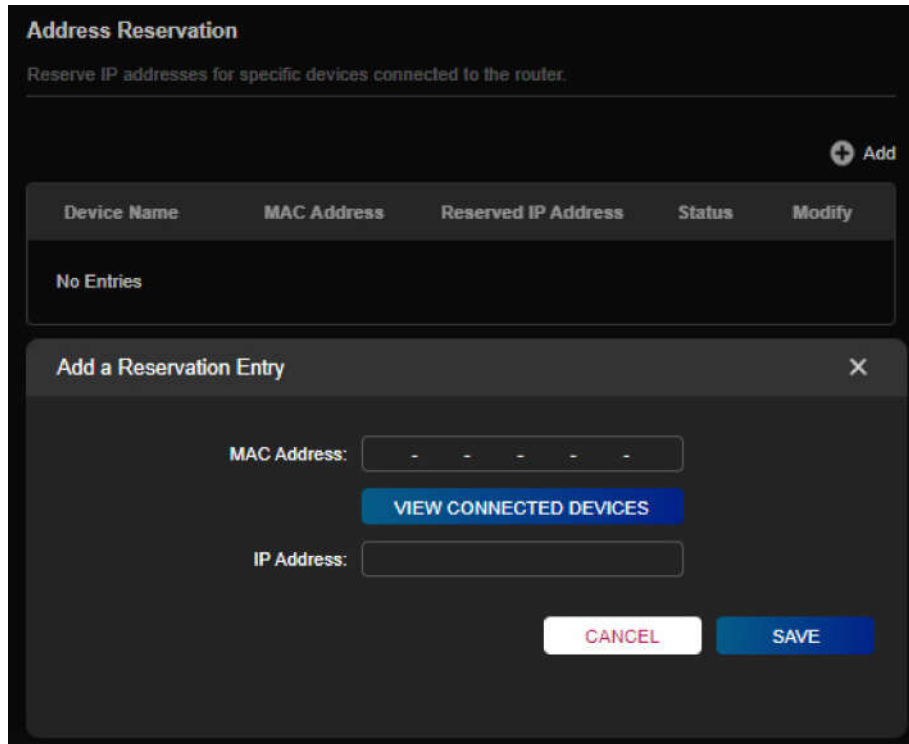
Primary DNS: (Optional)

Secondary DNS: (Optional)

1. Tick the [Enable](#) checkbox.
2. Enter the starting and ending IP addresses in the [IP Address Pool](#).
3. Enter other parameters if the ISP offers. The [Default Gateway](#) is automatically filled in and is the same as the LAN IP address of the router.
4. Click [SAVE](#).

- **To reserve an IP address for a specified client device:**

1. Click [Add](#) in the [Address Reservation](#) section.



2. Click [VIEW CONNECTED DEVICES](#) and select the you device you want to reserve an IP for. Then the [MAC Address](#) will be automatically filled in. Or enter the [MAC address](#) of the client device manually.
3. Enter the [IP address](#) to reserve for the client device.
4. Click [SAVE](#).

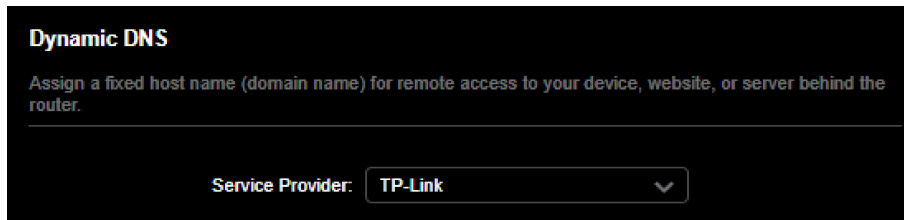
16.7. Set Up a Dynamic DNS Service Account

Most ISPs assign a dynamic IP address to the router and you can use this IP address to access your router remotely. However, the IP address can change from time to time and you don't know when it changes. In this case, you might apply the DDNS (Dynamic Domain Name Server) feature on the router to allow you and your friends to access your router and local servers (FTP, HTTP, etc.) using a domain name without 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 router.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced > Network > Dynamic DNS](#).
3. Select the DDNS [Service Provider](#): TP-Link, NO-IP or DynDNS. It is recommended to select TP-Link so that you can enjoy TP-Link's superior DDNS service. Otherwise,

please select NO-IP or DynDNS. If you don't have a DDNS account, you have to register first by clicking [Register Now](#).



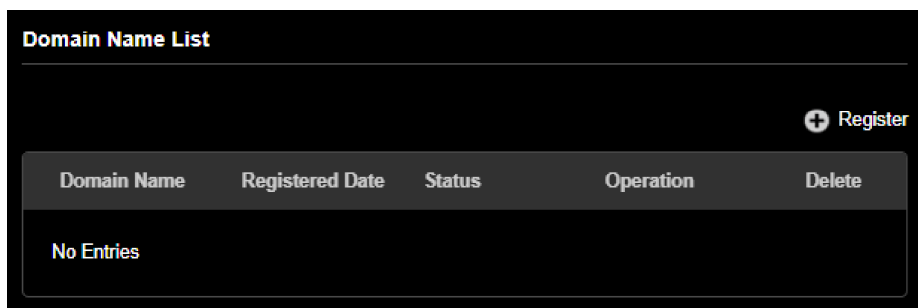
Dynamic DNS

Assign a fixed host name (domain name) for remote access to your device, website, or server behind the router.

Service Provider: **TP-Link** ▼

Note: To enjoy TP-Link's DDNS service, you have to log in with a TP-Link ID. If you have not logged in with one, click [log in](#).

4. Click [Register](#) in the [Domain Name List](#) if you have selected TP-Link, and enter the [Domain Name](#) as needed.

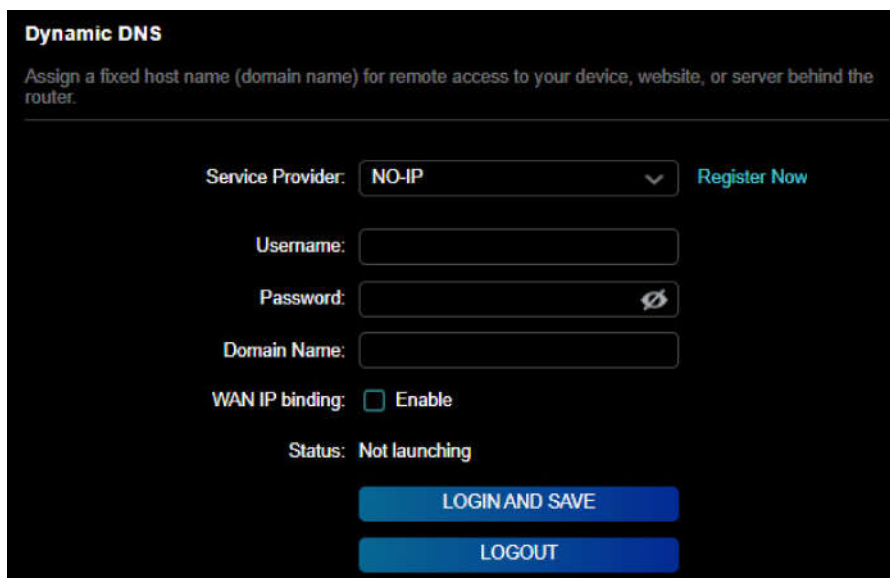


Domain Name List

+ Register

Domain Name	Registered Date	Status	Operation	Delete
No Entries				

If you have selected NO-IP or DynDNS, enter the username, password and domain name of your account.




Dynamic DNS

Assign a fixed host name (domain name) for remote access to your device, website, or server behind the router.

Service Provider: **NO-IP** ▼ [Register Now](#)

Username:

Password: 

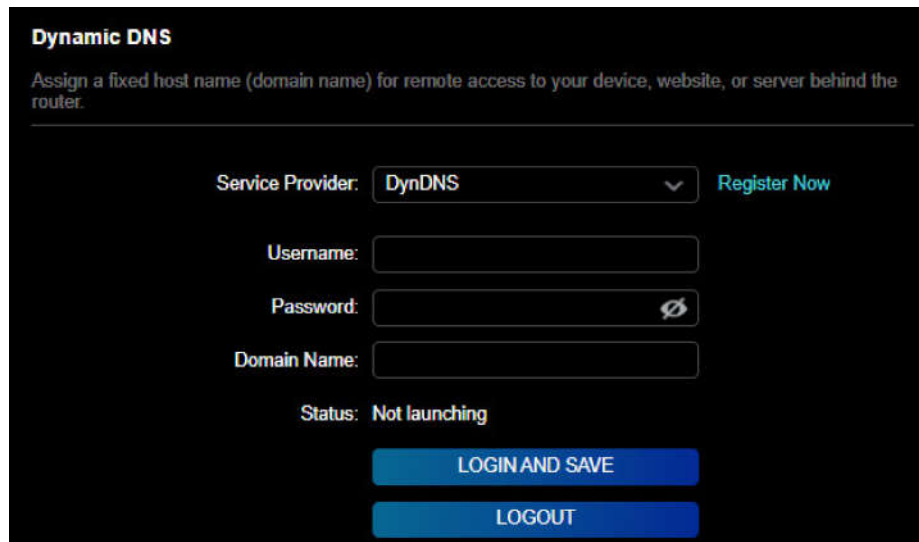
Domain Name:

WAN IP binding: Enable

Status: Not launching

[LOGIN AND SAVE](#)

[LOGOUT](#)



Dynamic DNS

Assign a fixed host name (domain name) for remote access to your device, website, or server behind the router.

Service Provider: [Register Now](#)

Username:

Password:


Domain Name:

Status: Not launching

[LOGIN AND SAVE](#)

[LOGOUT](#)

5. Click [LOGIN AND SAVE](#).

 **Tips:** If you want to use a new DDNS account, please click [Logout](#) first, and then log in with a new account.

16.8. Create Static Routes

Static routing is a form of routing that is configured manually by a network administrator or a user by adding entries into a routing table. The manually-configured routing information guides the router in forwarding data packets to the specific destination.

I want to:

Visit multiple networks and servers at the same time.

For example, in a small office, my PC can surf the internet through Router A, but I also want to visit my company's network. Now I have a switch and Router B. I connect the devices as shown in the following figure 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.