



User Guide

AX1800 Dual Band Wi-Fi 6 Router

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.Top Panel	4
1. 2. 2.Back 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.....	11
Chapter 4. Set Up Internet Connection	13
4. 1. Use Quick Setup Wizard	14
4. 2. Quick Setup Via TP-Link Tether App.....	14
4. 3. Manually Set Up Your Internet Connection	15
4. 4. Set Up the Router as an Access Point	17
4. 5. Set Up an IPv6 Internet Connection.....	18
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	24
5. 3. 1.Add TP-Link ID to Manage the Router.....	25
5. 3. 2.Remove TP-Link ID(s) from Managing the Router.....	25
5. 4. Manage the Router via the TP-Link Tether App	26
Chapter 6. Wireless Settings	27
6. 1. Specify Wireless Settings	28
6. 2. Schedule Your Wireless Function	30
6. 3. Use WPS for Wireless Connection	31
6. 3. 1.Connect via the Client's PIN	31
6. 3. 2.Connect via the Router's PIN	31

6. 3. 3.Push the WPS Button.....	32
6. 4. Advanced Wireless Settings	32
Chapter 7. Guest Network.....	34
7. 1. Create a Network for Guests	35
7. 2. Customize Guest Network Options.....	36
Chapter 8. Parental Controls	37
8. 1. Setting Up Access Restrictions	38
8. 2. Monitoring Internet Usage	42
Chapter 9. QoS.....	43
Chapter 10.EasyMesh with Seamless Roaming.....	45
10. 1. Add a Router as a Satellite Device.....	46
10. 2. Add a Range Extender as a Satellite Device	47
10. 3. Manage Devices in the EasyMesh Network.....	47
Chapter 11.Network Security	51
11. 1. Protect the Network from Cyber Attacks	52
11. 2. Access Control	52
11. 3. IP & MAC Binding	55
11. 4. ALG	57
Chapter 12.NAT Forwarding.....	58
12. 1. Share Local Resources on the Internet by Port Forwarding	59
12. 2. Open Ports Dynamically by Port Triggering.....	61
12. 3. Make Applications Free from Port Restriction by DMZ	62
12. 4. Make Xbox Online Games Run Smoothly by UPnP	63
Chapter 13.VPN Server & Client.....	65
13. 1. Use OpenVPN to Access Your Home Network.....	66
13. 2. Use PPTP VPN to Access Your Home Network	67
13. 3. Use L2TP/IPSec VPN to Access Your Home Network	72
13. 4. Use WireGuard VPN to Access Your Home Network	80
13. 5. Use VPN Client to Access a Remote VPN Server	83
Chapter 14.Customize Your Network Settings.....	89
14. 1. Change the LAN Settings	90

14. 2. Set Up Link Aggregation	90
14. 3. Flow Controller	91
14. 4. Configure to Support IPTV Service.....	91
14. 5. Specify DHCP Server Settings.....	93
14. 6. Set Up a Dynamic DNS Service Account	94
14. 7. Create Static Routes.....	95
Chapter 15.Manage the Router	99
15. 1. Update the Firmware.....	100
15. 1. 1.Online Update	100
15. 1. 2.Local Update	101
15. 2. Backup and Restore Configuration Settings.....	101
15. 3. Change the Login Password	102
15. 4. Password Recovery.....	103
15. 5. Local Management	104
15. 6. Remote Management.....	105
15. 7. System Log.....	107
15. 8. Test the Network Connectivity	109
15. 9. Set System Time and Language	111
15. 10. Set the Router to Reboot Regularly.....	113
15. 11. Control the LED.....	114
FAQ	116

About This Guide

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

Note: Features available in the 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 enable or disable the corresponding entry. Click to view more information about items on the page.

More Info

The latest software, management app and utility can be found at [Download Center](#) 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](#) 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, wireless coverage and number of connected devices are not guaranteed and will vary as a result of network conditions, client limitations, and environmental factors, including building materials, obstacles, volume and density of traffic, and client location.

[#]Use of 802.11ax (Wi-Fi 6), and features including OFDMA and 1024-QAM requires clients to also support corresponding features.

[§]The 802.11ax white paper defines standardized modifications to both the IEEE 802.11 physical layers (PHY) and the IEEE 802.11 Medium Access Control (MAC) layer as enabling at least one mode of operation capable of supporting improvement of at least four times the average throughput per station (measured at the MAC data service access point) in a dense deployment scenario.

[△]1,000 Mbps internet speeds require compatible service plans and equipment.

^{*}Use of WPA3 requires clients to also support WPA3.

^{**}This router may not support all the mandatory features as ratified in the IEEE 802.11AX specification.

^{***}Further software upgrades for feature availability may be required.

^{****} This product is compatible with standardized EasyMesh technology but has not obtained the Wi-Fi EasyMesh™ certification. TP-Link EasyMesh-compatible products can network with other devices that use EasyMesh. Failed connections may be due to firmware conflicts of different vendors. The EasyMesh-Compatible function is still being developed on some models and will be supported in subsequent software updates.

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 AX router, with next-generation 802.11ax Wi-Fi Technology, achieves Wi-Fi performance at its ultimate level. The revolutionary combination of OFDMA and 1024QAM improve throughput by 4 times and dramatically increase the whole network capacity and efficiency. It's also backwards compatible with 802.11a/b/g/n/ac.

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

1. 2. Appearance

1. 2. 1. Top Panel



The router's LEDs (view from left to right) are located on the front. You can check the router's working status by following the LED Explanation table.

LED Explanation

Name	Status	Indication
(Power)	On	The system has started up successfully.
	Flashing	The system is starting up or the firmware is being upgraded. Do not disconnect or power off your router.
	Off	Power is off.
(2.4 GHz Wireless)	On	The 2.4 GHz wireless band is enabled.
	Off	The 2.4 GHz wireless band is disabled.

Name	Status	Indication
 (5 GHz Wireless)	On	The 5 GHz wireless band is enabled.
	Off	The 5 GHz wireless band is disabled.
 (Internet)	Green On	Internet service is available.
	Orange On	The router's Internet port is connected, but the internet service is not available.
	Off	The router's Internet port is unplugged.
 (Ethernet)	On	At least one powered-on device is connected to the router's Ethernet port.
	Off	No powered-on device is connected to the router's Ethernet port.
 (WPS)	On/Off	This light remains on for 5 minutes when a WPS connection is established, then turns off.
	Blinking	WPS connection is in progress. This may take up to 2 minutes.

1. 2. 2. Back Panel



The following parts (view from left to right) are located on the back panel.

Item	Description
WPS/Wi-Fi Button	Press this button for 1 second, and immediately press the WPS button on your client device to start the WPS process.
	Press and hold this button for more than 2 seconds to turn on or off the wireless function of your router.
Reset Button	Press and hold the button for about 6 seconds until the Power LED blinks to reset the router to its factory default settings.

Item	Description
WAN Port	For connecting to a modem or an Ethernet outlet.
LAN Port (1-4)	For connecting your PC or other wired devices to the router.
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.
Antennas	Used for wireless operation and data transmit.

Chapter 2

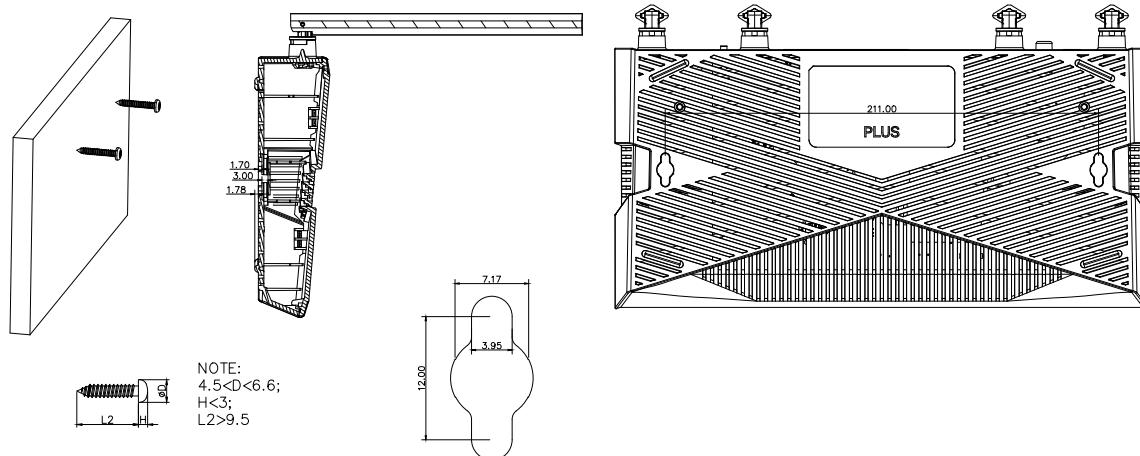
Connect the Hardware

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. The device also can be mounted on the wall as shown in the following figure.



Note:

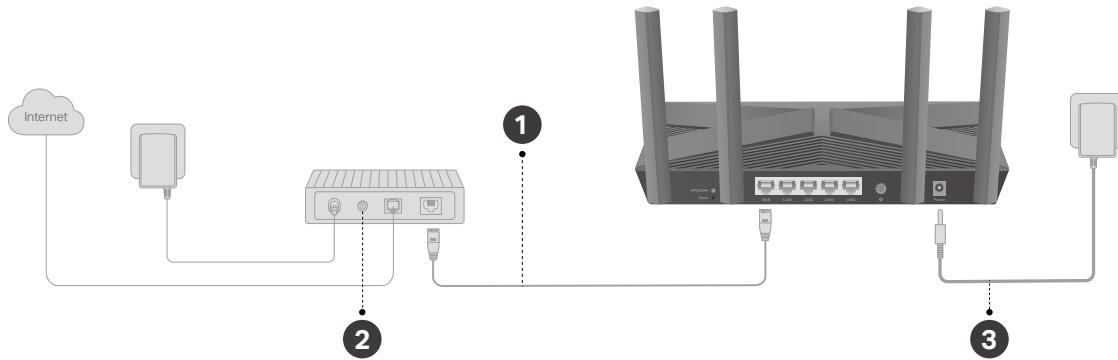
The diameter of the screw head, $4.5\text{mm} < D < 6.6\text{mm}$, and the distance of two screws is 211mm. The screw that project from the wall need around 6.48 mm based, and the length of the screw need to be at least 9.5mm to withstand the weight of the product.

2.2. Connect Your Router

Before you start:

- Turn off your modem, if any, and remove the backup battery if it has one.
- Place the router horizontally and orient the antennas vertically.

If your internet comes from an Ethernet outlet instead of a DSL / Cable / Satellite modem, connect the router's WAN port to it, then follow steps 3 and 4 to complete the hardware connection.



1. Connect the **powered-off modem** to the router's **WAN port** with an Ethernet cable.
2. Turn on the modem, and then wait about **2 minutes** for it to restart.
3. Connect the power adapter to the router and turn on the router.
4. Verify that the hardware connection is correct by checking the following LEDs.

Note:

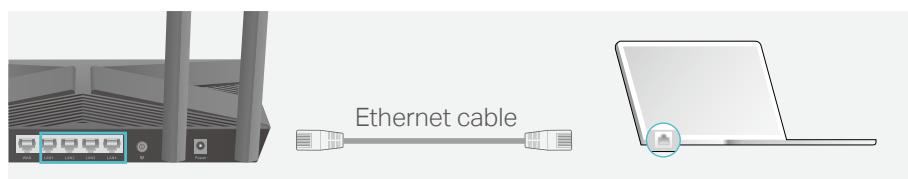
If the 2.4GHz LED and 5GHz LED are off, press and hold the WPS/Wi-Fi button on the back for more than 2 seconds, then release the button. Both the LEDs should turn solid on.



5. Connect your computer to the router.

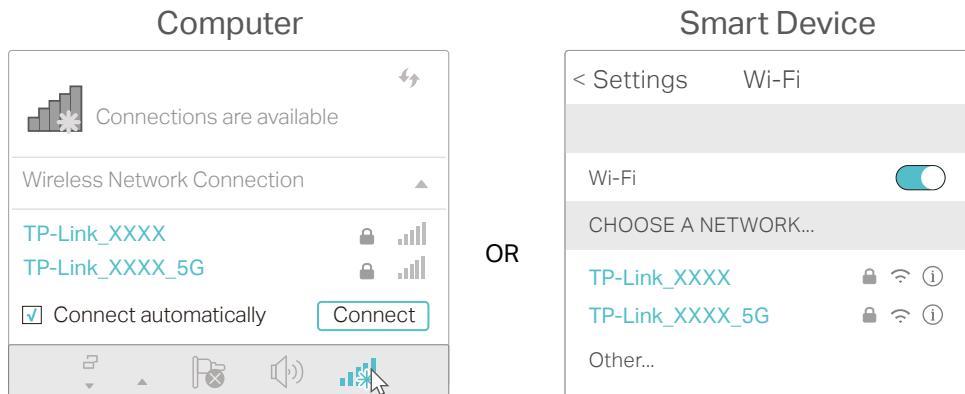
- **Method 1: Wired**

Turn off the Wi-Fi on your computer and connect the devices as shown below.



- **Method 2: Wirelessly**

- 1) Find the SSID (Network Name) 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.



- **Method 3: Use the WPS button**

Wireless devices that support WPS, including Android phones, tablets, and most USB network cards, can be connected to your router through this method.

Note:

- WPS is not supported by iOS devices.
- The WPS function cannot be configured if the wireless function of the router is disabled. Also, the WPS function will be disabled if your wireless encryption is WEP. Please make sure the wireless function is enabled and is configured with the appropriate encryption before configuring the WPS.

- 1) Tap the WPS icon on the device's screen. Here we take an Android phone for instance.
- 2) Within two minutes, press the WPS/Wi-Fi button on your router for 1 second.



Chapter 3

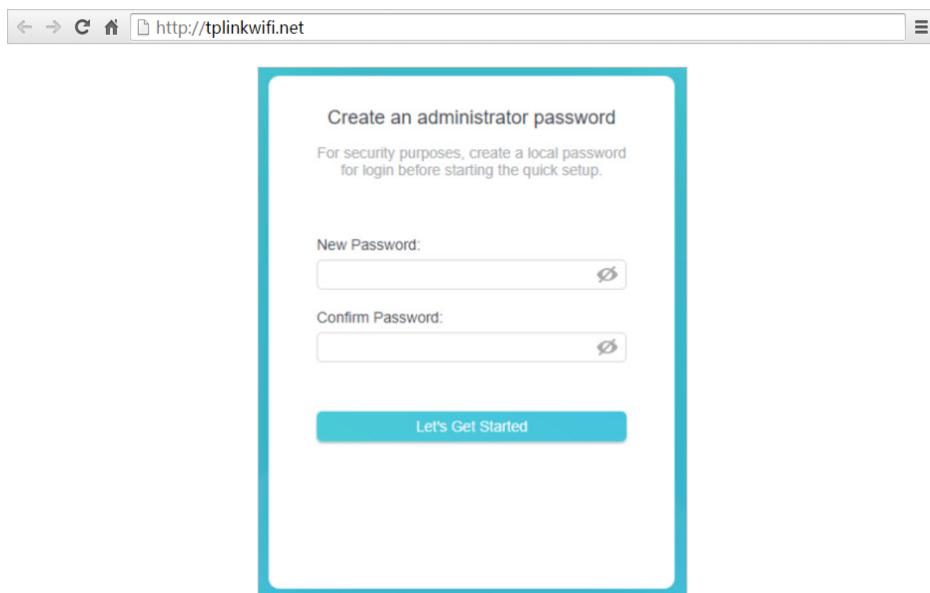
Log In to Your Router

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

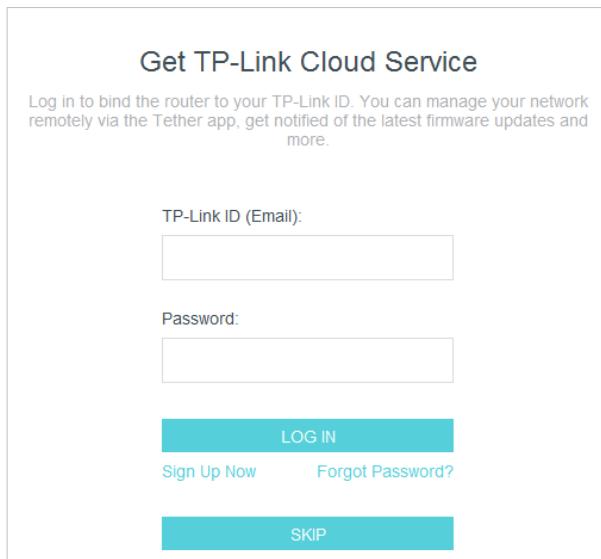
The Quick Setup Wizard will guide you to set up your router.

» **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 or click [Sign Up Now](#) to get one. 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 **Add a Router**. Follow the steps to complete the setup and connect to the internet.

■ Note: Due to Tether app updates, your actual user interface and pathway may differ from those described here.

4. Connect your devices to the newly configured wireless networks of the router 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 your internet connection type from the drop-down list.

A screenshot of a web-based configuration interface for setting up an internet connection. The top bar is labeled 'Internet' and has a sub-instruction: 'Set up an internet connection with the service information provided by your ISP (internet service provider)'. Below this is a dropdown menu labeled 'Internet Connection Type' with 'Dynamic IP' selected. A small note next to it says: 'Select this type if your ISP doesn't provide any information for internet connection.'

4. 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

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: 00 - 0A - EB - 13 - 7B - 01

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

Internet

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

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

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:	<input type="text"/>
Password:	<input type="password"/> 
<input checked="" type="radio"/> Dynamic IP <input type="radio"/> Static IP	
VPN Server IP/Domain Name:	<input type="text"/>

- 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

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:	<input type="text"/>
Password:	<input type="password"/> 
<input checked="" type="radio"/> Dynamic IP <input type="radio"/> Static IP	
VPN Server IP/Domain Name:	<input type="text"/>

5. 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.

Operation Mode

Select an operation mode according to your needs.

Wireless Router Mode (Current)

In this mode, the router can provide internet access for multiple wired and wireless devices. This mode is required most commonly.



Access Point Mode

In this mode, the router changes an existing wired (Ethernet) network into a wireless one.



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

4. 5. Set Up an IPv6 Internet Connection

Your ISP provides information about one of the following IPv6 internet connection types: PPPoE, Dynamic IP(SLAAC/DHCPv6), Static IP, 6to4 tunnel, Pass-Through (Bridge). After setting up the IPv6 internet connection, you can add IPv6 firewall rules to protect your IPv6 network.

- **Set up an IPv6 Internet 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**.
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:

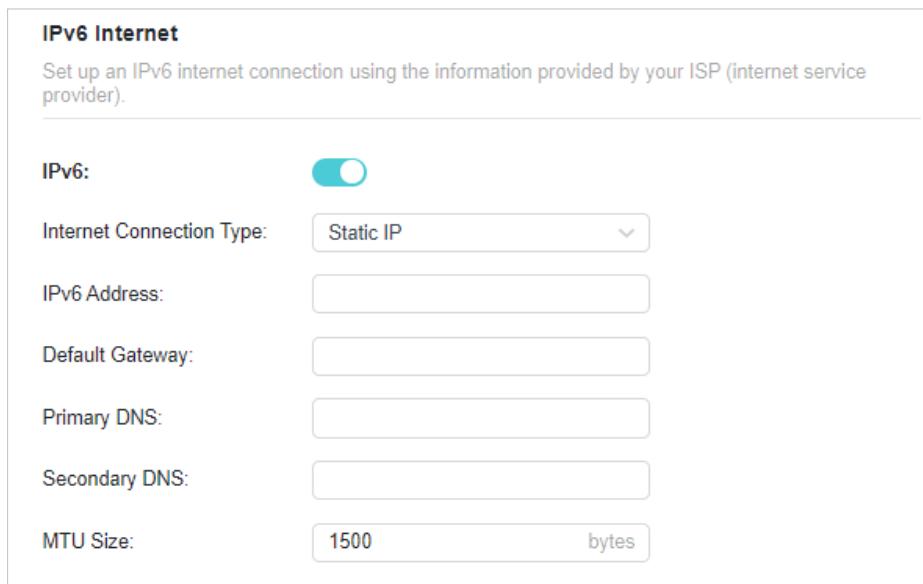
IPv6 Address:

Default Gateway:

Primary DNS:

Secondary DNS:

MTU Size: bytes



- 2) **Dynamic IP(SLAAC/DHCPv6):** Click **Advanced** 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: ::

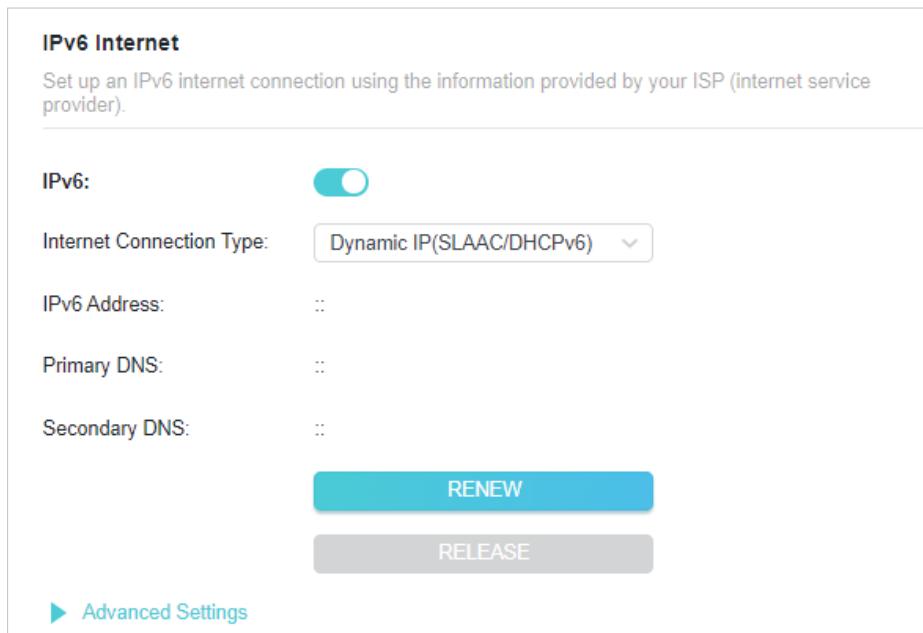
Primary DNS: ::

Secondary DNS: ::

RENEW

RELEASE

► Advanced Settings



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

Note:

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

IPv6 Internet

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

IPv6:

Internet Connection Type:

Share the same PPPoE session with IPv4

Username:

Password:

IPv6 Address: ::

▶ Advanced Settings

- 4) **6to4 Tunnel:** An IPv4 internet connection type is a prerequisite for this connection type ([Manually Set Up Your Internet Connection](#)). Click **Advanced Settings** 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:

IPv4 Address: 0.0.0.0

IPv4 Subnet Mask: 0.0.0.0

IPv4 Default Gateway: 0.0.0.0

Tunnel Address: ::

▶ Advanced Settings

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

IPv6 Internet

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

IPv6:

Internet Connection Type:

5. Configure LAN ports. Windows users are recommended to choose from DHCPv6 and SLAAC+Stateless DHCP. Fill in **Address Prefix** provided by your ISP, and click **SAVE**.

IPv6 LAN

Configure the LAN IPv6 address of the router and set the configuration type to assign IPv6 addresses to the clients.

Assigned Type: ND Proxy
 DHCPv6
 SLAAC+Stateless DHCP
 SLAAC+RDNSS

Address Prefix: /64

Address: FE80::20A:EBFF:FE13:7B00/64

6. In **MAC Clone** section, set the MAC address of your router. Use the default address unless your ISP allows internet access from only a specific MAC address.

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:

00 - 0A - EB - 13 - 7B - 01

7. Click **Status** to check whether you have successfully set up an IPv6 connection.

» **Tips:**

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

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 or click **TP-Link ID** on the very top of the page.
3. Click **Sign Up** and follow the instructions to register a TP-Link ID.

TP-Link ID

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

Create a TP-Link ID

Select Country or Region

Email Address

Password

Confirm Password

I have fully read and accepted the [Privacy Policy](#) and [Terms of Use](#).

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

SIGN UP

I already have TP-Link ID

Remote Control
Access and control your network remotely

Smart Home
Support Amazon Alexa and Google Assistant

HomeShield
Get full protection on your network security

QR code for Scan for Tether

DOWNLOAD ON THE App Store

GET IT ON Google Play

Scan for Tether Search Tether

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 **Admin**.

TP-Link ID

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

TP-Link ID (Email):

Password:

LOG IN

SIGN UP

[Forgot Password?](#)

Remote Control
Access and control your network remotely

Smart Home
Support Amazon Alexa and Google Assistant

HomeShield
Get full protection on your network security

QR code for Scan for Tether

DOWNLOAD ON THE App Store

GET IT ON Google Play

Scan for Tether Search Tether

Note:

- To learn more about the [Admin](#) and [User](#) TP-Link ID, refer to [Manage the User TP-Link IDs](#).
- Once you have registered a TP-Link ID on the web management page, you can only register another TP-Link ID via the 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.

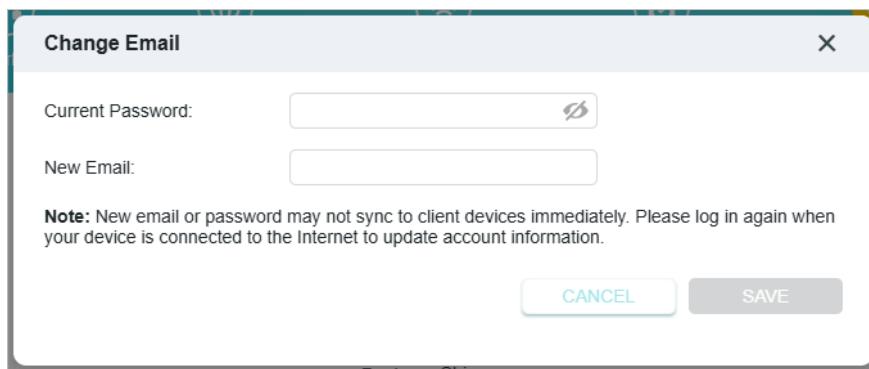
5.2. Change Your TP-Link ID Information

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 [Account Information](#) section.

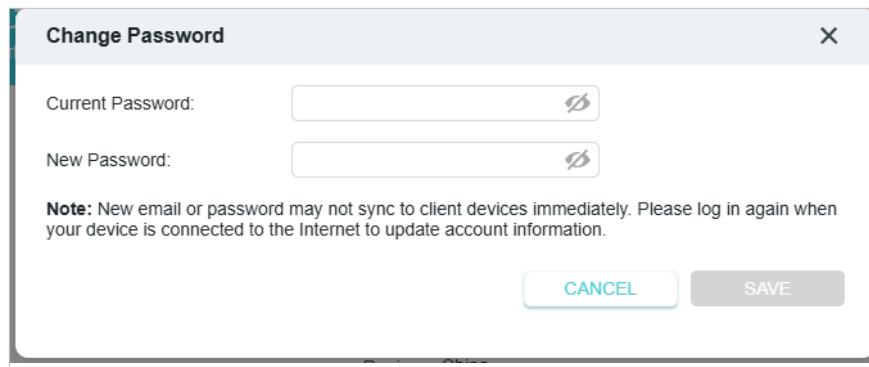
- **To change your email address:**

1. Click  behind the Email.
2. Enter the password of your TP-Link ID, then a new email address. And click [SAVE](#).



- **To change your password:**

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



5. 3. Manage the User TP-Link IDs

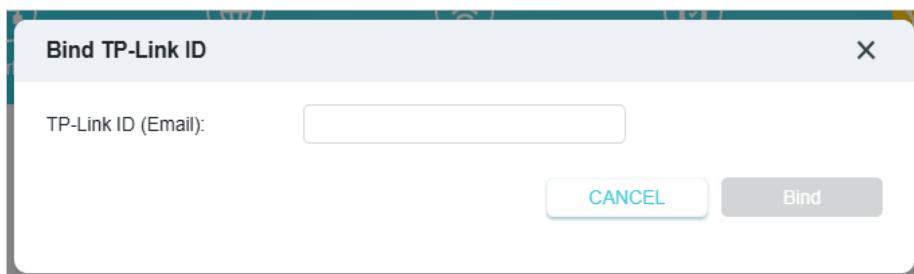
The TP-Link ID used to log in to the router for the first time will be automatically bound as the [Admin](#) account. An admin account can add or remove other TP-Link IDs to or from the same router as [Users](#). All accounts can monitor and manage the router locally or remotely, but user accounts cannot:

- 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.

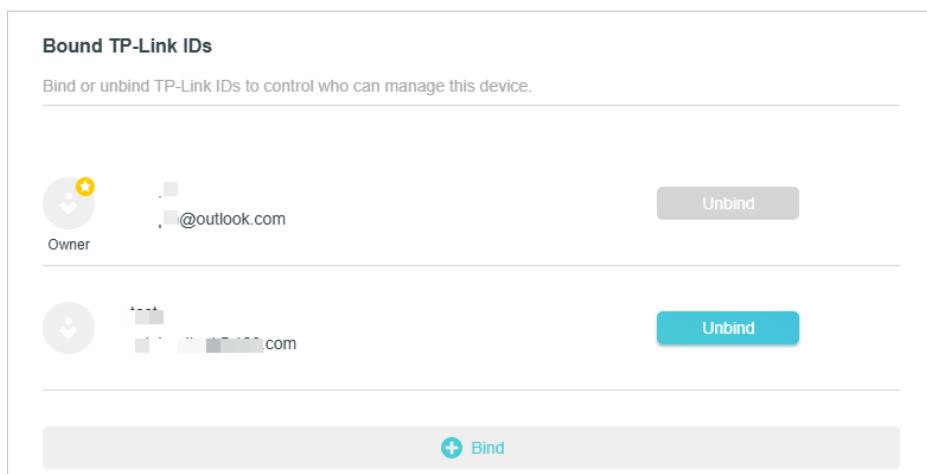
5.3.1. Add TP-Link ID to Manage the Router

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 Accounts section.
 3. Click  Bind, enter another TP-Link ID as needed and click **SAVE**.

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



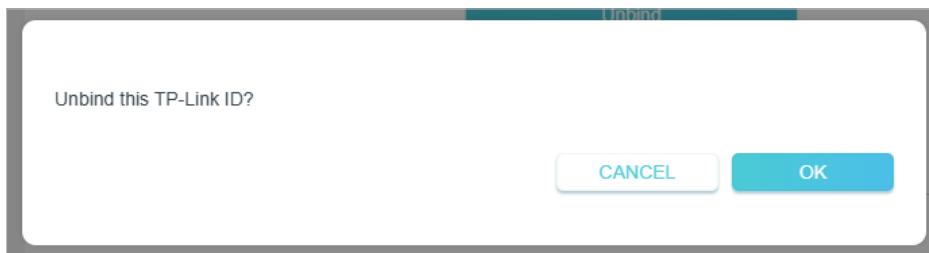
4. The new TP-Link ID will be displayed in the Bound Accounts table as a [User](#).



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 Accounts](#) section.
3. Tick the checkbox(es) of the TP-Link ID(s) you want to remove and click [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

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](#)

6. 1. Specify Wireless Settings

The router's wireless network name (SSID) and password, and security option are preset in the factory. The preset SSID and password can be found on the 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**.

The screenshot shows the 'Wireless Settings' page. At the top, it says 'Personalize settings for each band or enable Smart Connect to configure the same settings for 2.4 GHz and 5 GHz bands.' Below this, there are several configuration options:

- OFDMA:** Enabled (checkbox checked)
- TWT:** Enabled (checkbox checked)
- Smart Connect:** Enabled (checkbox checked)
- 2.4 GHz / 5 GHz:** Enabled (checkbox checked) with a 'Share Network' link next to it.
- Network Name (SSID):** TP-Link_7B00 with a 'Hide SSID' checkbox.
- Security:** WPA2-PSK[AES]
- Password:** 03717660

Below these, under '2.4 GHz / 5 GHz Advanced Settings', are the following options:

- Transmit Power:** High
- 2.4 GHz Channel Width:** 20/40 MHz
- 2.4 GHz Channel:** Auto
- 5 GHz Channel Width:** 20/40/80 MHz
- 5 GHz Channel:** Auto

- **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 use the Smart Connect function:**

The Smart Connect function lets you enjoy a more high-speed network by assigning your devices to best wireless bands based on actual conditions to balance network demands.

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 2.4GHz and 5GHz wireless networks. If you want to configure the wireless settings separately for each band, untick 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 function is enabled by default. If you want to disable the wireless function of the router, just untick the [Enable](#) checkbox of each wireless network. In this case, all the wireless settings will be invalid.

- **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: [None](#), [WPA/WPA2-Personal](#), [WPA2/WPA3-Personal](#), [WPA/WPA2-Enterprise](#). We recommend you don't change the default settings unless necessary.

- **To change the transmit power and channel settings:**

1. Go to [Advanced > Wireless > Wireless Settings](#).
2. Select an option from the [Transmit Power](#) drop-down list: [High](#), [Middle](#) or [Low](#). The default and recommended setting is [High](#).
3. If Smart Connect is disabled, you can also change the following settings:
 - [Channel Width](#) - Select a channel width (bandwidth) for the wireless network.

- **Channel** - 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.
- **Mode** - Select a transmission mode according to your wireless client devices. It is recommended to just leave it as default.

6.2. 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.

Wireless Schedule

Schedule when to automatically turn off your wireless network.

Wireless Schedule: Enabled

Current Time: 2022-10-19 12:21:06 AM

Note: Before using this feature, make sure **System Time** is set to "Get from Internet".

4. Click **Add** to add a schedule.

Add

Wireless Off Time	Repeat	Modify
There is no entry!		

5. Specify a wireless off period during which you need the wireless off automatically, and click **SAVE**.

Add Schedule

Wireless Off Time: From 11 PM (next day) To 7 AM (next day)

Repeat: **S** **M** **T** **W** **T** **F** **S**

CANCEL **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 be automatically turned on after the time period you set.

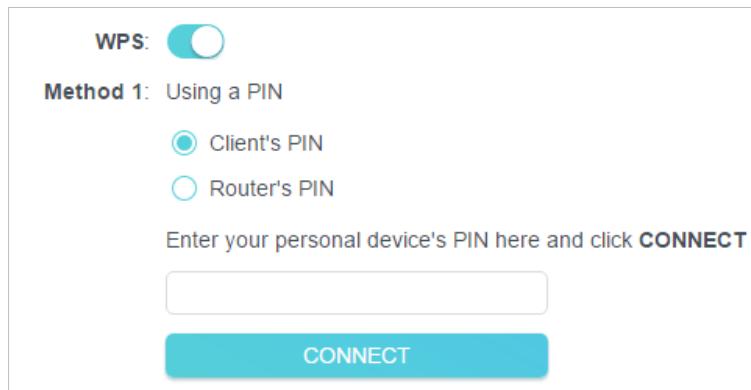
6.3. Use WPS for Wireless Connection

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

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

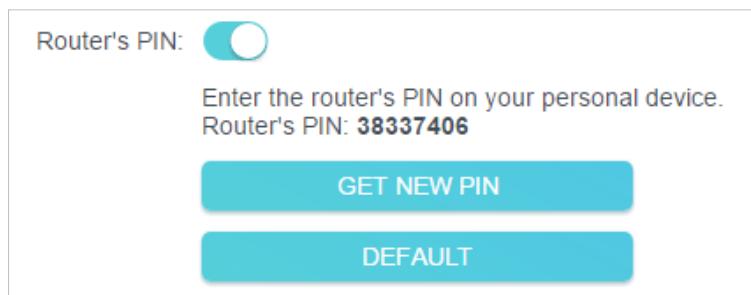
6.3.1. Connect via the Client's PIN

Enter the PIN of your device and click **Connect**. Then your device will get connected to the router.



6.3.2. 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.

6.3.3. 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 flashing to solid on, indicating successful WPS connection.

Method 2: Using the button below

Click the button below, then enable WPS on your personal device within 2 minutes.



Method 3: Using the router's WPS button

Press the router's WPS button, then enable WPS on your personal device within 2 minutes.

6.4. 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.

Additional Settings

Check advanced wireless settings for your device.

WMM:	<input checked="" type="checkbox"/> Enabled
AP Isolation:	<input type="checkbox"/> Enabled
Airtime Fairness:	<input type="checkbox"/> Enabled
Beacon Interval:	100
RTS Threshold:	2346
DTIM Interval:	1
Group Key Update Period:	0 <input type="button" value="s"/>

- **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 7

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](#)

7.1. Create a Network for Guests

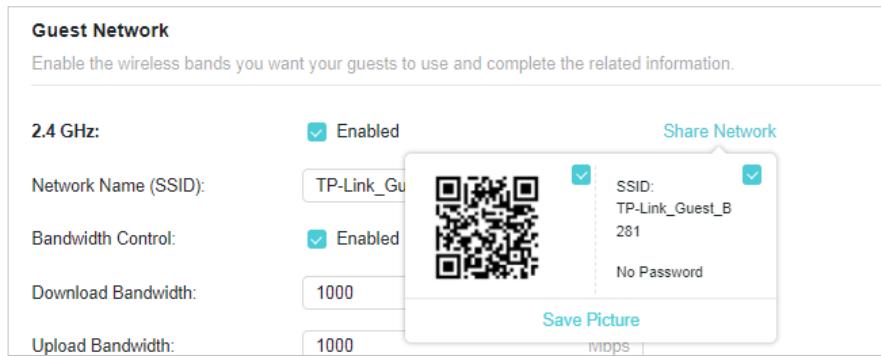
1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > Wireless > Guest Network** or click **Wireless** on the top page. Locate the **Guest Network** section.
3. Create a guest network as needed.
 - 1) Tick the **Enable** checkbox for the 2.4GHz or 5 GHz 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 to keep the guest network.
 - 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.

2.4 GHz:	<input checked="" type="checkbox"/> Enabled	Share Network
Network Name (SSID):	<input type="text" value="TP-Link_Guest_7B00"/>	
Bandwidth Control:	<input type="checkbox"/> Enabled	
5 GHz:	<input checked="" type="checkbox"/> Enabled	Share Network
Network Name (SSID):	<input type="text" value="TP-Link_Guest_7B00_5G"/>	
Bandwidth Control:	<input type="checkbox"/> Enabled	
Effective Time:	<input type="text" value="No Limit"/>	
Security:	<input type="text" value="Open"/>	

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

4. Click **SAVE**. Now your guests can access your guest network using the SSID and password you set!
5. 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.

7.2. Customize Guest Network Options

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**. Locate the **Guest Permissions** section.
3. Customize guest network options according to your needs.

Guest Permissions

Control the data that guests can access.

Allow guests to see each other
 Allow guests to access your local network

- **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.

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

Chapter 8

Parental Controls

Parental Controls allows you to set up unique restrictions on internet access for each member of your family. You can block inappropriate, explicit and malicious websites, and control access to specified websites at specified time.

It contains the following sections:

- [Setting Up Access Restrictions](#)
- [Monitoring Internet Usage](#)

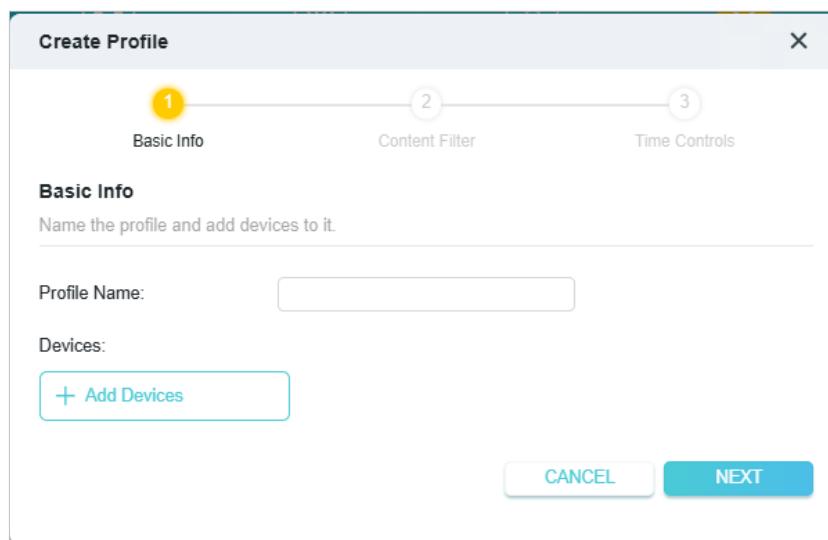
8. 1. Setting Up Access Restrictions

I want to:

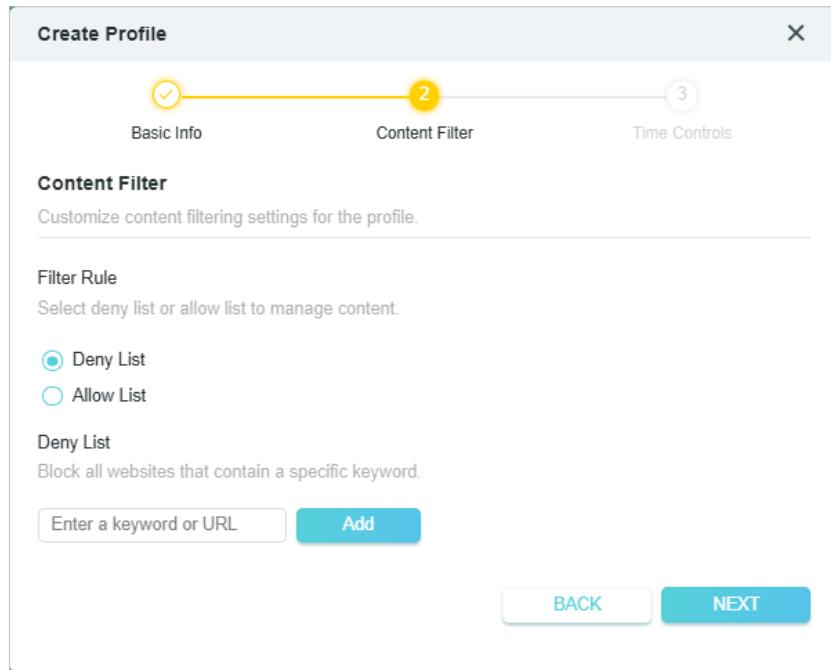
Block access to inappropriate online content for my kids' devices, limit when and how long they can access the internet.

How can I do that?

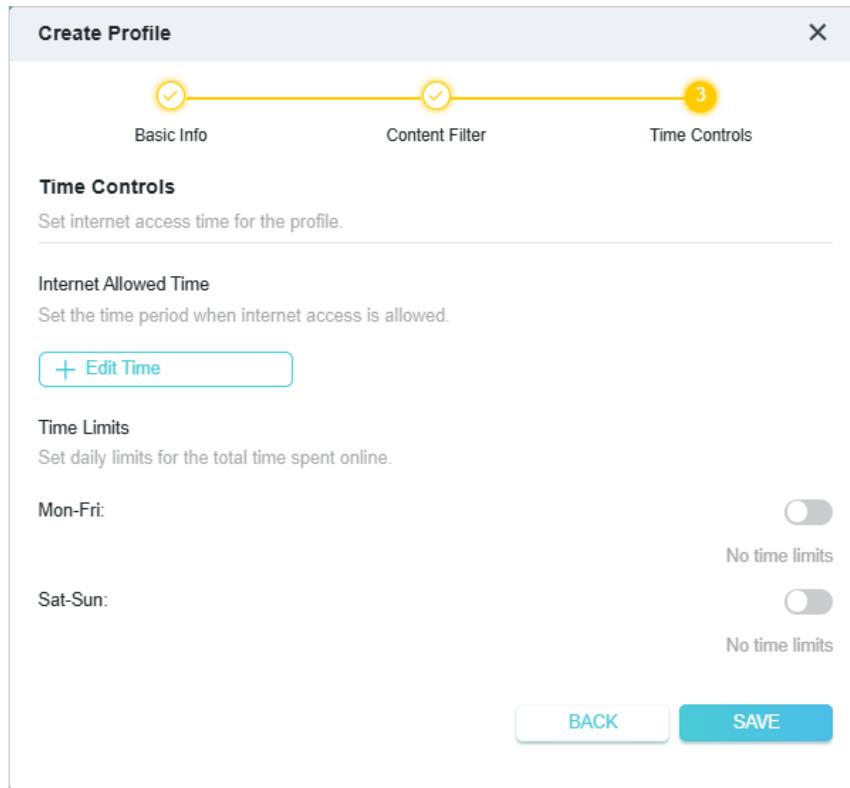
1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > Parental Controls.
3. Click Add to create a profile for a family member.
4. Add basic profile information.



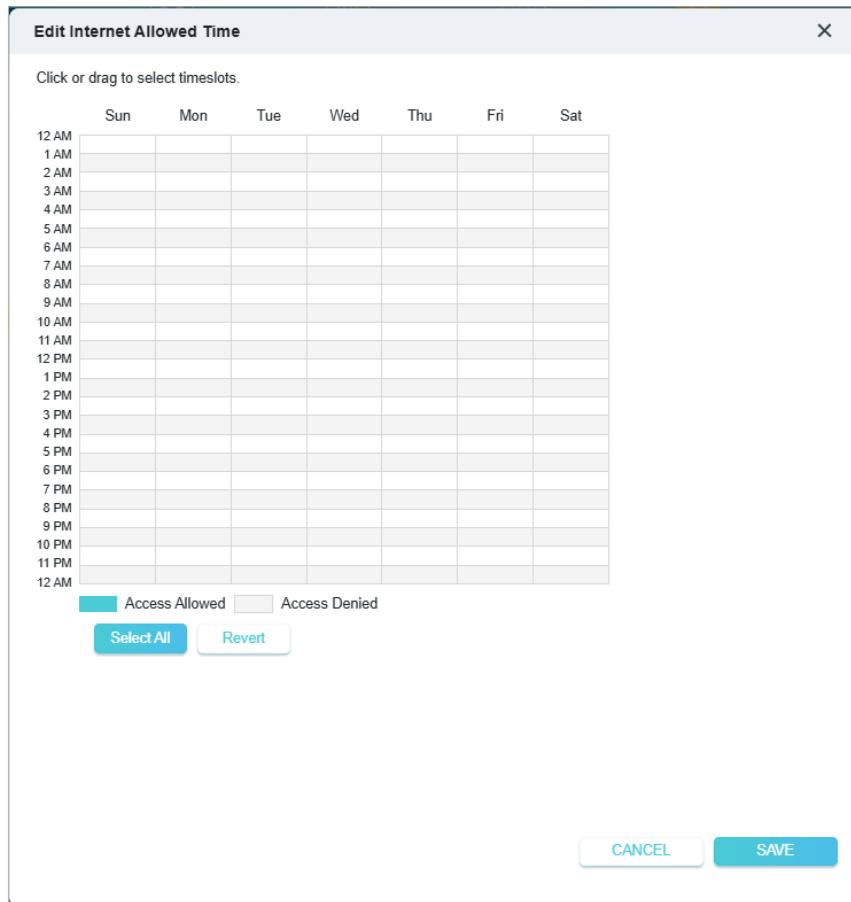
- 1) Enter a **Name** for the profile to make it easier to identify.
 - 2) Under **Devices**, click **Add Devices**.
 - 3) Select the devices that belong to this family member. Access restrictions will be applied to these devices. Click **ADD** when finished.
Note: Only devices that have previously been 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.
 - 4) Click **NEXT**.
5. Customize the **Content Filter** for this profile according to your needs.



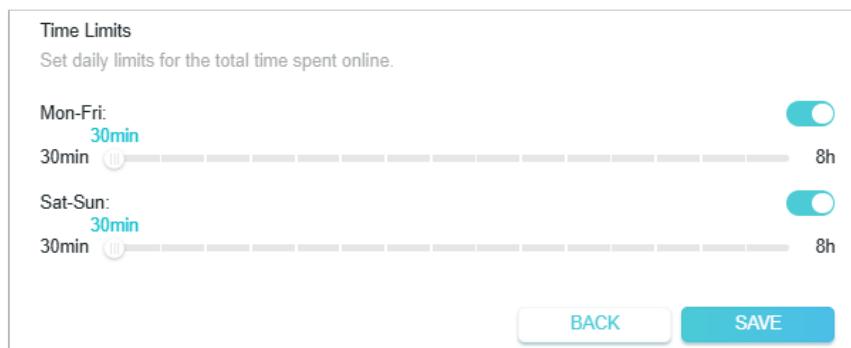
- 1) Select **Deny List** or **Allow List** as the **Filter Rule**, enter a keyword (for example, "Facebook") or a URL (for example, "www.facebook.com"), then click **ADD**.
 - **Deny List:** All websites containing the specified keywords will be blocked.
 - **Allow List:** Only websites that contain the specified keywords will be allowed.
 - 2) Click **NEXT**.
6. Set time restrictions on internet access.



- 1) Click **Edit Time** to select the **Internet Allowed Time**, devices under this profile can only access internet during the specified period.



- 2) Enable **Time Limits** on Monday to Friday and Saturday & Sunday, and set the total time limit for the profile each day.



- 3) Save the settings.

Done!

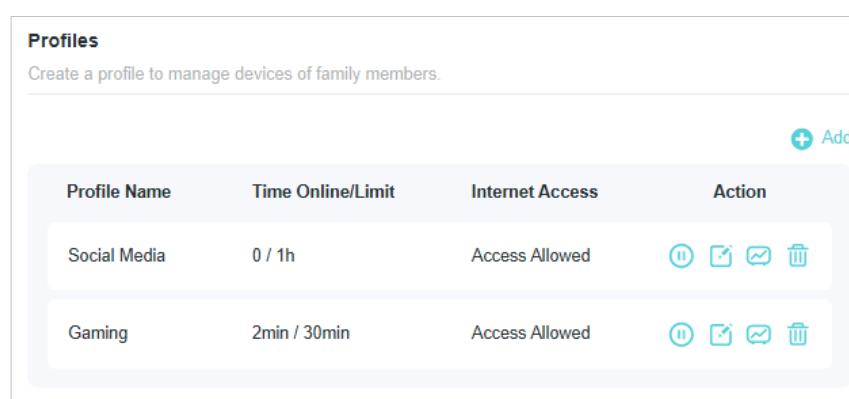
The amount of time your child spends online is controlled and inappropriate content is blocked on their devices.

8. 2. Monitoring Internet Usage

Parental Controls allows you to easily monitor the internet usage of your kids, you can pause the internet at any time, and check which websites your kids have visited and how much time they have spent online recently, then you can configure parental controls rules accordingly to protect your kids from malicious content.

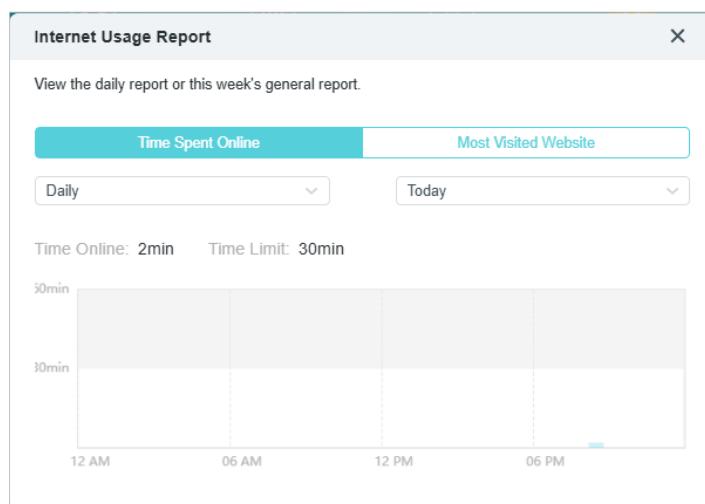
1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > Parental Controls**, locate the **Profiles** area, you can see how much time each profile has spent.

 Note: If you have not set up a profile for your child yet, add a profile by referring to [Setting Up Access Restrictions](#).



Profile Name	Time Online/Limit	Internet Access	Action
Social Media	0 / 1h	Access Allowed	
Gaming	2min / 30min	Access Allowed	

- Click / to pause/resume internet access for a profile at any time as you like.
- Click to edit the profile like adding devices, filtering content and changing time limits.
- Click to view the detailed reports of internet usage like time spent online and most visited websites.



- Click the to delete this profile.

Chapter 9

QoS

QoS (Quality of Service) allows you to prioritize the internet traffic of specific devices to guarantee a faster connection when you need it the most. Devices set as high priority will be allocated more bandwidth even when there is heavy traffic on the network.

I want to:

Ensure a fast connection for a device when I need it the most.

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 > QoS**.
3. Configure global QoS settings.

Global Settings
Prioritize the Internet traffic of specific device to guarantee a faster connection.

QoS: Enabled

Download Bandwidth: 1000 Mbps

Upload Bandwidth: 1000 Mbps

- 1) Enable **QoS**.
- 2) Enter the maximum upload and download bandwidth provided by your internet service provider.
- 3) Save the settings.
4. Set the device priority.
 - 1) In the **Device Priority** section, find your desired device and toggle on **Priority**.
 - 2) Set **Timing** according to your needs.

Device Info	Real-time Rate	Traffic Usage	High Priority	Timing
My Phone 5G	↑ 2.7 Kbps ↓ 0 Kbps	3.4 MB	<input checked="" type="checkbox"/>	Always
My Computer Wired	↑ 0.55 Kbps ↓ 0 Kbps	8.5 MB	<input type="checkbox"/>	---

- To prioritize your device at any time, click the entry in the **Timing** column and choose **Always**.
- To prioritize your device for next few hours, click the entry in the **Timing** column and choose the desired duration (like **2 hours**).

Done! You can now enjoy using your device when you need it the most.

Chapter 10

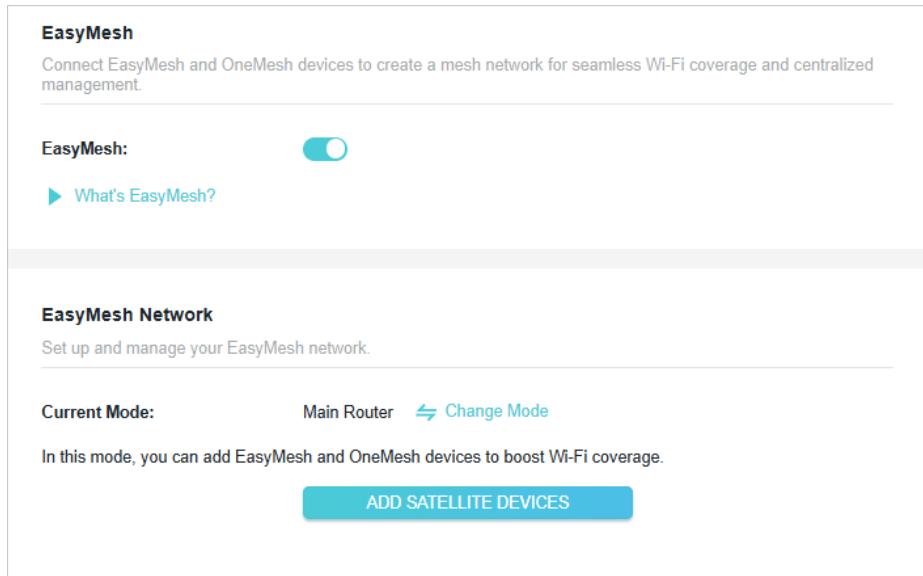
EasyMesh with Seamless Roaming

This product is compatible with EasyMesh. You can experience strong, stable, and seamless wireless connections throughout your home with EasyMesh. This chapter introduces the EasyMesh feature. It contains the following sections:

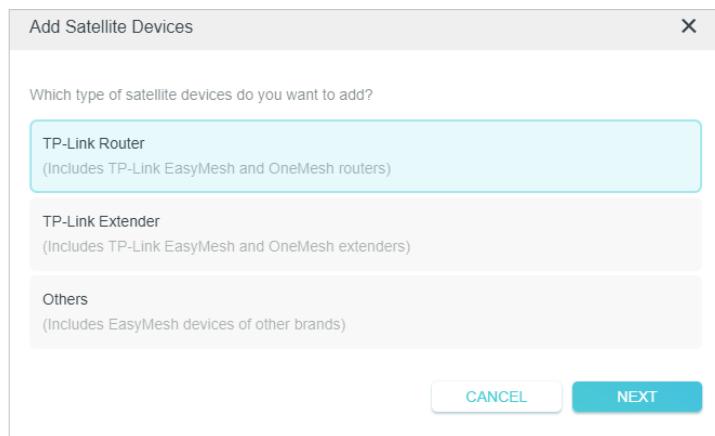
- [Add a Router as a Satellite Device](#)
- [Add a Range Extender as a Satellite Device](#)
- [Manage Devices in the EasyMesh Network](#)

10.1. Add a Router as a Satellite Device

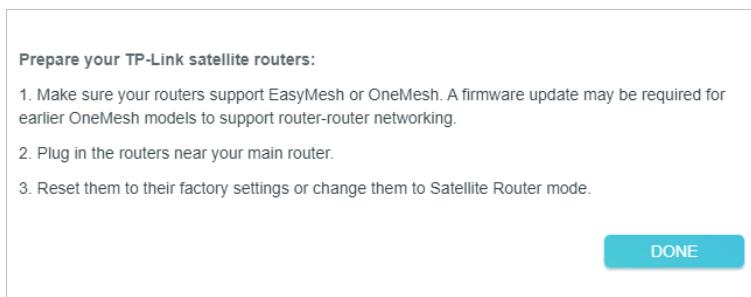
1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > EasyMesh, and enable EasyMesh.



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



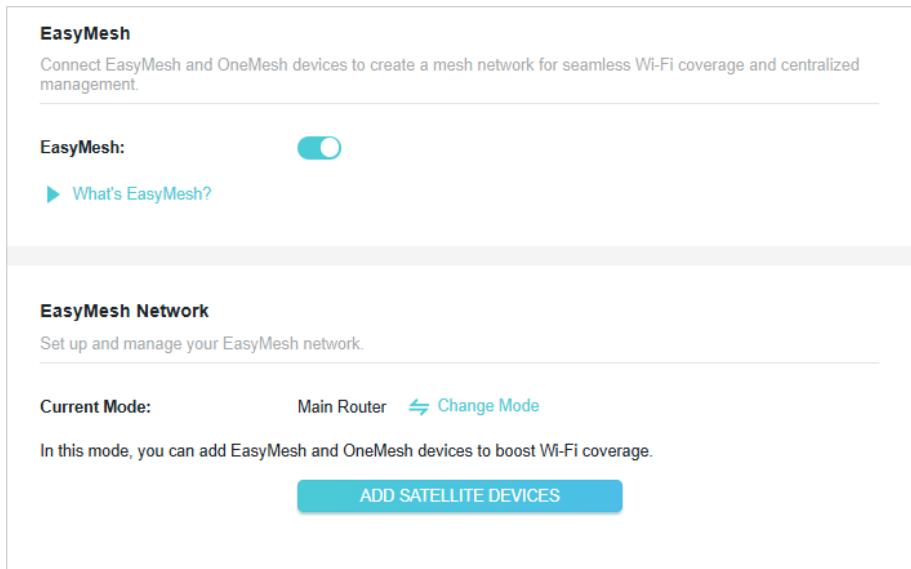
4. Follow the page instructions to prepare your satellite router, then click DONE.



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

10.2. 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**. Locate **EasyMesh Network** section.



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.

10.3. 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.

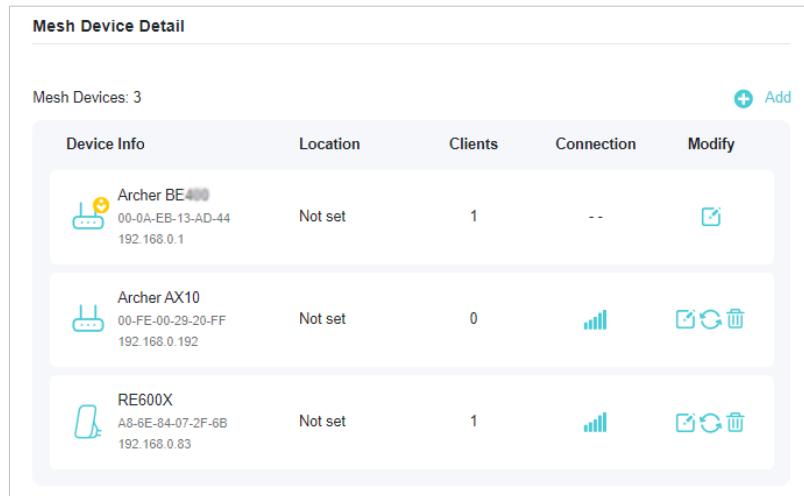
- **To view mesh devices and connected clients in the network:**

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  to view all mesh devices, and click  to view all connected clients.

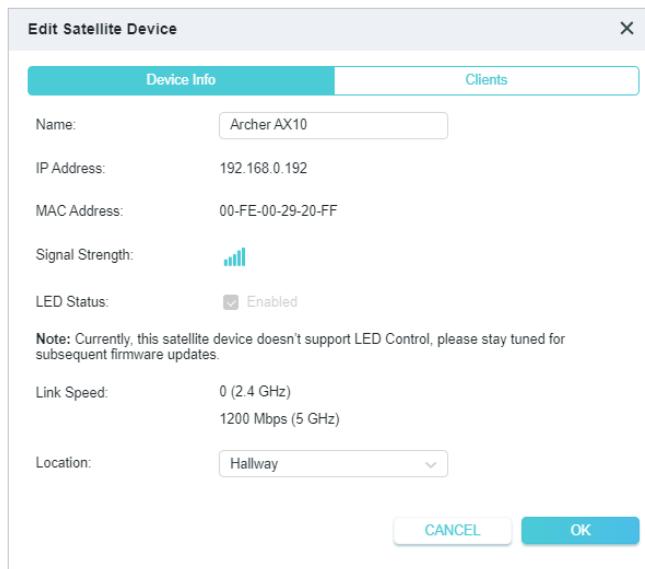
- **To manage an EasyMesh device in the network:**

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. Locate EasyMesh Network section.



Device Info	Location	Clients	Connection	Modify
Archer BE400 00-0A-EB-13-AD-44 192.168.0.1	Not set	1	--	
Archer AX10 00-FE-00-29-20-FF 192.168.0.192	Not set	0		
RE600X A8-6E-84-07-2F-6B 192.168.0.83	Not set	1		

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



Device Info		Clients
Name:	Archer AX10	
IP Address:	192.168.0.192	
MAC Address:	00-FE-00-29-20-FF	
Signal Strength:		
LED Status:	<input checked="" type="checkbox"/> Enabled	
Note: Currently, this satellite device doesn't support LED Control, please stay tuned for subsequent firmware updates.		
Link Speed:	0 (2.4 GHz) 1200 Mbps (5 GHz)	
Location:	Hallway	
<input type="button" value="CANCEL"/>		<input type="button" value="OK"/>

- Change device information.

Chapter 11

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.

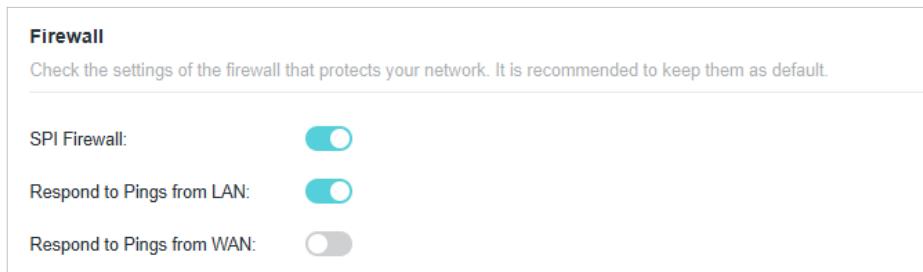
It contains the following sections:

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

11.1. 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.



11.2. 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. 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) Make sure your current Access Control mode is **Deny List**. If not, click **Change Mode**, select Deny List and, click **CHANGE**.

The screenshot shows the 'Access Control' section of a network configuration interface. At the top, it says 'Control the access to your network from the specified devices.' Below this is a toggle switch labeled 'Access Control:' which is turned on. Underneath is a section for 'Current Mode' with a 'Deny List' button and a 'Change Mode' link. A large 'Add' button with a plus sign is located at the top right of the main area. The main table has columns for 'Device Type', 'Device Name', 'MAC Address', and 'Modify'. A message 'There is no entry!' is displayed below the table.

- 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.

The screenshot shows the 'Add Devices' dialog box. It has two options: 'Select From Device List' (selected) and 'Add Manually'. Below is a table with columns for 'Type', 'Device Name', 'IP', and 'MAC'. It lists two devices: '19233109-BG' and 'My Phone'. Each device row has a checkbox and a '...' button. At the bottom are 'CANCEL' and 'ADD' buttons.

Type	Device Name	IP	MAC
<input type="checkbox"/>	19233109-BG	192.168.1.161	4 [redacted]
<input type="checkbox"/>	My Phone	192.168.1.132	7 [redacted] 8 [redacted] 9 [redacted] 0 [redacted]

To allow specific device(s):

- 1) click Change Mode, select Allow List, and click CHANGE.

The screenshot shows the 'Change Mode' dialog box. It has two options: 'Deny List' and 'Allow List'. 'Allow List' is selected. Below each option is a brief description. At the bottom are 'CANCEL' and 'CHANGE' buttons.

Deny List
Configure a deny list to only block access to your network from the specified devices.

Allow List
Configure a allow list to only allow access to your network from the specified devices.

- 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.

Device Type	Device Name	MAC Address	Modify
	My Phone	72-FA-9B-20-4C-29	
	19233109-BG	40-ED-00-22-05-93	

- **Add connected devices**

- 1) Click [Select From Device List](#).
- 2) Select the devices you want to be allowed and click [ADD](#).

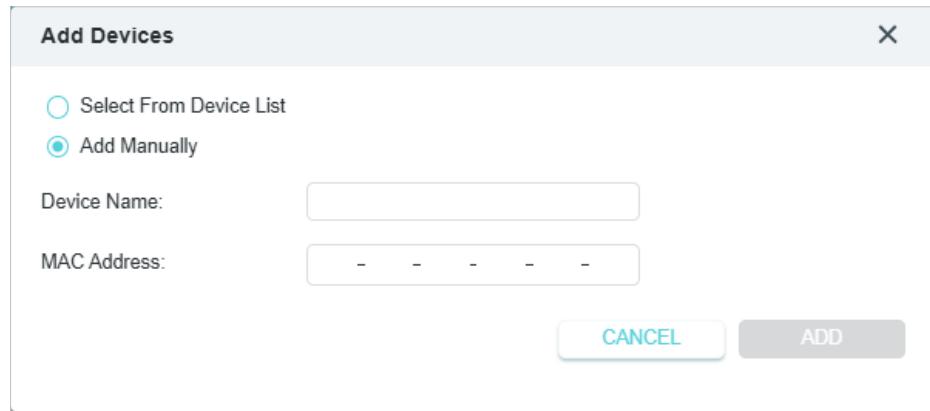
Add Devices

Select From Device List
 Add Manually

Type	Device Name	IP	MAC
<input type="checkbox"/> 	19233109-BG	192.168.1.161	
<input type="checkbox"/> 	My Phone	192.168.1.132	

[CANCEL](#) [ADD](#)

- 3) The [Operation Succeeded](#) message will appear on the screen, which means the selected devices have been successfully added to the allow list.
- **Add unconnected devices**
- 1) Click [Add Manually](#).
 - 2) Enter the [Device Name](#) and [MAC Address](#) of the device you want to be allowed and click [ADD](#).



- 3) The **Operation Succeeded** message will appear on the screen, which means the device has been successfully added to the allow list.

Done!

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

11.3. IP & MAC Binding

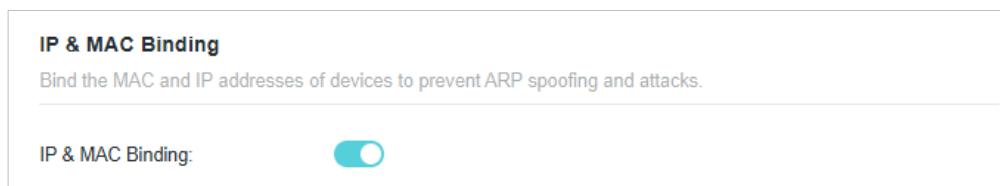
IP & MAC Binding, namely, ARP (Address Resolution Protocol) Binding, is used to bind network device's IP address to its MAC address. This will prevent ARP Spoofing and other ARP attacks by denying network access to a device with matching IP address in the Binding list, but unrecognized MAC address.

I want to:

Prevent ARP spoofing and ARP attacks.

How can I do that?

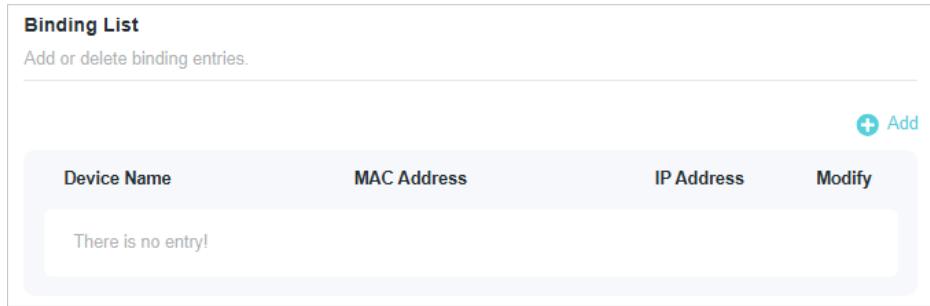
1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [Security](#) > [IP & MAC Binding](#).
3. Enable [IP & MAC Binding](#).



4. Bind your device(s) according to your need.

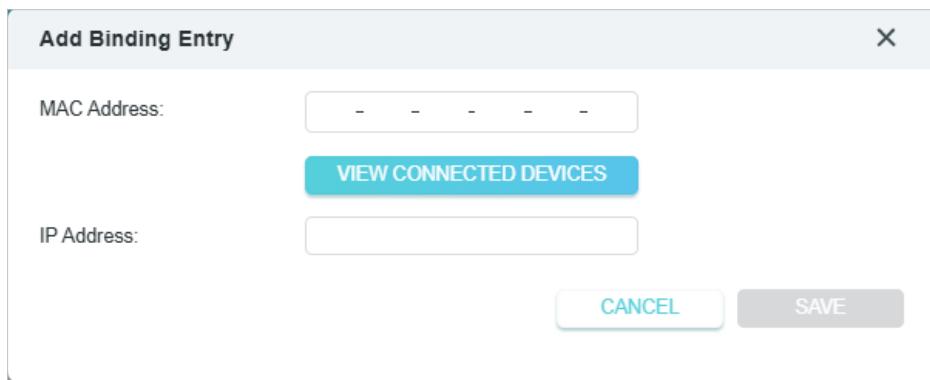
To bind the connected device(s):

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



The screenshot shows a "Binding List" interface. At the top, there's a header with the title "Binding List" and a sub-instruction "Add or delete binding entries." Below this is a table with four columns: "Device Name," "MAC Address," "IP Address," and "Modify." A large message box at the bottom states "There is no entry!"

- 2) Click [VIEW CONNECTED DEVICES](#) and select the device you want to bind. The [MAC Address](#) and [IP Address](#) fields will be automatically filled in.

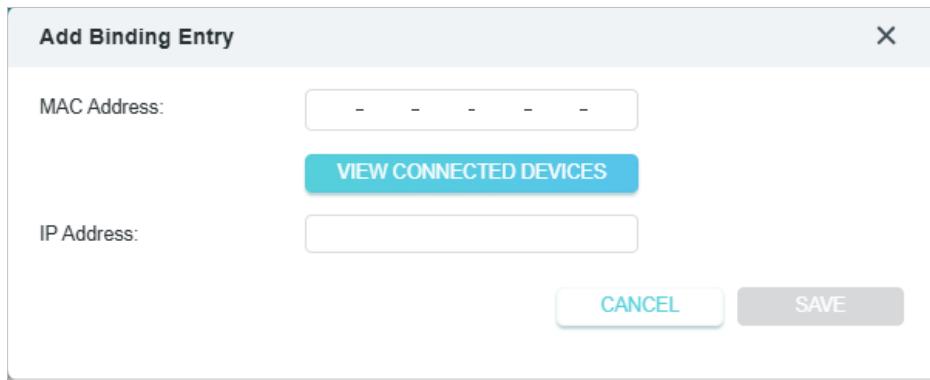


The screenshot shows an "Add Binding Entry" dialog box. It contains fields for "MAC Address" and "IP Address," both currently empty. In the center is a blue button labeled "VIEW CONNECTED DEVICES." At the bottom right are two buttons: "CANCEL" and "SAVE".

- 3) Click [SAVE](#).

To bind the unconnected device:

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



This screenshot is identical to the one above, showing the "Add Binding Entry" dialog box with empty fields for "MAC Address" and "IP Address," and the "VIEW CONNECTED DEVICES" button highlighted.

- 2) Enter the [MAC Address](#) and [IP Address](#) that you want to bind.
- 3) Click [SAVE](#).

Done!

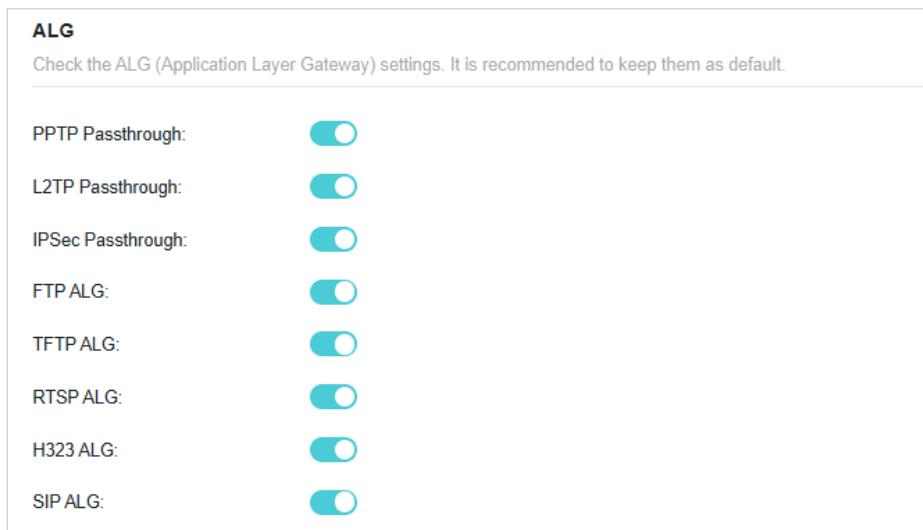
Now you don't need to worry about ARP spoofing and ARP attacks!

11.4. 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.



Chapter 12

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](#)

12.1. Share Local Resources on the Internet by Port Forwarding

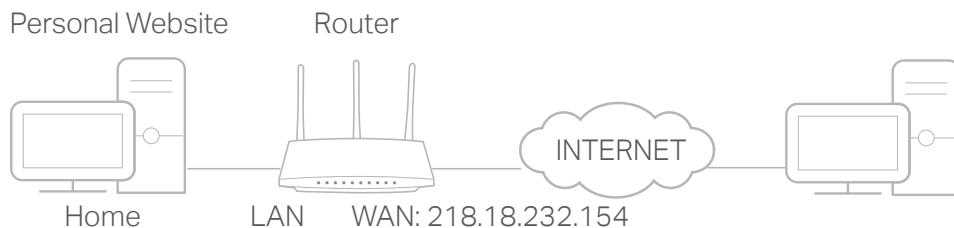
When you build up a server on the local network and want to share it on the internet, Port Forwarding can realize the service and provide it to internet users. At the same time Port Forwarding can keep the local network safe as other services are still invisible from the internet.

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**.
4. Click **Add**.

Port Forwarding

Specify ports to make specific devices or services on your local network accessible over the internet.

Service Name	Device IP Address	External Port	Internal Port	Protocol	Status	Modify
There is no entry!						

5. Click **VIEW COMMON SERVICES** and select **HTTP**. The **External Port**, **Internal Port** and **Protocol** will be automatically filled in.
6. 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.
7. Click **SAVE**.

Add a Port Forwarding Entry

Note: Add a rule for an individual external port or port range. For nonconsecutive ports (example: 100 and 200), add multiple rules. For more info, refer to [Port Forwarding FAQ](#).

Service Name:	<input type="text" value="HTTP"/>
VIEW COMMON SERVICES	
Device IP Address:	<input type="text" value="192.168.0.63"/>
VIEW CONNECTED DEVICES	
External Port:	<input checked="" type="radio"/> Individual Port <input type="radio"/> Port Range <input type="text" value="80"/>
Internal Port:	<input type="text" value="80"/> (Optional)
Protocol:	<input type="button" value="TCP"/>
Enable This Entry:	<input checked="" type="checkbox"/> Enabled
CANCEL 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:

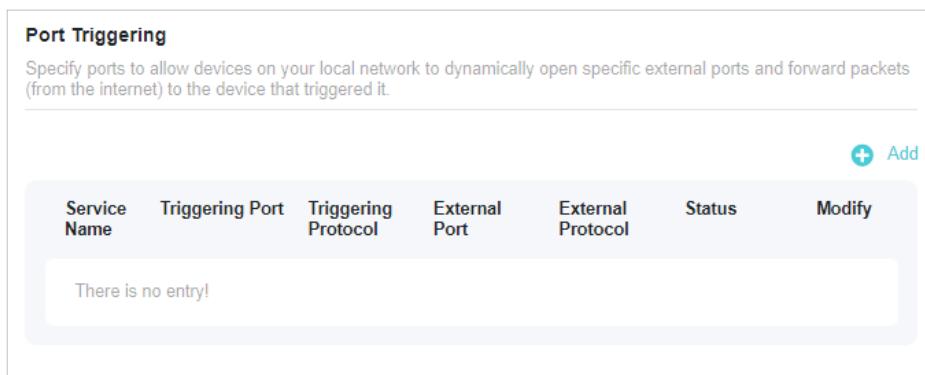
- The WAN IP should be a public IP address. For the WAN IP is assigned dynamically by the ISP, it is recommended to apply and register a domain name for the WAN referring to [Set Up a Dynamic DNS Service Account](#). Then users on the internet can use <http:// domain name> to visit the website.
- If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

12.2. 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:

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 > Port Triggering](#) and click .



Service Name	Triggering Port	Triggering Protocol	External Port	External Protocol	Status	Modify
There is no entry!						

3. 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.

Add a Port Triggering Entry X

Service Name:	MSN Gaming Zone
VIEW COMMON SERVICES	
Triggering Port:	47624
Triggering Protocol:	All
External Port:	2300-2400,28800-29000
External Protocol:	All
Enable This Entry:	<input checked="" type="checkbox"/> Enabled
CANCEL SAVE	

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.

12.3. 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.

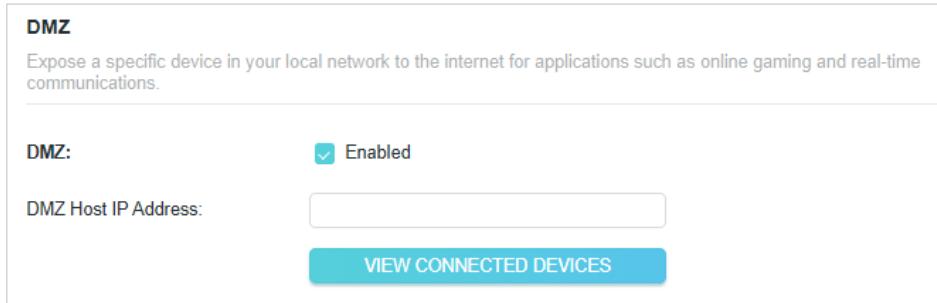
I want to:

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.

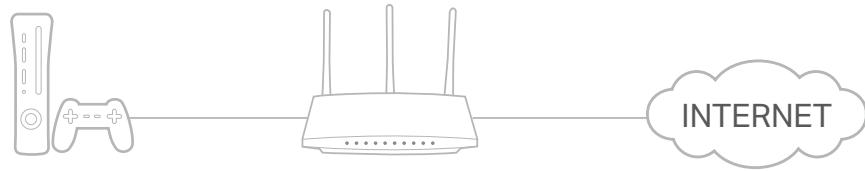
12.4. Make Xbox Online Games Run Smoothly by UPnP

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:

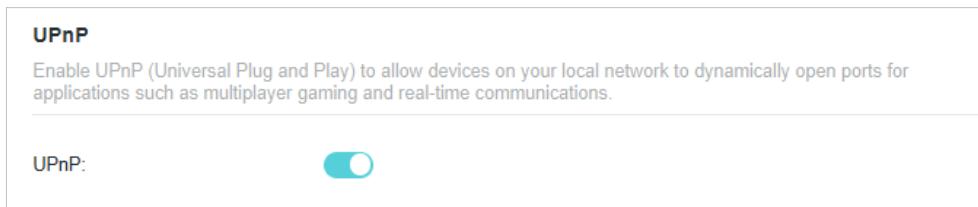
- UPnP is enabled by default in this router.
- Only the application supporting UPnP protocol can use this feature.
- UPnP feature needs the support of operating system (e.g. Windows Vista/ Windows 7/ Windows 8, etc. Some of operating system need to install the UPnP components).

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 13

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.

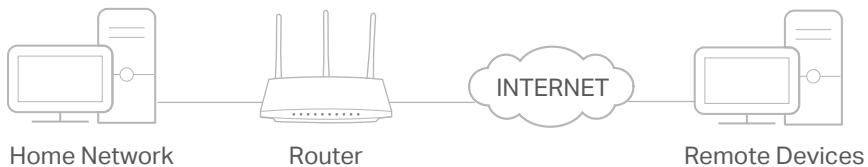
VPN Client allows devices in your home network to access remote VPN servers, without the need to install VPN software on each device.

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](#)

13.1. Use OpenVPN to Access Your Home Network

In the OpenVPN connection, the home network can act as a server, and the remote device can access the server through the router which acts as an OpenVPN Server gateway. To use the VPN feature, you should enable OpenVPN Server on your router, and install and run VPN client software on the remote device. 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:	<input checked="" type="checkbox"/> Enabled
Service Type:	<input checked="" type="radio"/> UDP <input type="radio"/> TCP
Interface Type:	TUN
Service Port:	1194
VPN Subnet:	10.8.0.0
Netmask:	255.255.255.0
Client Access:	Home Network Only

Note:

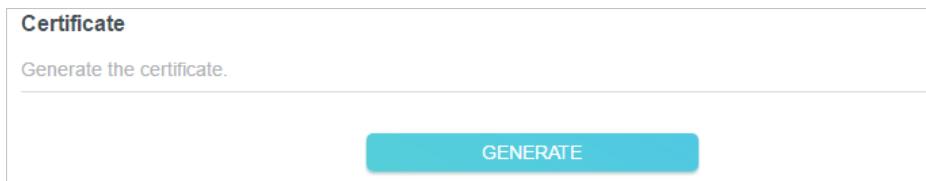
- Before you enable VPN Server, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router's WAN port and synchronize your System Time with internet.
- The first time you configure the OpenVPN Server, you may need to [Generate](#) a certificate before you enable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

13. 2. Use PPTP VPN to Access Your Home Network

PPTP VPN Server is used to create a VPN connection for remote device. To use the VPN feature, you should enable PPTP VPN Server on your router, and configure the PPTP connection on the remote device. 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.

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

PPTP: Enabled

Client IP Address: 10.0.0.11 - 10.0.0.20

Allow Samba (Network Place) access

Allow NetBIOS passthrough

Allow Unencrypted connections

■ 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.

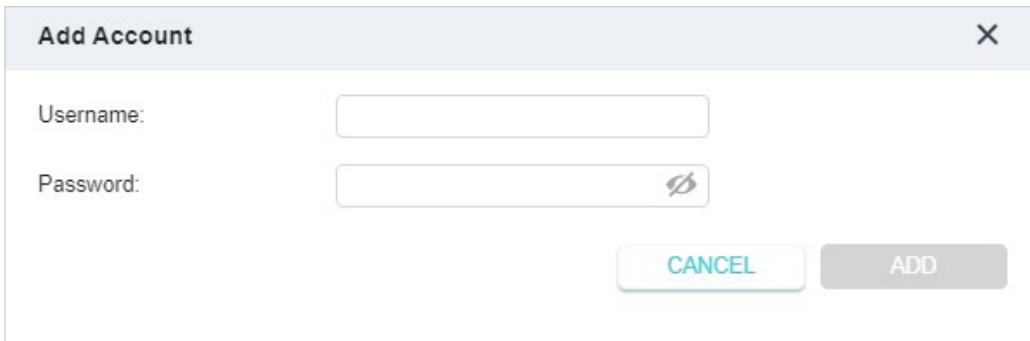
Account List
Configure accounts (up to 16) that can be used by remote clients to connect to the VPN server.

Add

Username	Password	Modify
admin	

1) Click **Add**.

2) Enter the **Username** and **Password** to authenticate devices to the PPTP VPN Server.

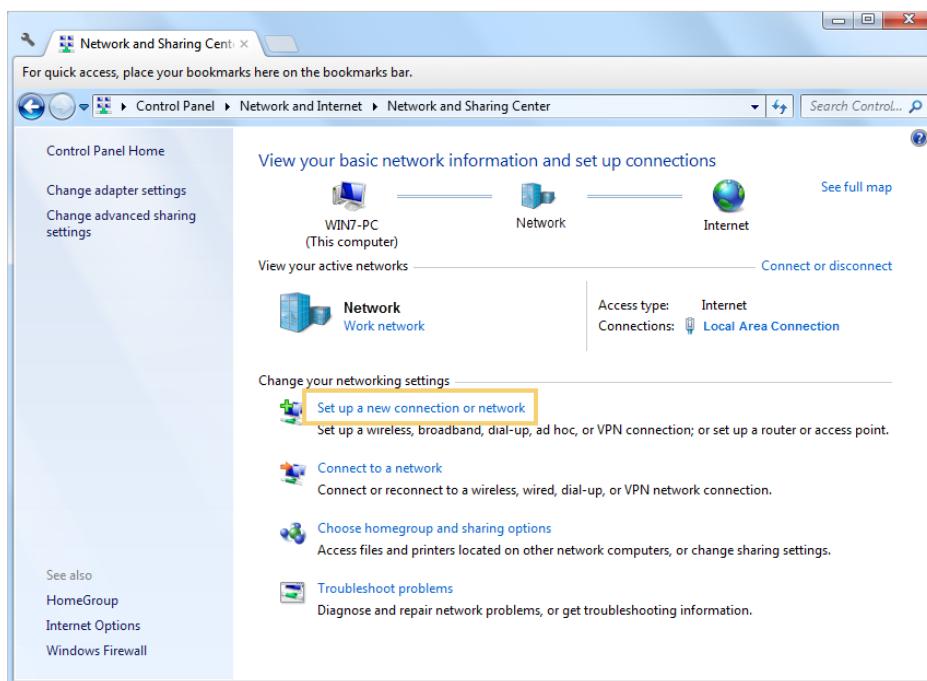


3) Click **ADD**.

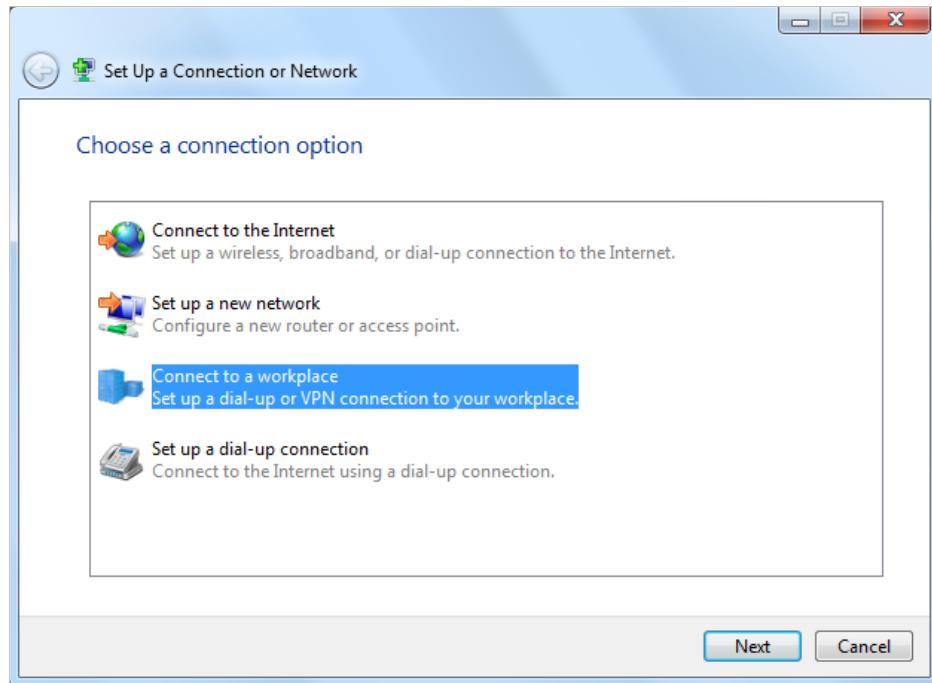
Step 2. Configure PPTP VPN Connection on Your Remote Device

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.

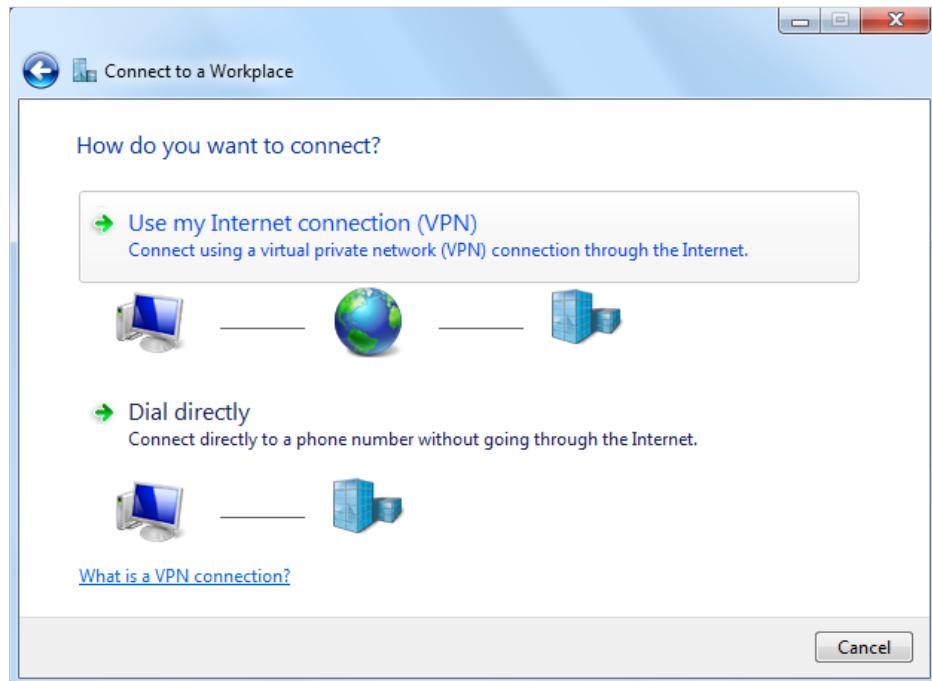
1. Go to [Start > Control Panel > Network and Internet > Network and Sharing Center](#).
2. Select [Set up a new connection or network](#).



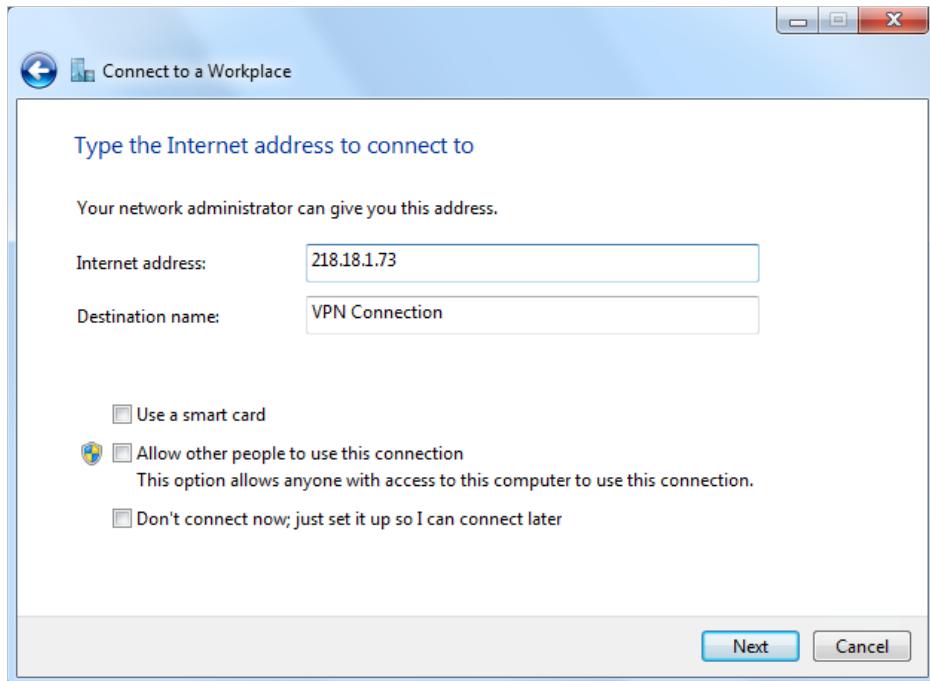
3. Select [Connect to a workplace](#) and click **Next**.



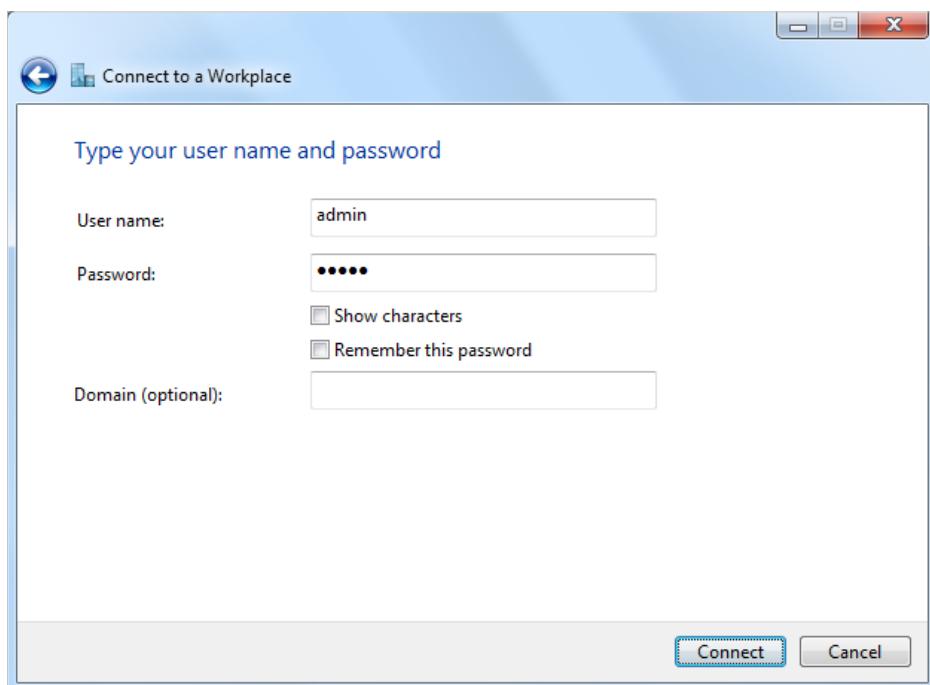
4. Select **Use my Internet connection (VPN)**.



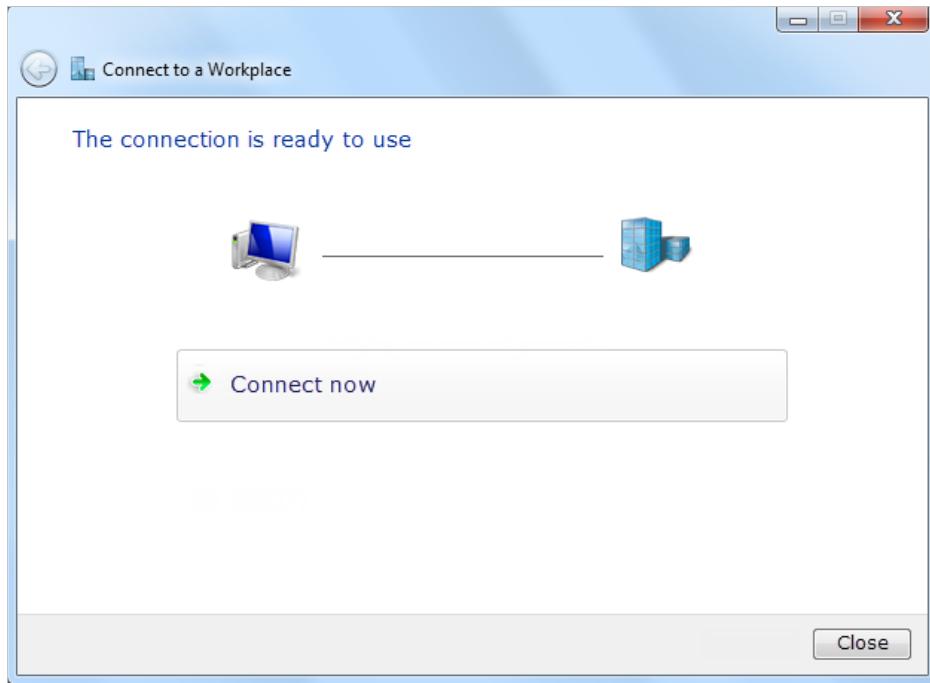
5. Enter the internet IP address of the router (for example: 218.18.1.73) in the **Internet address** field. Click **Next**.



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



7. The PPTP VPN connection is created and ready to use.

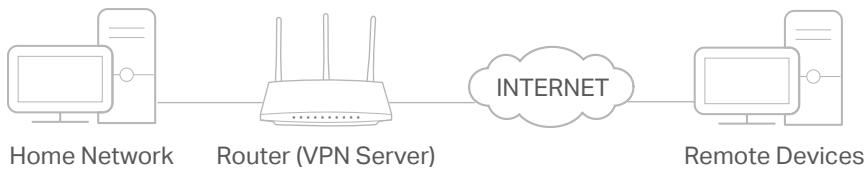


13.3. Use L2TP/IPSec VPN to Access Your Home Network

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.

*Image may differ from your actual product.



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/IP Sec

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

L2TP/IPSec:	<input checked="" type="checkbox"/>
Client IP Address:	<input type="text" value="10.9.0.11"/> - <input type="text" value="10.9.0.20"/>
IPSec Encryption:	<input type="button" value="Encrypted"/>
IPSec Pre-Shared Key:	<input type="text" value="admin"/>
<input type="checkbox"/> Allow NetBIOS passthrough	

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**.
- Note:** Enable NetBIOS Passthrough function to allow NetBIOS packets to be broadcasted through VPN tunnel.
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.

Username	Password	Modify
admin	admin	

Add

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

Add Account

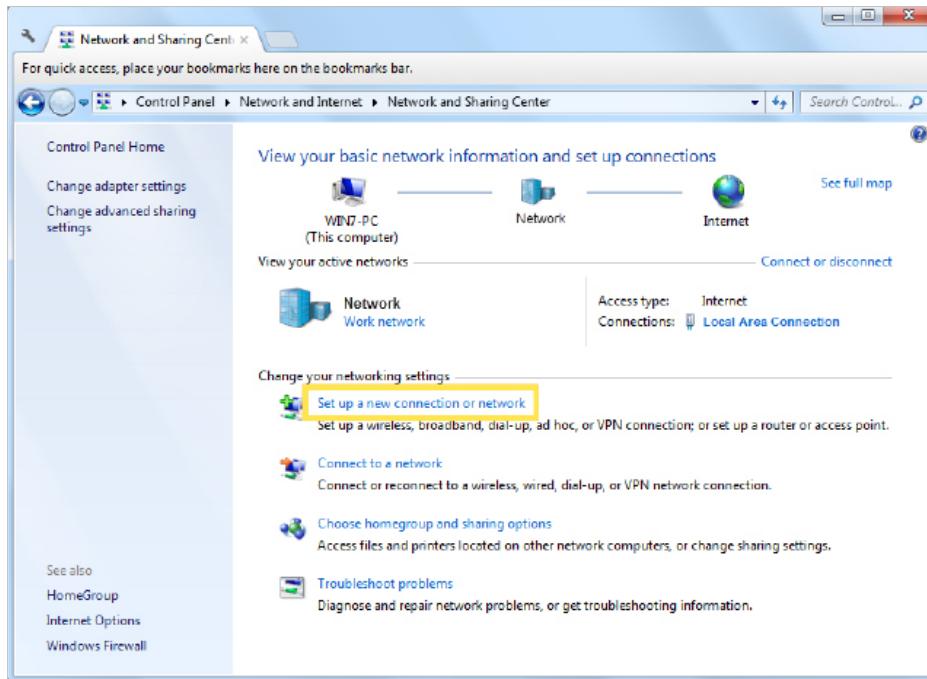
Username:	<input type="text"/>
Password:	<input type="password"/>
CANCEL ADD	

- 6) Click **ADD**.

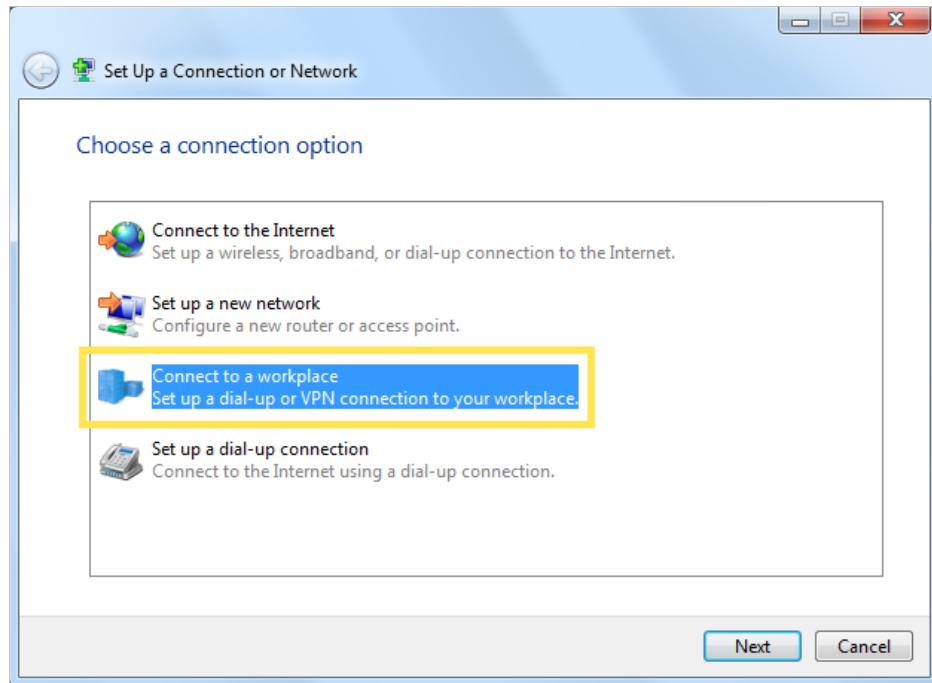
Step 2. Configure L2TP/IPSec VPN Connection on Your Remote Device

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.

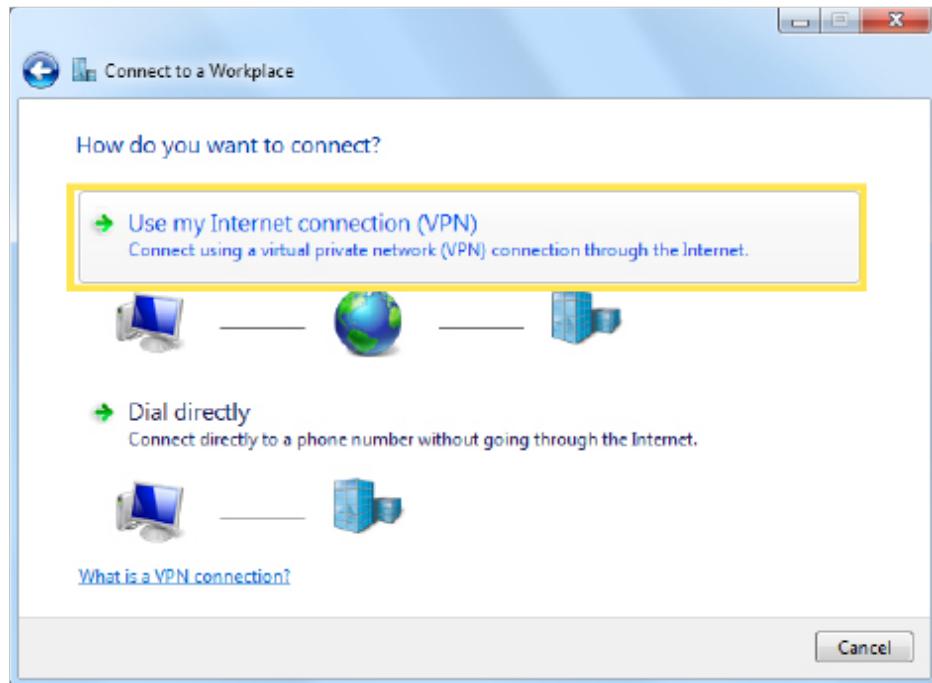
1. Go to [Start > Control Panel > Network and Internet > Network and Sharing Center](#).
2. Select [Set up a new connection or network](#).



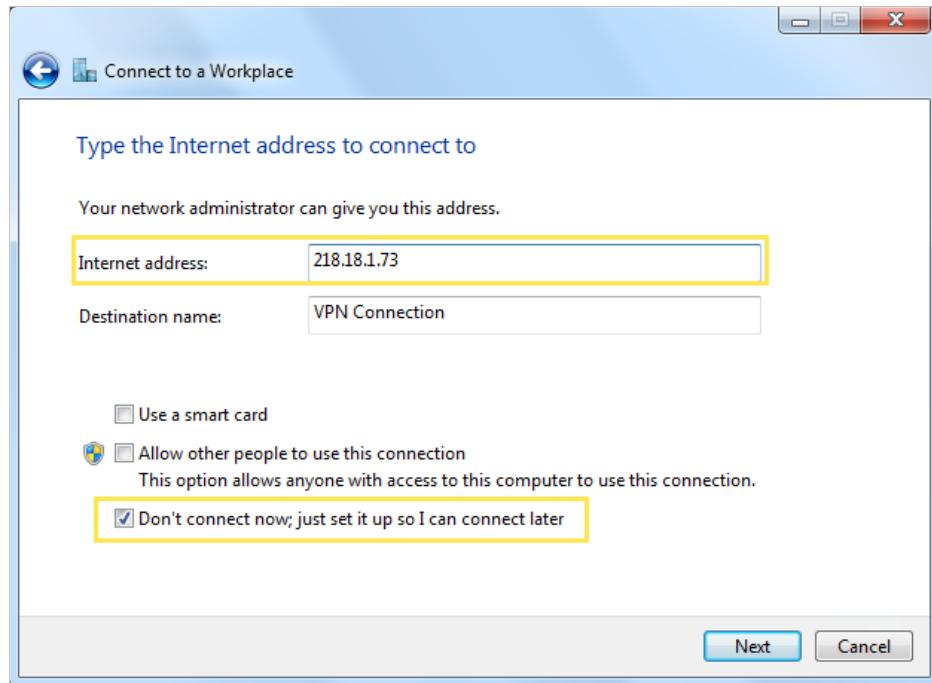
3. Select [Connect to a workplace](#) and click [Next](#).



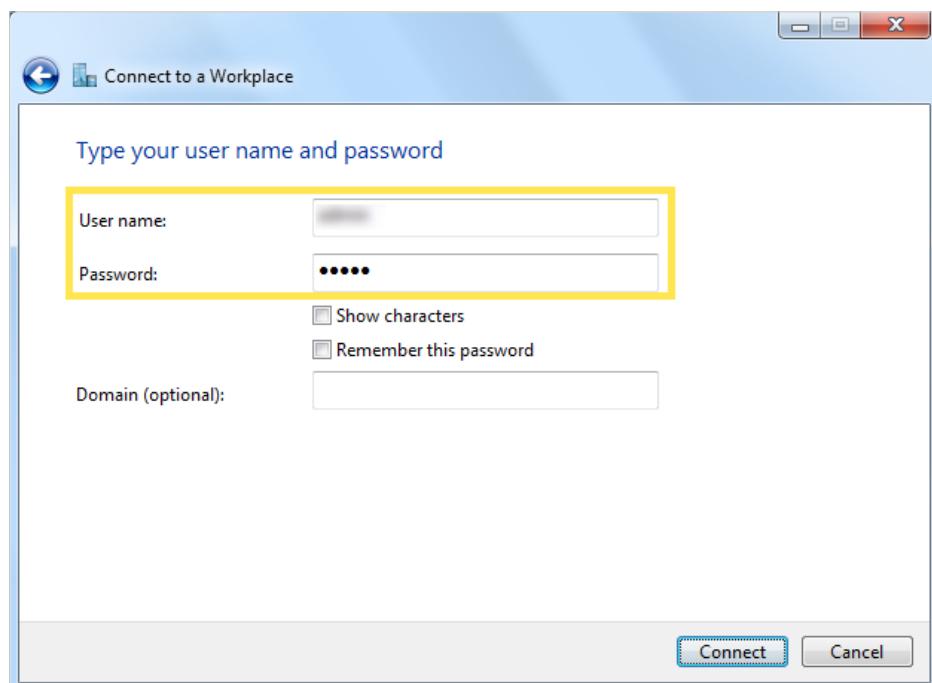
4. Select **Use my Internet connection (VPN)**.



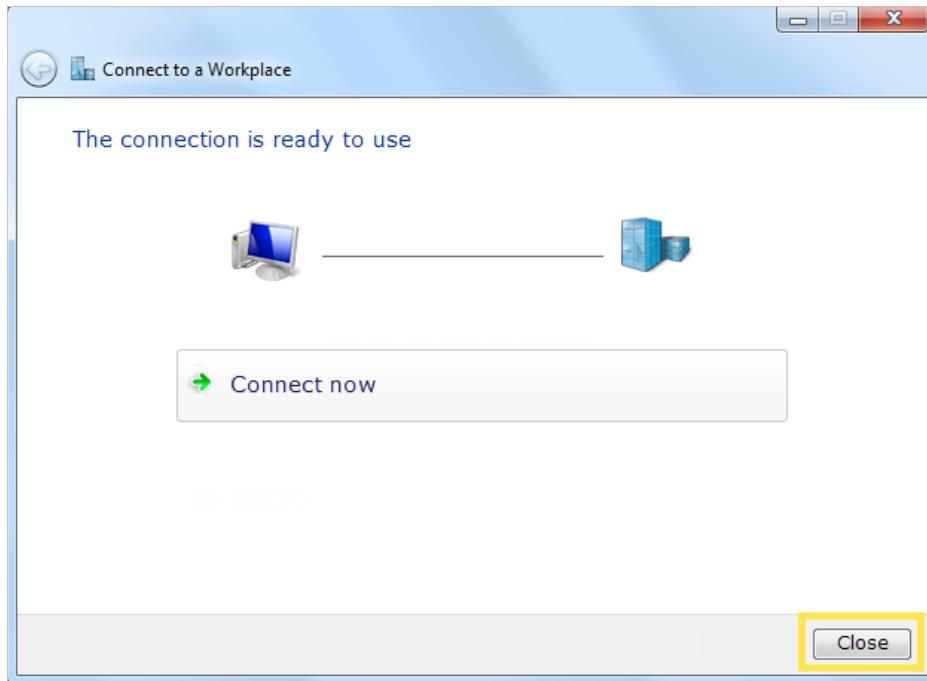
5. Enter the internet IP address of the router (for example: 218.18.1.73) in the **Internet address** field, and select the checkbox **Don't connect now; just set it up so I can connect later**. Click **Next**.



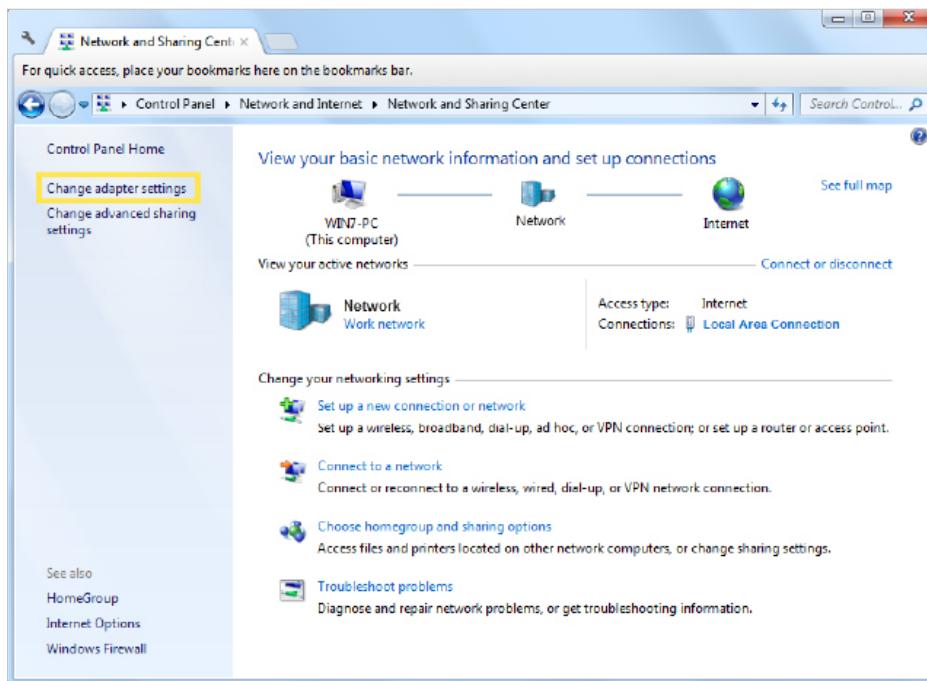
6. Enter the **User name** and **Password** you have set for the L2TP/IPSec VPN server on your router, and click **Connect**.



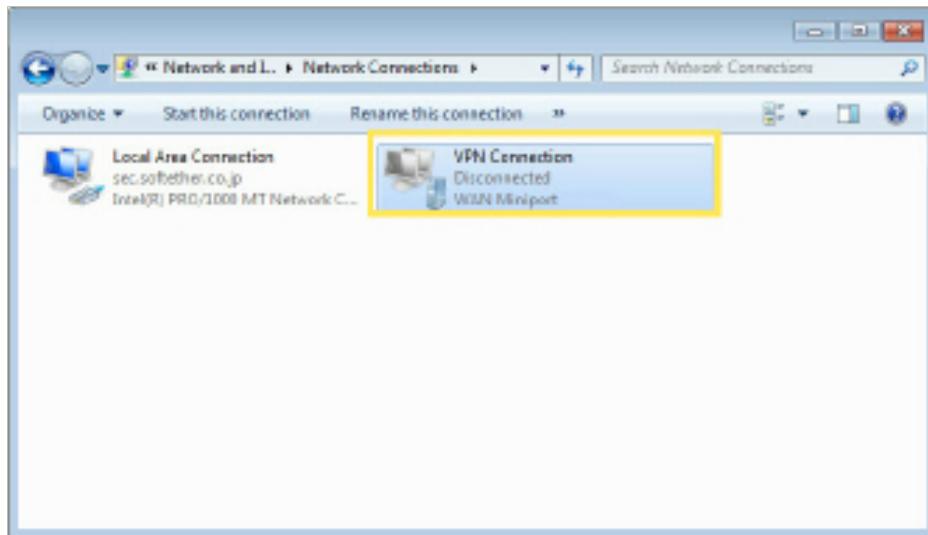
7. Click **Close** when the VPN connection is ready to use



8. Go to Network and Sharing Center and click Change adapter settings.



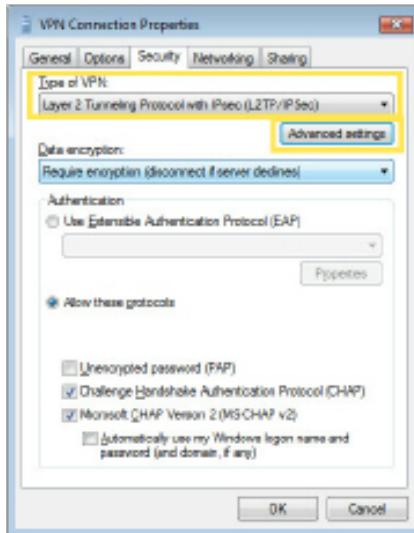
9. Find the VPN connection you created, then double-click it.



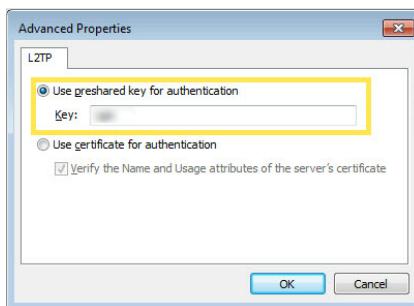
10. Enter the **User name** and **Password** you have set for the L2TP/IPSec VPN server on your router, and click **Properties**.



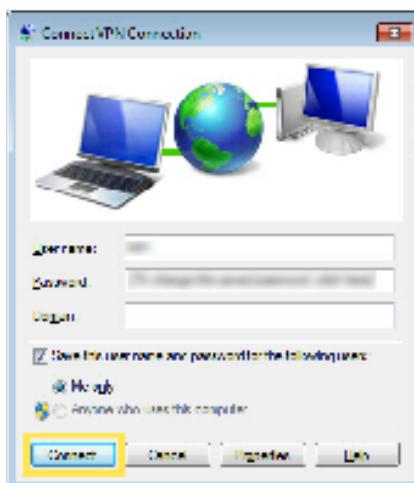
11. Switch to the **Security** tab, select **Layer 2 Tunneling Protocol with IPsec (L2TP/ IPsec)** and click **Advanced settings**.



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.



13.4. 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**.

The screenshot shows the 'WireGuard' configuration page. The 'WireGuard:' section has the 'Enabled' checkbox checked. The 'Tunnel IP Address:' field contains '10.5.5.1/32'. The 'Listen Port:' field contains '51820'. The 'Client Access:' dropdown is set to 'Internet and Home Network'. Below this, the 'Advanced Settings' section is expanded, showing 'DNS: Enabled' (unchecked), 'Persistent Keepalive: 25', and the 'Private Key' and 'Public Key' fields containing long strings of characters. A blue 'RENEW KEY' button is at the bottom.

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.

Add

Username:	<input type="text"/>
Address:	10.5.5.2/32
Allowed IPs (Client):	0.0.0.0/0
Allowed IPs (Server):	10.5.5.2/32
Pre-shared Key (Secret):	<input type="checkbox"/> Enabled

CANCEL **SAVE**

2. Give a **Username** to this account.
3. View 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.

Connect to Server

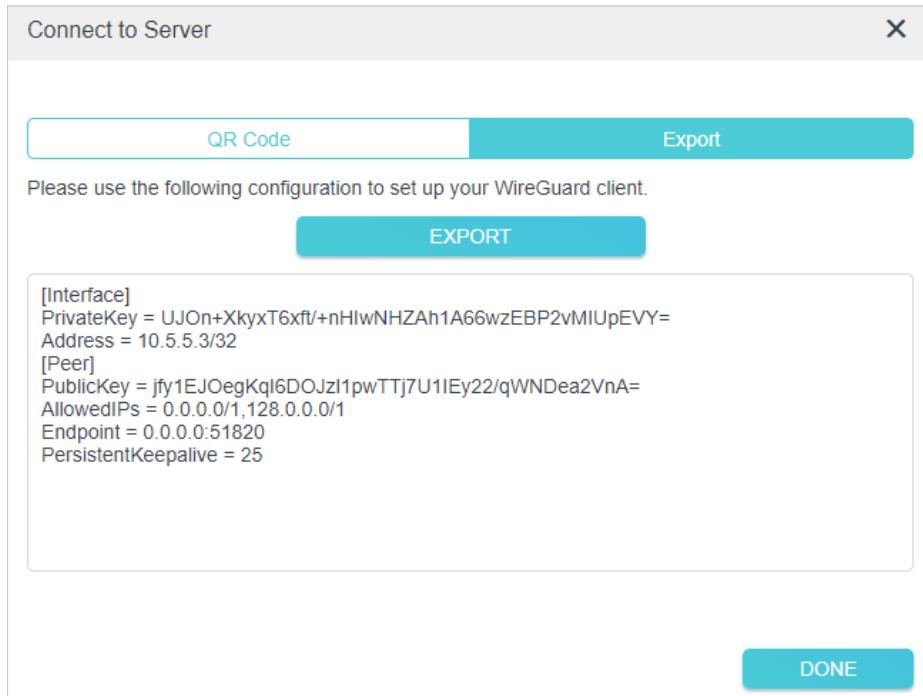
QR Code **Export**

Please download WireGuard App from Google Play or Apple Store, then use the App to scan the QR Code to connect to this server.

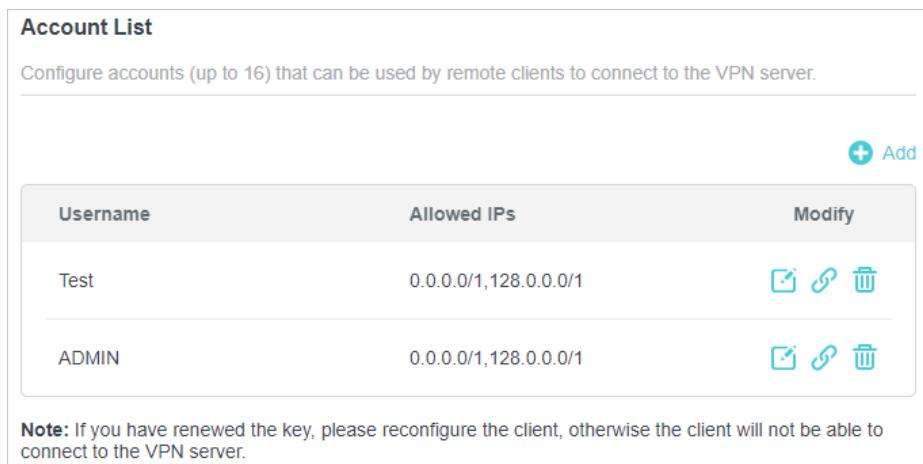


8. Connect to the WireGuard server.

- For mobile phones, download WireGuard App from Google Play or Apple Store, then use the App to scan the QR Code to connect to this server.
- For other devices (e.g. TP-Link WireGuard VPN client), Click **EXPORT** to save the WireGuard VPN configuration file which will be used by the remote device to access your router.



9. On the account list, you can click the button to modify the VPN server settings, connect to the server, or delete the account.

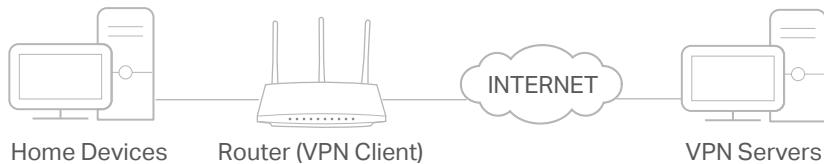


13.5. Use VPN Client to Access a Remote VPN Server

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:

*Image may differ from your actual product.



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**.

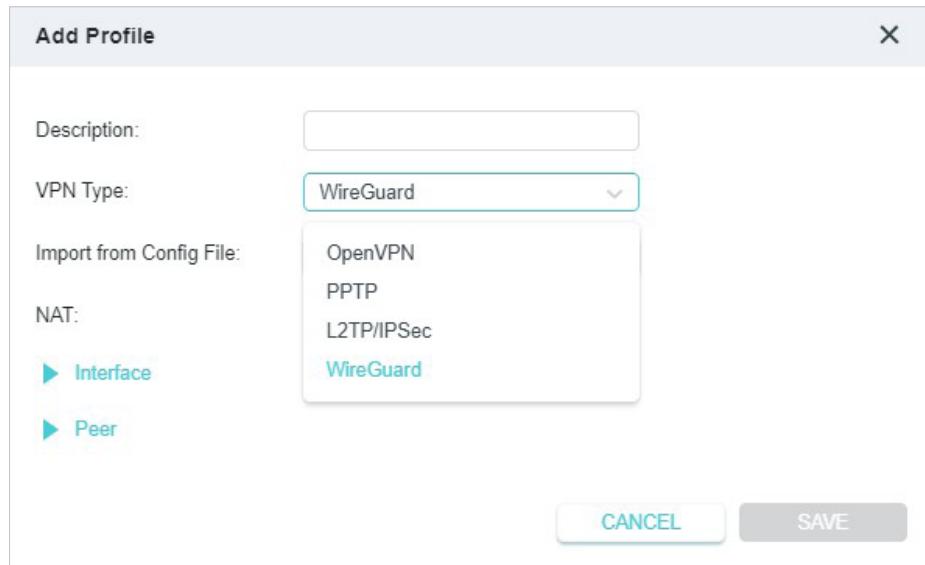
Note: Firmware update may be required to support VPN Client.

3. Enable **VPN Client**, then save the settings.

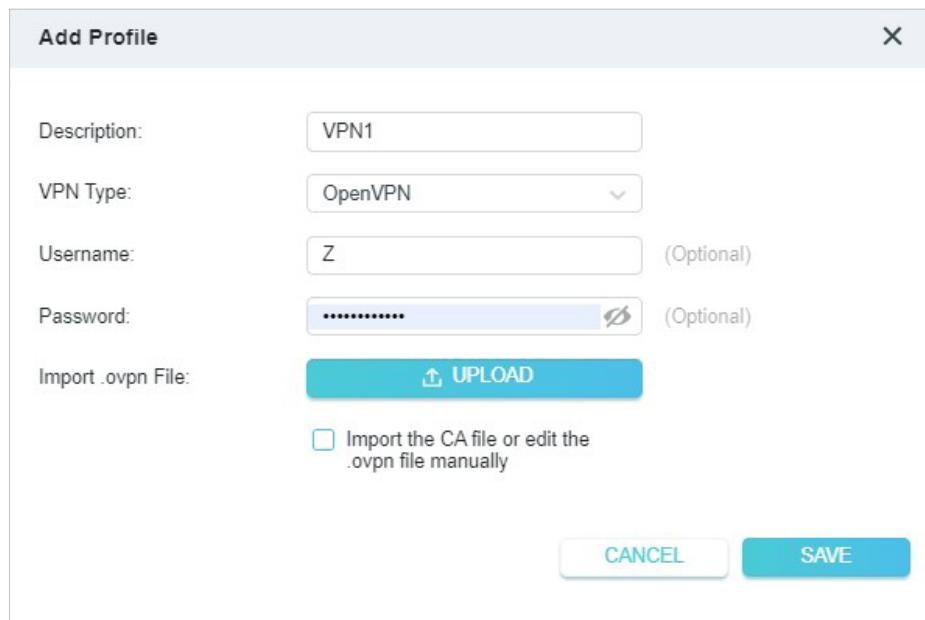


4. Add VPN servers, and enable the one you need.

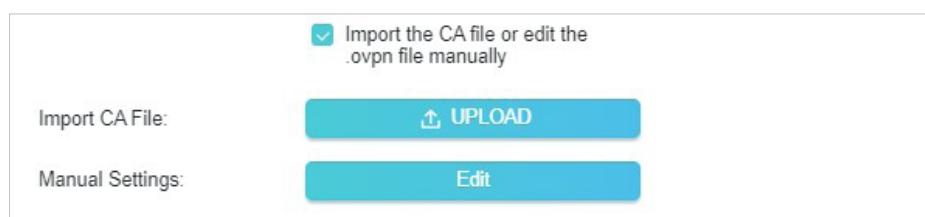
- 1) In the **Server List** section, click **Add**.
- 2) Specify a **Description** for the VPN, and choose the **VPN Type**.



- 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 the 'Add Profile' dialog box. It has a title bar 'Add Profile' at the top left and a close button 'X' at the top right. The form contains the following fields:

- Description: A text input field containing 'VPN1'.
- VPN Type: A dropdown menu set to 'PPTP'.
- VPN Server: An empty text input field.
- Username: An empty text input field.
- Password: An empty text input field with a small circular icon containing a gear symbol to its right.
- Encryption: A dropdown menu set to 'Auto'.

At the bottom right are two buttons: 'CANCEL' and a larger 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 the 'Add Profile' dialog box. It has a title bar 'Add Profile' at the top left and a close button 'X' at the top right. The form contains the following fields:

- Description: A text input field containing 'VPN1'.
- VPN Type: A dropdown menu set to 'L2TP/IPSec'.
- VPN Server: An empty text input field.
- Username: An empty text input field.
- Password: An empty text input field with a small circular icon containing a gear symbol to its right.
- IPSec Pre-Shared Key: An empty text input field.

At the bottom right are two buttons: 'CANCEL' and a larger 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:	VPN1
VPN Type:	WireGuard
Import from Config File:	<input type="button" value="UPLOAD"/>
NAT:	<input checked="" type="checkbox"/> Enabled
▼ Interface	
Private Key:	
Address:	
DNS Server 1:	(Optional)
DNS Server 2:	(Optional)
MTU Size:	1420 bytes (Optional)
▼ Peer	
Public Key:	
Pre-Shared Key:	(Optional)
Allowed IPs:	
Endpoint Address:	
Endpoint Port:	
Persistent Keepalive:	25 (Optional)
<input type="button" value="CANCEL"/> <input type="button" value="SAVE"/>	

- 4) Save the settings.
- 5) In the server list, enable the VPN server you need.

Server List				
Add or edit VPN server. Up to 6 VPN servers can be added.				
Description	VPN Type	Status	ENABLE	Modify
vpn3	L2TP/IPSec	Disconnected	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input type="button" value="Delete"/>
vpn2	PPTP	Disconnected	<input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="button" value="Delete"/>
vpn1	OpenVPN	Disconnected	<input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="button" value="Delete"/>
vpn4	WireGuard	Disconnected	<input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="button" value="Delete"/>

5. Add and manage the devices that will use the VPN function.

- 1) In the **Device List** section, click **Add**.
- 2) Choose and add the devices that will access the VPN server you have configured.

Add Profile

Description:	<input type="text"/>
VPN Type:	<input checked="" type="button" value="WireGuard"/> <input type="button" value="OpenVPN"/> <input type="button" value="PPTP"/> <input type="button" value="L2TP/IPSec"/>
Import from Config File:	<input type="button" value="OpenVPN"/> <input type="button" value="PPTP"/> <input type="button" value="L2TP/IPSec"/> <input checked="" type="button" value="WireGuard"/>
NAT:	<input type="button" value="Interface"/> <input type="button" value="Peer"/>
	<input type="button" value="CANCEL"/> <input checked="" type="button" value="SAVE"/>

6. Save the settings.

Device List				
Manage devices that will use the VPN function.				
Type	Device Name	MAC Address	VPN Access	Modify
...	FC:AA:14:55:FB:5D	<input checked="" type="checkbox"/>	
...	My iPhone	86:D2:DE:B9:18:62	<input checked="" type="checkbox"/>	

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

Chapter 14

Customize Your Network Settings

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

It contains the following sections:

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

14.1. 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.

LAN

View and configure LAN settings.

MAC Address: 98-DA-C4-B4-01-D8

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

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.

14.2. Set Up Link Aggregation

The Link Aggregation feature combines two ports (LAN2 & LAN3) 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**.

Link Aggregation

Combine two ports(LAN2 and LAN3) together to make a single high-bandwidth data path.

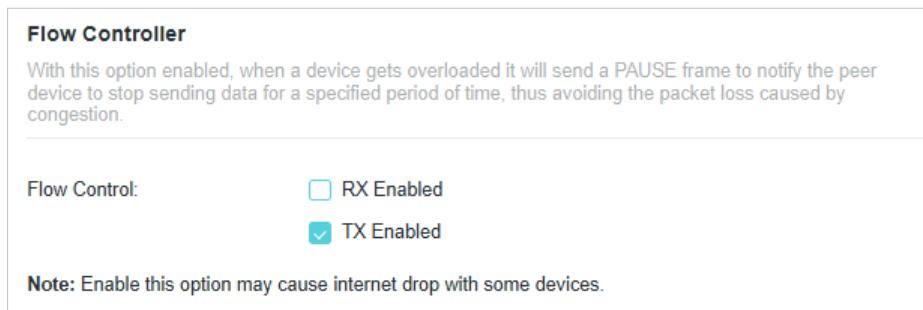
Link Aggregation: Enabled

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

14.3. 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.



14.4. 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.

IGMP
Check the multicast settings. It is recommended to keep them as default.

IGMP Proxy: Enabled

IGMP Snooping: Enabled

IGMP Version: V2

2) Click **SAVE**.

3) 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.

IPTV/VLAN
Configure IPTV/VLAN settings if you want to enjoy IPTV or VoIP service, or if your ISP requires VLAN tags.

IPTV/VLAN: Enabled

Mode: Bridge

LAN 1: Internet

LAN 2: Internet

LAN 3: IPTV

LAN 4: IPTV

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.

14.5. 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
Dynamically assign IP addresses to the devices connected to the router.

DHCP Server:	<input checked="" type="checkbox"/> Enabled
IP Address Pool:	192.168.1.2 - 192.168.1.253
Address Lease Time:	120 minutes
Default Gateway:	192.168.1.1 (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:**

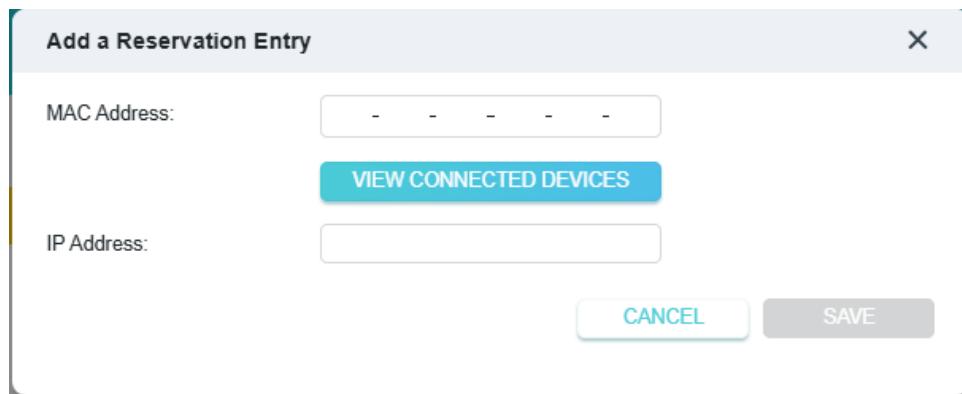
1. Click **Add** in the **Address Reservation** section.

Address Reservation
Reserve IP addresses for specific devices connected to the router.

Device Name	MAC Address	Reserved IP Address	Status	Modify
There is no entry!				

+ Add

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.

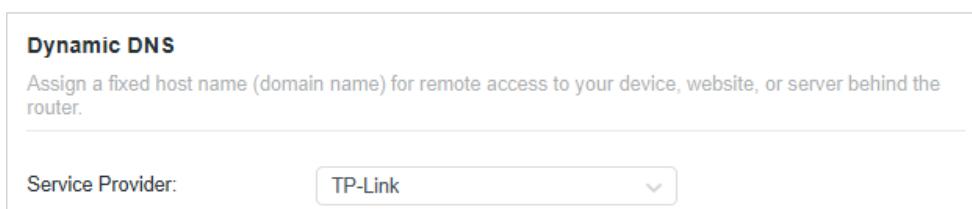
4. Click **SAVE**.

14. 6. 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**.



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.

The screenshot shows the 'Dynamic DNS' configuration page. At the top, there is a note: 'Assign a fixed host name (domain name) for remote access to your device, website, or server behind the router.' Below this, a dropdown menu shows 'Service Provider: TP-Link'. A 'Current Domain Name:' field is present. A 'Domain Name List' table is shown, with a 'Register' button at the top right. The table has columns: Domain Name, Registered Date, Status, Operation, and Delete. It displays the message 'No Entries'.

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

The screenshot shows the login interface for NO-IP or DynDNS. It includes fields for 'Service Provider' (set to 'NO-IP'), 'Username', 'Password' (with a visibility icon), 'Domain Name', 'WAN IP binding' (checkbox labeled 'Enabled'), and 'Status' (set to 'Not launching'). At the bottom are 'LOGIN AND SAVE' and 'LOGOUT' buttons.

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.

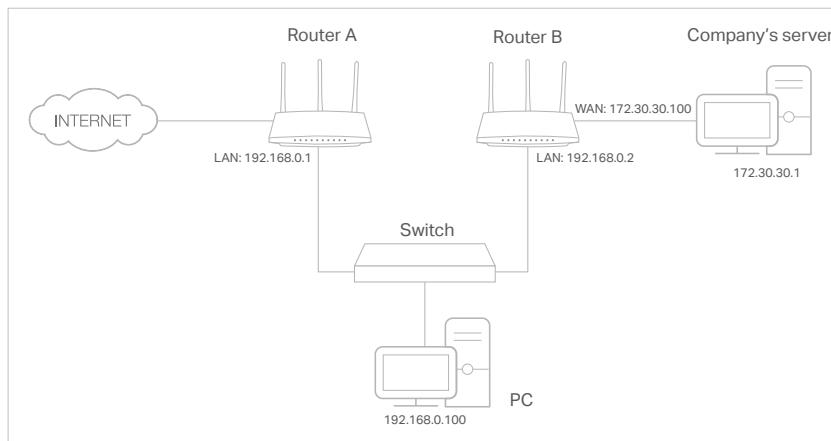
14.7. Create Static Routes

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.



How can I do that?

1. Change the routers' LAN IP addresses to two different IP addresses on the same subnet. Disable Router B's DHCP function.
2. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for Router A.
1. Go to Advanced > Network > Routing.

Static Routing

Predetermine a fixed route for network packets to reach a specific host or network.

Network Destination	Subnet Mask	Default Gateway	Interface	Description	Status	Modify
There is no entry!						

2. Click **Add** and finish the settings according to the following explanations:

Add a Routing Entry

Network Destination:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Default Gateway:	<input type="text"/>
Interface:	- Please Select -
Description:	<input type="text"/>

CANCEL **SAVE**

Network Destination: The destination IP address that you want to assign to a static route. This IP address cannot be on the same subnet with the WAN IP or LAN IP of Router A. In the example, the IP address of the company network is the destination IP address, so here enter 172.30.30.1.

Subnet Mask: Determines the destination network with the destination IP address. If the destination is a single IP address, enter 255.255.255.255; otherwise, enter the subnet mask of the corresponding network IP. In the example, the destination network is a single IP, so here enter 255.255.255.255.

Default Gateway: The IP address of the gateway device to which the data packets will be sent. This IP address must be on the same subnet with the router's IP which sends out data. In the example, the data packets will be sent to the LAN port of Router B and then to the Server, so the default gateway should be 192.168.0.2.

Interface: Determined by the port (WAN/LAN) that sends out data packets. In the example, the data are sent to the gateway through the LAN port of Router A, so **LAN/WLAN** should be selected.

Description: Enter a description for this static routing entry.

3. Click **SAVE**.
4. Check the **Routing Table** below. If you can find the entry you've set, the static routing is set successfully.

Routing Table			
View all valid routing entries that are currently in use.			
Active Route Number: 3		 Refresh	
Network Destination	Subnet Mask	Gateway	Interface
0.0.0.0	0.0.0.0	192.168.0.1	WAN
192.168.0.0	255.255.255.0	0.0.0.0	WAN
192.168.1.0	255.255.255.0	0.0.0.0	LAN

Done!

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

Chapter 15

Manage the Router

This chapter will show you the configuration for managing and maintaining your router.

It contains the following sections:

- [Update the Firmware](#)
- [Backup and Restore Configuration Settings](#)
- [Change the Login Password](#)
- [Password Recovery](#)
- [Local Management](#)
- [Remote Management](#)
- [System Log](#)
- [Test the Network Connectivity](#)
- [Set System Time and Language](#)
- [Set the Router to Reboot Regularly](#)
- [Control the LED](#)

15.1. Update the Firmware

TP-Link aims at providing better network experience for users.

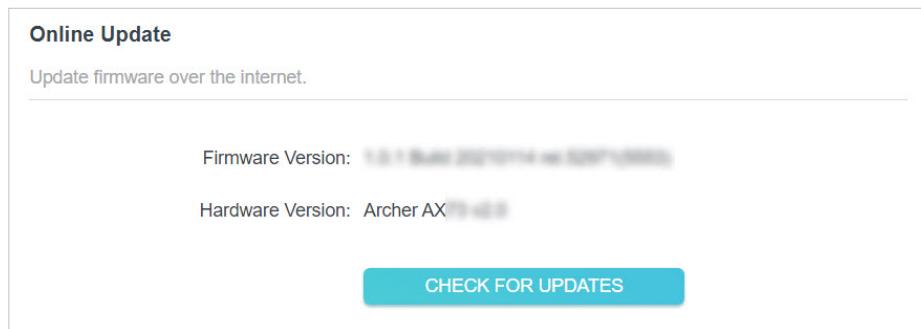
We will inform you through the web management page if there's any new firmware available for your router. Also, the latest firmware will be released at the TP-Link official website www.tp-link.com, and you can download it from the [Support](#) page for free.

■ Note:

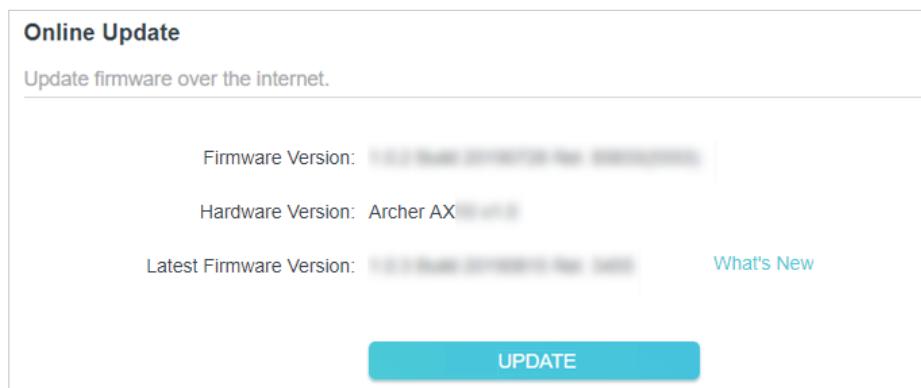
- Back up your router's configurations before firmware update.
- Do NOT turn off the router during the firmware update.

15.1.1. Online Update

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. When the latest firmware is available for your router, the update icon  will display in the top-right corner of the page. Click the icon to go to the [Firmware Update](#) page.
Alternatively, you can go to [Advanced > System > Firmware Update](#), and click **CHECK FOR UPDATES** to see whether the latest firmware is released.



3. Focus on the [Online Update](#) section, and click **UPDATE** if there is new firmware.

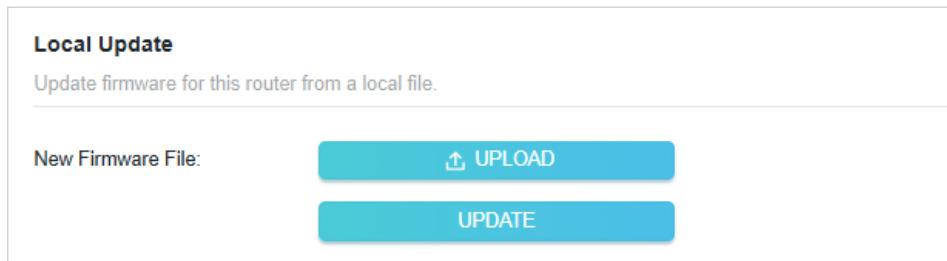


4. Wait a few minutes for the update and reboot to complete.

🕒 Tips: If there's a new and important firmware update for your router, you will see the prompt notification on your computer as long as a web browser is opened. Click to update, and log in to the web management page with the username and password you set for the router. You will see the [Firmware Update](#) page.

15.1.2. Local Update

1. Download the latest firmware file for the router from www.tp-link.com.
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 > System > Firmware Update.
4. Focus on the Local Update section. Click BROWSE to locate the downloaded new firmware file, and click UPDATE.



5. Wait a few minutes for the update and reboot to complete.

■ Note: If you fail to update the firmware for the router, please contact our [Technical Support](#).

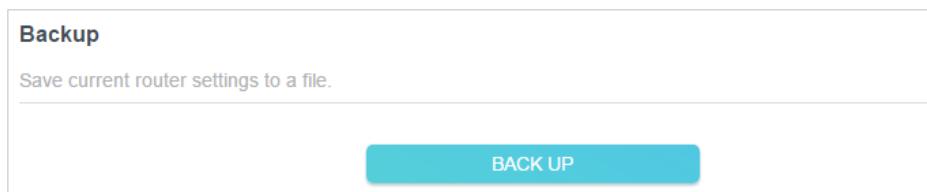
15.2. Backup and Restore Configuration Settings

The configuration settings are stored as a configuration file in the router. You can backup the configuration file to your computer for future use and restore the router to a previous settings from the backup file when needed. Moreover, if necessary you can erase the current settings and reset the router to the default factory 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 > System Tools > Backup & Restore.

- **To backup configuration settings:**

Click BACK UP to save a copy of the current settings to your local computer. A '.bin' file of the current settings will be stored to your computer.



- **To restore configuration settings:**

1. Click BROWSE to locate the backup configuration file stored on your computer, and click RESTORE.

Restore
Restore settings from a backup file.

File:

UPLOAD

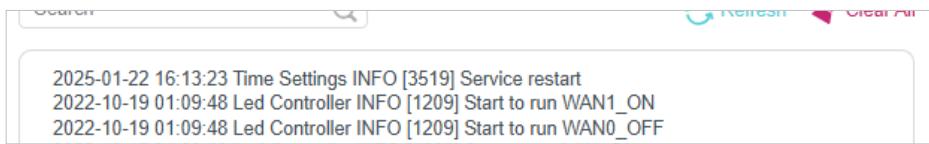
RESTORE

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

■ Note: During the restoring process, do not turn off or reset the router.

- **To reset the router except your login password and TP-Link ID:**

1. In the Factory Default Restore section, click RESTORE.



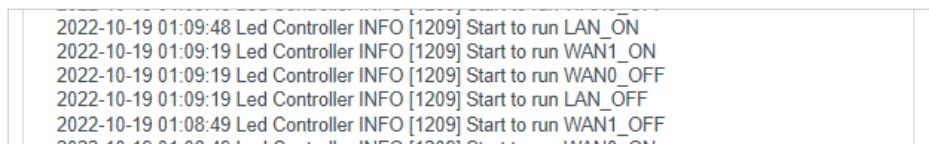
2. Wait a few minutes for the resetting and rebooting.

■ Note:

- During the resetting process, do not turn off the router.
- After reset, you can still use the current login password or the TP-Link ID to log in to the web management page.

- **To reset the router to factory default settings:**

1. Click FACTORY RESTORE to reset the router.



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

■ Note:

- During the resetting process, do not turn off or reset the router.
- We strongly recommend you backup the current configuration settings before resetting the router.

15.3. Change the Login Password

The account management feature allows you to change your login password of the web management page.

■ Note: If you are using a TP-Link ID to log in to the web management page, the account management feature will be disabled. To manage the TP-Link ID, go to [Advanced > TP-Link ID](#).

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced > System > Administration](#) and focus on the [Change Password](#) section.

Change Password

Change the router's local management password.

Old Password:	<input type="text"/>	
New Password:	<input type="text"/>	
Confirm New Password:	<input type="text"/>	

3. Enter the old password, then a new password twice (both case-sensitive). Click **SAVE**.
4. Use the new password for future logins.

15.4. Password Recovery

This feature allows you to recover the login password you set for your router in case you forget it.

 Note: If you are using a TP-Link ID to log in to the web management page, the Password Recovery feature will be disabled. To manage the TP-Link ID, go to [Advanced > TP-Link ID](#).

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced > System > Administration](#) and focus on the [Password Recovery](#) section.
3. Tick the [Enable](#) box of [Password Recovery](#).

Password Recovery

Reset local management password via preset questions and answers.

Password Recovery:	<input checked="" type="checkbox"/> Enabled
From:	<input type="text"/>
To:	<input type="text"/>
SMTP Server:	<input type="text"/>
Authentication:	<input type="checkbox"/> Enabled

4. Specify a [mailbox \(From\)](#) for sending the recovery letter and enter its [SMTP Server](#) address. Specify a [mailbox \(To\)](#) for receiving the recovery letter. If the mailbox (From) to send the recovery letter requires encryption, Tick the [Enable](#) box of [Authentication](#) and enter its username and password.

 **Tips:**

- SMTP server is available for users in most webmail systems. For example, the SMTP server address of Gmail is smtp.gmail.com.
- Generally, Authentication should be enabled if the login of the mailbox requires username and password.

5. Click **SAVE**.

To recover the login password, please visit <http://tplinkwifi.net>, click **Forgot Password?** on the login page and follow the instructions to set a new password.

15.5. Local Management

This feature allows you to limit the number of client devices on your LAN from accessing the router by using the MAC address-based authentication.

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 > Administration** and complete the settings In **Local Management** section as needed.

- **Access the router via HTTPS and HTTP:**

Tick the **Enable** box of **Local Management via HTTPS** to access the router via HTTPS and HTTP, or keep it disabled to access the router only via HTTP.

Local Management
Access and manage the router from local network devices.

Local Management via HTTPS: Enabled

Local Managers:

- **Allow all LAN connected devices to manage the router:**

Select **All Devices** for **Local Managers**.

Local Management
Access and manage the router from local network devices.

Local Management via HTTPS: Enabled

Local Managers:

- **Allow specific devices to manage the router:**

1. Select **All Devices** for **Local Managers** and click **SAVE**.

Local Management
Access and manage the router from local network devices.

Local Management via HTTPS: Enabled

Local Managers: Specified Devices

Add Device

Description	MAC Address	Modify
There is no entry!		

2. Click **Add Device**.

Add Device

Description: (Optional)

VIEW CONNECTED DEVICES

MAC Address:

CANCEL SAVE

3. Click **VIEW CONNECTED DEVICES** and select the device to manage the router from the Connected Devices list, or enter the MAC address of the device manually.
4. Specify a **Description** for this entry.
5. Click **SAVE**.

15.6. Remote Management

This feature allows you to control remote devices' authority to manage 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 > System > Administration** and complete the settings in **Remote Management** section as needed.
 - **Forbid all devices to manage the router remotely:**

Do not tick the **Enable** checkbox of **Remote Management**.

Remote Management

Access and manage the router over the internet.

Note: Remote Management is not supported when you are connected to the internet only via IPv6. If you want to use Remote Management, please make sure you have set up an IPv4 connection first.

Remote Management: Enabled

- **Allow all devices to manage the router remotely:**

Remote Management

Access and manage the router over the internet.

Note: Remote Management is not supported when you are connected to the internet only via IPv6. If you want to use Remote Management, please make sure you have set up an IPv4 connection first.

Remote Management: Enabled

HTTPS Port: 443

Web Address for Management: <https://192.168.0.101:443>

Remote Managers: All Devices

1. Tick the **Enable** checkbox of **Remote Management**.
2. Keep the HTTPS and HTTP port as default settings (recommended) or enter a value between 1024 and 65535.
3. Select **All Devices** for **Remote Managers**.
4. Click **SAVE**.

Devices on the internet can log in to <http://Router's WAN IP address:port number> (such as <http://113.116.60.229:1024>) to manage the router.

 **Tips:**

- You can find the WAN IP address of the router on [Network Map > Internet](#).
- The router's WAN IP is usually a dynamic IP. Please refer to [Set Up a Dynamic DNS Service Account](#) if you want to log in to the router through a domain name.

- **Allow a specific device to manage the router remotely:**

Remote Management

Access and manage the router over the internet.

Note: Remote Management is not supported when you are connected to the internet only via IPv6. If you want to use Remote Management, please make sure you have set up an IPv4 connection first.

Remote Management:	<input checked="" type="checkbox"/> Enabled
HTTPS Port:	443
Web Address for Management:	https://192.168.0.101:443
Remote Managers:	Specified Device
Only this IP Address:	

1. Tick the **Enable** checkbox of **Remote Management**.
2. Keep the HTTPS and HTTP port as default settings (recommended) or enter a value between 1024 and 65535.
3. Select **Specified Device** for **Remote Managers**.
4. In the **Only this IP Address** field, enter the IP address of the remote device to manage the router.
5. Click **SAVE**.

Devices using this WAN IP can manage the router by logging in to <http://Router's WAN IP:port number> (such as <http://113.116.60.229:1024>).

 **Tips:** The router's WAN IP is usually a dynamic IP. Please refer to [Set Up a Dynamic DNS Service Account](#) if you want to log in to the router through a domain name.

15.7. System Log

When the router does not work normally, you can save the system log and send it to the technical support for troubleshooting.

- **To save the system log locally:**

1. Visit <http://tplinkwifi.net>, and log in your TP-Link ID or the password you set for the router.
2. Go to **Advanced > System > System Log**.
3. Choose the type and level of the system logs as needed.

System Log

View a detailed record of system activities.

Current Time: 2025-01-22 04:13:37 PM

All

Search

Refresh Clear All

```
2025-01-22 16:13:23 Time Settings INFO [3519] Service restart
2022-10-19 01:09:48 Led Controller INFO [1209] Start to run WAN1_ON
2022-10-19 01:09:48 Led Controller INFO [1209] Start to run WAN0_OFF
2022-10-19 01:09:48 Led Controller INFO [1209] Start to run LAN_ON
2022-10-19 01:09:19 Led Controller INFO [1209] Start to run WAN1_ON
2022-10-19 01:09:19 Led Controller INFO [1209] Start to run WAN0_OFF
2022-10-19 01:09:19 Led Controller INFO [1209] Start to run LAN_OFF
2022-10-19 01:08:49 Led Controller INFO [1209] Start to run WAN1_OFF
2022-10-19 01:08:49 Led Controller INFO [1209] Start to run WAN0_ON
2022-10-19 01:08:49 Led Controller INFO [1209] Start to run LAN_OFF
2022-10-19 01:08:04 Led Controller INFO [1209] Start to run WAN1_ON
2022-10-19 01:08:04 Led Controller INFO [1209] Start to run WAN0_OFF
2022-10-19 01:08:04 Led Controller INFO [1209] Start to run LAN_OFF
2022-10-19 01:08:04 Led Controller INFO [1209] Start to run WAN1_ON
2022-10-19 01:08:04 Led Controller INFO [1209] Start to run WAN0_OFF
2022-10-19 01:08:04 Led Controller INFO [1209] Start to run LAN_OFF
```

4. In the **Save Log** section, click **SAVE TO LOCAL** to save the system logs to a local disk.

Save Log

Send system log to a specific email address or save locally.

MAIL LOG

SAVE TO LOCAL

- **To send the system log to a mailbox at a fixed time:**

For example, I want to check my router's working status at a fixed time every day, however, it's too troublesome to log in to the web management page every time I want to go checking. It would be great if the system logs could be sent to my mailbox at 8 a.m. every 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 > System Tools > System Log.
3. In the Save Log section, click **MAIL LOG**.
4. Enter the information required:

Mail Log

Note: Set your mail information below.

Email From:

Require Password

Username:

Email Password: 

SMTP Server:

Email To:

Mail Log Automatically

Frequency:

Mail Time: :

- 1) **Email From:** Enter the email address used for sending the system log.
 - 2) Select **Require Password**.
tips: Generally, Require Password should be selected if the login of the mailbox requires username and password.
 - 3) **Username:** Enter the email address used for sending the system log.
 - 4) **Email Password:** Enter the password to login the sender's email address.
 - 5) **SMTP Server:** Enter the SMTP server address.
tips: SMTP server is available for users in most webmail systems. For example, the SMTP server address of Hotmail is smtp-mail.outlook.com.
 - 6) **Email To:** Enter the recipient's email address, which can be the same as or different from the sender's email address.
 - 7) Select **Mail Log Automatically**.
tips: The router will send the system log to the designated email address if this option is enabled.
 - 8) **Frequency:** This determines how often the recipient will receive the system log .
5. Click **SAVE**.

15.8. Test the Network Connectivity

Diagnostics is used to test the connectivity between the router and the host or other network 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 > System > Diagnostics.

The screenshot shows the 'Diagnostics' page with the following settings:

- Diagnostics Tools: Ping
- IP Address/Domain Name: (empty field)
- Ping Count: 4
- Ping Packet Size: 64 Bytes

A large blue 'START' button is at the bottom.

3. Enter the information:

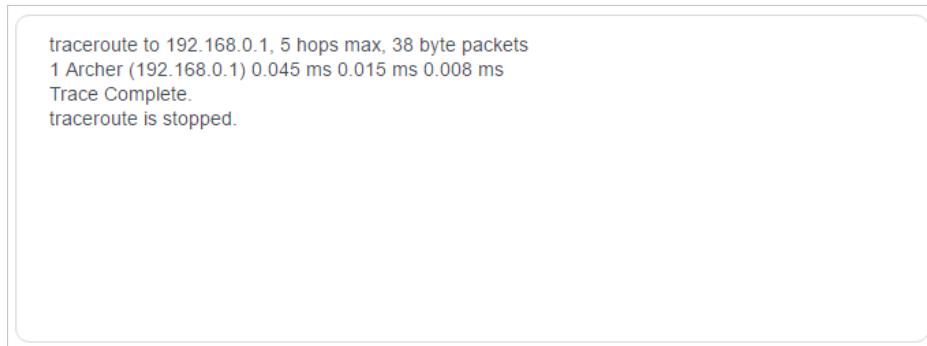
- 1) Choose **Ping** or **Traceroute** as the diagnostic tool to test the connectivity;
 - **Ping** is used to test the connectivity between the router and the tested host, and measure the round-trip time.
 - **Traceroute** is used to display the route (path) your router has passed to reach the tested host, and measure transit delays of packets across an Internet Protocol network.
- 2) Enter the **IP Address** or **Domain Name** of the tested host.
- 3) Modify the **Ping Count** number and the **Ping Packet Size**. It's recommended to keep the default value.
- 4) If you have chosen **Traceroute**, you can modify the **Traceroute Max TTL**. It's recommended to keep the default value.

4. Click **START** to begin the diagnostics.

The figure below indicates the proper connection between the router and the Yahoo server (www.Yahoo.com) tested through **Ping**.

```
PING 192.168.0.1 (192.168.0.1): 64 data bytes
Reply from 192.168.0.1: bytes=64 ttl=64 seq=1 time=0.322 ms
Reply from 192.168.0.1: bytes=64 ttl=64 seq=2 time=0.308 ms
Reply from 192.168.0.1: bytes=64 ttl=64 seq=3 time=0.286 ms
Reply from 192.168.0.1: bytes=64 ttl=64 seq=4 time=0.334 ms
--- Ping Statistic "192.168.0.1" ---
Packets: Sent=4, Received=4, Lost=0 (0.00% loss)
Round-trip min/avg/max = 0.286/0.312/0.334 ms
ping is stopped.
```

The figure below indicates the proper connection between the router and the Yahoo server (www.Yahoo.com) tested through [Traceroute](#).



15.9. Set System Time and Language

System time is the time displayed while the router is running. The system time you configure here will be used for other time-based functions like Parental Controls. You can choose the way to obtain the system time as needed.

System language is the language displayed when you log into the router. You can change the system language as needed.

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 > Time & Language](#).

- **To get time from the internet:**

1. Enable [24-Hour Time](#) if you want the time to display in a 24-hour way.

2. In the [Set Time](#) field, select [Get from Internet](#).

System Time	
Set the router's system time.	
Current Time:	2025-01-22 16:18:41
24-Hour Time:	<input checked="" type="checkbox"/>
Set Time:	Get from Internet
Time Zone:	(UTC-10:00) Hawaii
NTP Server I:	us.pool.ntp.org
NTP Server II:	north-america.pool.ntp.org <small>(Optional)</small>

3. Select your local [Time Zone](#) from the drop-down list.

4. In the **NTP Server I** field, enter the IP address or domain name of your desired NTP Server.
5. (Optional) In the **NTP Server II** field, enter the IP address or domain name of the second NTP Server.
6. Click **SAVE**.

- **To get time from your computer:**

1. In the **Set Time** field, select **Get from Managing Device**.

System Time
Set the router's system time.

Current Time: 2025-01-22 16:19:07

24-Hour Time:

Set Time: **Get from Managing Device**

Time Zone: (UTC-10:00) Hawaii

2. The time of your computer will then be displayed and click **SAVE**.

- **To manually set the date and time:**

1. In the **Set Time** field, select **Manually**.

System Time
Set the router's system time.

Current Time: 2025-01-22 16:19:53

24-Hour Time:

Set Time: **Manually**

Time Zone: (UTC-10:00) Hawaii

Date: 2025/01/22

Time: 16 : 18 : 25

2. Set the current **Date** (In **MM/DD/YYYY** format).

3. Set the current **Time** (In **HH/MM/SS** format).

4. Click **SAVE**.

- **To set Daylight Saving Time:**

1. Tick the **Enable** box of **Daylight Saving Time**.

Daylight Saving Time

Automatically synchronize the system time with daylight saving time.

Daylight Saving Time: Enabled

Start: 2025 Mar 2nd
Sun 02:00

End: 2025 Nov First
Sun 02:00

Running Status: Daylight Saving Time is off.

2. Select the correct **Start** date and time when daylight saving time starts at your local time zone.
3. Select the correct **End** date and time when daylight saving time ends at your local time zone.
4. Click **SAVE**.

- **To set system language:**

Select the language from the dropdown list, then click **SAVE**.

Language

Set the router's system language.

Language: English

15. 10. Set the Router to Reboot Regularly

The Scheduled Reboot feature cleans the cache to enhance the running performance of 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 > System > Reboot**.
3. Tick the **Enable** box of **Reboot Schedule**.

Reboot Schedule

Set when and how often the router reboots automatically.

Reboot Schedule: Enabled

Note: Before using this feature, make sure [System Time](#) is set to "Get from Internet".

Reboot Time: :

Repeat:

4. Specify the [Reboot Time](#) when the router reboots and [Repeat](#) to decide how often it reboots.
5. Click [SAVE](#).

15. 11. Control the LED

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

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

LED Control
Turn the router's LEDs on or off.

LED Status:

Note: TP-Link satellite routers will follow the main router's LED Control Settings.

Night Mode
Set a time period when the LEDs will be off automatically.

Night Mode: Enabled

Note: Before using this feature, make sure [System Time](#) is set to "Get from Internet".

Current Time: 2025-01-22 16:32:39

LED Off From: 22 : 00

To: 6 : 00 (next day)

FAQ

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

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

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

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

- If you are using a TP-Link ID to log in, or you have enabled the Password Recovery feature of the router, click [Forgot password](#) on the login page and then follow the instructions to reset it.
- Alternatively, press and hold the [Reset](#) button of the router for about 6 seconds until the Power LED blinks to restore factory default settings, and then visit <http://tplinkwifi.net> to create a new login password.

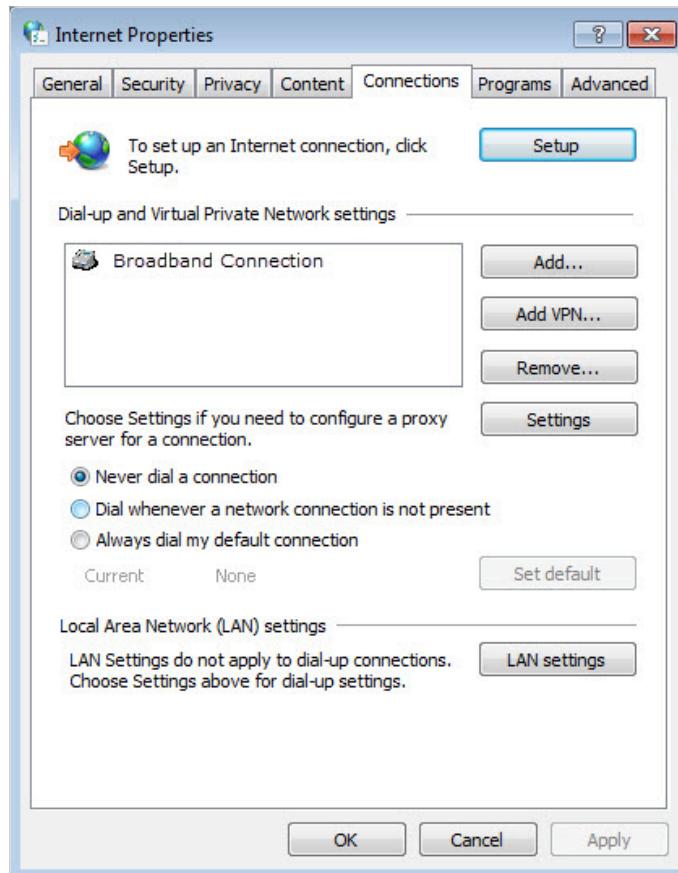
■ Note:

- Please refer to [Password Recovery](#) to learn how to configure Password Recovery.
- You'll need to reconfigure the router to surf the internet once the router is reset, and please mark down your new password for future use.

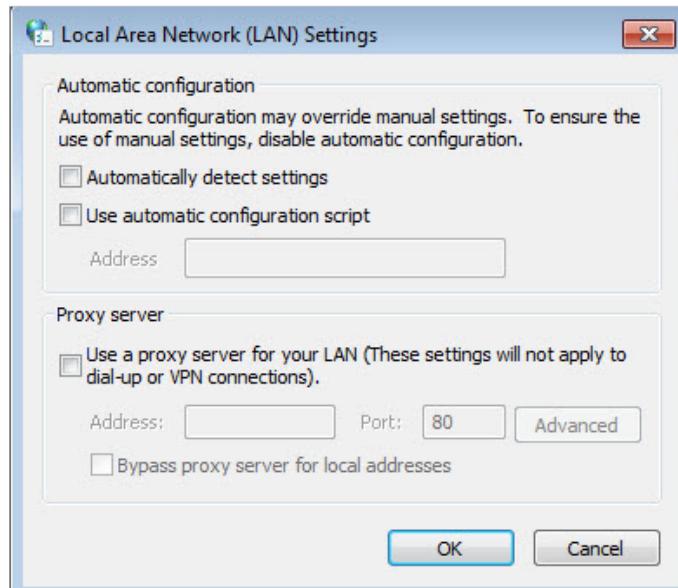
Q3. What should I do if I can't log in to the router's web management page?

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

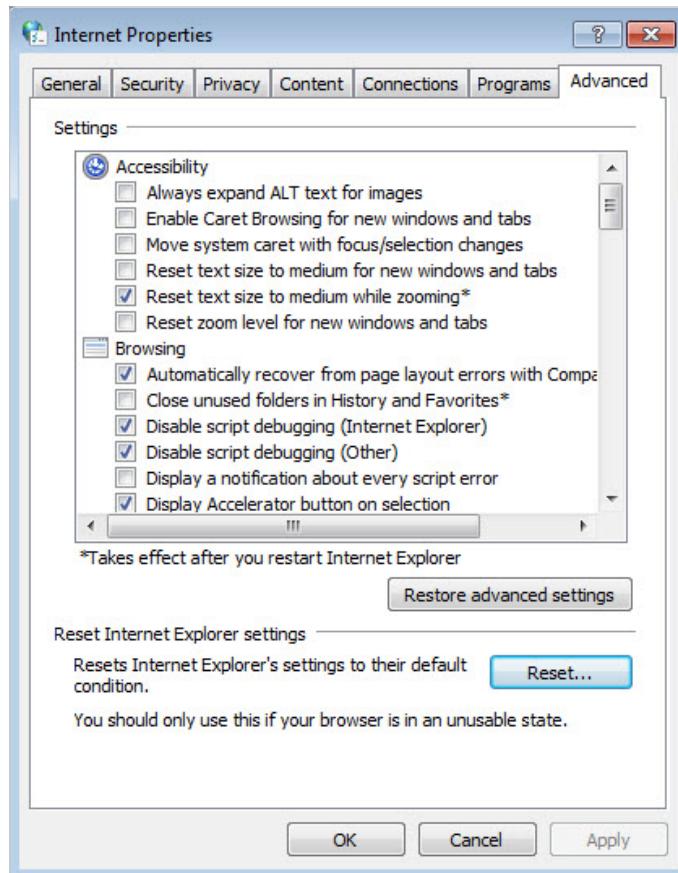
- Make sure your computer is connected to the router correctly and the corresponding LED indicator(s) light up.
- Make sure the IP address of your computer is configured as [Obtain an IP address automatically](#) and [Obtain DNS server address automatically](#).
- Make sure <http://tplinkwifi.net> or <http://192.168.0.1> is correctly entered.
- Check your computer's settings:
 - 1) Go to [Start > Control Panel > Network and Internet](#), and click [View network status and tasks](#).
 - 2) Click [Internet Options](#) on the bottom left.
 - 3) Click [Connections](#) and select [Never dial a connection](#).



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



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



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

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

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

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

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

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

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

DHCP Server

Dynamically assign IP addresses to the devices connected to the router.

DHCP Server:	<input checked="" type="checkbox"/> Enable
IP Address Pool:	192.168.0.100 - 192.168.0.249
Address Lease Time:	120 minutes
Default Gateway:	192.168.0.1 (Optional)
Primary DNS:	8.8.8.8 (Optional)
Secondary DNS:	(Optional)

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

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

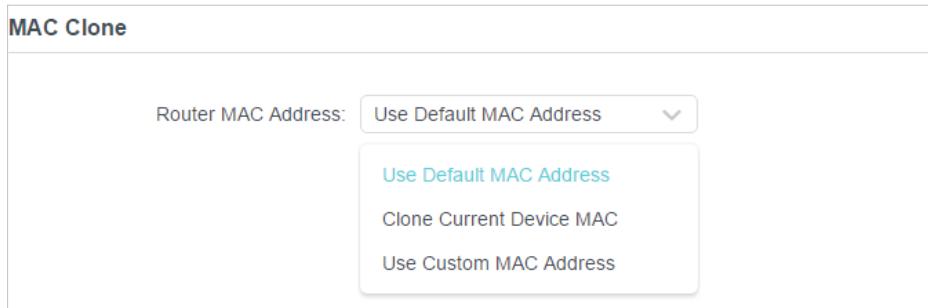
Status

Internet status overview is displayed on this page.

Internet
Status: WAN port is unplugged
Internet Connection Type: Dynamic IP
IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Default Gateway: 0.0.0.0
Primary DNS: 0.0.0.0
Secondary DNS: 0.0.0.0

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

- 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** or **Advanced > Network > Internet** and focus on the **MAC Clone** section.
- 3) Choose an option as needed (enter the MAC address if **Use Custom MAC Address** is selected), and click **SAVE**.



Tips:

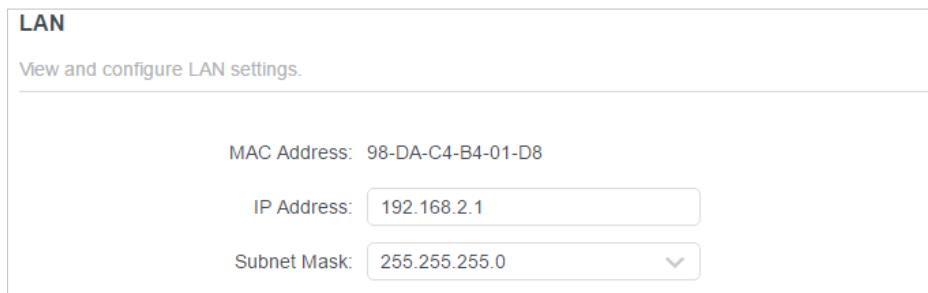
- Some ISP will register the MAC address of your computer when you access the internet for the first time through their Cable modem, if you add a router into your network to share your internet connection, the ISP will not accept it as the MAC address is changed, so we need to clone your computer's MAC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

• **Modify the LAN IP address of the router.**

Note:

Most TP-Link routers use 192.168.0.1/192.168.1.1 as their default LAN IP address, which may conflict with the IP range of your existing ADSL modem/router. If so, the router is not able to communicate with your modem and you can't access the internet. To resolve this problem, we need to change the LAN IP address of the router to avoid such conflict, for example, 192.168.2.1.

- 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) Modify the LAN IP address as the follow picture shows. Here we take 192.168.2.1 as an example.
- 4) Click **SAVE**.



• **Restart the modem and the router.**

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

Internet

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

Internet Connection Type: **Dynamic IP**

IP Address: Static IP

Subnet Mask: **Dynamic IP**

Default Gateway: PPPoE

Primary DNS: L2TP

Secondary DNS: PPTP

Secondary DNS: 0.0.0.0

RENEW

RELEASE

- 6) Restart the modem and the router again.
- Please upgrade the firmware of the router.

If you've tried every method above but still cannot access the internet, please contact the technical support.

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

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

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

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

- **On Windows 7**

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

- **On Windows XP**

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

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

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

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

- **Authenticating problem/password mismatch:**

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



- 2) If you cannot find the PIN or PIN failed, you may choose [Connecting using a security key instead](#), and then type in the [Wireless Password/Network Security Key](#).
- 3) If it continues to show note of [Network Security Key Mismatch](#), it is suggested to confirm the wireless password of your wireless router.

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

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

FCC compliance information statement



Product Name: AX1800 Dual Band Wi-Fi 6 Router

Model Number: Archer AX20/ Archer AX23/ Archer AX1800

Component Name	Model
I.T.E. Power Supply	T120150-2B1

Responsible party:

TP-Link Systems Inc.

Address: 10 Mauchly, Irvine, CA 92618

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

Tel: +1 626 333 0234

Fax: +1 909 527 6803

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

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

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

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

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

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

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

FCC RF Radiation Exposure Statement

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

"To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 44 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

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

FCC compliance information statement

Product Name: I.T.E. Power Supply

Model Number: T120150-2B1

Responsible party:

TP-Link Systems Inc.

Address: 10 Mauchly, Irvine, CA 92618

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

Tel: +1 626 333 0234

Fax: +1 909 527 6803

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

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

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

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

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

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

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

Issue Date: 2025-03-05

CE Mark Warning



OPERATING FREQUENCY(the maximum transmitted power)

2400 MHz -2483.5 MHz (20dBm)

5150 MHz -5250 MHz (23dBm)

EU Declaration of Conformity

TP-Link hereby declares that the device is in compliance with the essential requirements and other relevant provisions of directives 2014/53/EU, 2009/125/EC, 2011/65/EU and (EU)2015/863.

The original EU Declaration of Conformity may be found at

<https://www.tp-link.com/en/support/ce/>

RF Exposure Information

This device meets the EU requirements (2014/53/EU Article 3.1a) on the limitation of exposure of the general public to electromagnetic fields by way of health protection.

The device complies with RF specifications when the device used at 20 cm from your body.

Frequency band: 5150 - 5250 MHz:

Indoor use: Inside buildings only. Installations and use inside road vehicles and train carriages are not permitted. Limited outdoor use: If used outdoors, equipment shall not be attached to a fixed installation or to the external body of road vehicles, a fixed infrastructure or a fixed outdoor antenna. Use by unmanned aircraft systems (UAS) is limited to within the 5170 - 5250 MHz band.

	AT	BE	BG	CH	CY	CZ	DE	DK
	EE	EL	ES	FI	FR	HR	HU	IE
	IS	IT	LI	LT	LU	LV	MT	NL
	NO	PL	PT	RO	SE	SI	SK	UK(NI)

UKCA Mark



UK Declaration of Conformity

TP-Link hereby declares that the device is in compliance with the essential requirements and other relevant provisions of the Radio Equipment Regulations 2017.

The original UK Declaration of Conformity may be found at
<https://www.tp-link.com/support/ukca>

National Restrictions

Attention: This device may only be used indoors in Great Britain.



Canadian Compliance Statement

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

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

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

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

Caution:

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

Avertissement:

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

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 27cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 27 cm de distance entre la source de rayonnement et votre corps.

Industry Canada Statement

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

Korea Warning Statements:

당해 무선설비는 운용중 전파혼신 가능성이 있음.

NCC Notice & BSMI Notice:

注意！

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

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

前述合法通信，指依電信管理法規定作業之無線電通信。

低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

應避免影響附近雷達系統之操作。

高增益指向性天線只得應用於固定式點對點系統。

安全諮詢及注意事項

- 請使用原裝電源供應器或只能按照本產品注明的電源類型使用本產品。
- 清潔本產品之前請先拔掉電源線。請勿使用液體、噴霧清潔劑或濕布進行清潔。
- 注意防潮，請勿將水或其他液體潑灑到本產品上。
- 插槽與開口供通風使用，以確保本產品的操作可靠並防止過熱，請勿堵塞或覆蓋開口。
- 請勿將本產品置放於靠近熱源的地方。除非有正常的通風，否則不可放在密閉位置中。

- 請不要私自打開機殼，不要嘗試自行維修本產品，請由授權的專業人士進行此項工作。

限用物質含有情況標示聲明書

設備名稱：AX1800 Dual Band Wi-Fi 6 Router Equipment name			型號（型式）：Archer AX20/Archer AX23/Archer AX1800 Type designation (Type)			
單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛 Lead (Pb)	汞 Mercury (Hg)	鎘 Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr ⁶⁺)	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
PCB	○	○	○	○	○	○
外殼	○	○	○	○	○	○
電源供應器	—	○	○	○	○	○
其他及其 配件	—	○	○	○	○	○

備考1. “超出0.1 wt %” 及 “超出0.01 wt %” 係指限用物質之百分比含量超出百分比含量基準值
Note 1: “Exceeding 0.1 wt %” and “exceeding 0.01 wt %” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2. “○” 係指該項限用物質之百分比含量未超出百分比含量基準值。
Note 2: “○” indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3. “—” 係指該項限用物質為排除項目。
Note 3: The “—” indicates that the restricted substance corresponds to the exemption.



Продукт сертифіковано згідно з правилами системи УкрСЕПРО на відповідність вимогам нормативних документів та вимогам, що передбачені чинними законодавчими актами України.

EAC



Safety Information

- Keep the device away from water, fire, humidity or hot environments.

- Do not attempt to disassemble, repair, or modify the device. If you need service, please contact us.
- Do not use damaged charger or USB cable to charge the device.
- Do not use any other chargers than those recommended
- Do not use the device where wireless devices are not allowed.
- Adapter shall be installed near the equipment and shall be easily accessible.
- Use only power supplies which are provided by manufacturer and in the original packing of this product. If you have any questions, please don't hesitate to contact us.
- Operating Temperature: 0°C ~ 40°C (32°F ~ 104°F)
- Storage Temperature: -40°C ~ 60°C (-40°F ~ 140°F)

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

Explanations of the symbols on the product label

Note: The product label can be found at the bottom of the product and its I.T.E. power supply. Symbols may vary from products.

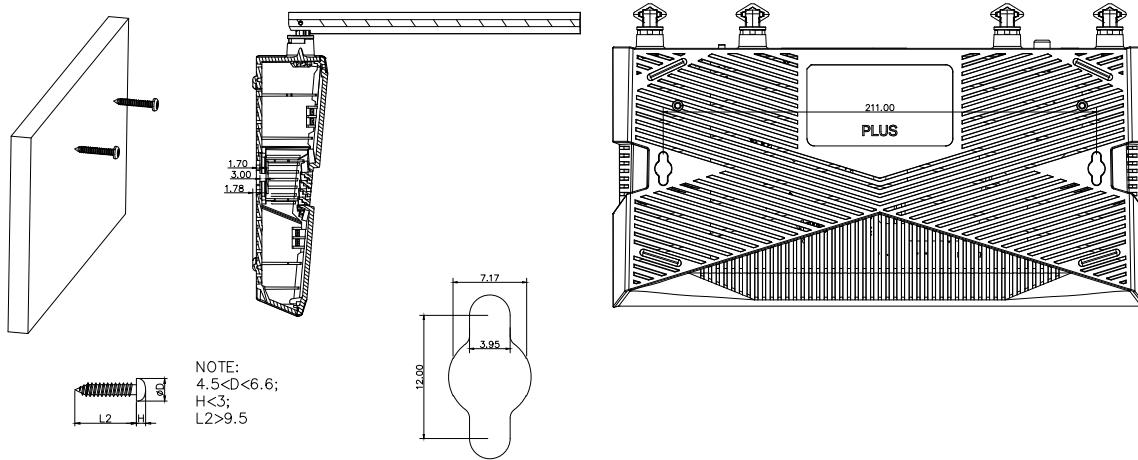
Symbol	Explanation
	Class II equipment
	Class II equipment with functional earthing
	Alternating current
	Direct current
	Polarity of d.c. power connector
	For indoor use only
	Dangerous voltage
	Caution, risk of electric shock
	Energy efficiency Marking
	Protective earth

Symbol	Explanation
	Earth
	Frame or chassis
	Functional earthing
	Caution, hot surface
	Caution
	Operator's manual
	Stand-by
	"ON"/"OFF" (push-push)
	Fuse
	Fuse is used in neutral N
RECYCLING	
	This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/EU in order to be recycled or dismantled to minimize its impact on the environment.
	User has the choice to give his product to a competent recycling organization or to the retailer when he buys a new electrical or electronic equipment.
	Caution, avoid listening at high volume levels for long periods
	Disconnection, all power plugs
m	Switch of mini-gap construction
μ	Switch of micro-gap construction (for US version) Switch of micro-gap / micro-disconnection construction (for other versions except US)
ϵ	Switch without contact gap (Semiconductor switching device)

Appendix I

定位您的路由器

- 產品不應放置在會受潮濕或過高溫度的地方。
- 將路由器放置在能夠連接多個設備並接上電源的地方。
- 請確保線和電源線放置在安全位置，以免造成絆倒的危險。
- 路由器可以放置在架子上或桌面上。
- 將路由器遠離具有強烈電磁干擾的設備，例如藍牙設備、無線電話和微波爐。
- 通常，路由器放置在水平的表面上，例如在架子上或桌面上。該設備還可以安裝在牆上，如下圖所示。



■ 注意：

螺絲頭直徑為 $4.5 < D < 6.6$ mm，兩個螺絲之間的距離為211mm。從牆壁突出的螺絲需要約6.48mm的基底，並且螺絲的長度至少需要9.5mm才能承受產品的重量。

產品標籤上符號的解釋

符號可能因產品而異。

注意：產品標籤可以在產品底部和其I.T.E.電源供應器上找到。

注意：產品標籤可在產品底部找到。

符號	說明
	二級設備
	具有接地功能的二級設備
	交流電
	DC電壓

符號	說明
	輸出端點的極性
	僅供室內使用
	危險電壓
	請注意，有觸電的危險
	能源效率標誌
	保護接地
	接地
	框架或外殼
	功能接地
	請注意，表面過熱
	警告
	操作手冊
	待機
	“開啟” / “關閉” (按壓式)
	保險絲
	保險絲用於中性線N
	回收 “這個產品帶有歐盟指令2012/19/EU中關於廢棄電氣電子設備 (WEEE) 的選擇性分類標誌。這意味著，該產品必須按照該指令處理，以便進行回收或拆解，從而最大限度地減少對環境的影響。用戶可以選擇將產品交給有資格的回收機構，或在購買新的電器或電子設備時將其交給零售商進行回收。”
	請小心，避免長時間以高音量收聽。

符號	說明
	斷線，所有電源插頭
m	迷你間隙結構開關
μ	“小間隙結構開關（US版本） 小間隙/小斷開結構的開關（非US版）”
ε	無接觸間隙的開關（半導體開關設備）

運作溫度: 0°C~40°C (32°F~104°F)

適配器應安裝在設備附近，並應易於接近。

請使用製造商提供的電源適配器。如果您有任何問題，請隨時與我們聯繫。