User Guide

BE24000 Quad-Band Wi-Fi 7 Router
Archer BE900

© 2023 TP-Link 1910013573 REV2.0.0

Contents

About This Guide 1

Chapter 1. Get to Know About Your Router 3

1. 1. Product Overview 4
1. 2. Appearance 4
1. 2. 1.Front Panel 4
1. 2. 2.Back Panel and Side Panel 6

Chapter 2. Connect the Hardware 7

2. 1. Position Your Router 8
2. 2. Connect Your Router 8

Chapter 3. Log In to Your Router 10

Chapter 4. Set Up Internet Connection 12

4. 1. Use Quick Setup Wizard 13
4. 2. Quick Setup Via TP-Link Tether App 13
4. 3. Manually Set Up Your Internet Connection 14
4. 4. Set Up the Router as an Access Point 17
4. 5. Set Up an IPv6 Internet Connection 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. Network Map 27

Chapter 7. Screen Display 31

Chapter 8. Wireless Settings 33

8. 1. Specify Wireless Settings 34

8. 2. Schedule Your Wireless Function 37
8. 3. Use WPS for Wireless Connection 38
8. 3. 1.Connect via the Client's PIN 38
8. 3. 2.Connect via the Router's PIN 39
8. 3. 3.Push the WPS Button. 39
8. 4. Advanced Wireless Settings 40

Chapter 9. Guest Network 42

9. 1. Create a Network for Guests 43
9. 2. Customize Guest Network Options. 44

Chapter 10.IoT Network 45

Chapter 11.USB Settings. 47

11. 1. Access the USB Storage Device 48
11. 1. 1.Access the USB Device Locally 48
11. 1. 2.Access the USB Device Remotely 49
11. 1. 3.Customize the Access Settings 51
11. 2. Media Sharing 53
11. 3. Time Machine 54

Chapter 12.HomeShield 56

12. 1. Network Check 57
12. 2. Parental Controls 57
12. 3. QoS 61
12. 4. More Features 61

Chapter 13.EasyMesh with Seamless Roaming 63

13. 1. Add a Router as a Satellite Device 64
13. 2. Add a Range Extender as a Satellite Device 65
13. 3. Manage Devices in the EasyMesh Network. 67

Chapter 14.Network Security 68

14. 1. Protect the Network from Cyber Attacks 69
14. 2. Access Control 69
14. 3. IP & MAC Binding 71
14. 4. ALG 73
14. 5. IoT Security 74

Chapter 15.NAT Forwarding..... 75

15. 1. Share Local Resources on the Internet by Port Forwarding 76
15. 2. Open Ports Dynamically by Port Triggering.....78
15. 3. Make Applications Free from Port Restriction by DMZ 79
15. 4. Make Xbox Online Games Run Smoothly by UPnP 80

Chapter 16.VPN Server&Client..... 82

16. 1. Use OpenVPN to Access Your Home Network.....83
16. 2. Use PPTP VPN to Access Your Home Network 84
16. 3. Use L2TP/IPSec VPN to Access Your Home Network 89
16. 4. Use WireGuard VPN to Access Your Home Network 96
16. 5. Use VPN Client to Access a Remote VPN Server 99

Chapter 17.Customize Your Network Settings..... 106

17. 1. Change the Internet Settings 107
17. 2. Change the LAN Settings 109
17. 3. Link Aggregation 109
17. 4. Configure to Support IPTV Service.....110
17. 5. Specify DHCP Server Settings.....111
17. 6. Set Up a Dynamic DNS Service Account 113
17. 7. Create Static Routes.....114

Chapter 18.Manage the Router 117

18. 1. Update the Firmware.....118
18. 1. 1.Auto Update 118
18. 1. 2.Online Update 118
18. 1. 3.Local Update 119
18. 2. Backup and Restore Configuration Settings.....120
18. 3. Change the Login Password 121
18. 4. Password Recovery.....122
18. 5. Local Management 123
18. 6. Remote Management.....124
18. 7. System Log.....126
18. 8. Test the Network Connectivity 128
18. 9. Set System Time and Language 130
18. 10. Set the Router to Reboot Regularly.....132
18. 11. Control the LED.....133

FAQ..... 134

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
Underlined	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	• 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 and wireless coverage are not guaranteed and will vary as a result of 1) environmental factors, including building materials, physical objects, and obstacles, 2) network conditions, including local interference, volume and density of traffic, product location, network complexity, and network overhead, and 3) client limitations, including rated performance, location, connection, quality, and client condition.
* Use of Wi-Fi 6 (802.11ax), Wi-Fi 6E, and features including OFDMA, 1024-QAM, and HE160 require clients to also support the corresponding features. Seven 160MHz channels may not be all available in the 6 GHz band in some regions/countries due to regulatory restrictions.
* Saving clients' battery power requires clients to also support the 802.11ax Wi-Fi standard. Actual power reduction may vary as a result of network conditions, client limitations, and environmental factors.
* HomeShield includes the Free Basic Plan. Fees apply for the Pro Plan. Visit **tp-link.com/homeshield** for more information.
* Use of WPA3 requires clients to also support the corresponding feature.
* This router may not support all the mandatory features as ratified in Draft 3.0 of IEEE 802.11ax specification.
* Further software upgrades for feature availability may be required.

Chapter 1

Get to Know About Your Router

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

It chapter contains the following sections:

- Product Overview
- Appearance

1. 1. Product Overview

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

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

1. 2. Appearance

1. 2. 1. Front Panel

LED Screen

Commonly used functions and information can be visually displayed: weather, graphics, time, and more.

Status	Indication
	Pulsing LEDs. The router is starting up or being reset.
	Cycling graphics. The router is ready for setup.
	Display the information set in Tether, and cycle through the emoji by default. The router works fine and can access the internet.

Status	Indication
	Establishing a WPS connection. If successful, a √ will appear, if failed, an × will appear
	The router is being upgraded.
	The router is disconnected from the internet.
	LEDs in the top are pulsing in a line, indicating Wi-Fi is off.

Touchscreen

Use the touchscreen to check basic information, network status, connected clients, guest network, and more.

Swipe the home screen to display system time, network connection, CPU & memory, and weather information.

Tap to display system tools, such as Lock Screen and Firmware Update.

Tap to display the Wi-Fi setting screens, such as Guest Network, WPS, and Wi-Fi On/Off.

Tap to display LED screen and touchsreen settings, such as adjusting the brightness and turning off the screen. When the touchscreen is off, touch it to turn it on.

1. 2. 2. Back Panel and Side Panel

The following parts are located on the back panel.

Item	Description
Power On/Off Button	Press this button to power on or off the router.
POWER Port	For connecting the router to a power socket via the provided power adapter.
USB 3.0 Port	For connecting your USB storage devices to the router.
USB 2.0 Port	For connecting your USB storage devices to the router.
10Gbps Internet Port 1	The SFP+ Internet port 1 and the RJ45 Internet port 1 form the combo port. Only one port can be used at a time. RJ45 port: For connecting to your modem, the Ethernet outlet or other internet devices. Used as the WAN or LAN port. SFP+ port: For connecting to your optical module. Used as the WAN or LAN port.
10Gbps Internet Port 2	For connecting to your modem, the Ethernet outlet or other internet devices. Used as the WAN or LAN port.
1Gbps WAN/LAN Port	For connecting your PC or other wired devices to the router.
2.5Gbps WAN/LAN Port (1-4)	For connecting your PC or other wired devices to the router.

Note:

The 10Gbps Internet port 1 (the combo port), 10Gbps Internet port 2, 2.5Gbps WAN/LAN port, and the 1Gbps WAN/LAN port cannot be used as the WAN port at the same time. If you choose one of the ports as the WAN port for internet service, the other ports will be used as LAN by default. It's recommended to use the RJ45 Internet port 1 in the 10Gbps Combo pair as the WAN port.

Chapter 2

Connect the Hardware

This chapter contains the following sections:

- Position Your Router
- Connect Your Router

2. 1. Position Your Router

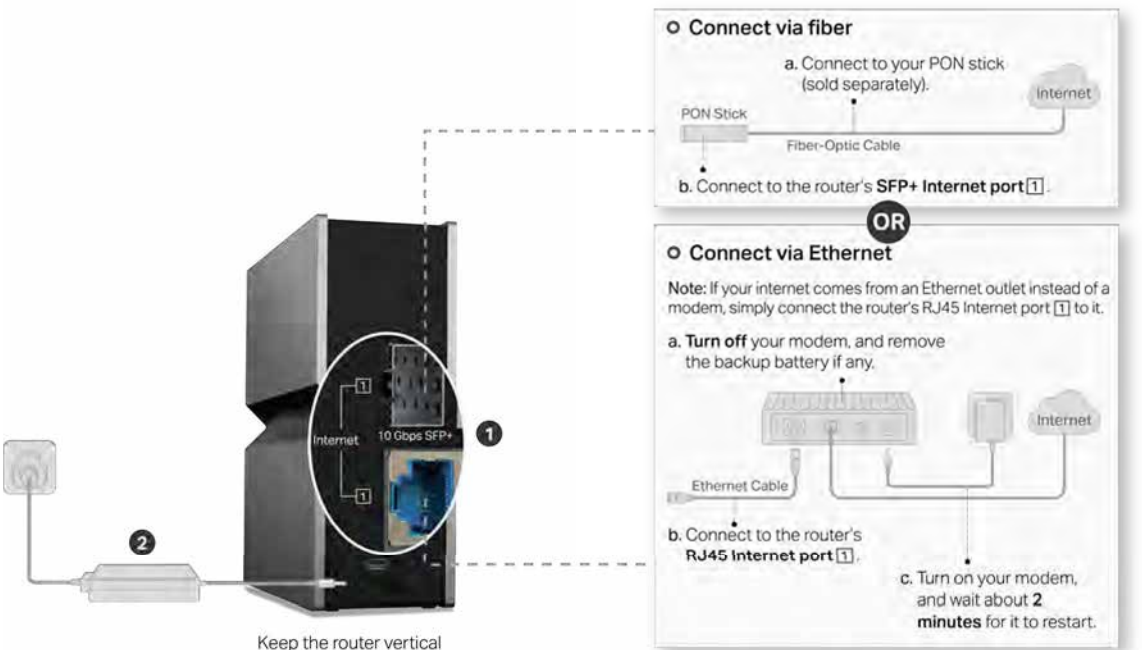
- The product should not be located in a place where it will be exposed to moisture or excessive heat.
- Place the router in a location where it can be connected to multiple devices as well as to a power source.
- Make sure the cables and power cord are safely placed out of the way so they do not create a tripping hazard.
- 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.
- Keep the router vertical.

2. 2. Connect Your Router

1. Connect the router's Internet port 1 to the internet via Ethernet or fiber network.

Note:

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



2. Connect the power adapter to the router and turn on the router.
3. Wait until the LED screen cycles through graphics and the touchscreen displays the Tether download screen before moving on.
4. Connect your computer to the router.

- **Method 1: Wired**

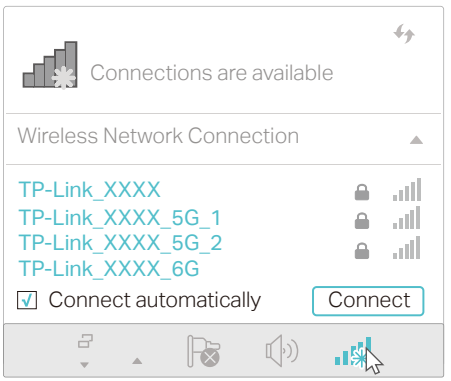
Turn off the Wi-Fi on your computer and connect the devices to the LAN port of your router.

- **Method 2: Wirelessly**

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

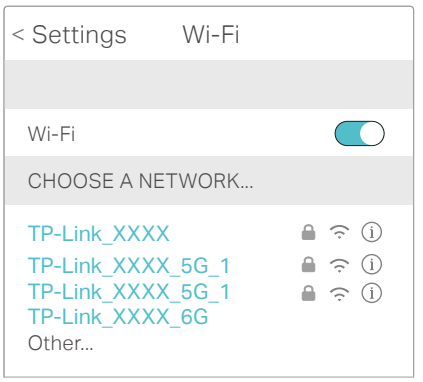
2) Click the network icon of your computer or go to Wi-Fi Settings of your smart device, and then select the SSID to join the network.

Computer



OR

Smart Device



Chapter 3

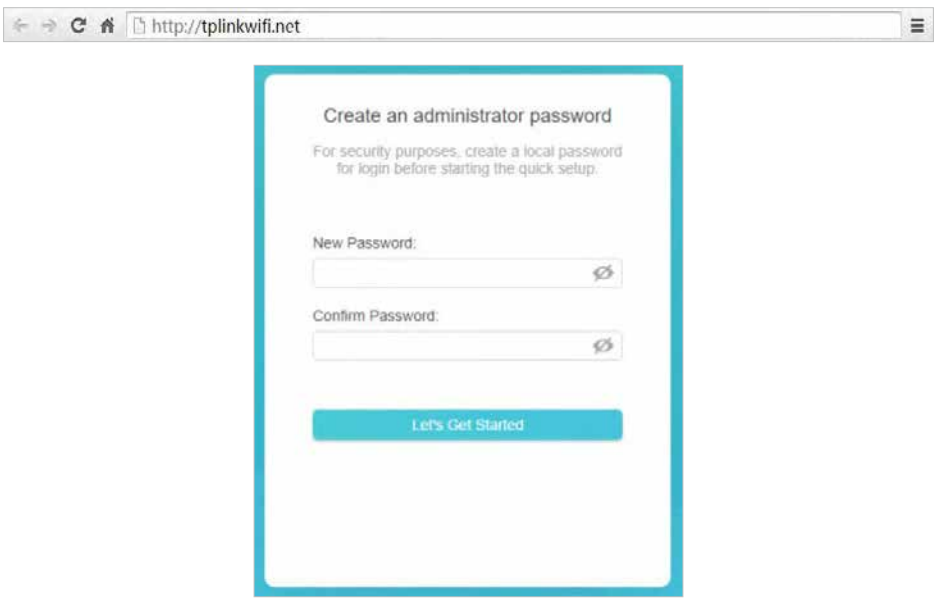
Log In to Your Router

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

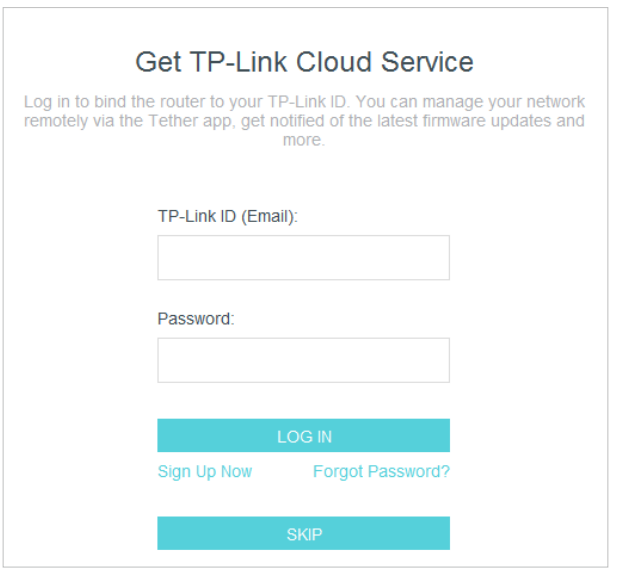
4. 1. Use Quick Setup Wizard

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.

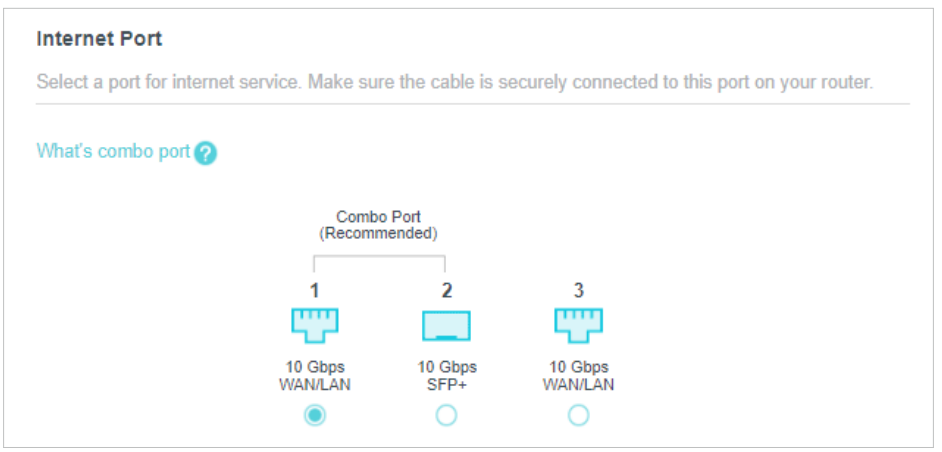
3. Tap the **+** button and select Wireless Router. In Specific Routers, find this router and tap it.
4. Follow the steps to complete the setup and connect to the internet.
5. Connect your devices to the newly configured wireless networks of the router and enjoy the internet!

4. 3. Manually Set Up Your Internet Connection

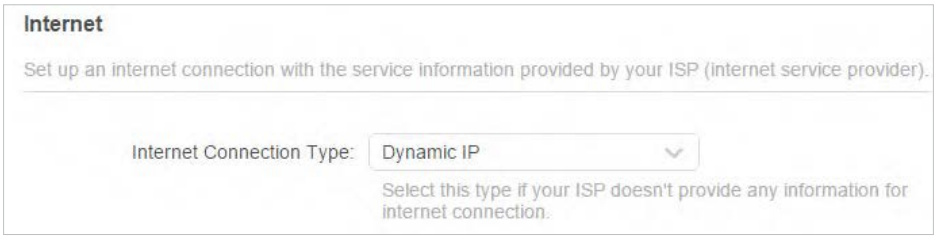
In this part, you can check your current internet connection settings. You can also modify the settings according to the service information provided by your ISP.

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 a port for internet service. Make sure the cable is securely connected to this port on your router.

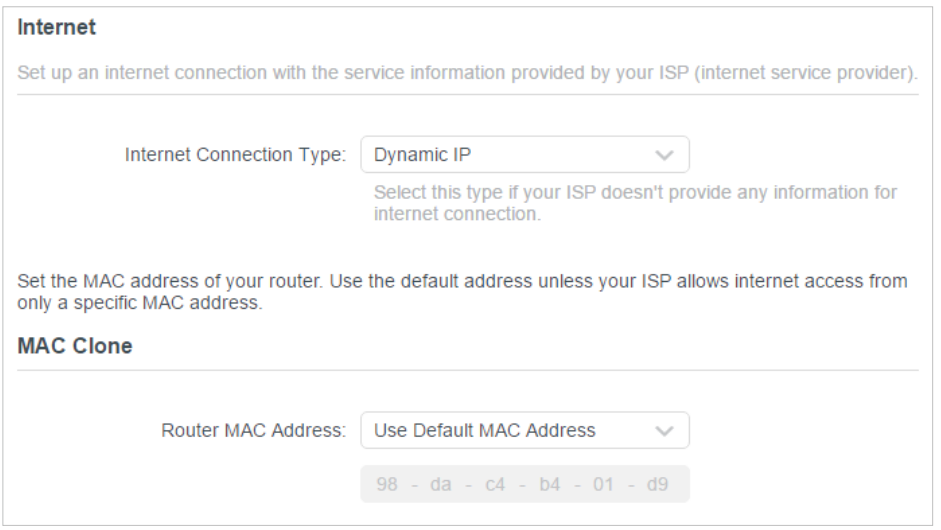


4. Select your internet connection type from the drop-down list.

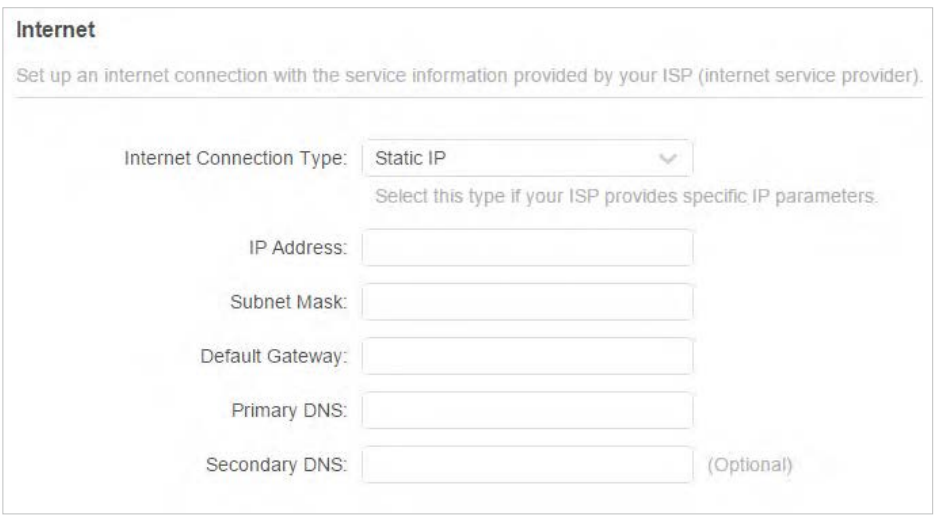


5. Follow the instructions on the page to continue the configuration. Parameters on the figures are just used for demonstration.

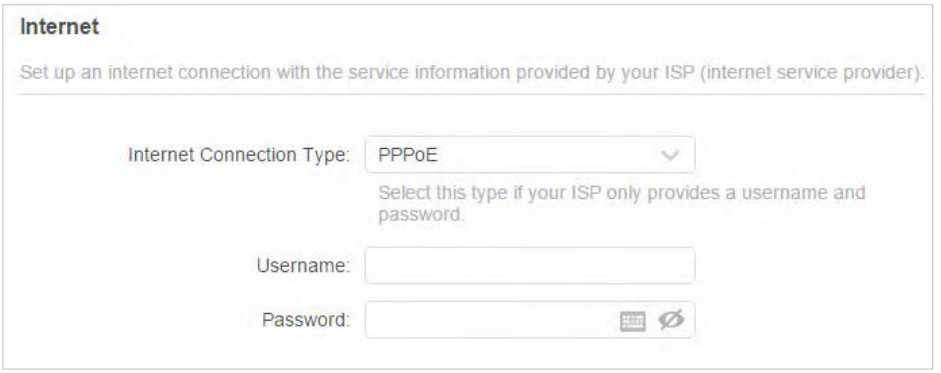
   1) If you choose Dynamic IP, you need to select whether to clone the MAC address. Dynamic IP users are usually equipped with a cable TV or fiber cable.



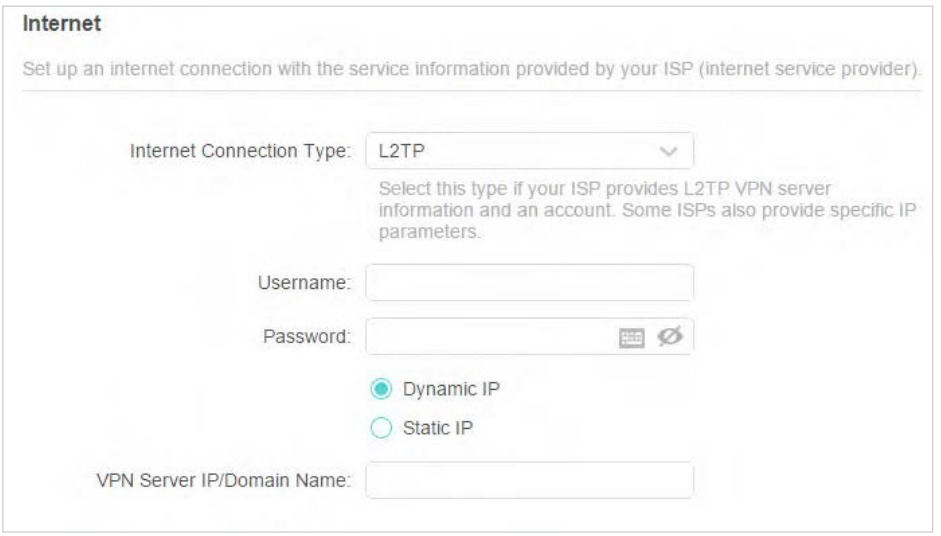
   2) If you choose Static IP, enter the information provided by your ISP in the corresponding fields.



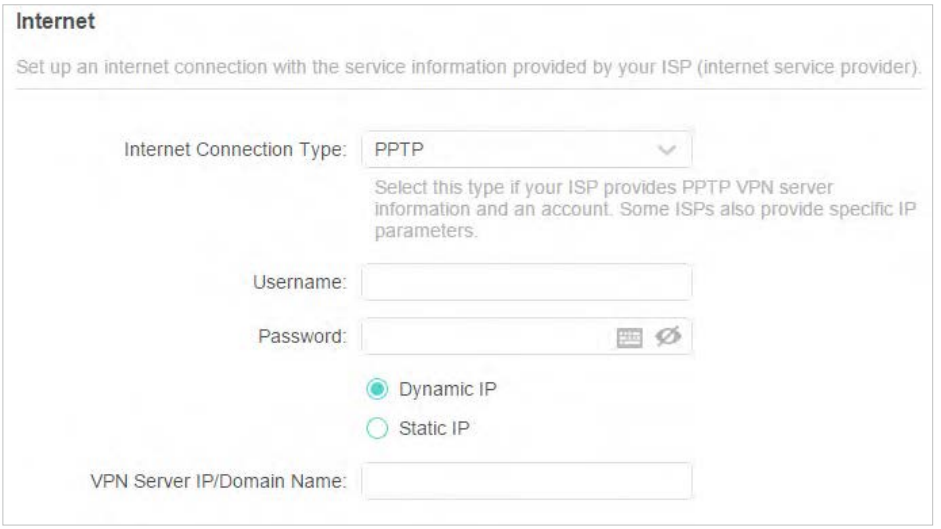
   3) If you choose PPPoE, enter the username and password provided by your ISP. PPPoE users usually have DSL cable modems.



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.



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.



6. Click SAVE.

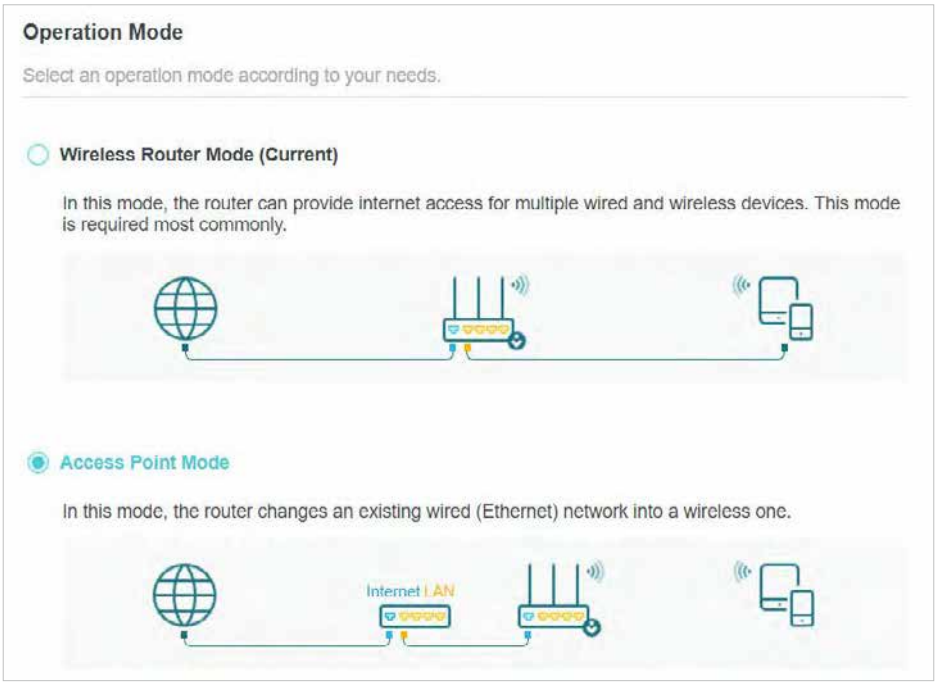
Tips:

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

4. 4. Set Up the Router as an Access Point

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

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



3. After rebooting, connect the router to your existing wired router via an Ethernet cable.
4. Log in again to the web management page http://tplinkwifi.net, and go to Advanced > Quick Setup.
5. Configure your wireless settings and click Next.
6. Confirm the information and click SAVE. Now, you can enjoy Wi-Fi.

Tips:
- Functions, such as Parental Controls, QoS 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.

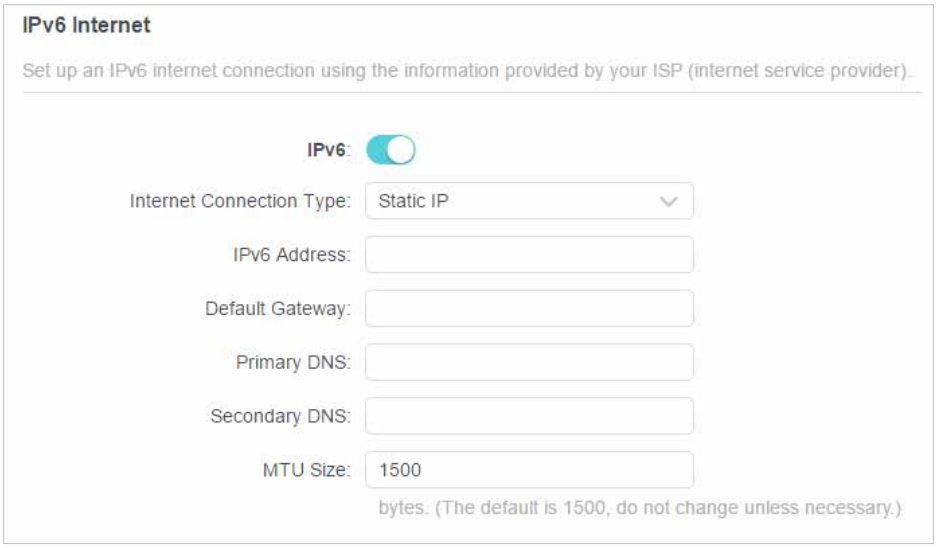
4. 5. Set Up an IPv6 Internet Connection

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).

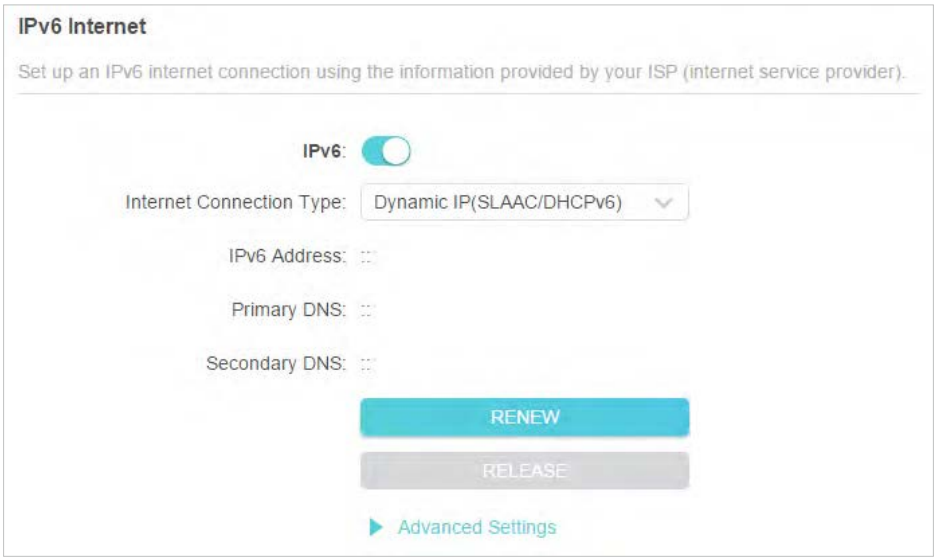
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > IPv6.
3. Enable IPv6 and select the internet connection type provided by your ISP.

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.



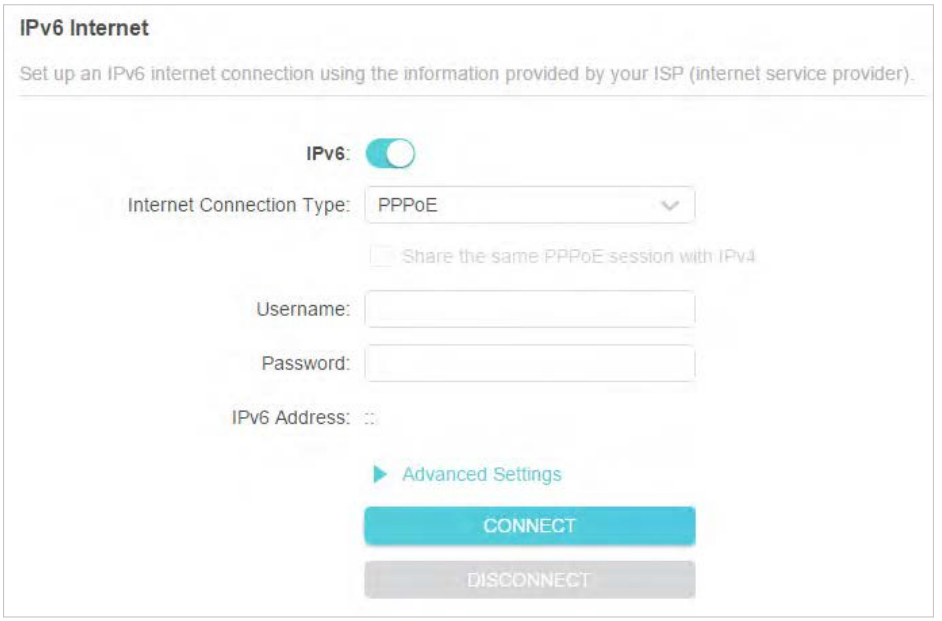
2) Dynamic IP(SLAAC/DHCPv6): Click Advanced to input further information if your ISP requires. Click SAVE and then click Renew.



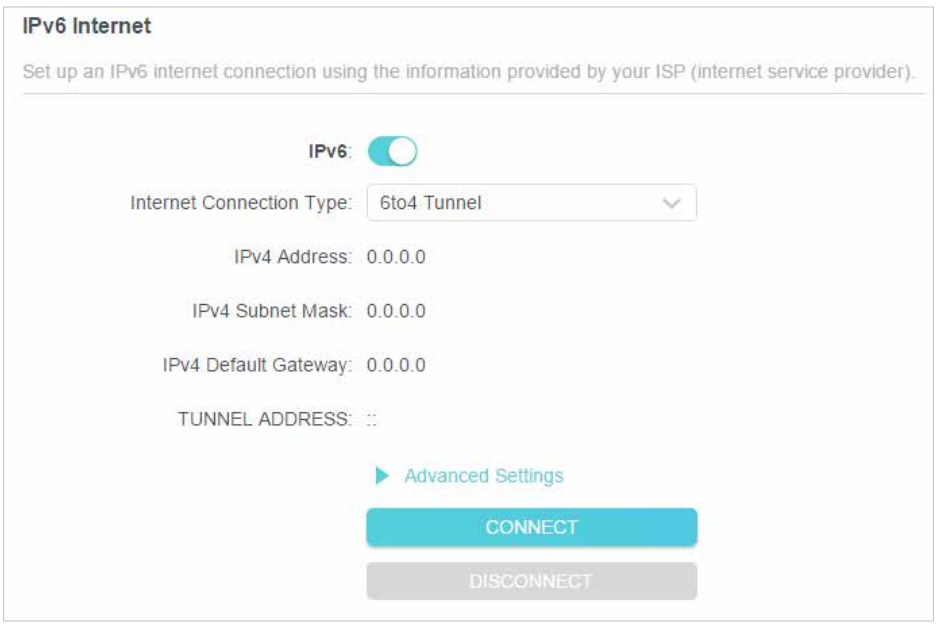
3) PPPoE: By default, the router uses the IPv4 account to connect to the IPv6 server. Click Advanced to input further information if your ISP requires. Click SAVE and then click Connect.

Note:

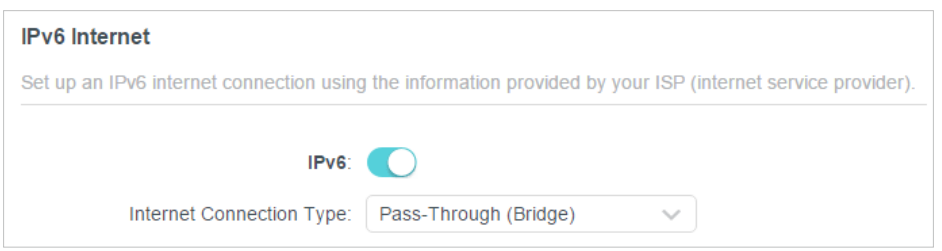
If your ISP provides two separate accounts for the IPv4 and IPv6 connections, manually enter the username and password for the IPv6 connection.



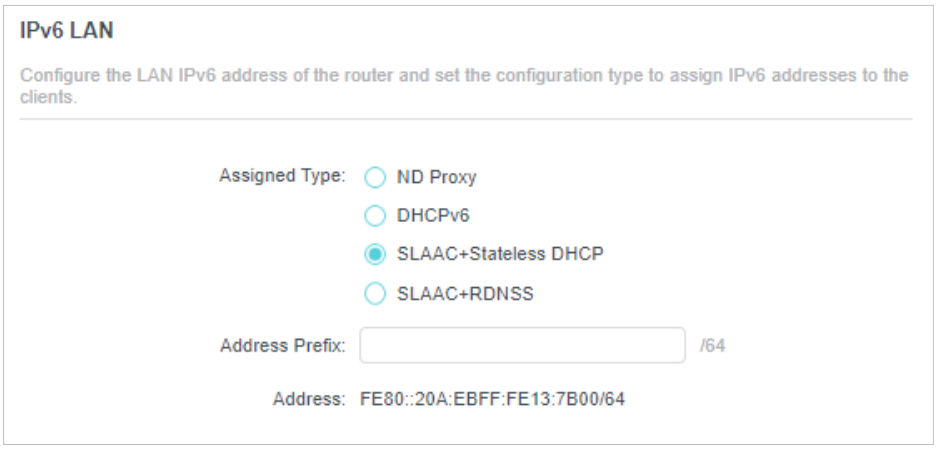
4) 6to4 Tunnel: An IPv4 internet connection type is a prerequisite for this connection type (Manually Set Up Your Internet Connection). Click Advanced to input further information if your ISP requires. Click SAVE and then click Connect.



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



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



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

Tips:
Visit the FAQ section if there is no internet connection.

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.

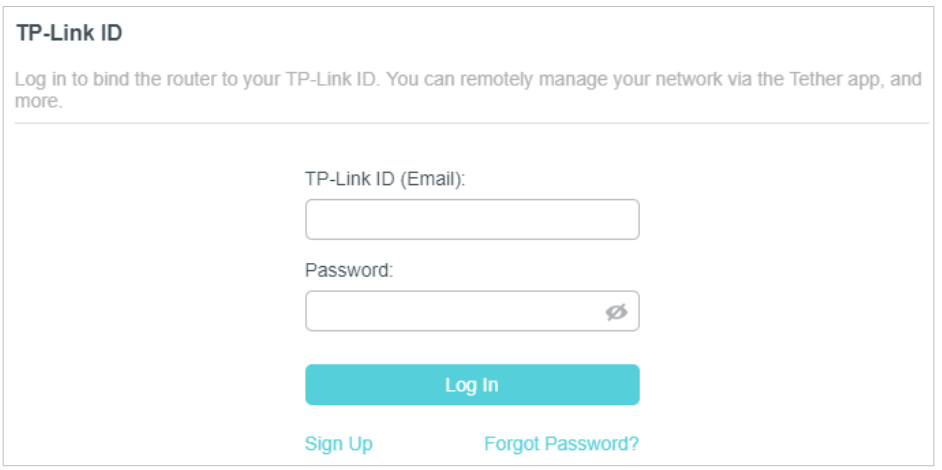
It contains the following sections:

- 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.



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.

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, an click Unbind in the Device Information section.

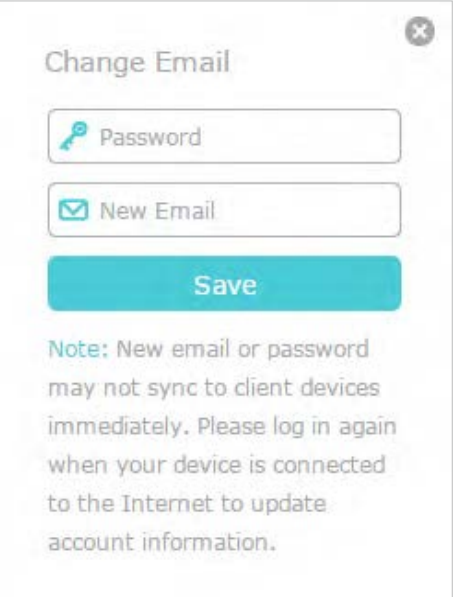
5. 2. Change Your TP-Link ID Information

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.

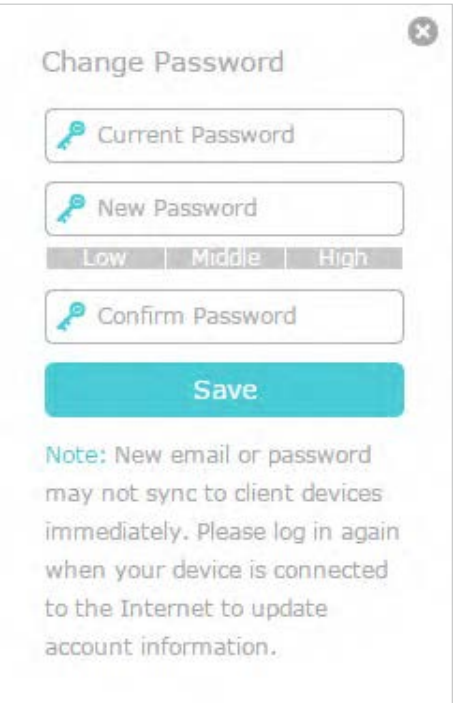
- **To change your email address**:

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

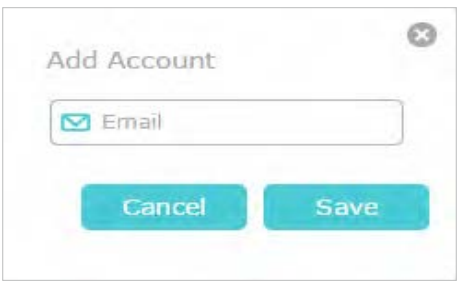
from the same router as Users. All accounts can monitor and manage the router locally or remotely, but user accounts cannot:

- 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.

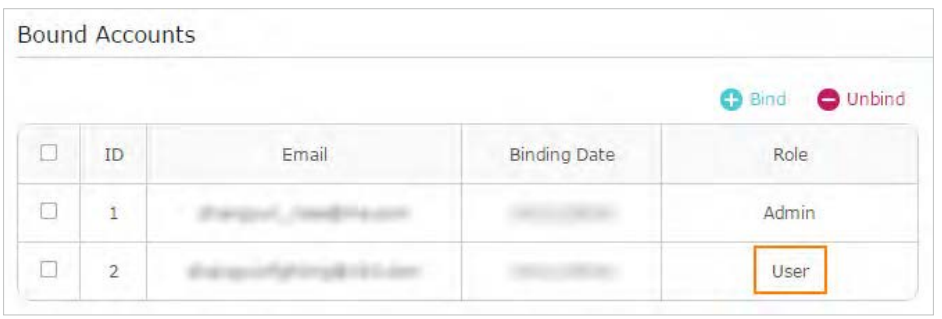
5. 3. 1. Add TP-Link ID to Manage the Router

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.

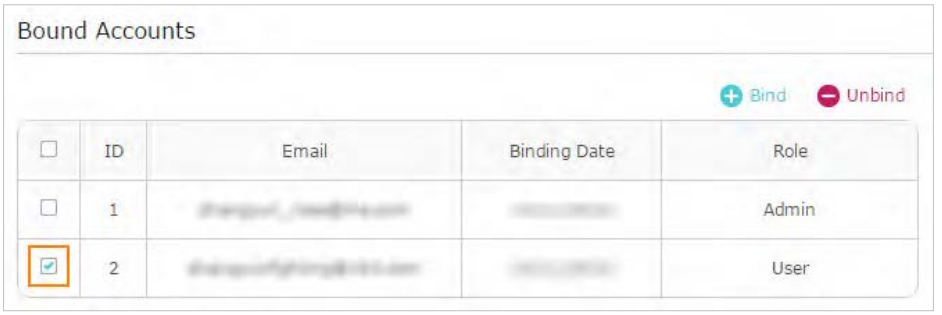


4. The new TP-Link ID will be displayed in the Bound Accounts table as a User.



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

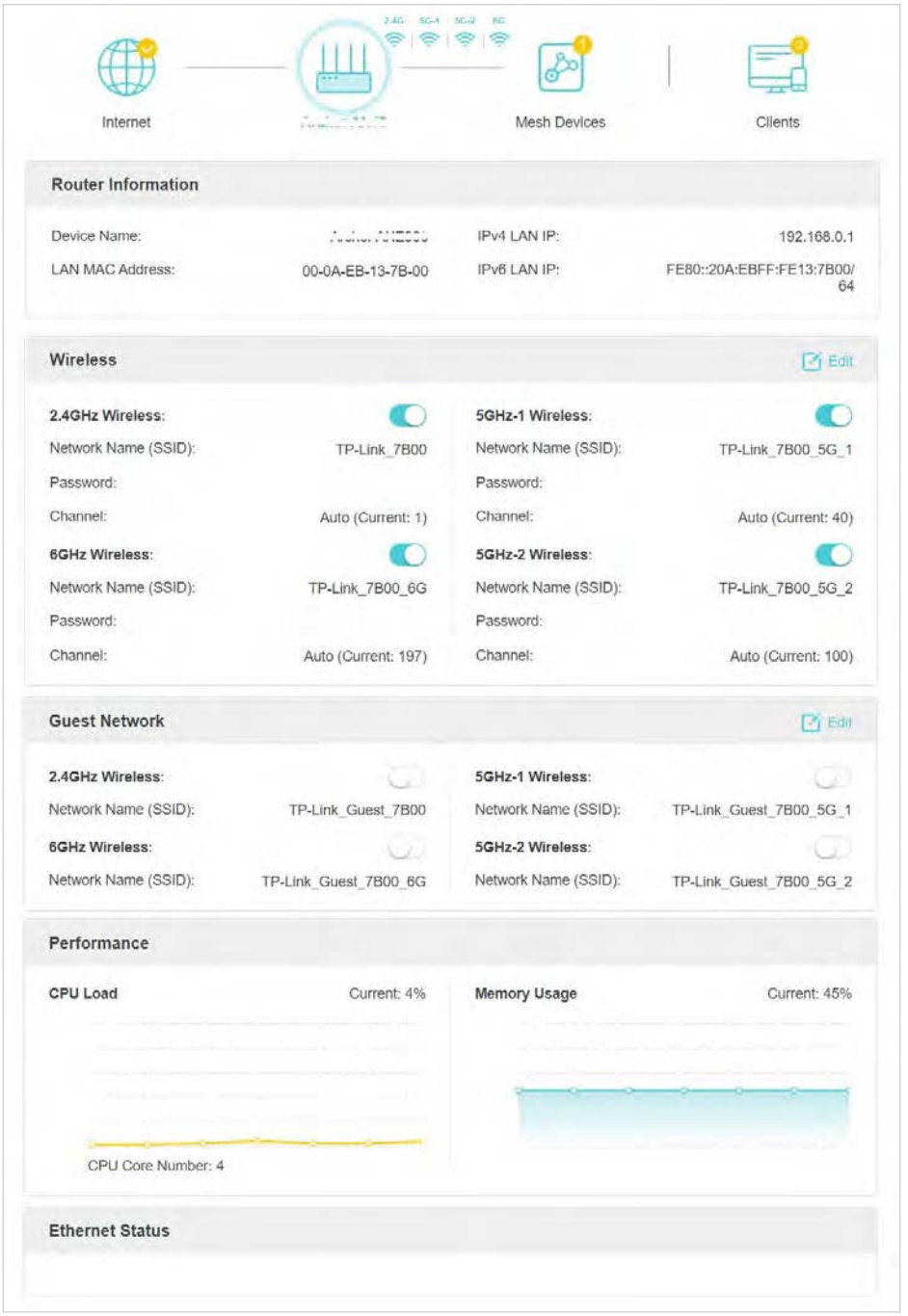
Network Map

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

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

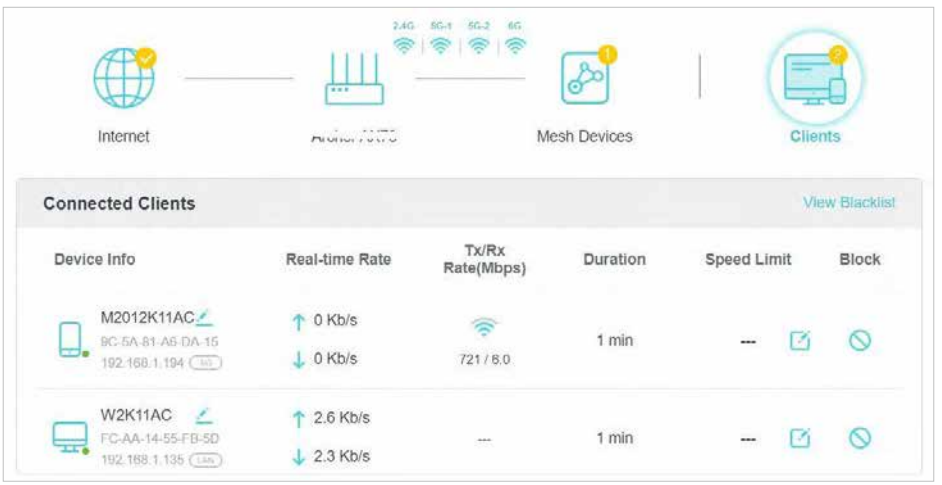
- Click Internet to check internet status.

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



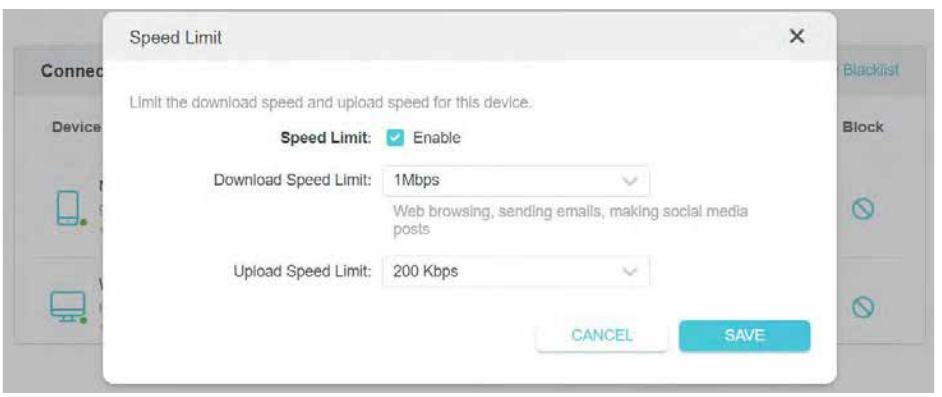
- Click Mesh Devices to view the devices that form a mesh network with the router.

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



To limit the speeds of a device:

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

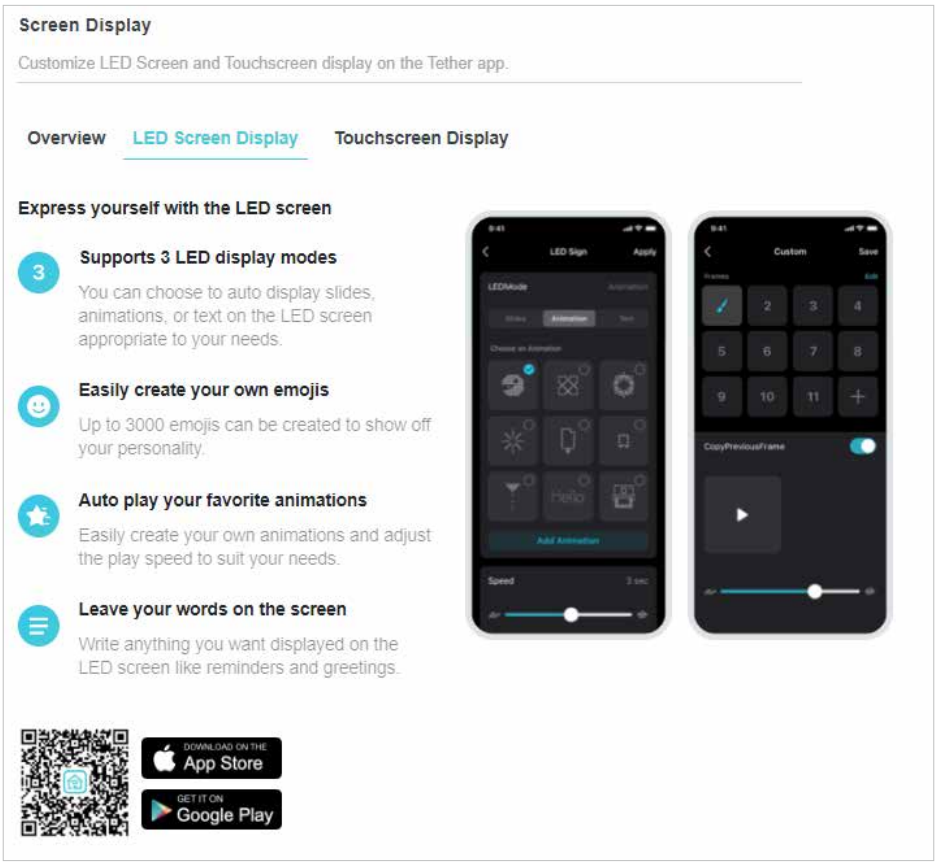


Chapter 7

Screen Display

Customize the touchscreen and LED screen to intuitively display real-time weather, time, text, emojis, and even your favorite custom content. The touchscreen also simplifies management and gives immediate responses.

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Screen Display.
3. Click LED Screen and Touchscreen to for detailed introduction.



4. Download TP-Link Tether app to enjoy the fun with the LED screen and touchscreen, also for easy network management.

Chapter 8

Wireless Settings

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

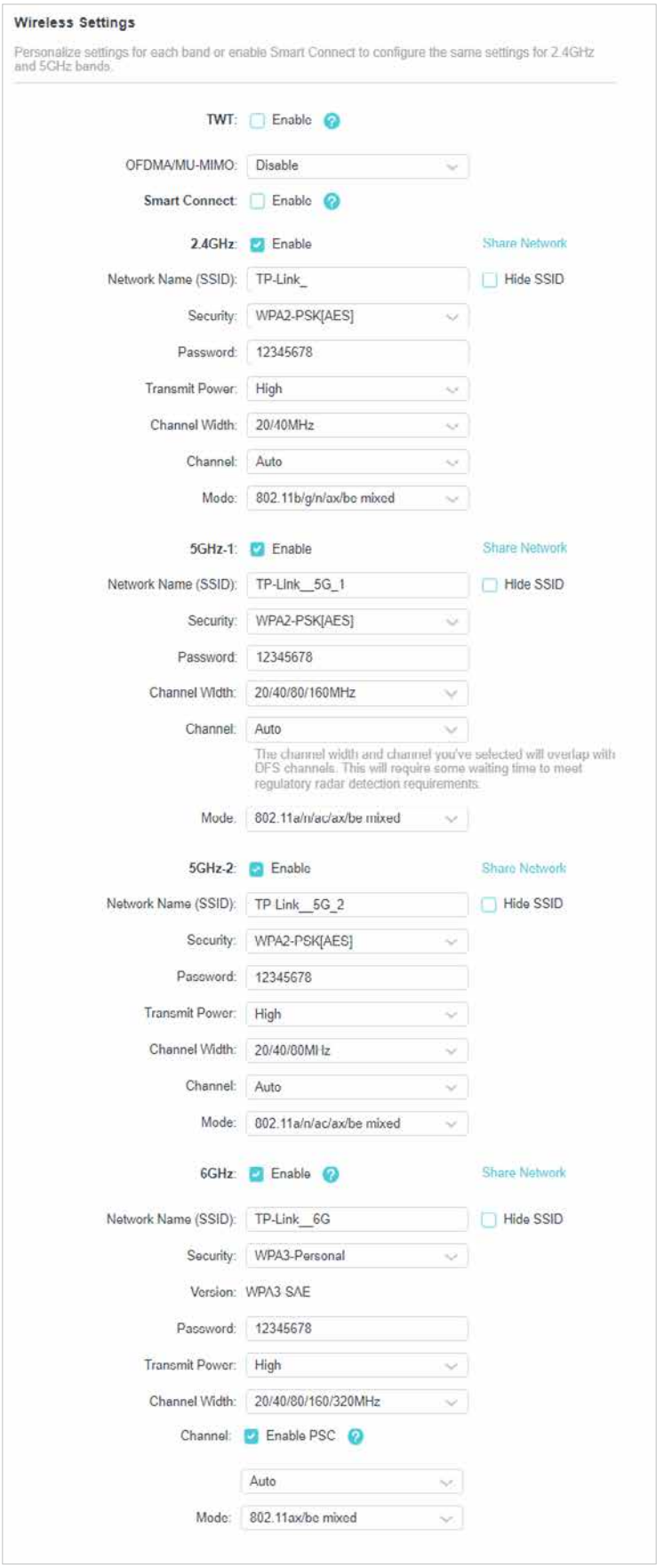
It contains the following sections:

- Specify Wireless Settings
- Schedule Your Wireless Function
- Use WPS for Wireless Connection
- Advanced Wireless Settings

8. 1. Specify Wireless Settings

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

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


Wireless Settings
Personalize settings for each band or enable Smart Connect to configure the same settings for 2.4GHz and 5GHz bands.
TWT: Enable
OFDMA/MU-MIMO: Disable
Smart Connect: Enable
2.4GHz: Enable
Share Network
Network Name (SSID): TP-Link_
Hide SSID
Security: WPA2-PSK[AES]
Password: 12345678
Transmit Power: High
Channel Width: 20/40MHz
Channel: Auto
Mode: 802.11b/g/n/ax/be mixed
5GHz-1: Enable
Share Network
Network Name (SSID): TP-Link_5G_1
Hide SSID
Security: WPA2-PSK[AES]
Password: 12345678
Channel Width: 20/40/80/160MHz
Channel: Auto
The channel width and channel you've selected will overlap with DFS channels. This will require some waiting time to meet regulatory radar detection requirements.
Mode: 802.11a/n/ac/ax/be mixed
5GHz-2: Enable
Share Network
Network Name (SSID): TP Link_5G_2
Hide SSID
Security: WPA2-PSK[AES]
Password: 12345678
Transmit Power: High
Channel Width: 20/40/80MHz
Channel: Auto
Mode: 802.11a/n/ac/ax/be mixed
6GHz: Enable
Share Network
Network Name (SSID): TP-Link_6G
Hide SSID
Security: WPA3-Personal
Version: WPA3 SAE
Password: 12345678
Transmit Power: High
Channel Width: 20/40/80/160/320MHz
Channel: Enable PSC
Auto
Mode: 802.11ax/be mixed

- **To enable or disable OFDMA:**

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

1. Go to Advanced > Wireless > Wireless Settings.
2. Enable OFDMA+MU-MIMO or OFDMA only.

- **To 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:**

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

1. Go to Advanced > Wireless > Wireless Settings.
2. Enable Smart Connect.

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

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

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

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

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

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

- **To hide SSID:**

1. Go to Wireless or Advanced > Wireless > Wireless Settings.
2. Select Hide SSID, and your SSID won't display when you scan for local wireless networks on your wireless device and you need to manually join the network.

- **To change the security option:**

1. Go to Advanced > Wireless > Wireless Settings.
2. Select an option from the Security drop-down list. We recommend you don't change the default settings unless necessary.

- **To change the transmit power:**

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.

- **To change channel settings:**

1. Go to Advanced > Wireless > Wireless Settings.
2. Select a Channel Width (bandwidth) for the wireless network. It is recommended to just leave it as default.
3. Select an operating Channel for the wireless network. It is recommended to leave the channel to Auto if you are not experiencing the intermittent wireless connection issue.

   For the 6 GHz network, you can select the Enable PSC checkbox. When PSC (Preferred Scanning Channel) is enabled, only channels with higher connectivity will be reserved to ensure 6 GHz device connections.

- **To change the transmission mode:**

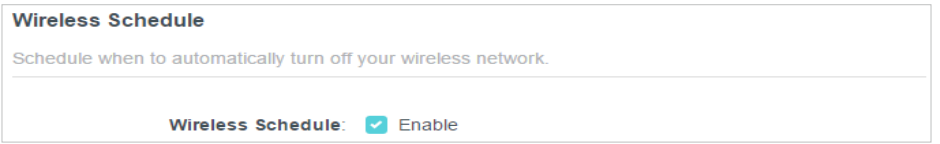
1. Go to Advanced > Wireless > Wireless Settings.
2. For the 2.4 GHz and 5 GHz networks, disable Smart Connect, then select a transmission Mode according to your wireless client devices. It is recommended to just leave it as default.

8. 2. Schedule Your Wireless Function

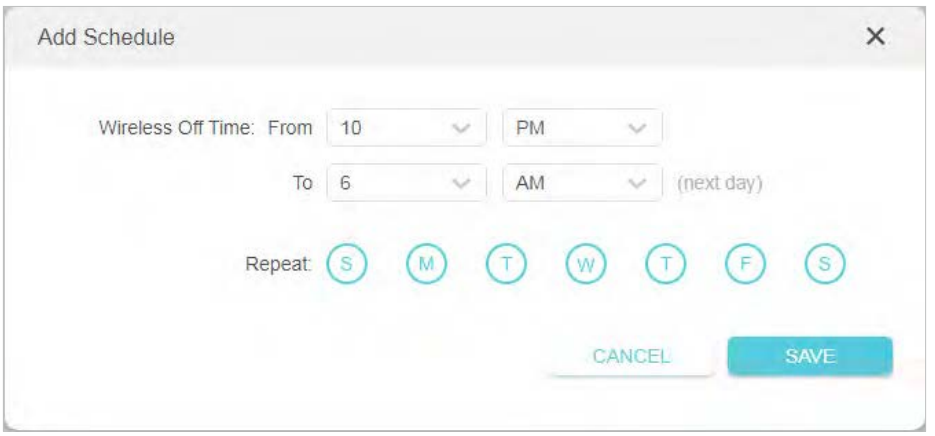
The wireless network can be automatically off at a specific time when you do not need the wireless connection.

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

3. Enable the Wireless Schedule feature.



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



Note:

- The Effective Time Schedule is based on the time of the router. You can go to Advanced > System > Time & Language to modify the time.
- The wireless network will be automatically turned on after the time period you set.

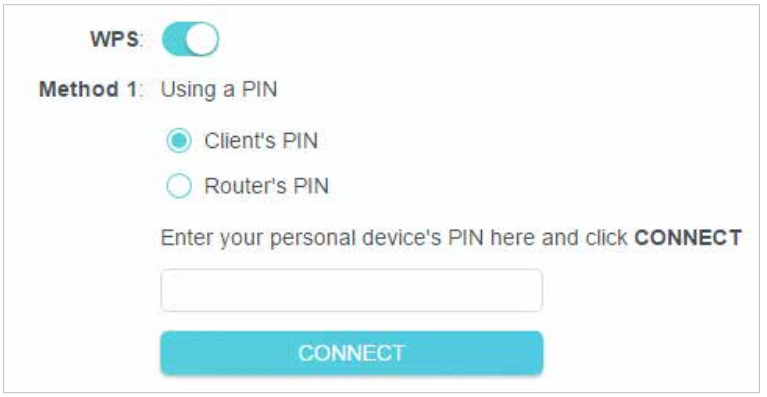
8. 3. Use WPS for Wireless Connection

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

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

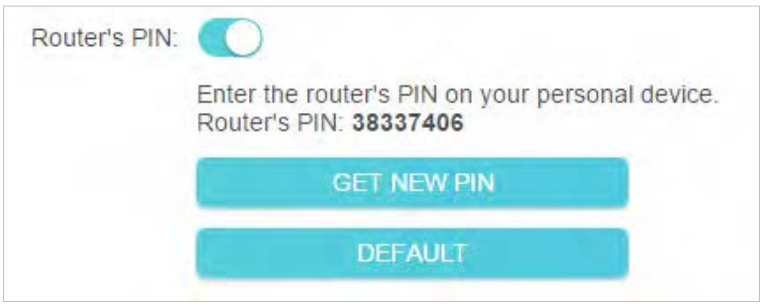
8. 3. 1. Connect via the Client's PIN

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



8. 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.

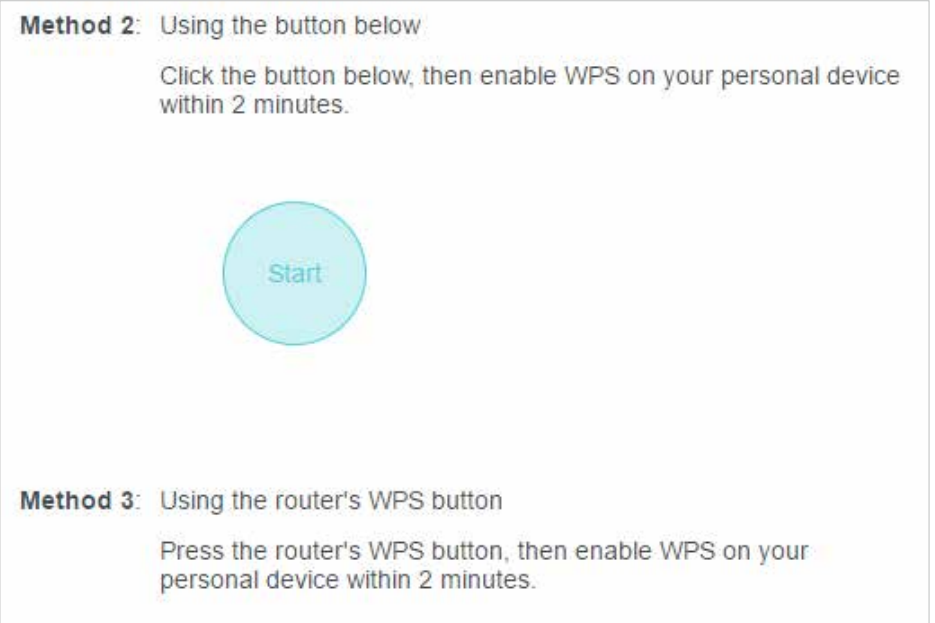


Note:

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.

8. 3. 3. Push the WPS Button

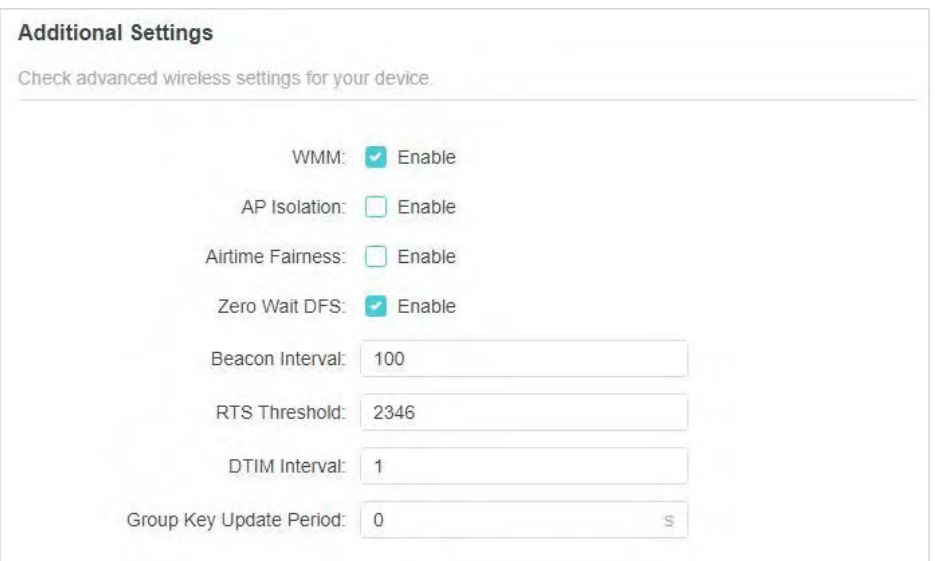
Click Start on the screen or directly press the router's WPS button on the touchscreen. Within two minutes, enable WPS on your personal device. Success will appear on the screen and the WPS LED of the router should change from flashing to solid on, indicating successful WPS connection.



8. 4. Advanced Wireless Settings

Check advanced wireless settings for your device.

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



- WMM - WMM function can guarantee the packets with high-priority messages being transmitted preferentially.

- AP Isolation - This function isolates all connected wireless stations so that wireless stations cannot access each other through WLAN.
- Airtime Fairness - This function can improve the overall network performance by sacrificing a little bit of network time on your slow devices.
- Zero Wait DFS - Zero Wait DFS (Dynamic Frequency Selection) allows the router to immediately reselect a new channel once the radar signal is detected on a channel allocated to radar devices to ensure lag-free network experience.
- 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 9

Guest Network

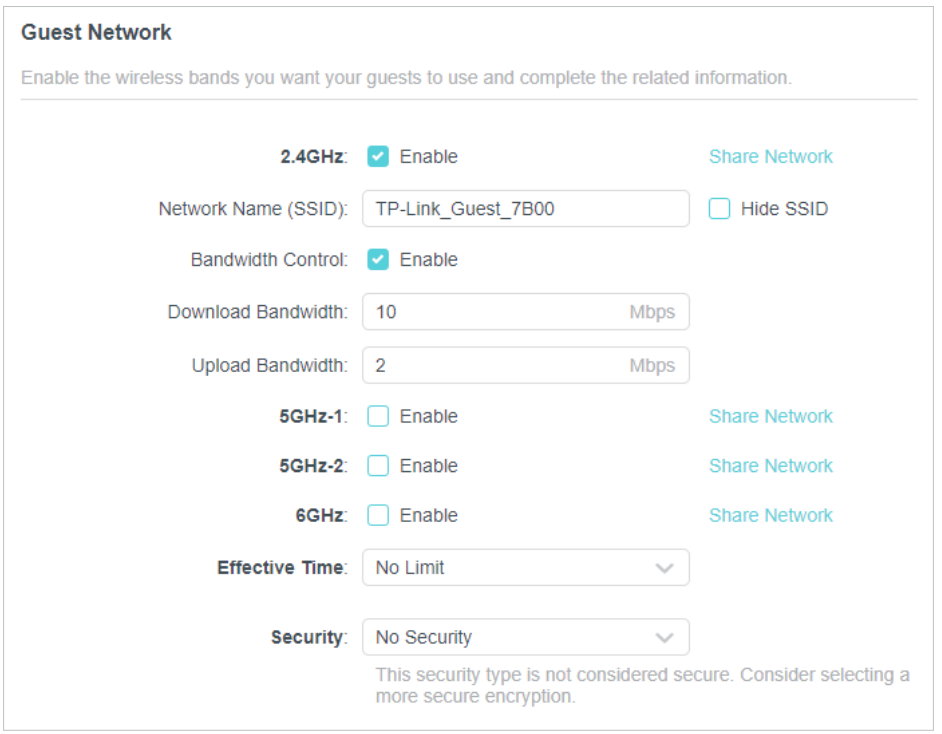
This function allows you to provide Wi-Fi access for guests without disclosing your main network. When you have guests in your house, apartment, or workplace, you can create a guest network for them. In addition, you can customize guest network options to ensure network security and privacy.

It contains the following sections:

- Create a Network for Guests
- Customize Guest Network Options

9. 1. Create a Network for Guests

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > Wireless > Guest Network or click Wireless on the top page. Locate the Guest Network section.
3. Create a guest network as needed.
   1) Tick the Enable checkbox for the 2.4GHz, 5 GHz-1, 5GHz-2 or 6GHz wireless network.
   2) Customize the SSID. Don't select Hide SSID unless you want your guests to manually input the SSID for guest network access.
   3) Enable Bandwidth Control if you want to limit the network speed of your guests. Then enter the limited bandwidth value.
   4) Set the effective time 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.



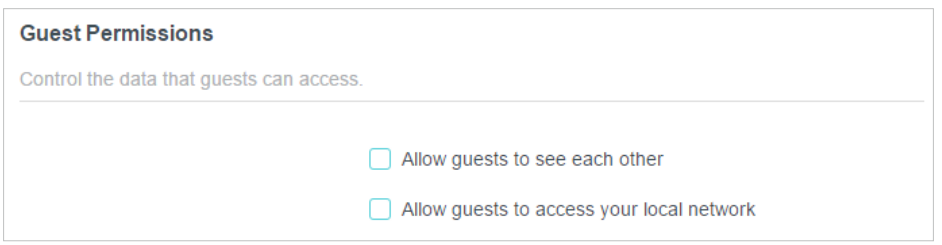
4. Click SAVE. Now your guests can access your guest network using the SSID and password you set!
5. You can also click Sharing Network to share the SSID and password to your guests.

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.

9. 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.



- 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.

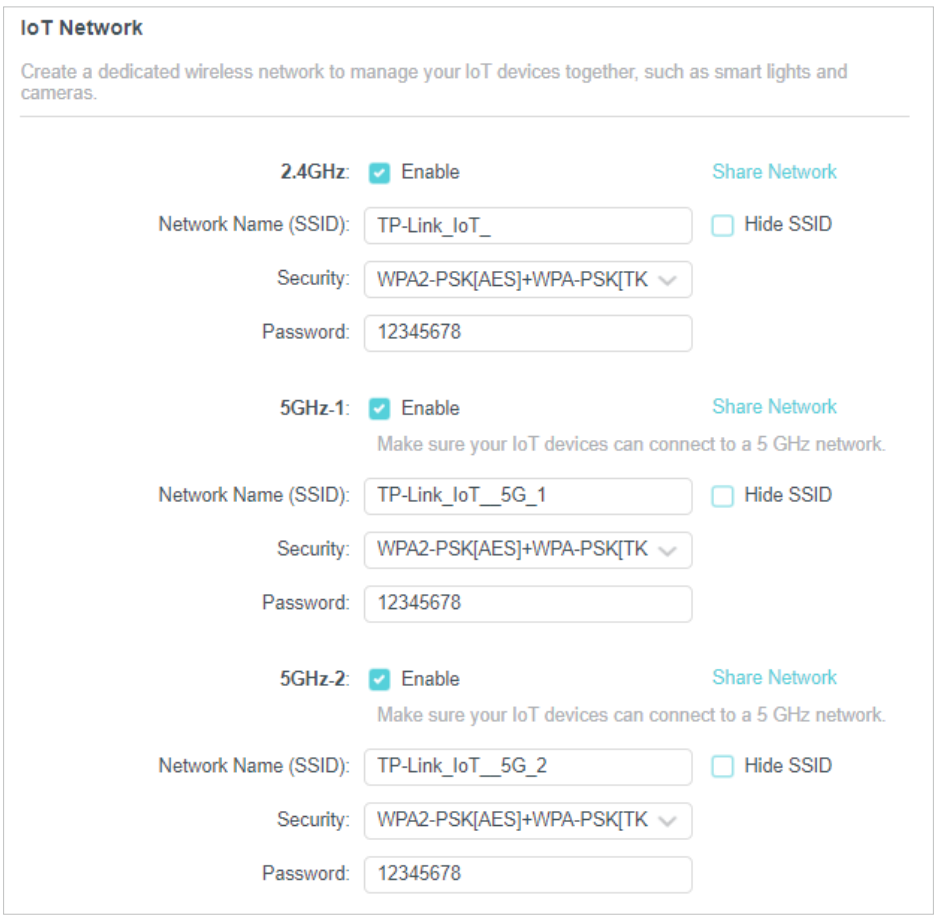
4. Click SAVE. Now you can ensure network security and privacy!

Chapter 10

IoT Network

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

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



4. Click SAVE. Now you can connect your IoT devices to the dedicated IoT network.
5. You can also click Sharing Network to share the SSID and password to others.

Chapter 11

USB Settings

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

The router supports USB external flash drives and hard drives.

It contains the following sections:

- Access the USB Storage Device
- Media Sharing
- Time Machine

11. 1. Access the USB Storage Device

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

Tips:

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

11. 1. 1. Access the USB Device Locally

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

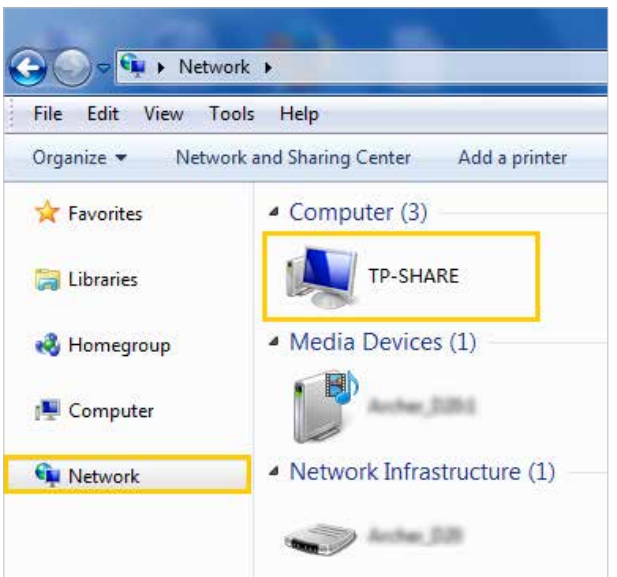
Windows computer

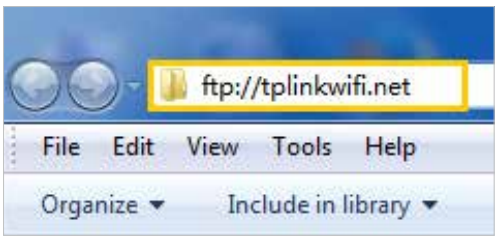
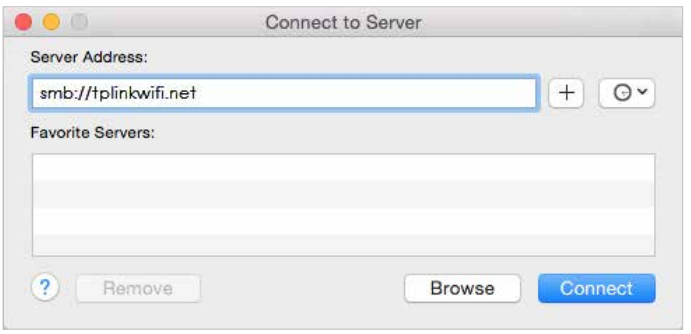
- **Method 1:**

Go to Computer > Network, then click the Network Server Name (TP-SHARE by default) in the Computer section.

Note:

Operations in different systems are similar. Here we take Windows 7 as an example.



Windows computer	• **Method 2:** Open the Windows Explorer (or go to Computer) and type the server address \\tplinkwifi.net or ftp://tplinkwifi.net in the address bar, then press Enter. 
Mac	1) Select Go > Connect to Server. 2) Type the server address smb://tplinkwifi.net. 3) Click Connect.  4) When prompted, select the Guest radio box. (If you have set up a username and a password to deny anonymous access to the USB disks, you should select the Registered User radio box. To learn how to set up an account for the access, refer to To Set Up Authentication for Data Security.)
Tablet	Use a third-party app for network files management.

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

11. 1. 2. Access the USB Device Remotely

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

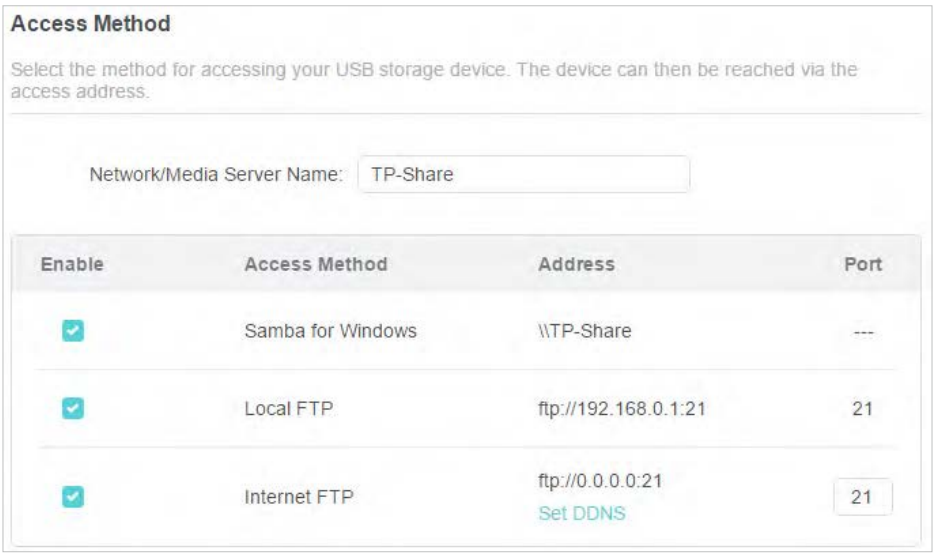
- Share photos and other large files with your friends without logging in to (and paying for) a photo-sharing site or email system.
- Get a safe backup for the materials for a presentation.
- Remove the files on your camera's memory card from time to time during the journey.

Note:

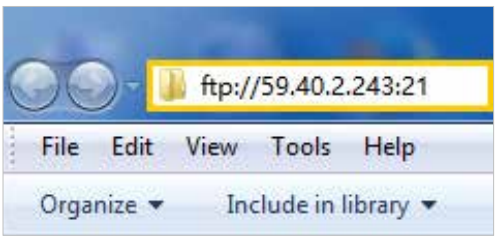
If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), you cannot use this feature because private addresses are not routed on the internet.

Follow the steps below to configure remote access settings.

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



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

Computer	1) Open the Windows Explorer (or go to Computer, only for Windows users) or open a web browser. 2) Type the server address in the address bar: Type in ftp://<WAN IP address of the router>:<port number> (such as ftp://59.40.2.243:21). If you have specified the domain name of the router, you can also type in ftp://<domain name>:<port number> (such as ftp://MyDomainName:21)  3) Press Enter on the keyboard. 4) Access with the username and password you set in To Set Up Authentication for Data Security. Tips: You can also access the USB disk via a third-party app for network files management, which can resume broken file transfers.
Tablet	Use a third-party app for network files management.

Tips:

Click Set Up a Dynamic DNS Service Account to learn how to set up a domain name for you router.

11. 1. 3. Customize the Access Settings

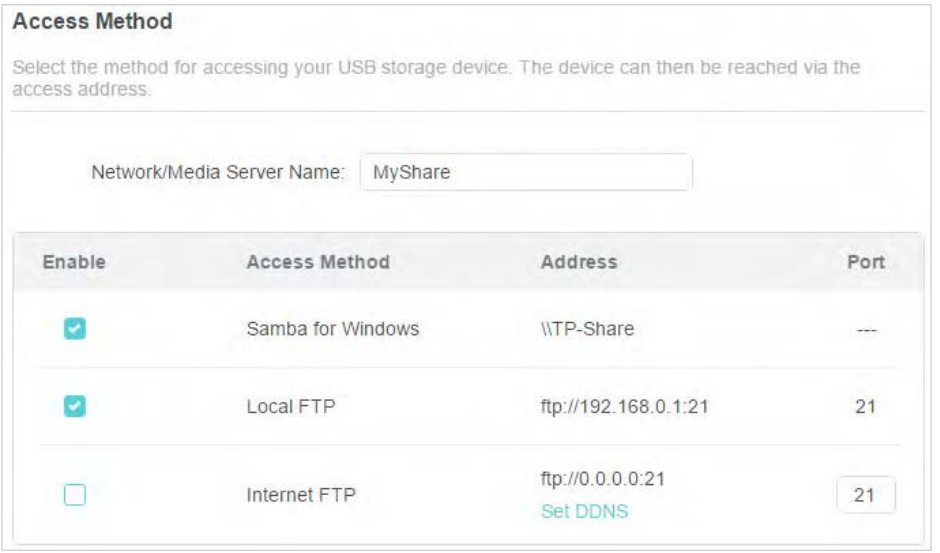
By default, all the network clients can access all folders on your USB disk. You can customize your sharing settings by setting a sharing account, sharing specific contents and setting a new sharing address on the router's web management page.

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

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

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

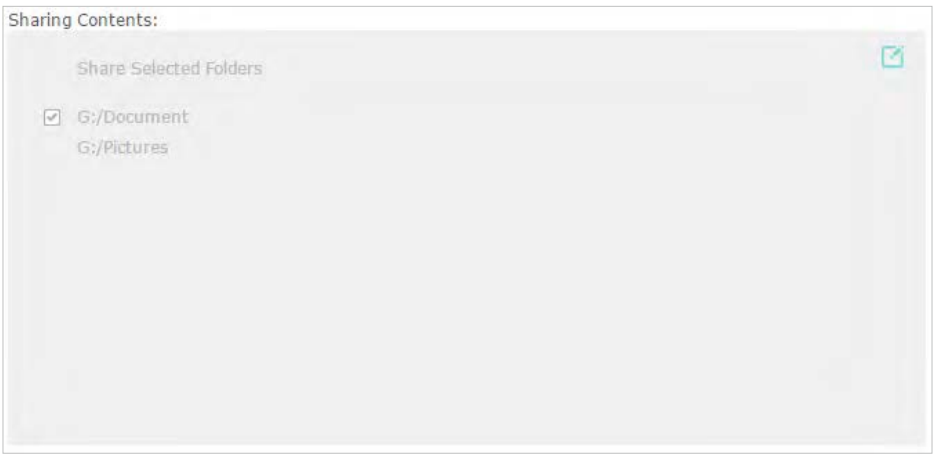
1. In the Access Method session, make sure Samba for Windows is ticked, and enter a Network/Media Server Name as you like, such as MyShare, then click SAVE.



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

- **To Only Share Specific Content**

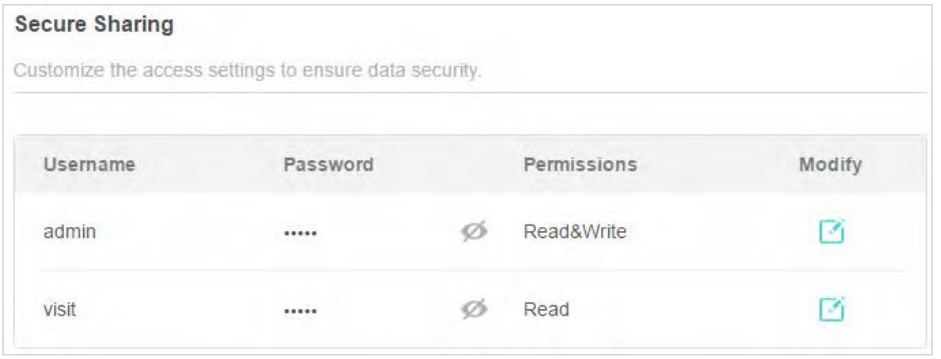
Focus on the File Sharing section. Specify sharing folders that you want to share and click SAVE.



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

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

1. In the File Sharing section, enable Secure Sharing.



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

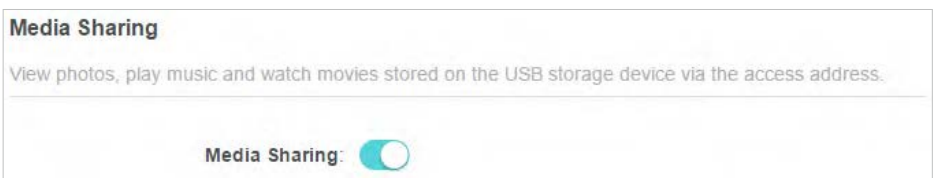
Note:

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

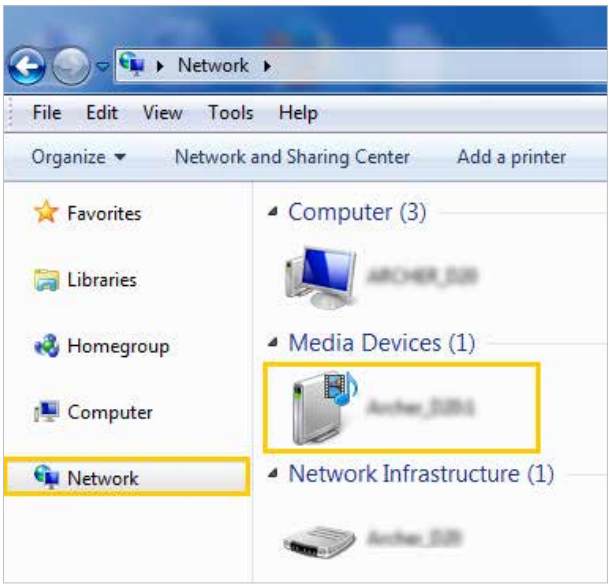
11. 2. Media Sharing

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

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



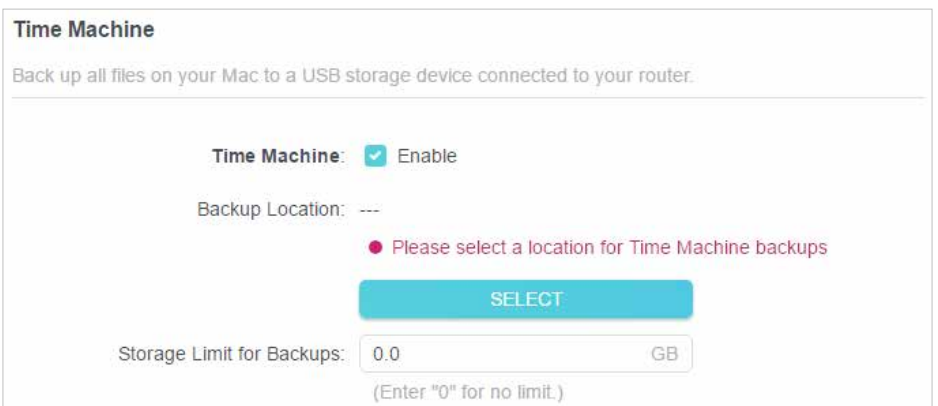
4. When your USB storage device is inserted into the router, your DLNA-supported devices (such as your computer and pad) connected to the router can detect and play the media files on the USB storage devices.
5. Refer to the following table for detailed instructions.

Windows Computer	• Go to Computer > Network, then click the Media Server Name (Model number-share by default) in the Media Devices section. **Note:** Here we take Windows 7 as an example. 
Tablet	• Use a third-party DLNA-supported player.

11. 3. Time Machine

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

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



3. Tick the checkbox to enable Time Machine.
4. Click Select to select a location for Time Machine backups.
5. Set the Size Limit for Backups.

Note: 0 means no limit for the space.

6. Click SAVE.

Chapter 12

HomeShield

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

It contains the following sections:

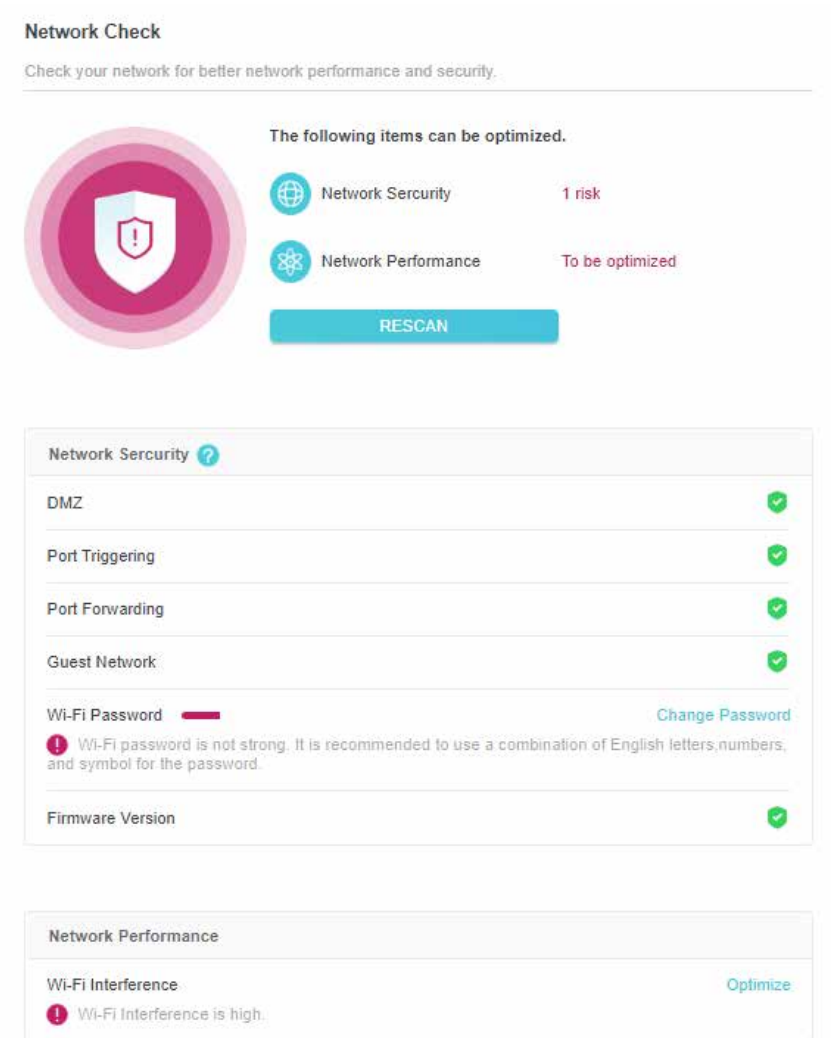
- Network Check
- Parental Controls
- QoS
- More Features

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

12. 1. Network Check

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

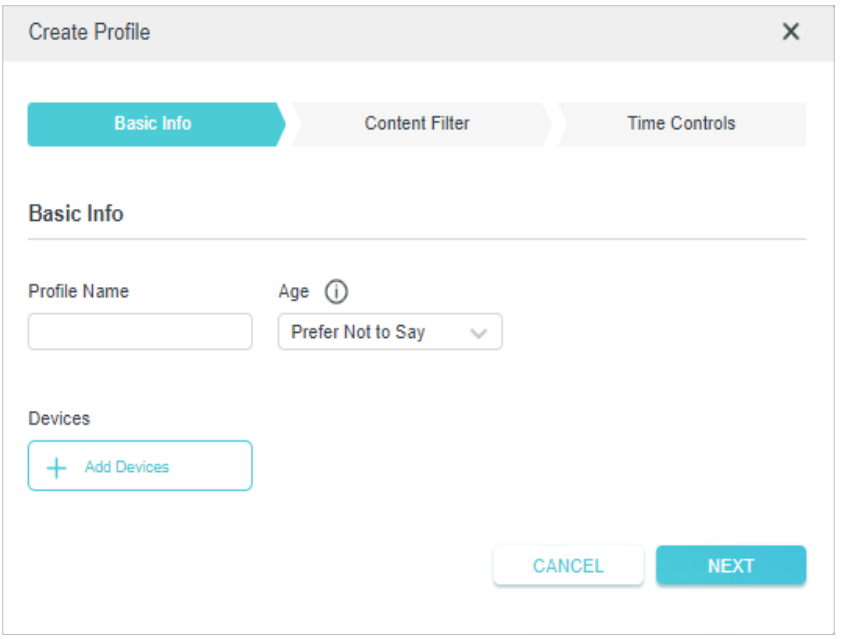
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > HomeShield > Network Check.
3. Click SCAN.
4. Optimize your network according to the tips.



12. 2. Parental Controls

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

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



1) Enter a Name for the profile to make it easier to identify. Set the age to get the corresponding filter level.

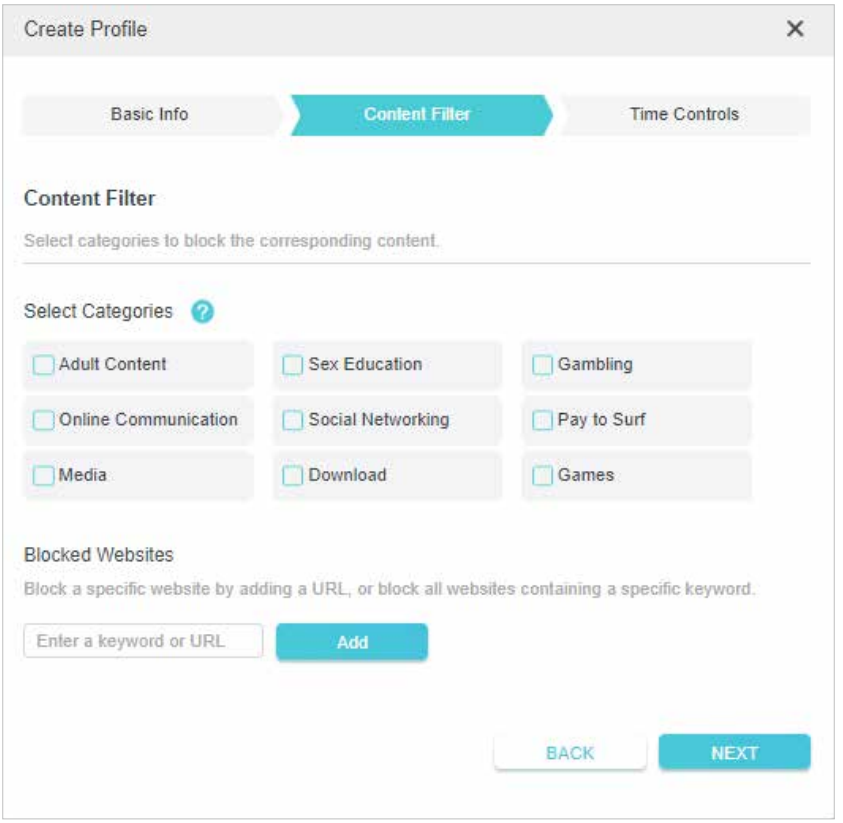
2) Under Devices, click +.

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. Block content for this profile.

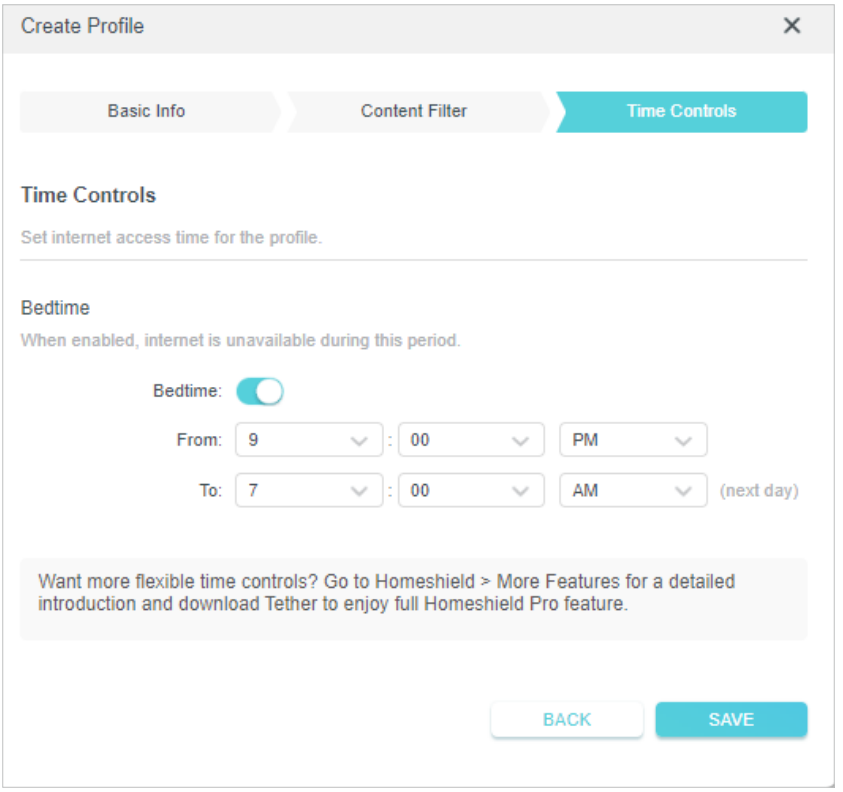


1) Select the content categories to block in the Content Filter list.

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

3) Click NEXT.

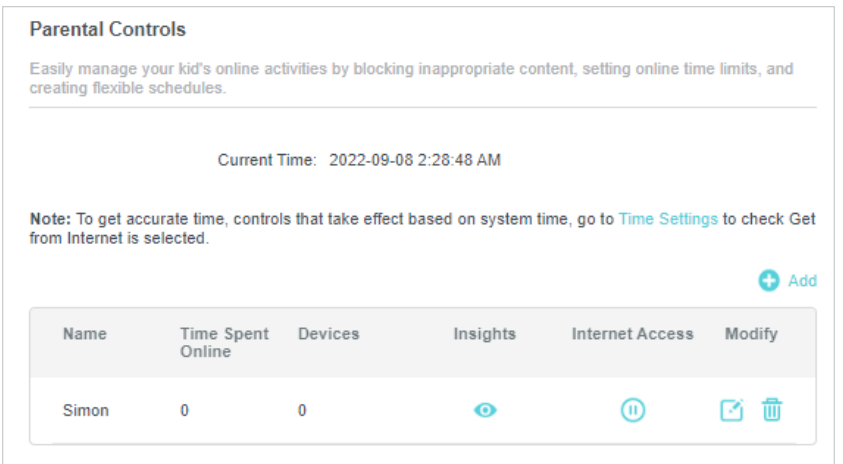
6. Set time restrictions on internet access.



4) Enable Bed Time and use the up/down arrows or enter times in the fields. Devices under this profile will be unable to access the internet during this time period.

5) Click SAVE.

6) After adding a profile, you can click the Insight icon to check the detailed visited history, and click the pause the network for this profile anytime.

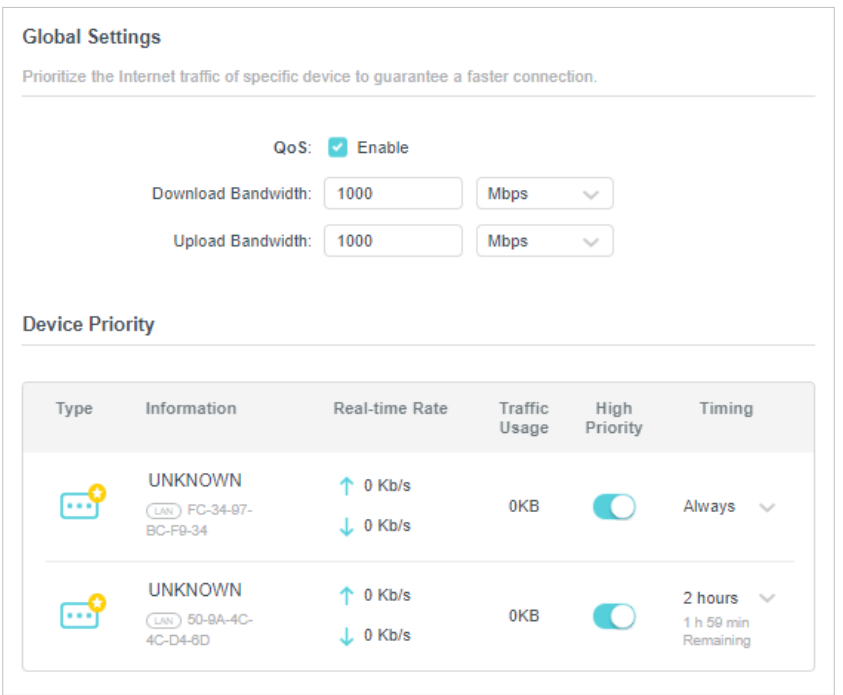


Note: You can go to Advanced > HomeShield > More Features for a detailed introduction and download Tether to enjoy full Homeshield Pro feature.

12. 3. QoS

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

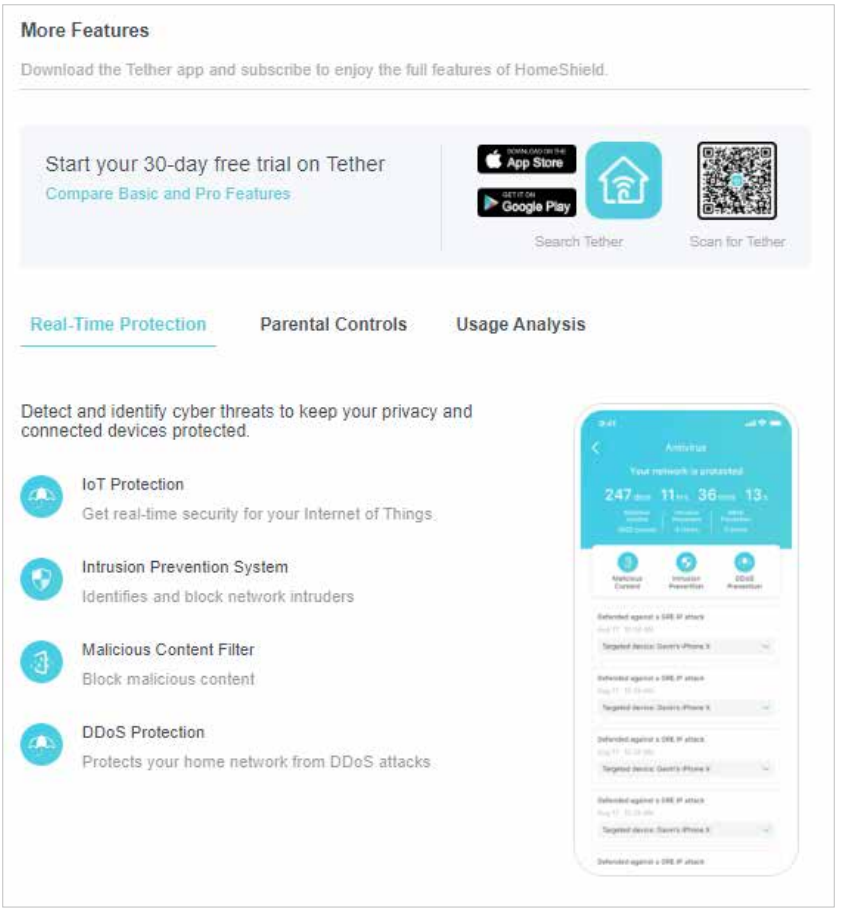
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > HomeShield > QoS.
3. Enable QoS to set the total bandwidth. Then click SAVE.
4. Enable High Priority for the desired device and set its effective time.



12. 4. More Features

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

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


More Features
Download the Tether app and subscribe to enjoy the full features of HomeShield.
Start your 30-day free trial on Tether
Compare Basic and Pro Features
App Store
Google Play
Search Tether
Scan for Tether
Real-Time Protection
Parental Controls
Usage Analysis
Detect and identify cyber threats to keep your privacy and connected devices protected.
IoT Protection
Get real-time security for your Internet of Things.
Intrusion Prevention System
Identifies and block network intruders
Malicious Content Filter
Block malicious content
DDoS Protection
Protects your home network from DDoS attacks

Chapter 13

EasyMesh with Seamless Roaming

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

It contains the following sections:

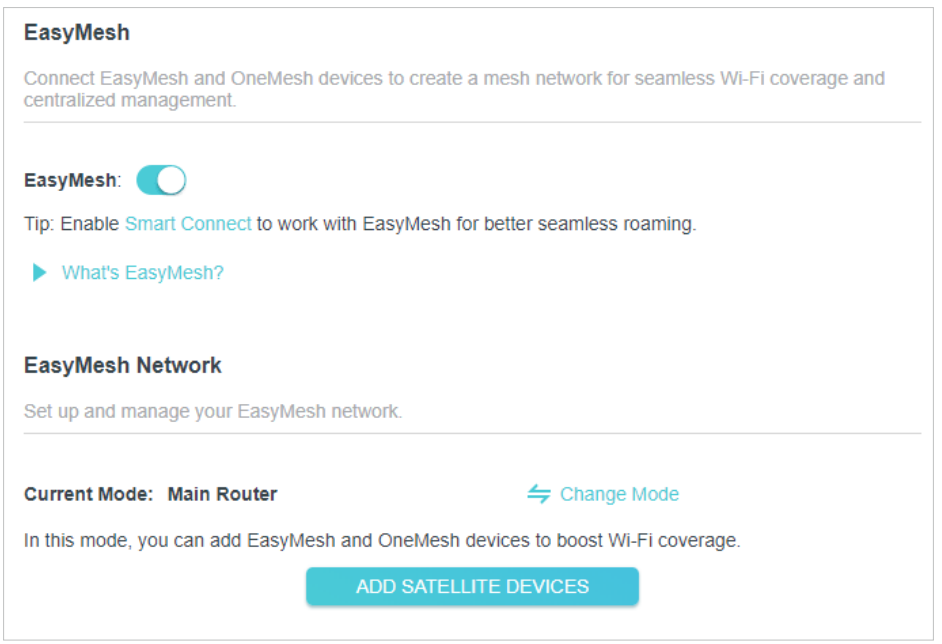
- Add a Router as a Satellite Device
- Add a Range Extender as a Satellite Device
- Manage Devices in the EasyMesh Network

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

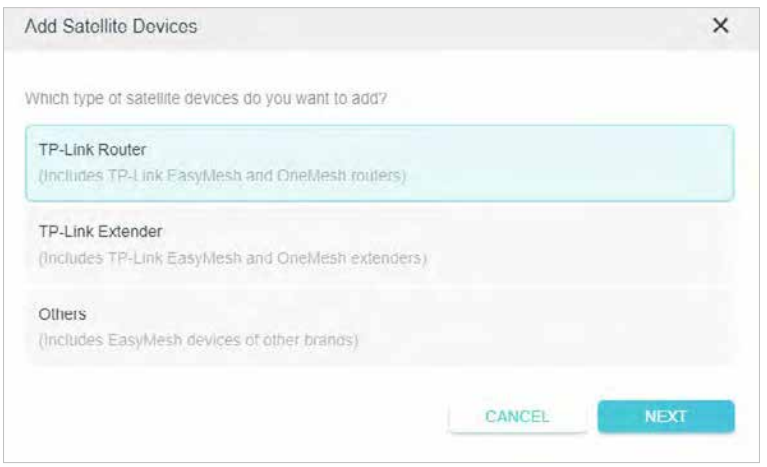
Note: Routers and range extenders must be compatible with EasyMesh or OneMesh™. Firmware upgrades may be required.

13. 1. Add a Router as a Satellite Device

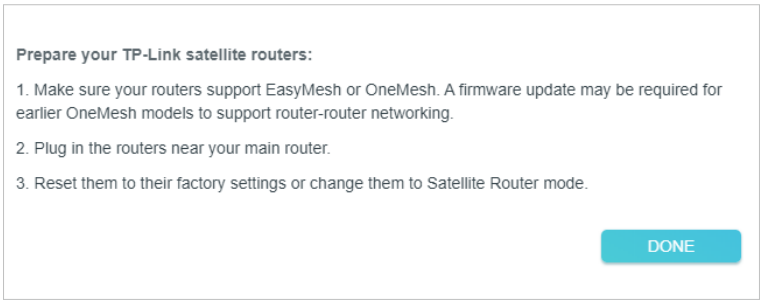
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > EasyMesh, and enable EasyMesh.



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



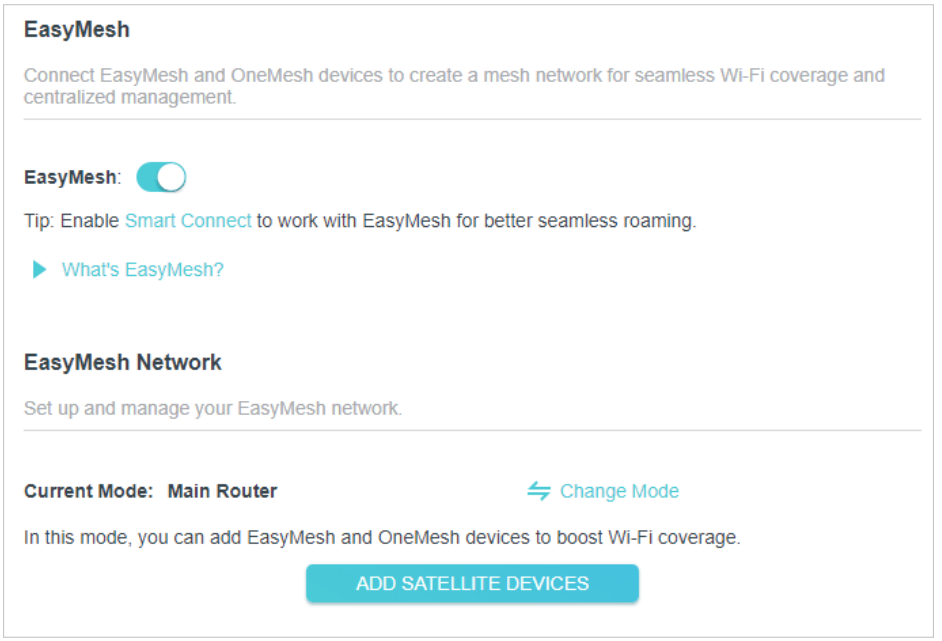
4. Follow the page instructions to prepare your satellite router, then click DONE.



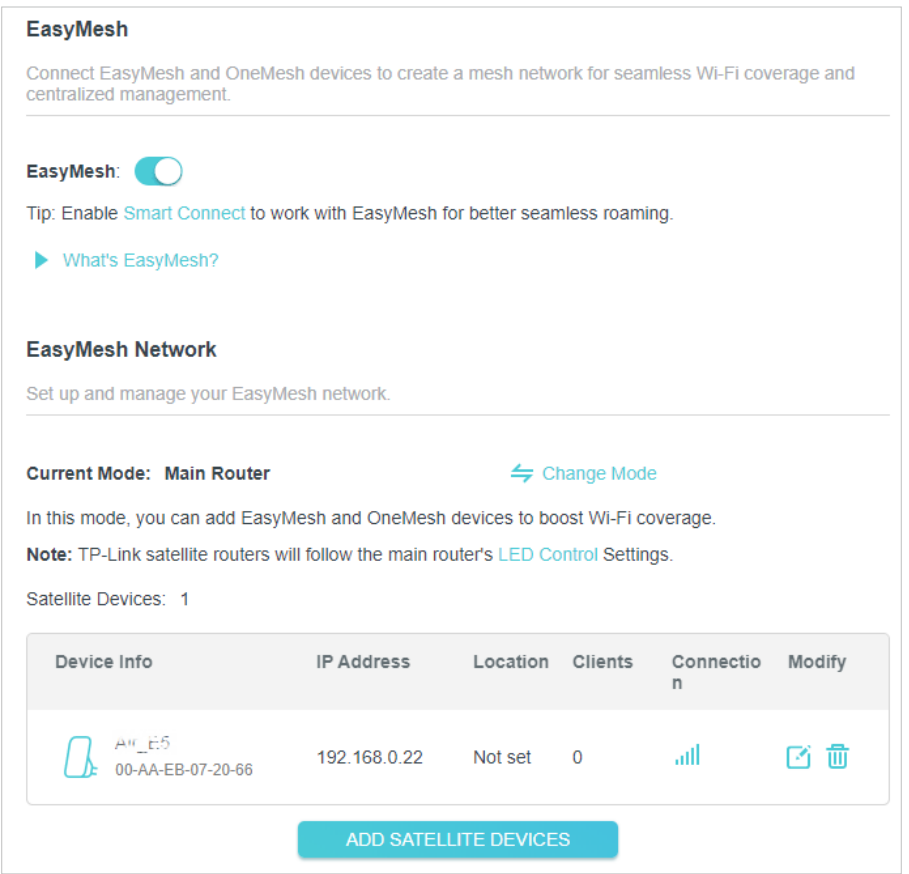
5. Click ADD. When prompted "This device has been added successfully", click OK, then click FINISH.

13. 2. Add a Range Extender as a Satellite Device

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



3. Plug in the extender next to the main router.
4. With in 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.



13. 3. Manage Devices in the EasyMesh Network

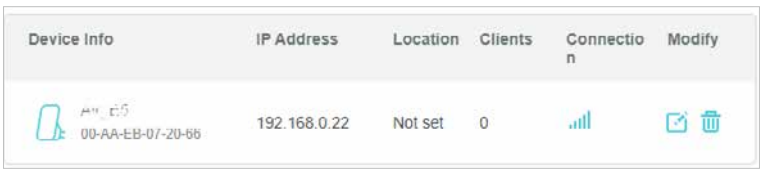
In an EasyMesh network, you can manage all mesh devices and connected clients on your main router's web page.

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

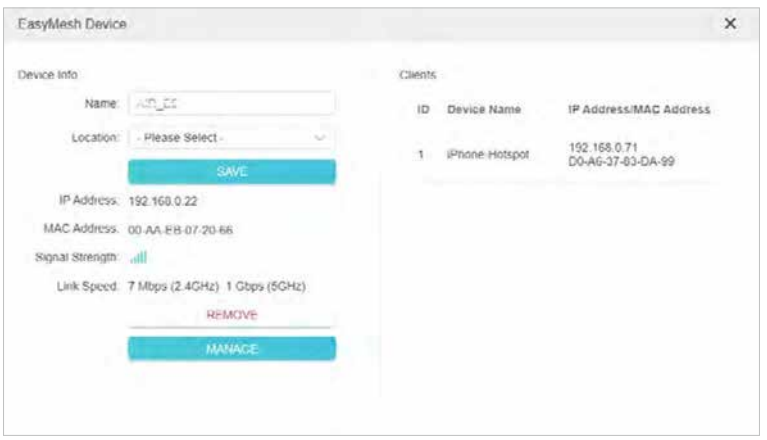
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Network Map.
3. Click to view all mesh devices, and click to view all connected clients.

- **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.



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



- Change device information.
- Click Manage to redirect to the web management page of this device.
- Click Remove to delete this device from the EasyMesh network.

Chapter 14

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, you can prevent ARP spoofing and ARP attacks using IP & MAC Binding, protect your network security by isolating your IoT devices.

It contains the following sections:

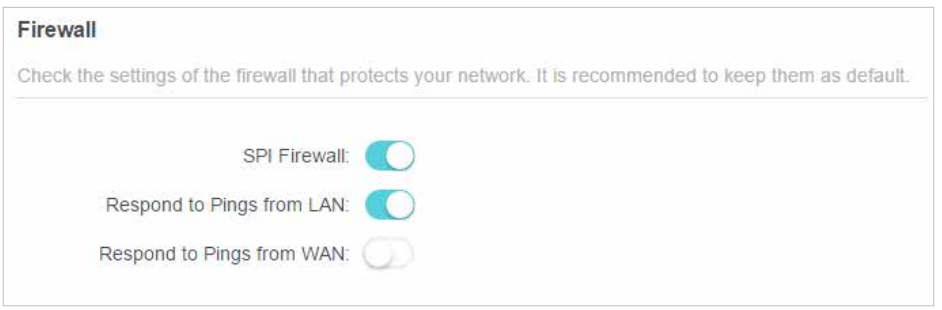
- Protect the Network from Cyber Attacks
- Access Control
- IP & MAC Binding
- ALG
- IoT Security

*For a more comprehensive home network protection system, refer to the HomeShield chapter.

14. 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.



14. 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 (Blacklist) or a list of allowed devices (Whitelist).

I want to:

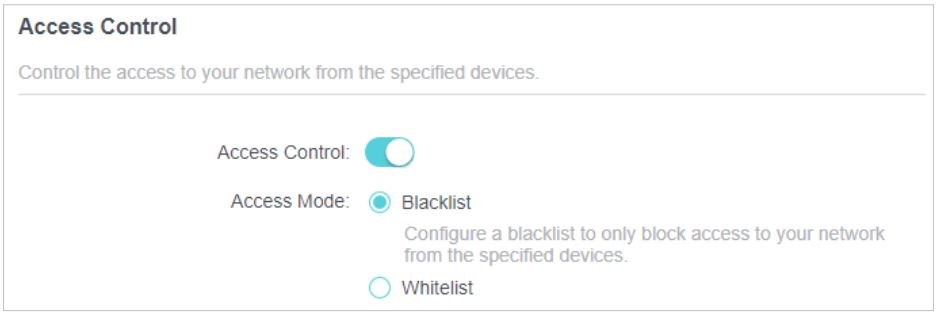
Block or allow specific client devices to access my network (via wired or wireless).

How can I do that?

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

   To block specific device(s):

   1) Select Blacklist.

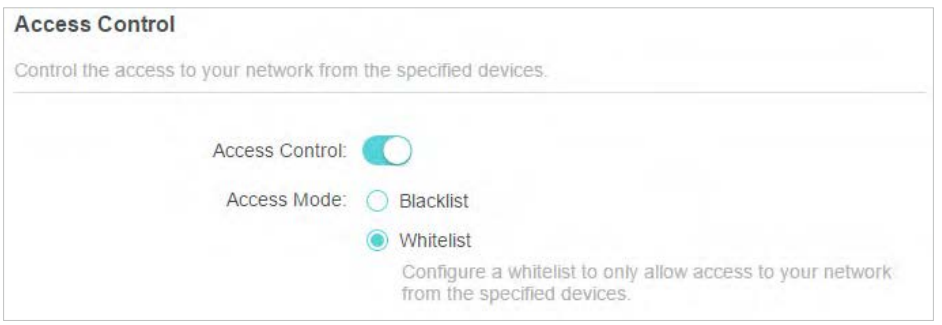


2) Click Add and select devices you want to be blocked and Click ADD.

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

To allow specific device(s):

1) Select Whitelist and click SAVE.

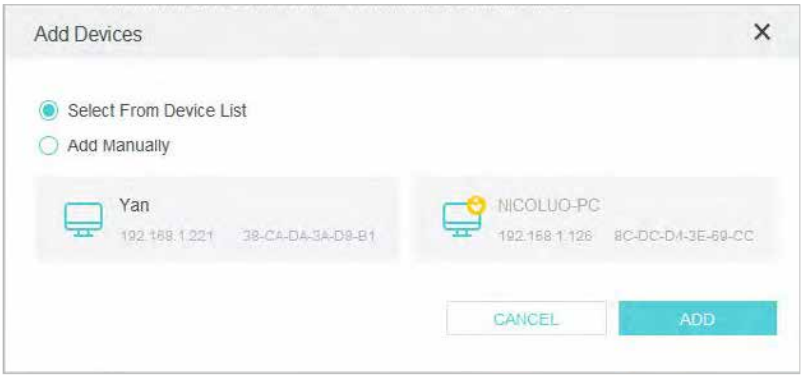


2) Your own device is in the whitelist by default and cannot be deleted. Click Add to add other devices to the whitelist.

- **Add connected devices**

1) Click Select From Device List.

2) Select the devices you want to be allowed and click ADD.

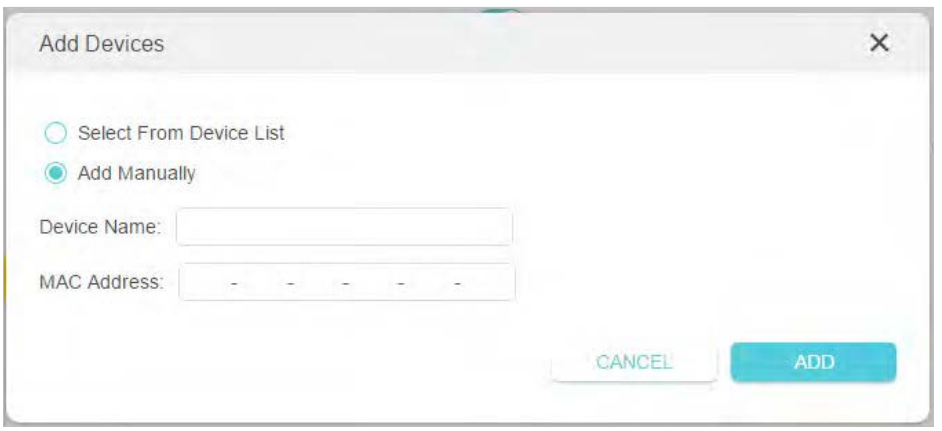


3) The Operation Succeeded message will appear on the screen, which means the selected devices have been successfully added to the whitelist.

- **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 whitelist.

Done!

Now you can block or allow specific client devices to access your network (via wired or wireless) using the Blacklist or Whitelist.

14. 3. IP & MAC Binding

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

I want to:

Prevent ARP spoofing and ARP attacks.

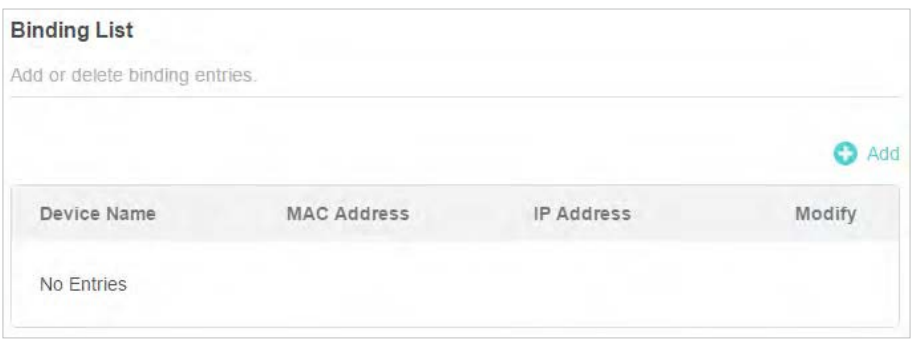
How can I do that?

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

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

   To bind the connected device(s):

   1) Click Add in the Binding List section.



   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.

   3) Click SAVE.

To bind the unconnected device:

1) Click Add in the Binding List section.

2) Enter the MAC Address and IP Address that you want to bind.

3) Click SAVE.

Done!

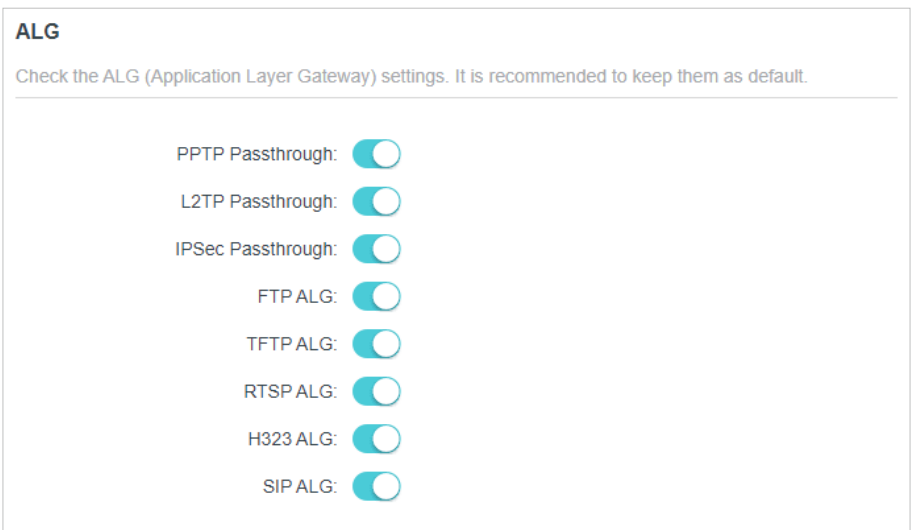
Now you don't need to worry about ARP spoofing and ARP attacks!

14. 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.

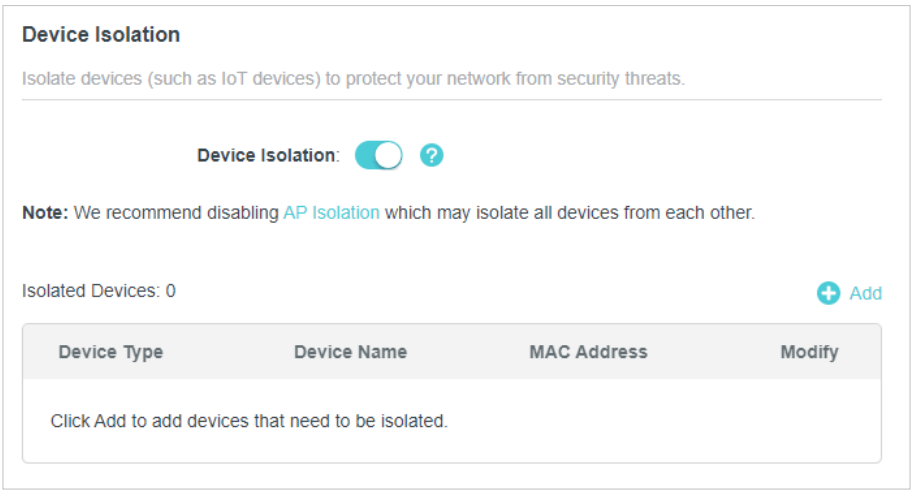
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > Security > ALG.



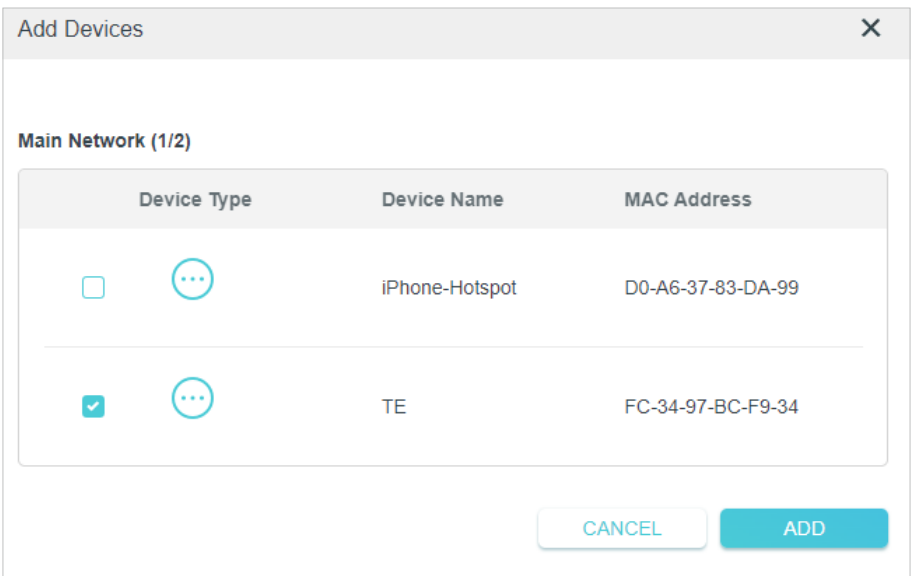
14. 5. IoT Security

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

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



3. Click Add to add your IoT devices.



Done!

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

Chapter 15

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

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

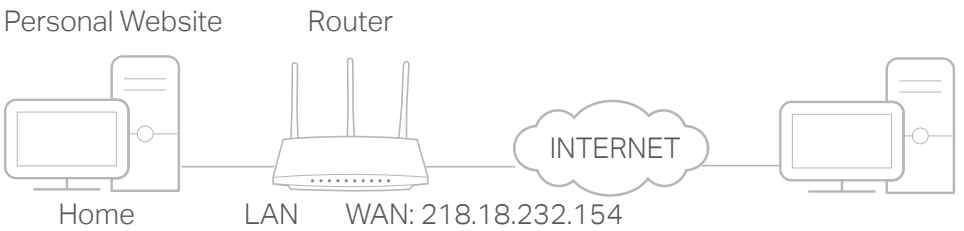
When you build up a server on the local network and want to share it on the internet, Port Forwarding can realize the service and provide it to internet users. At the same time Port Forwarding can keep the local network safe as other services are still invisible from the internet.

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:

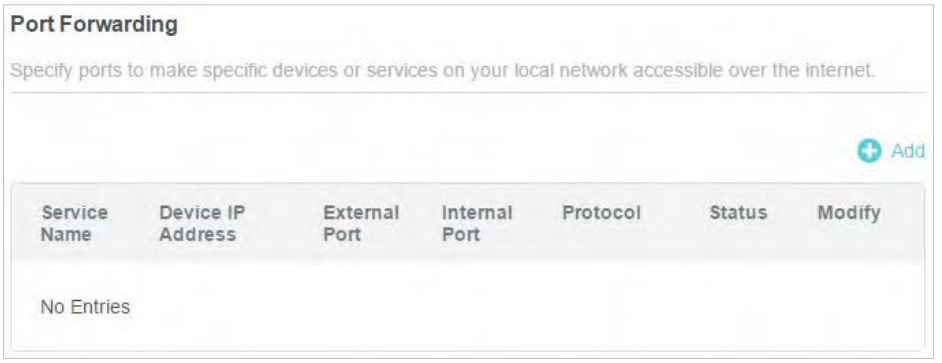
Share my personal website I've built in local network with my friends through the internet.

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.

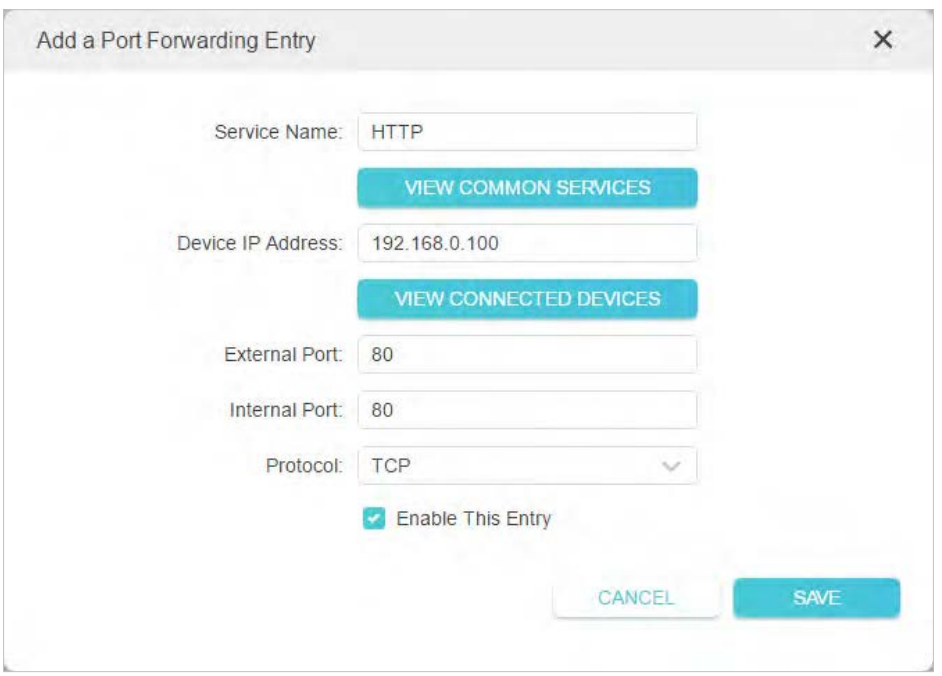


How can I do that?

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.



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.



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.

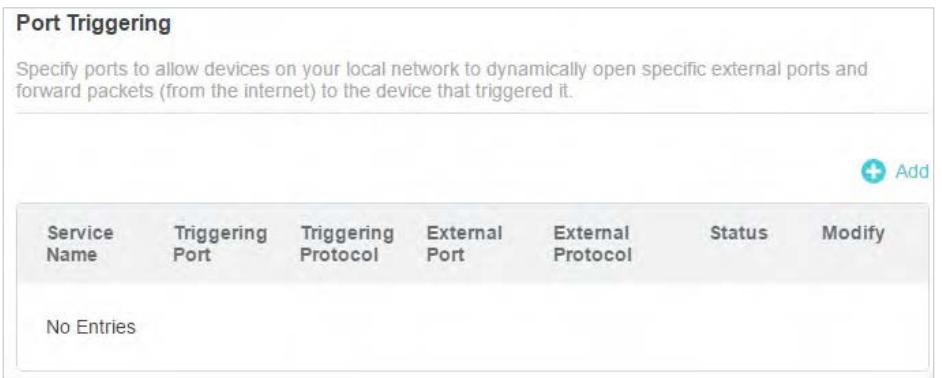
Tips:
- The WAN IP should be a public IP address. For the WAN IP is assigned dynamically by the ISP, it is recommended to apply and register a domain name for the WAN referring to Set Up a Dynamic DNS Service Account. Then users on the internet can use http:// domain name to visit the website.
- If you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

15. 2. Open Ports Dynamically by Port Triggering

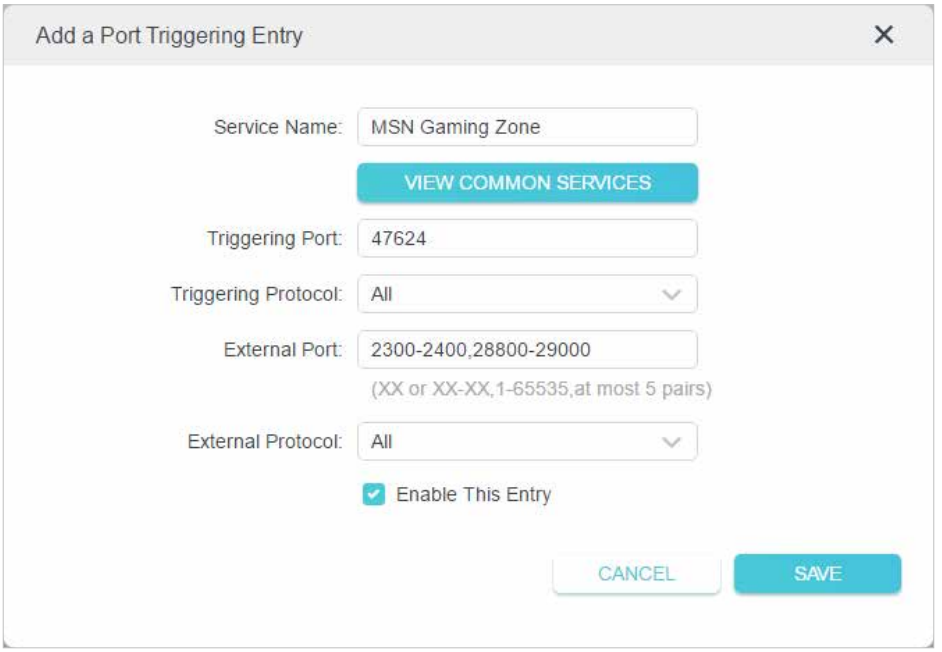
Port Triggering can specify a triggering port and its corresponding external ports. When a host on the local network initiates a connection to the triggering port, all the external ports will be opened for subsequent connections. The router can record the IP address of the host. When the data from the 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 Add.



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.



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.

15. 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.

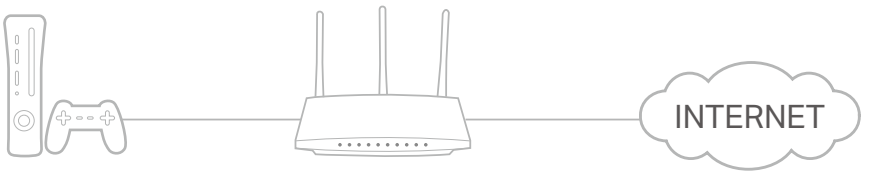
15. 4. Make Xbox Online Games Run Smoothly by UPnP

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).

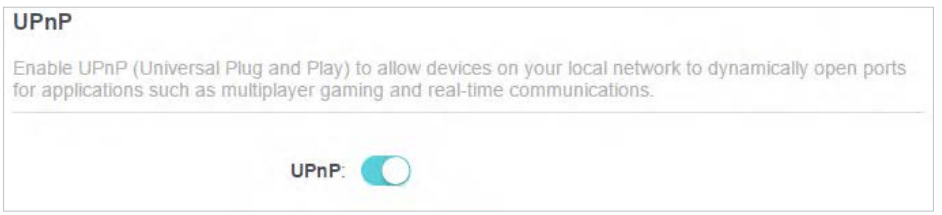
For example, when you connect your Xbox to the router which has connected to the internet to play online games, UPnP will send request to the router to open the

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 16

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.

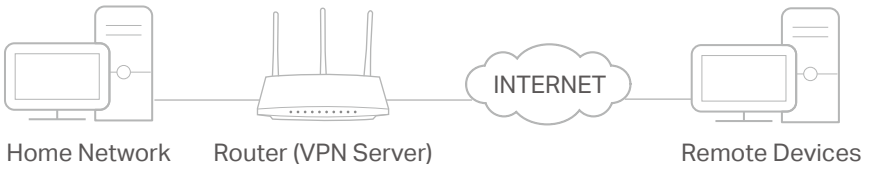
This chapter contains the following sections:

- 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

16. 1. Use OpenVPN to Access Your Home Network

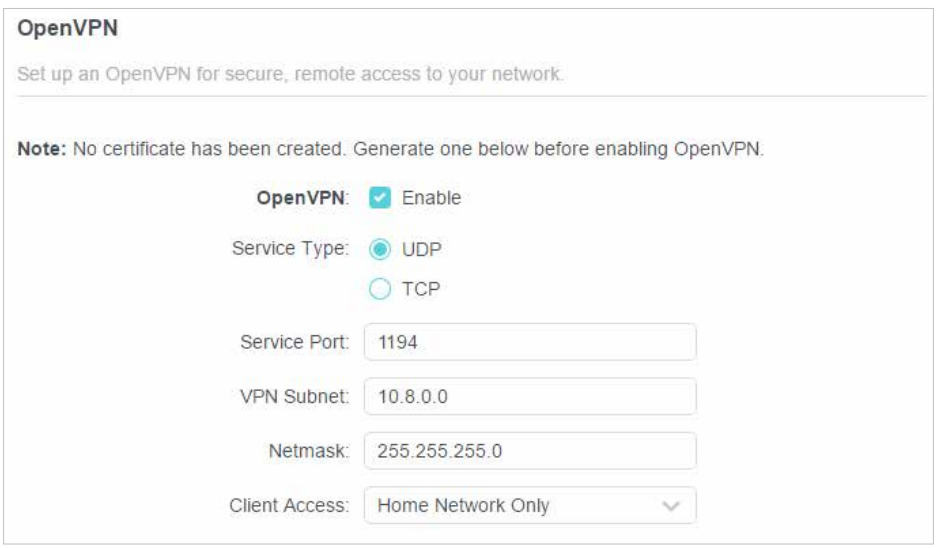
OpenVPN Server is used to create an OpenVPN connection for remote devices to access your home network.

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



Step1. Set up OpenVPN Server on Your Router

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

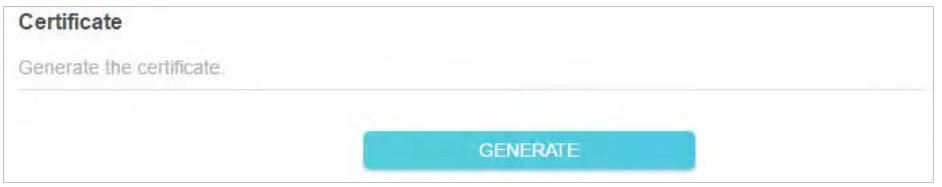


Note:

- 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.

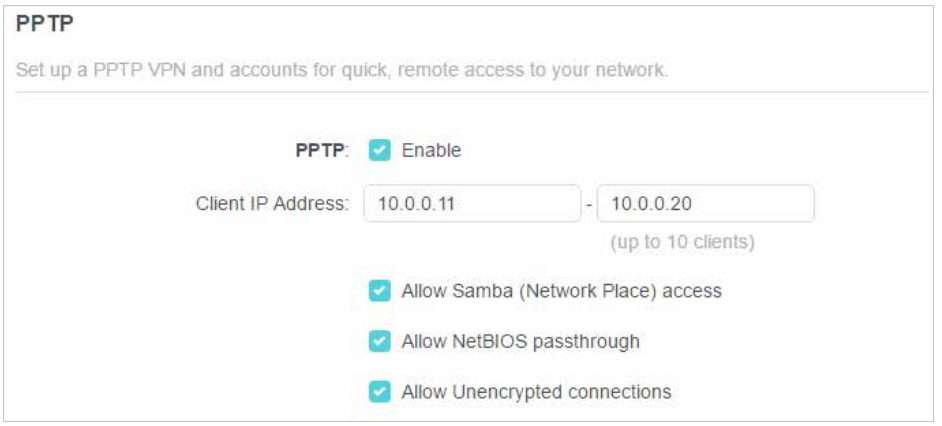
16. 2. Use PPTP VPN to Access Your Home Network

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

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

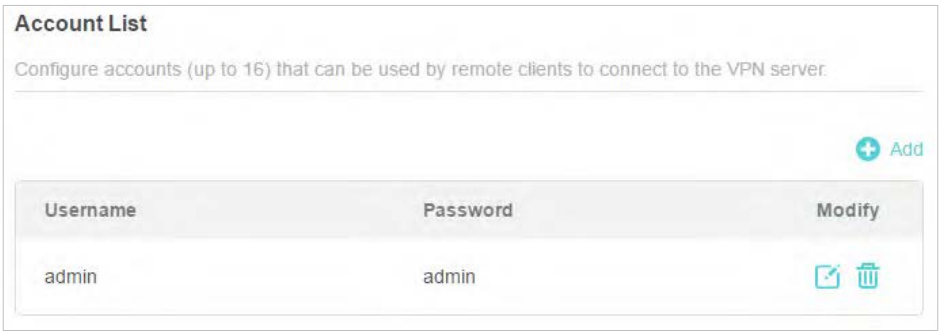
Step 1. Set up PPTP VPN Server on Your Router

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



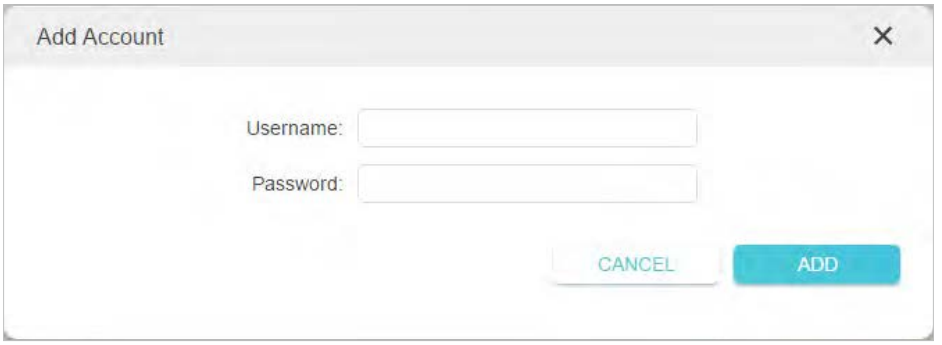
Note: Before you enable VPN Server, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router's WAN port and synchronize your System Time with internet.

3. In the Client IP Address field, enter the range of IP addresses (up to 10) that can be leased to the devices by the PPTP VPN server.
4. Set the PPTP connection permission according to your needs.
   - Select Allow Samba (Network Place) access to allow your VPN device to access your local Samba server.
   - Select Allow NetBIOS passthrough to allow your VPN device to access your Samba server using NetBIOS name.
   - Select Allow Unencrypted connections to allow unencrypted connections to your VPN server.
5. Click SAVE.
6. Configure the PPTP VPN connection account for the remote device. You can create up to 16 accounts.



1) Click Add.

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



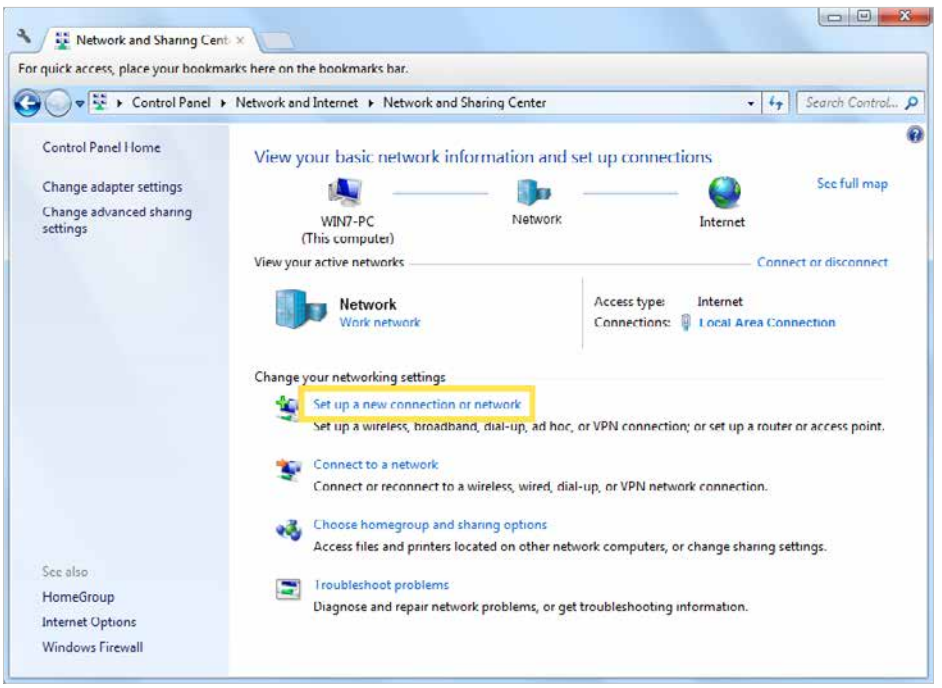
3) Click ADD.

Step 2. Configure PPTP VPN Connection on Your Remote Device

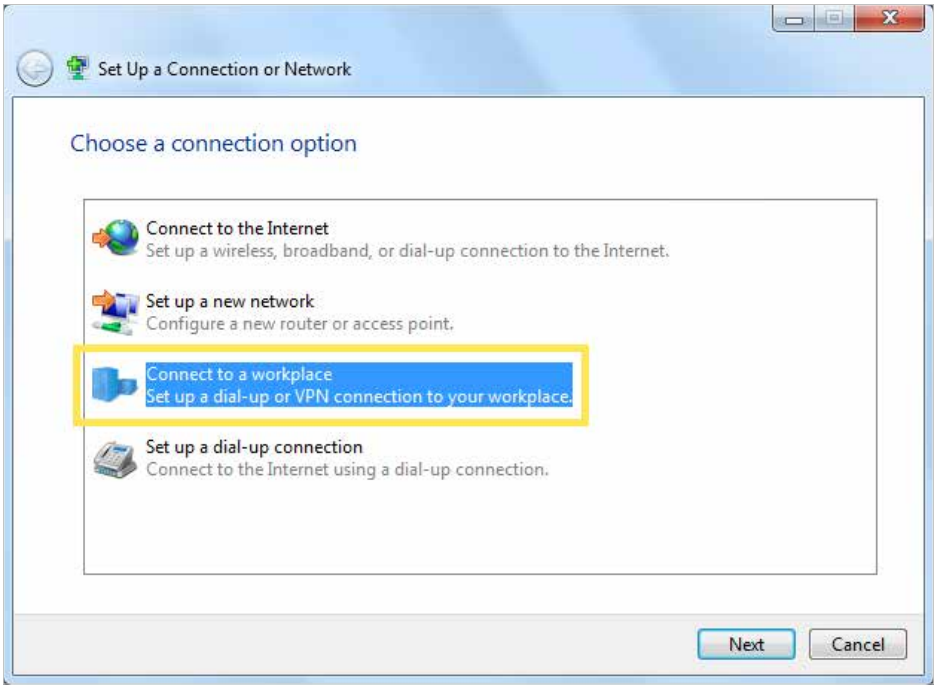
The remote device can use the Windows built-in PPTP software or a third-party PPTP software to connect to PPTP Server. Here we use the Windows built-in PPTP software as an example.

1. Go to Start > Control Panel > Network and Internet > Network and Sharing Center.

2. Select Set up a new connection or network.

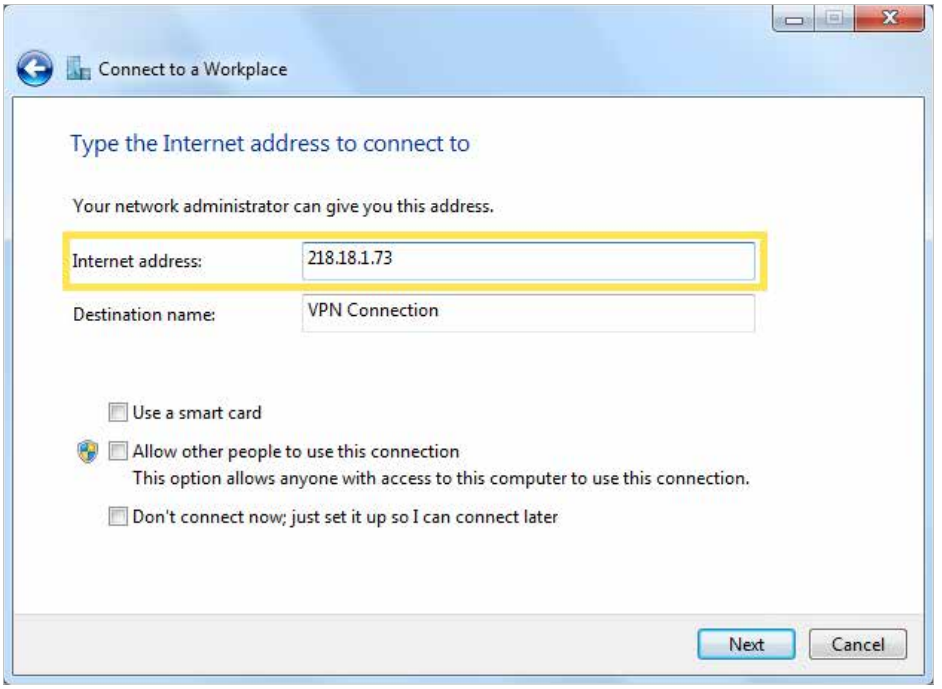


3. Select Connect to a workplace and click Next.

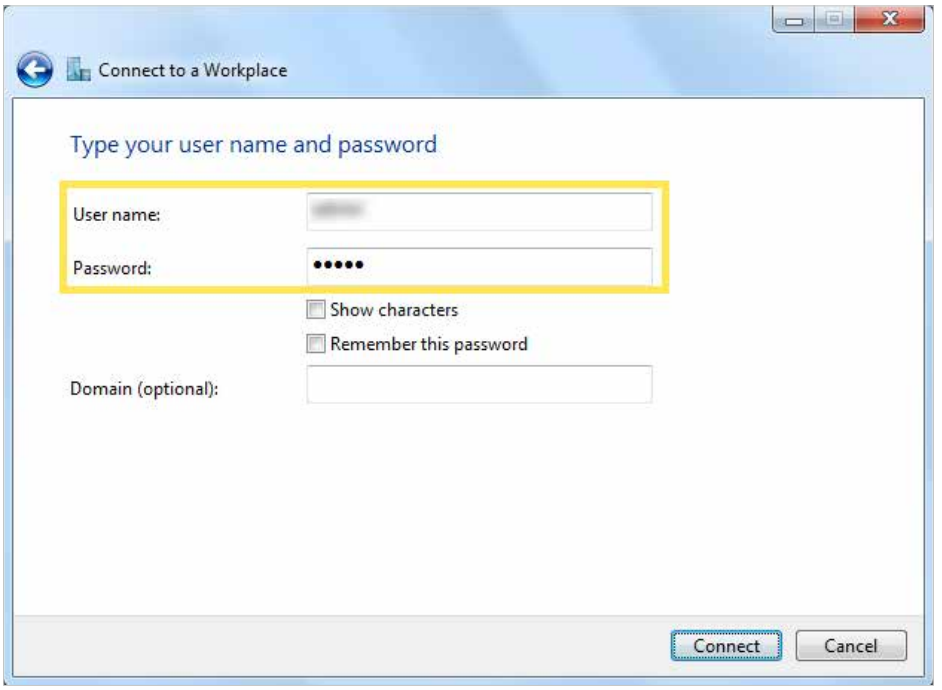


4. Select Use my Internet connection (VPN).

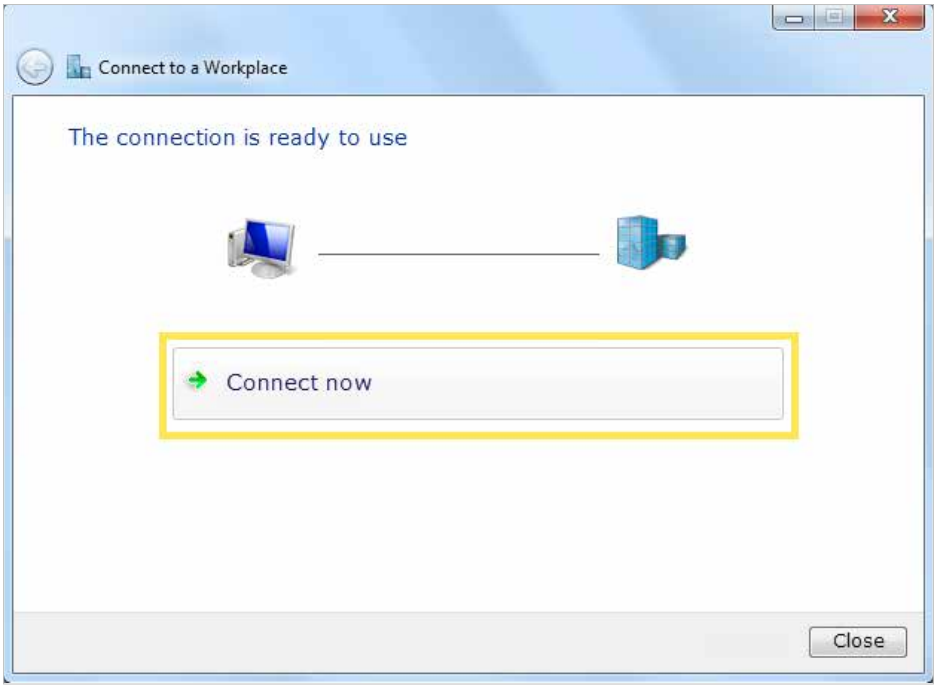
5. Enter the internet IP address of the router (for example: 218.18.1.73) in the Internet address field. Click Next.



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



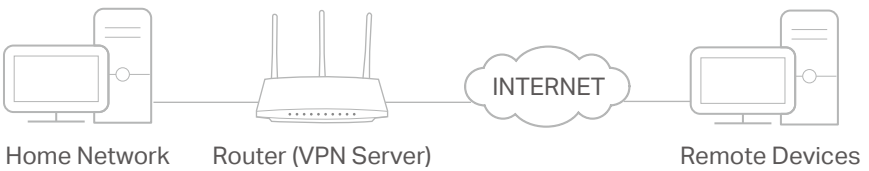
7. Click Connect Now when the VPN connection is ready to use.



16. 3. Use L2TP/IPSec VPN to Access Your Home Network

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

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

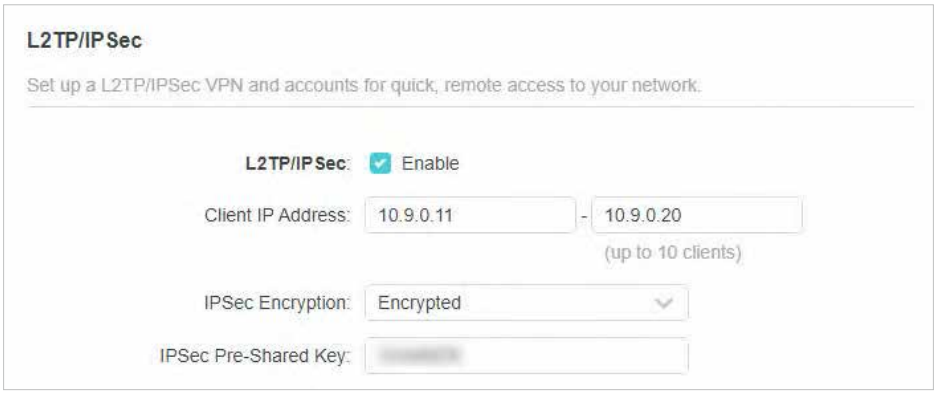


Step 1. Set up L2TP/IPSec VPN Server on Your Router

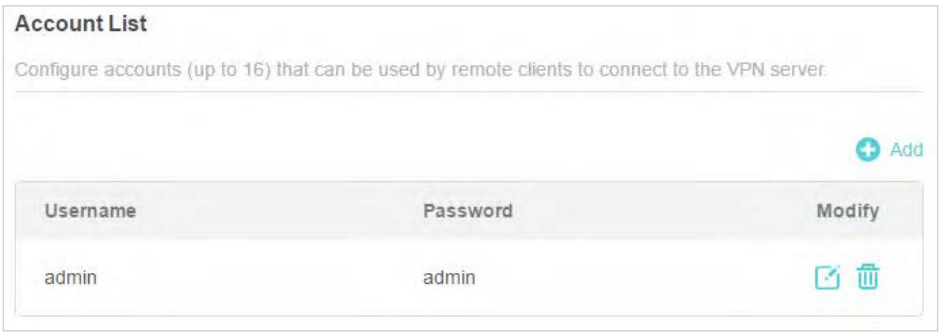
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > VPN Server > L2TP/IPSec, and enable L2TP/IPSec.

Note:

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

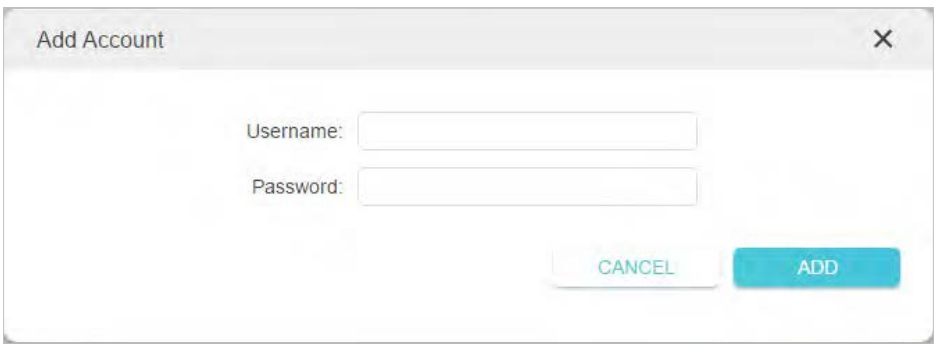


3. In the Client IP Address field, enter the range of IP addresses (up to 10) that can be leased to the devices by the L2TP/IPSec VPN server.
4. Keep IPSec Encryption as Encrypted and create an IPSec Pre-Shared Key.
5. Click SAVE.
6. Configure the L2TP/IPSec VPN connection account for the remote device. You can create up to 16 accounts.



4) Click Add.

5) Enter the Username and Password to authenticate devices to the L2TP/IPSec VPN Server.

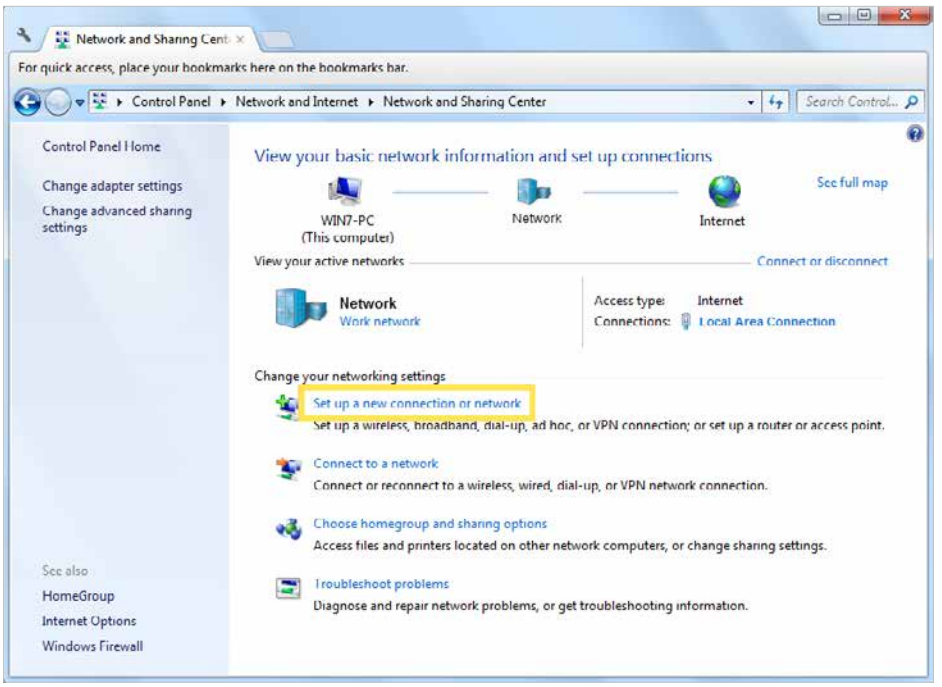


6) Click ADD.

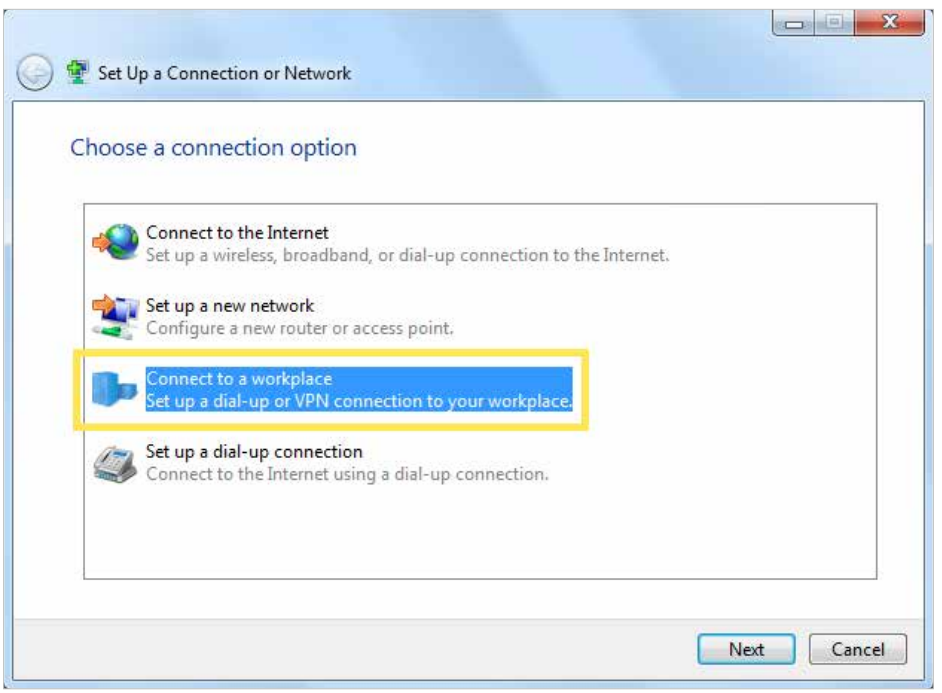
Step 2. Configure L2TP/IPSec VPN Connection on Your Remote Device

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.

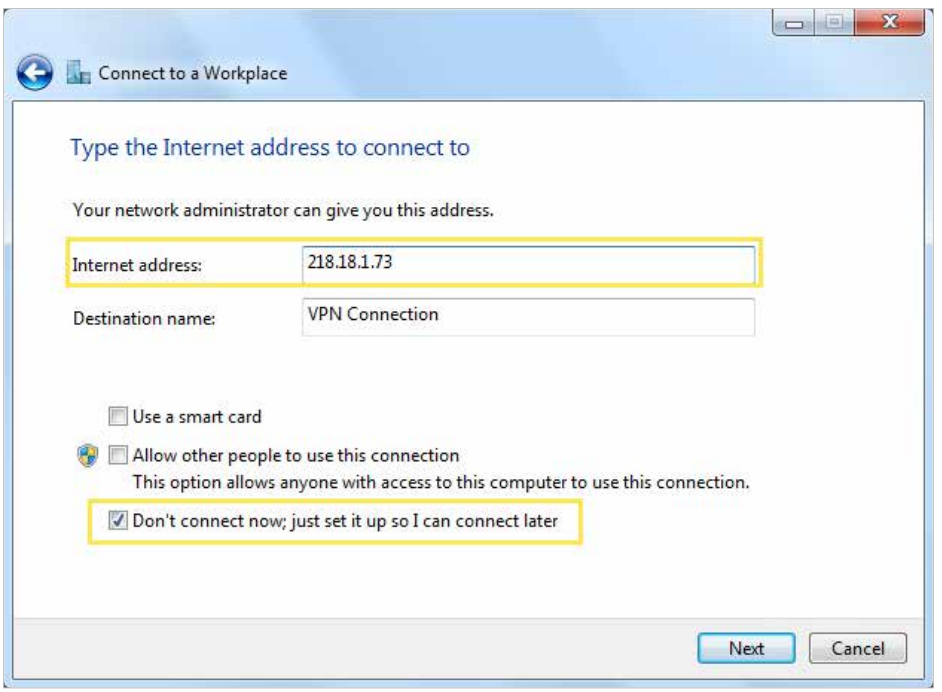


3. Select Connect to a workplace and click Next.

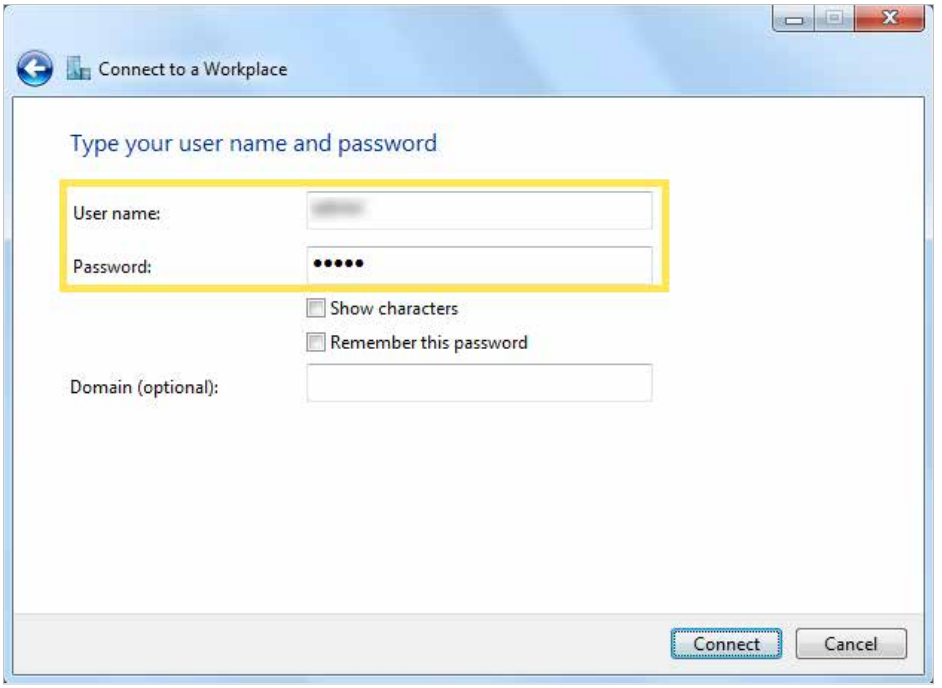


4. Select Use my Internet connection (VPN).

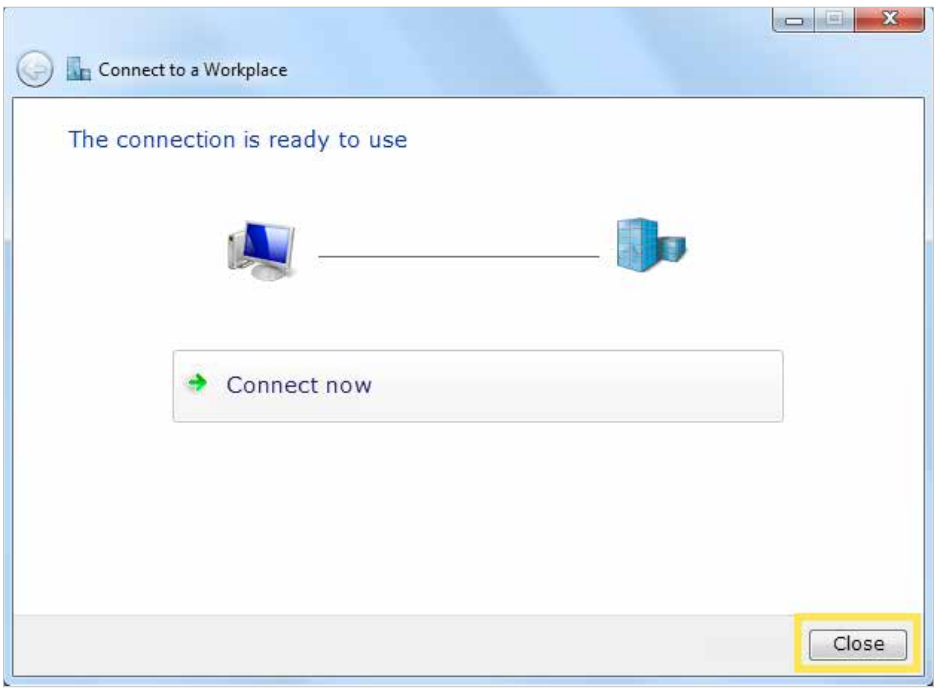
5. Enter the internet IP address of the router (for example: 218.18.1.73) in the Internet address field, and select the checkbox Don't connect now; just set it up so I can connect later. Click Next.



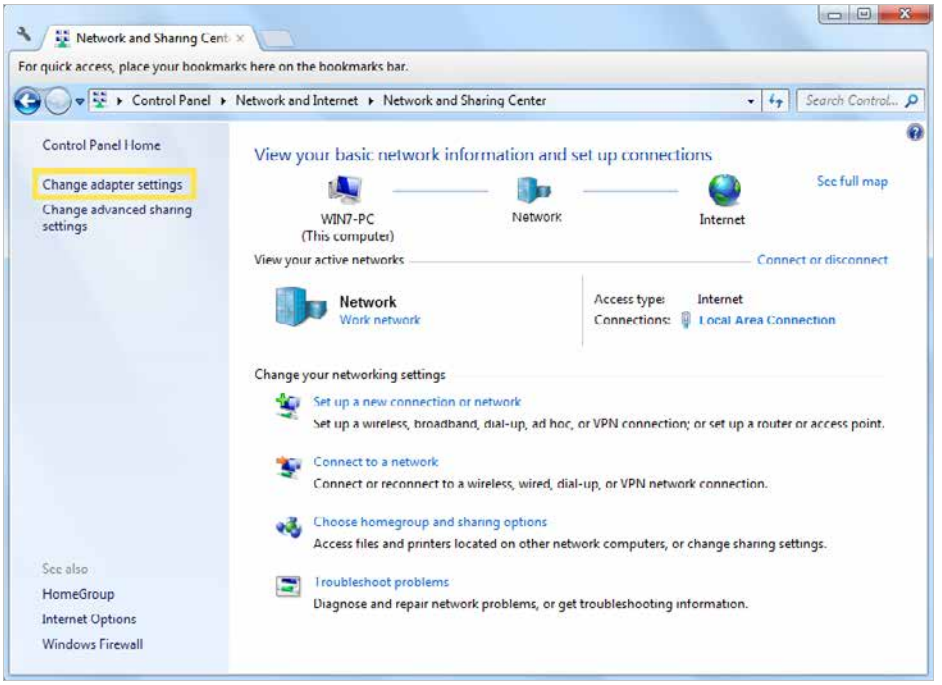
6. Enter the User name and Password you have set for the L2TP/IPSec VPN server on your router, and click Connect.



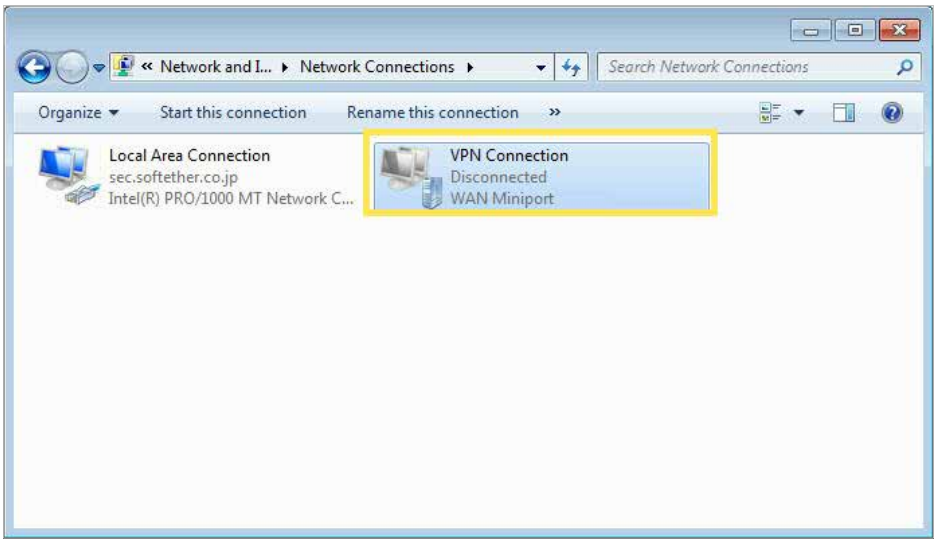
7. Click Close when the VPN connection is ready to use



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

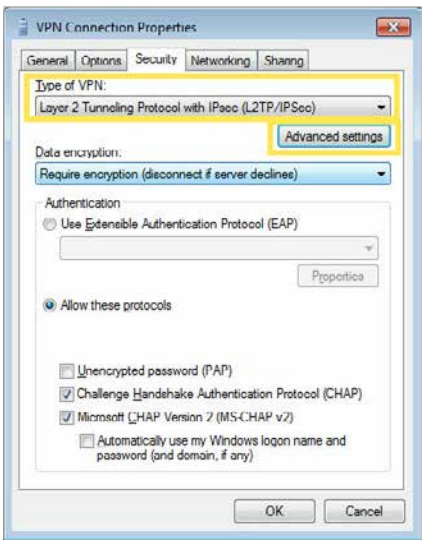


9. Find the VPN connection you created, then double-click it.

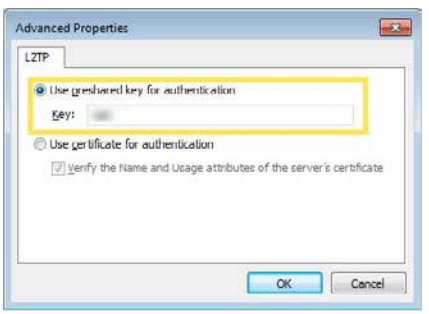


10. Enter the User name and Password you have set for the L2TP/IPSec VPN server on your router, and click Properties.

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.



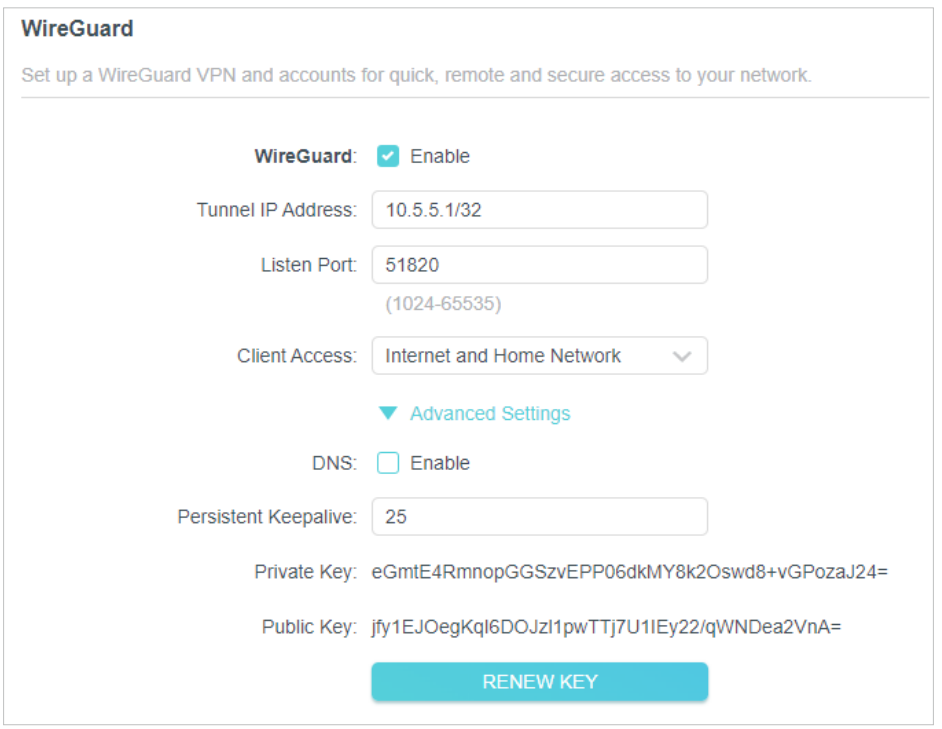
Done! Click Connect to start VPN connection.

16. 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

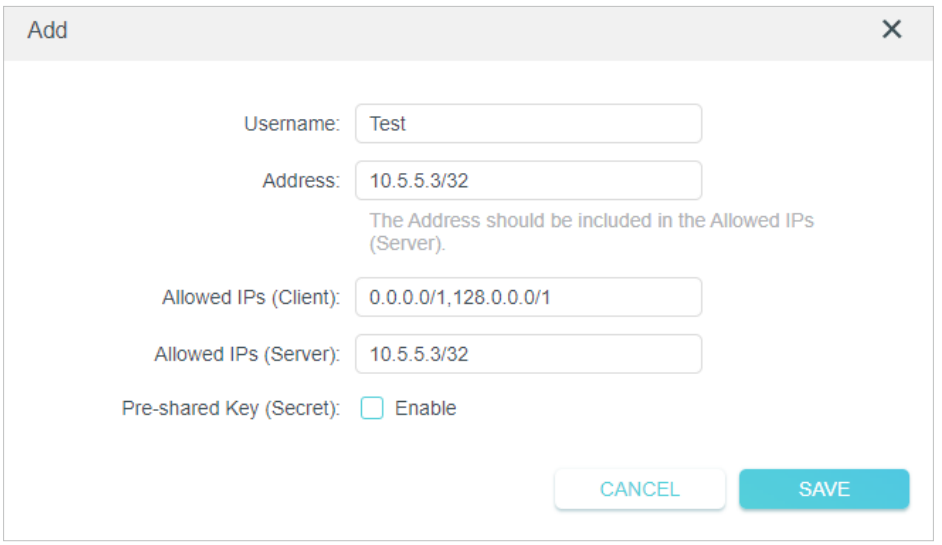
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > VPN Server > WireGuard, and tick the Enable box of WireGuard.



3. Set the tunnel IP address and listen port. Do NOT change it unless necessary.
4. Select your Client Access type. Select Home Network Only if you only want the remote device to access your home network; select Internet and Home Network if you also want the remote device to access internet through the VPN Server.
5. (Optional) Click Advanced Settings to display more settings. If DNS is turned on, the router will become the DNS server of the VPN client that establishes a connection with it. Change the Persistent Keepalive time (25 seconds by default) to send out heartbeat regularly, you can also click RENEW KEY to update the private key and public key.

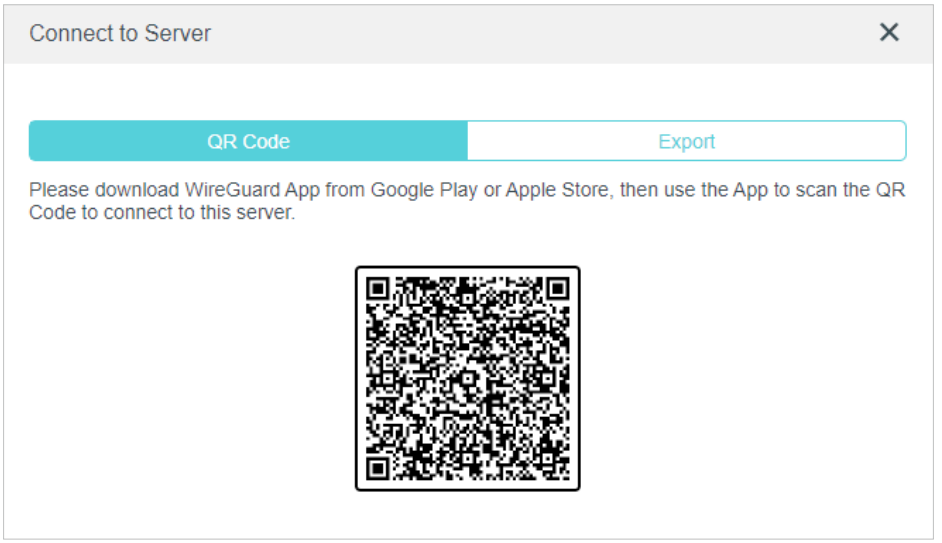
Step 2. Create accounts that can be used by remote clients to connect to the VPN server.

1. Locate the Account List section. Click Add to create an account.



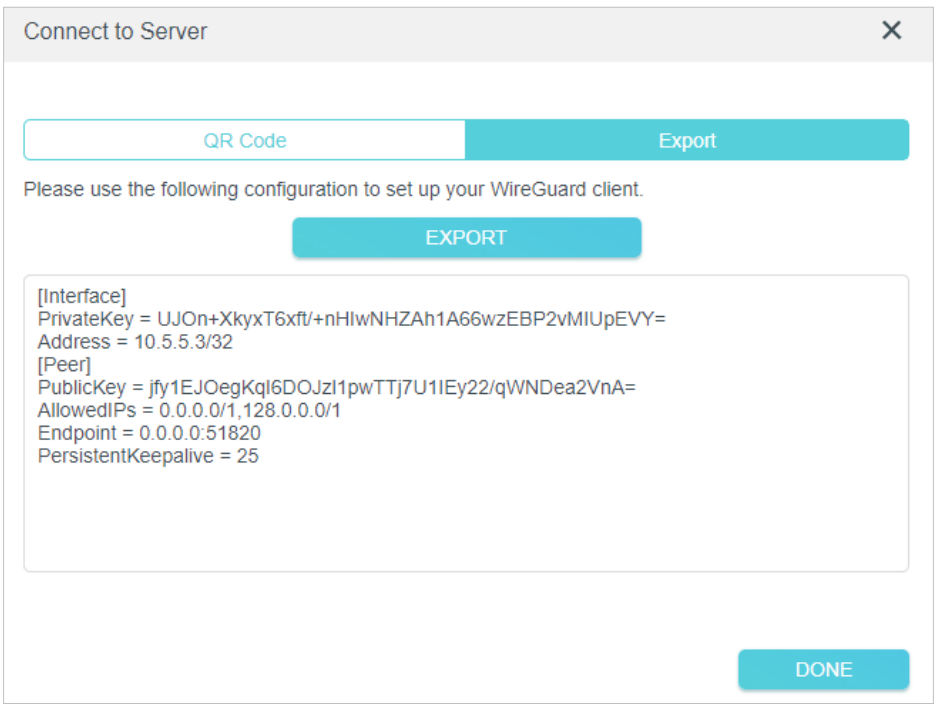
2. Give a name to this account.
3. Enter the address of the virtual interface assigned to this account. Do NOT change it unless necessary.
4. Traffic sent from the WireGard VPN client to the allowed IPs (client) will be transmitted through the tunnel. By default, all network traffic from clients will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

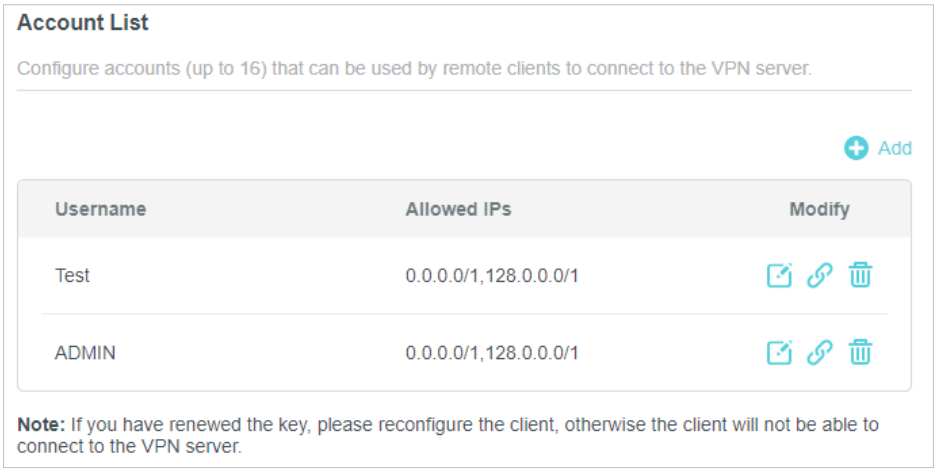


8. Connect to the WireGuard server.

- 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.



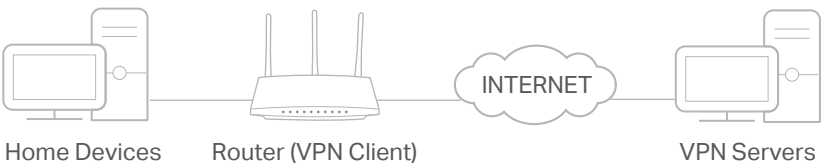
9. On the account list, you can click the button to modify the VPN server settings, connect to the server, or delete the account.



16. 5. Use VPN Client to Access a Remote VPN Server

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

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

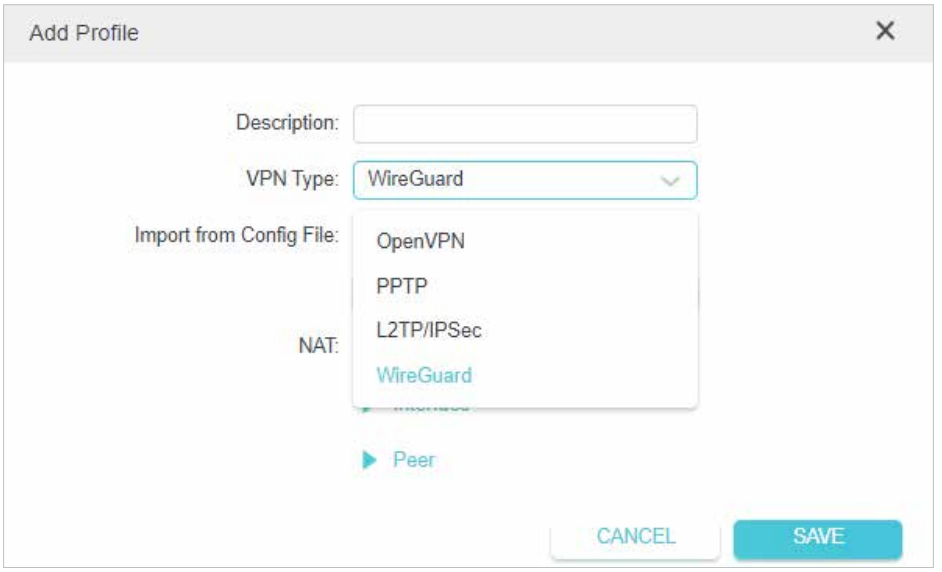


1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > VPN Client.

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

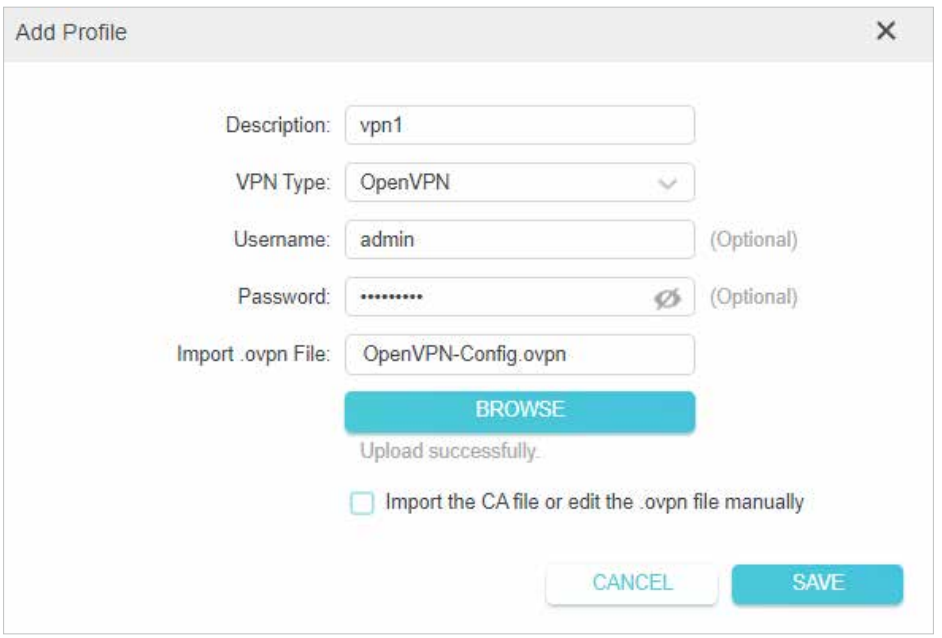
3. Enable VPN Client, then save the settings.

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

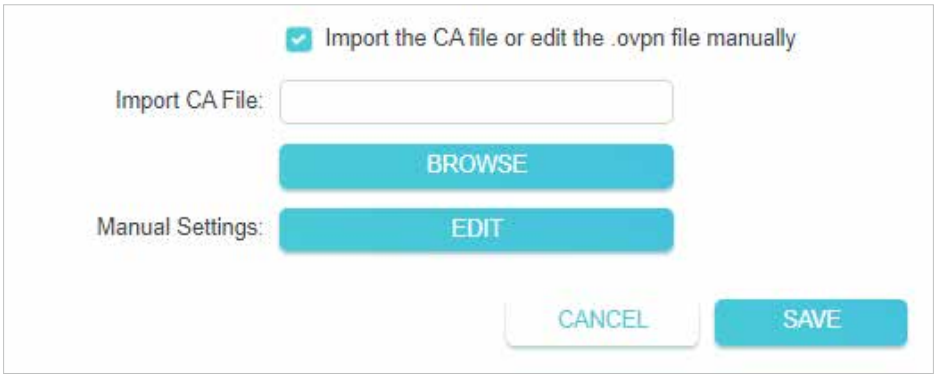


3) Enter the VPN information provided by your VPN provider.

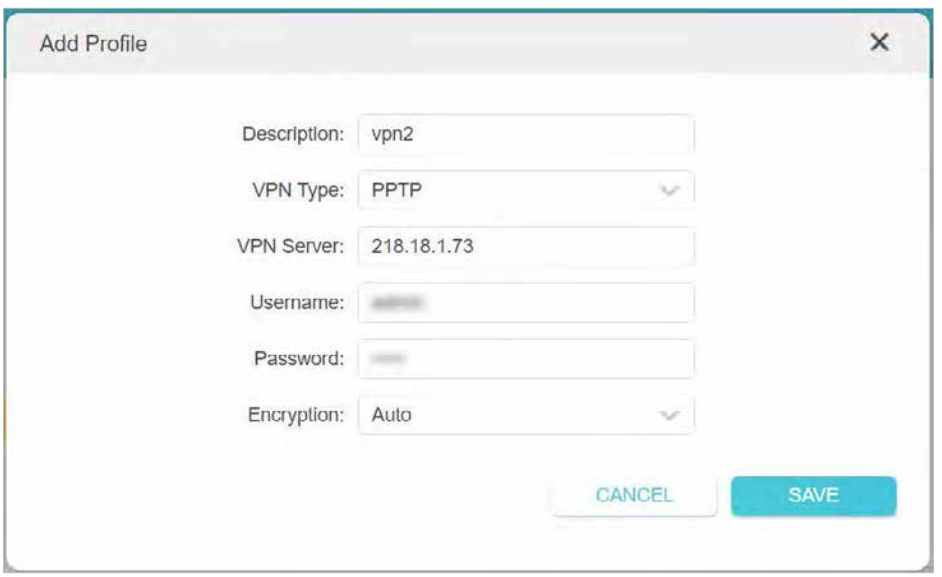
- OpenVPN: Enter the VPN username and password if required by your VPN provider, otherwise simply leave them empty. Then import the configuration file provided by your VPN provider.



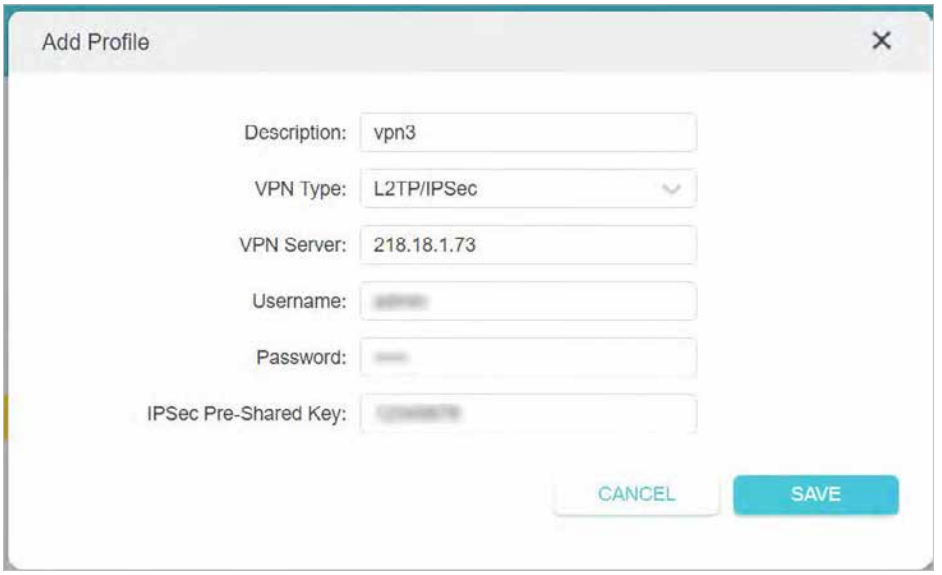
Note: You can also check the box of Import the CA file or edit the . ovpn file manually, then upload the CA file or manually configure the settings.



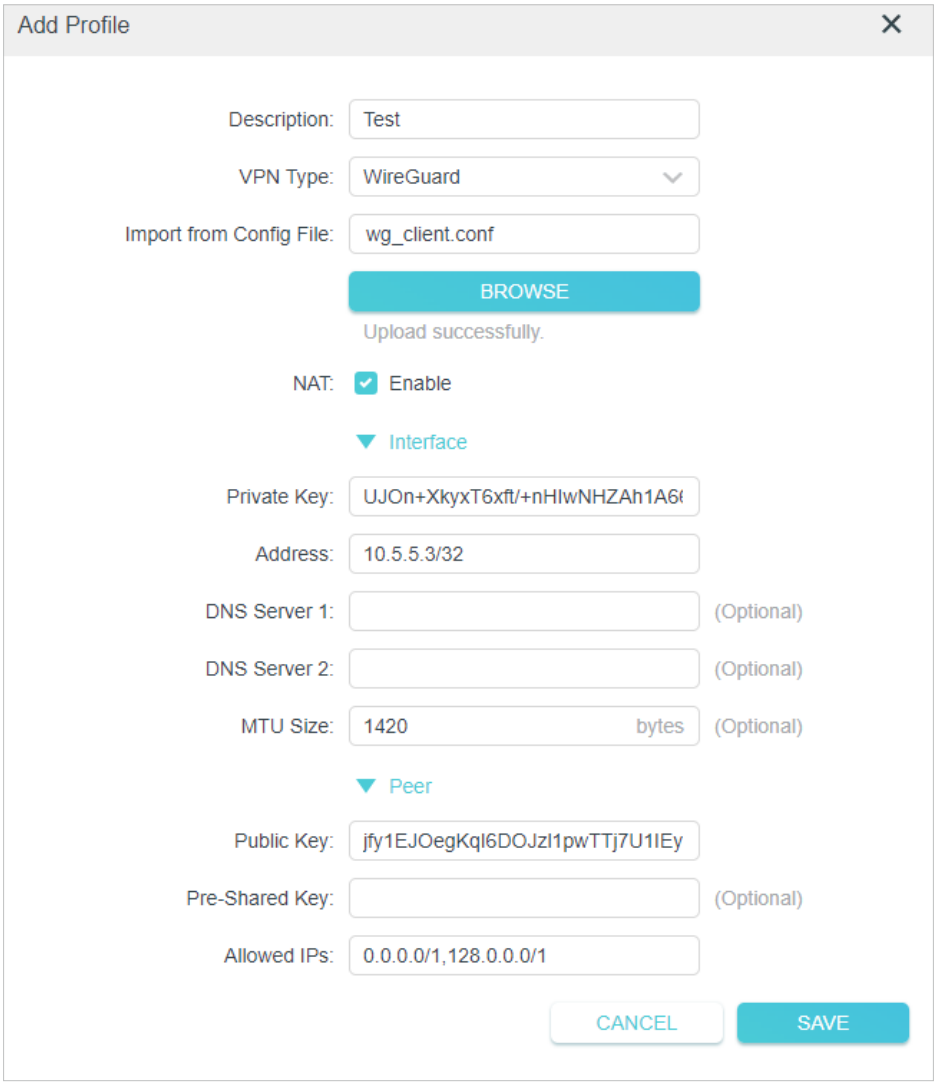
- PPTP: Enter the VPN server address (for example: 218.18.1.73) and the VPN username and password provided by your VPN provider.



- 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.

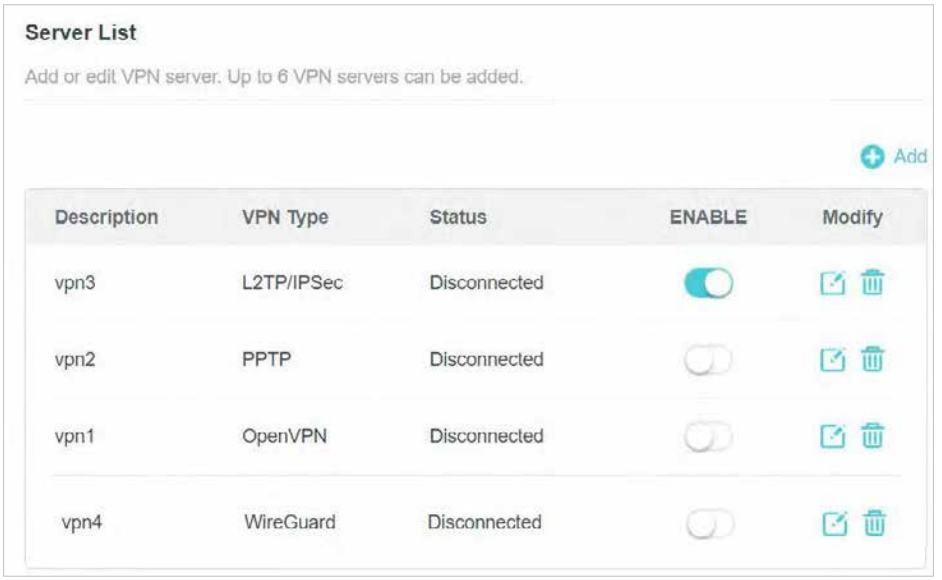


- WireGuard VPN: Give a description, and click BROWSE to import the WireGuard VPN server configuration. Then you will see the detailed parameters. Do NOT change the parameters unless necessary.



4) Save the settings.

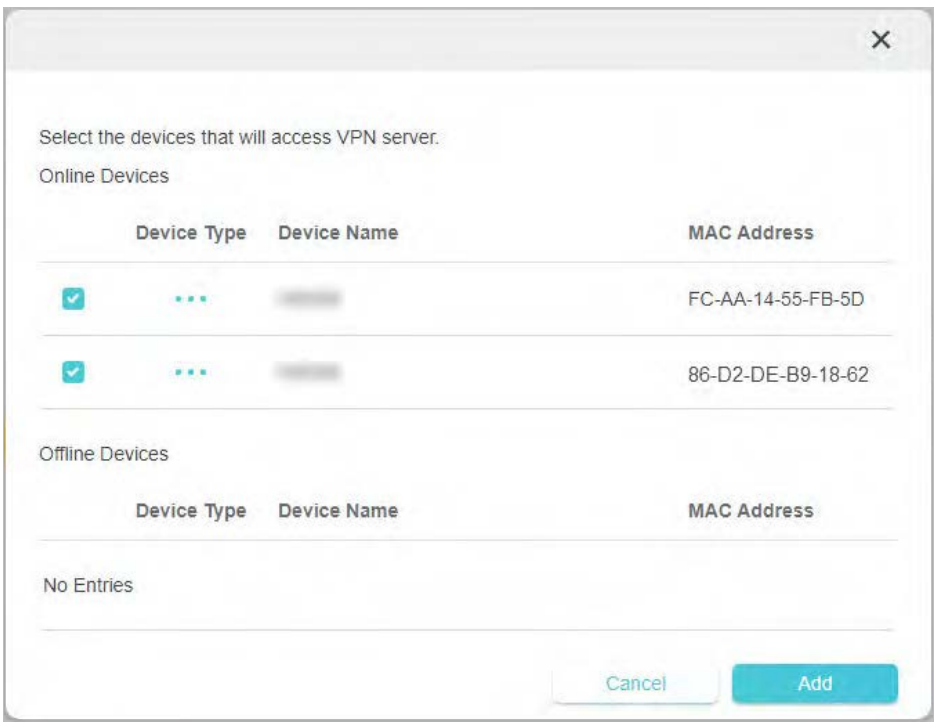
5) In the server list, enable the one you need.



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.



6. Save the settings.

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

Chapter 17

Customize Your Network Settings

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

It contains the following sections:

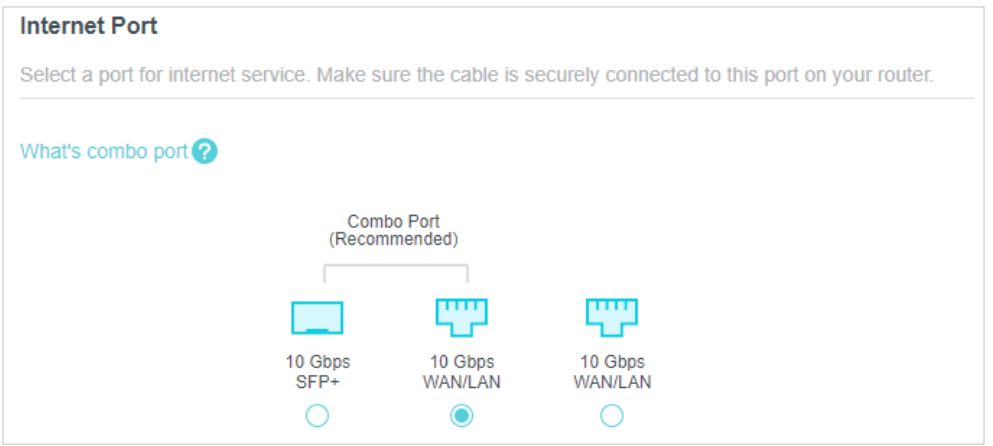
- Change the Internet Settings
- Change the LAN Settings
- Configure to Support IPTV Service
- Specify DHCP Server Settings
- Set Up a Dynamic DNS Service Account
- Create Static Routes

17. 1. Change the Internet Settings

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

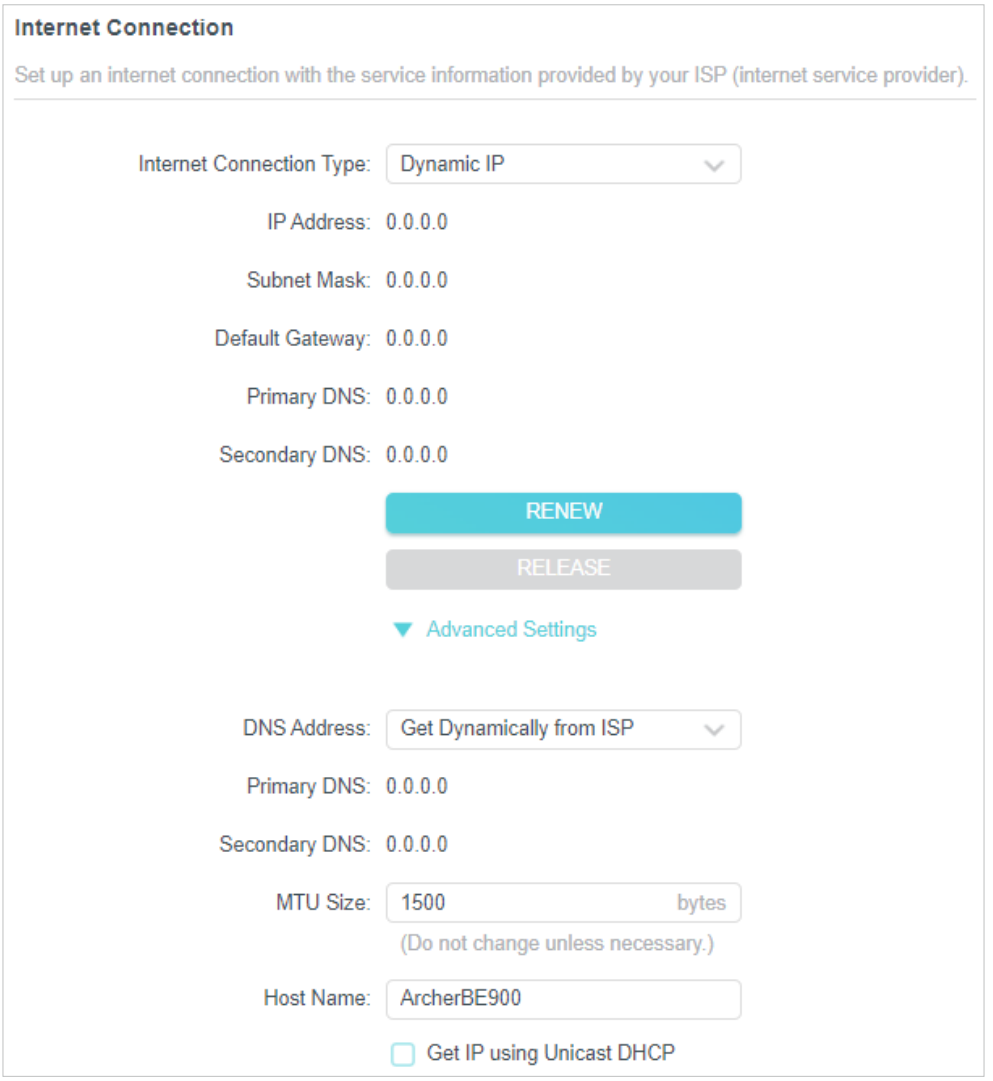
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > Network > Internet.

- **To change the internet port:**



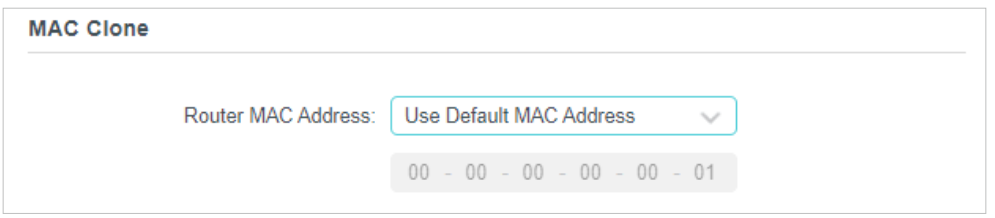
1. Select the desired internet port. Make sure the cable is securely connected to this port on your router.
2. Click SAVE.

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



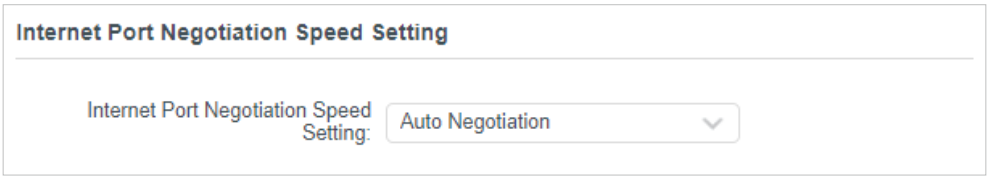
1. Select the internet connection type and configure the settings according to the information provided by your ISP.
2. Optional. Reveal the advanced settings and change the settings if needed. It's recommended to keep the default settings.
3. Click SAVE.

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



You have three options, Use Default MAC Address, Clone Current Device MAC, Use Custom MAC Address.

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



You can change the internet port speed mode. Auto Negotiation is recommended.

17. 2. Change the LAN Settings

The router is preset with a default LAN IP 192.168.0.1, which you can use to log in to its web management page. The LAN IP address together with the Subnet Mask also defines the subnet that the connected devices are on. If the IP address conflicts with another device on your local network or your network requires a specific IP subnet, you can change it.

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

4. Click SAVE.

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

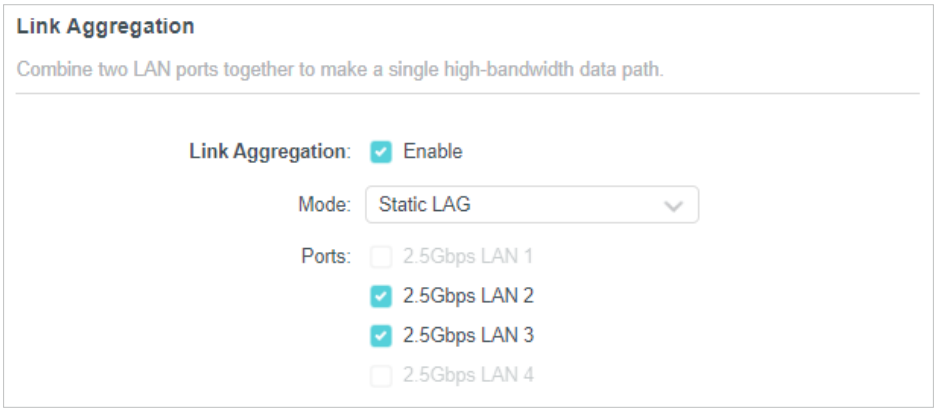
17. 3. Link Aggregation

The Link Aggregation feature combines two LAN ports together to make a single high-bandwidth 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.

3. Enable Link Aggregation.

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



4. Select the Static LAG or LACP mode. It's recommended that you select the same link aggregation mode for both ends of the link.
5. Click SAVE. The LAN2 and LAN3 ports will be used for Link Aggregation.

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.

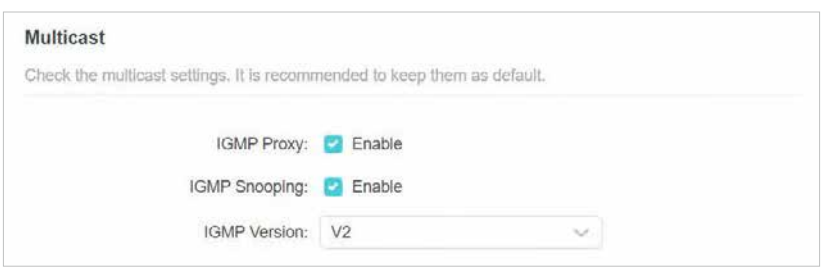
17. 4. Configure to Support IPTV Service

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.



2) Click SAVE.

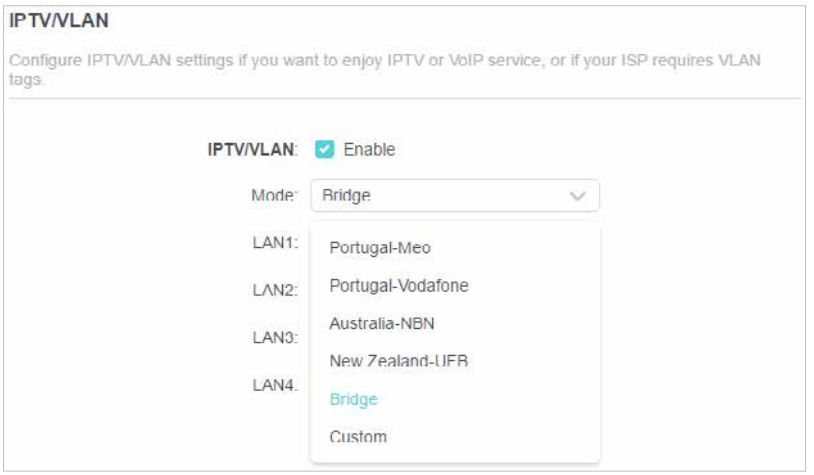
3) After configuring IGMP proxy, IPTV can work behind your router now. You can connect your set-top box to any of the router's Ethernet port.

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.



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.

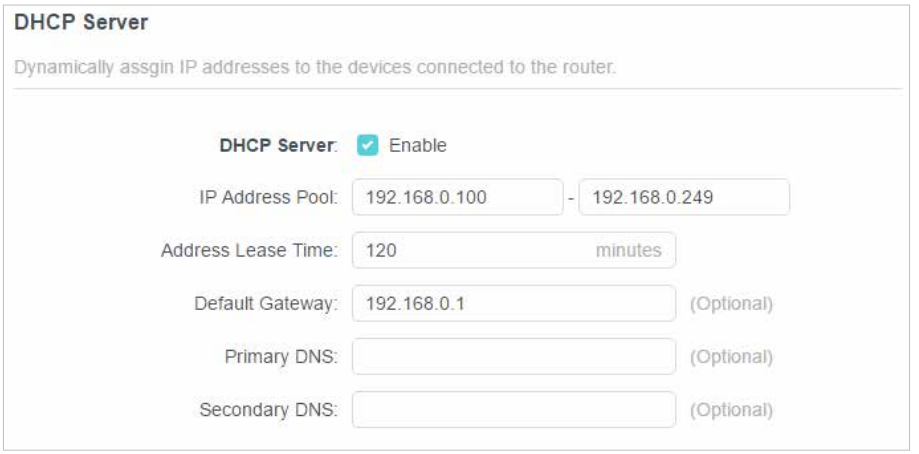
17. 5. Specify DHCP Server Settings

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.

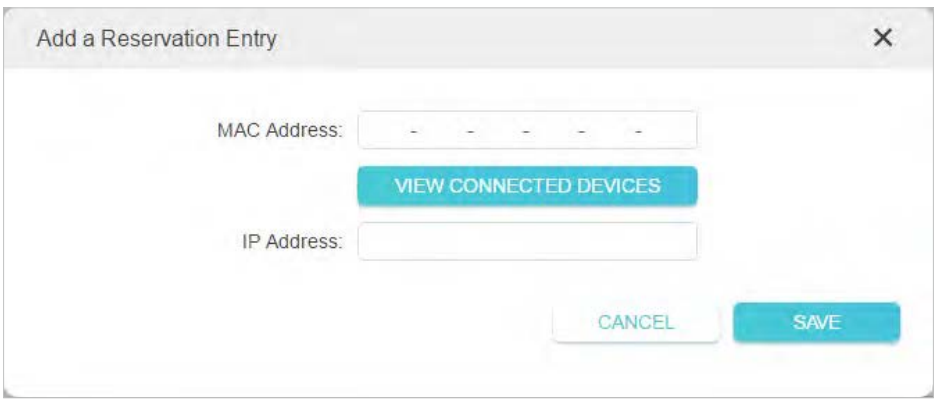
- **To specify the IP address that the router assigns:**



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

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

1. Click Add in the Address Reservation section.



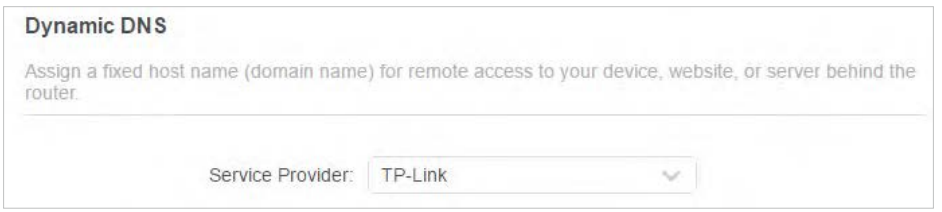
2. Click VIEW CONNECTED DEVICES and select the you device you want to reserve an IP for. Then the MAC Address will be automatically filled in. Or enter the MAC address of the client device manually.
3. Enter the IP address to reserve for the client device.
4. Click SAVE.

17. 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.

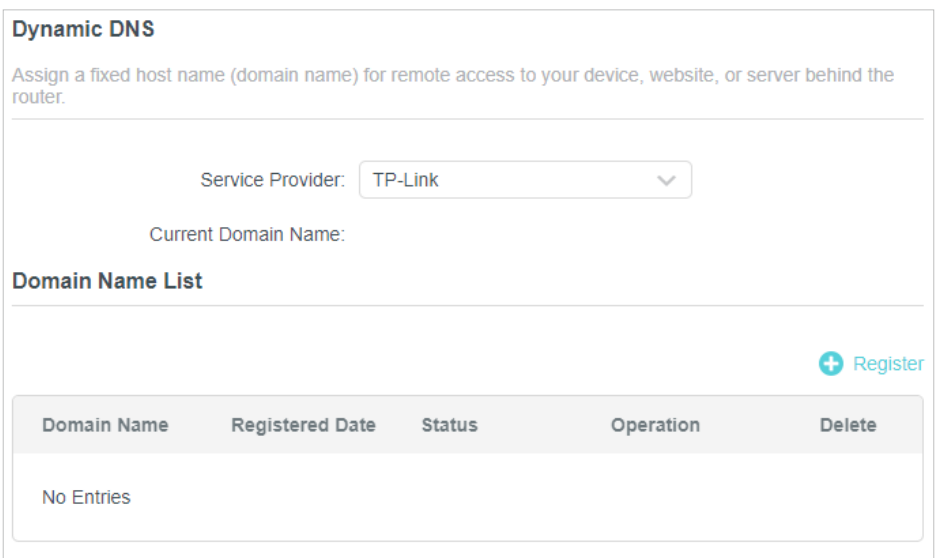
Note: DDNS does not work if the ISP assigns a private WAN IP address (such as 192.168.1.x) to the router.

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.

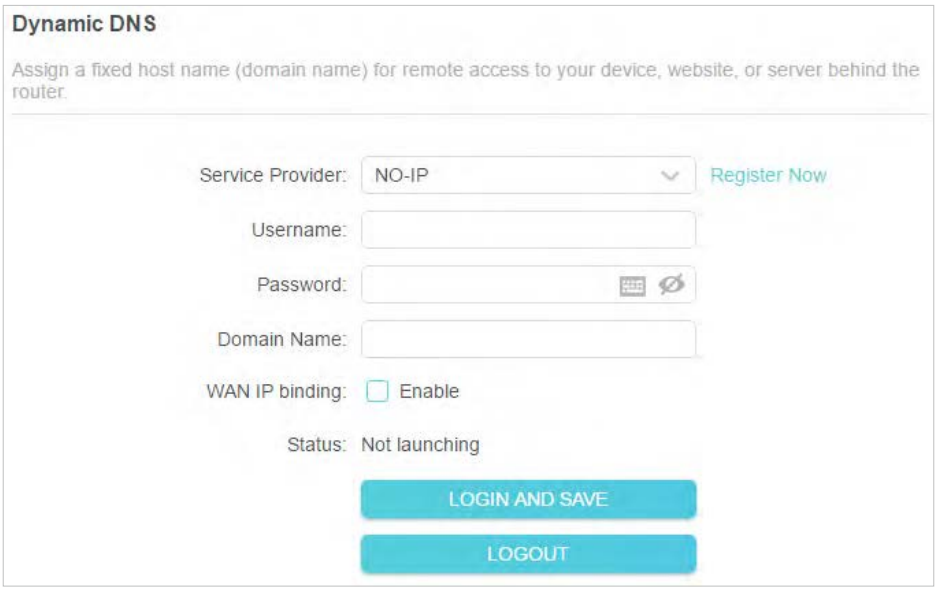


Note: To enjoy TP-Link's DDNS service, you have to log in with a TP-Link ID. If you have not logged in with one, click log in.

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



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



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.

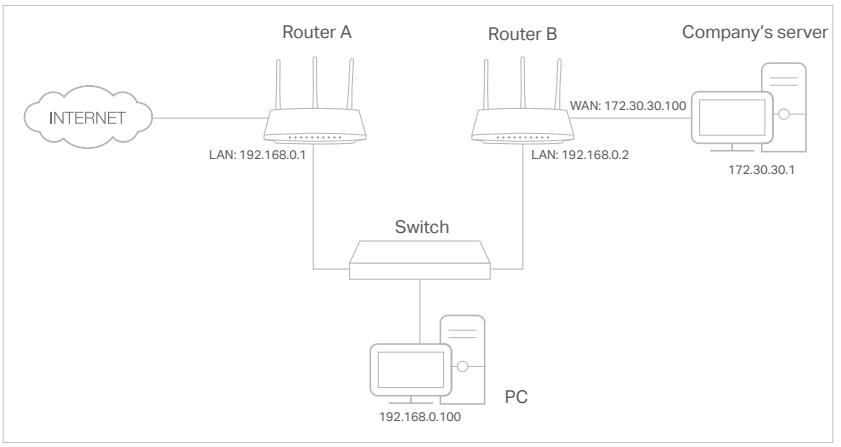
17. 7. Create Static Routes

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:

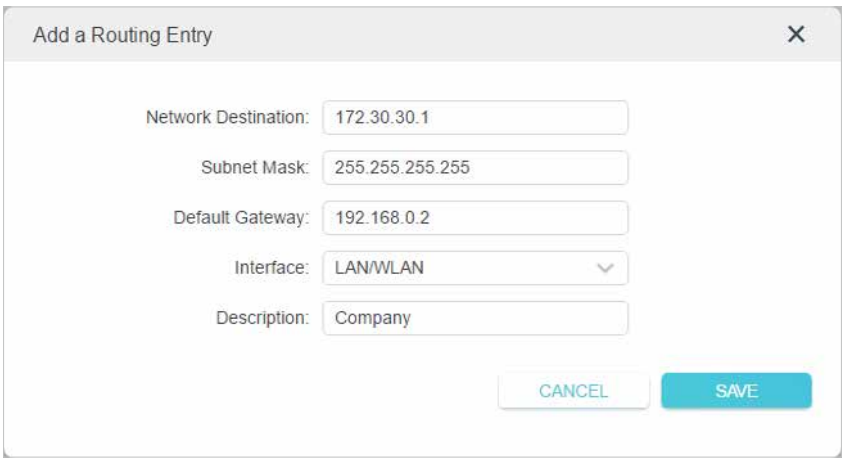
Visit multiple networks and servers at the same time.

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.
3. Go to Advanced > Network > Routing.
4. Click Add and finish the settings according to the following explanations:



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.

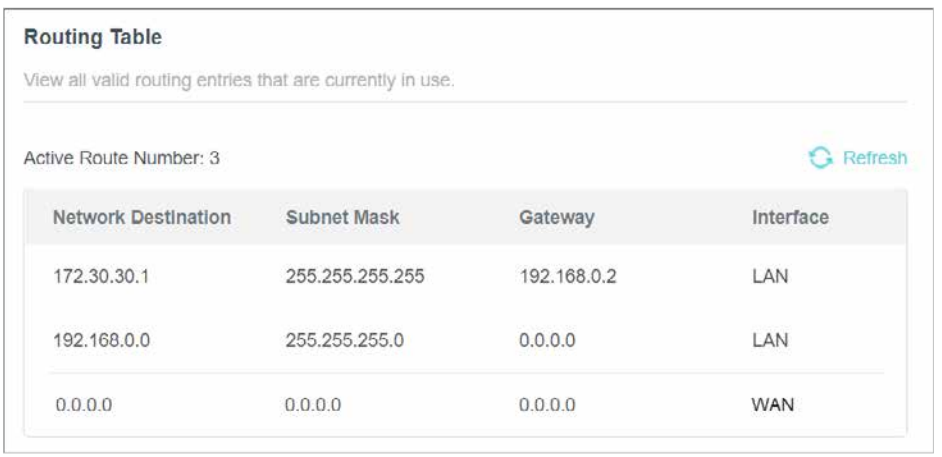
Default Gateway: The IP address of the gateway device to which the data packets

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.

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



Network Destination	Subnet Mask	Gateway	Interface
172.30.30.1	255.255.255.255	192.168.0.2	LAN
192.168.0.0	255.255.255.0	0.0.0.0	LAN
0.0.0.0	0.0.0.0	0.0.0.0	WAN

Done!

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

Chapter 18

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

18. 1. Update the Firmware

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

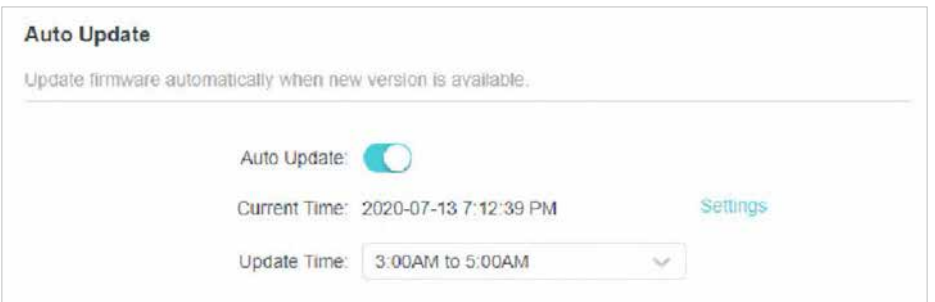
We will inform you through the web management page if there's any new firmware available for your router. Also, the latest firmware will be released at the TP-Link official website www.tp-link.com, and you can download it from the Support page for free.

Note:

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

18. 1. 1. Auto Update

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 > Firmware Update.
3. Enable Auto Update.



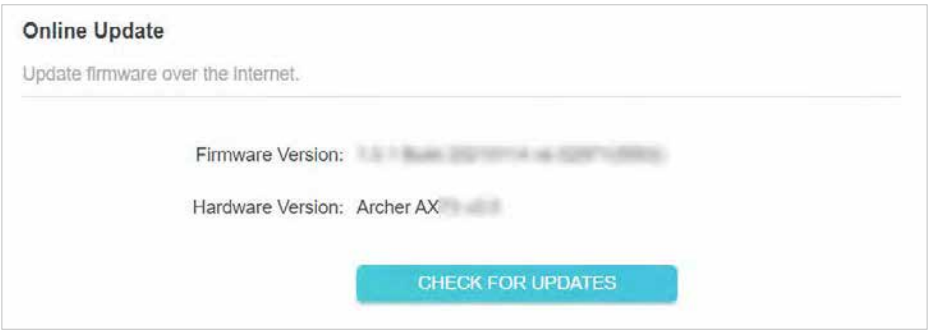
4. Specify the Update Time and save the settings.

The router will update firmware automatically at the specified time when new version is available.

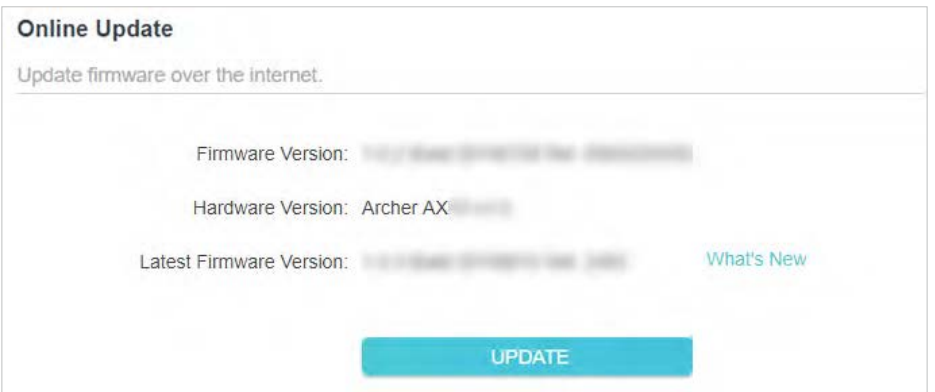
18. 1. 2. Online Update

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.

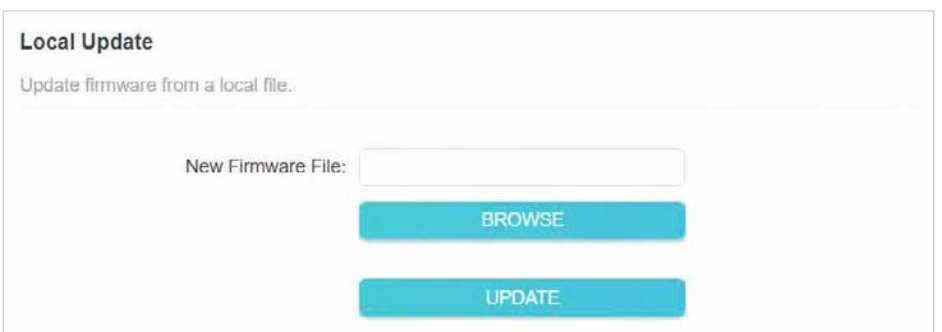


4. Wait a few minutes for the update and reboot to complete.

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.

18. 1. 3. 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.

18. 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.

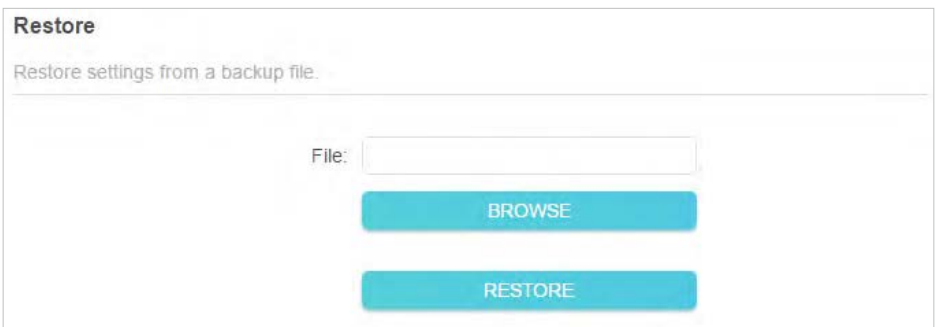
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > System Tools > Backup & Restore.

- **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.

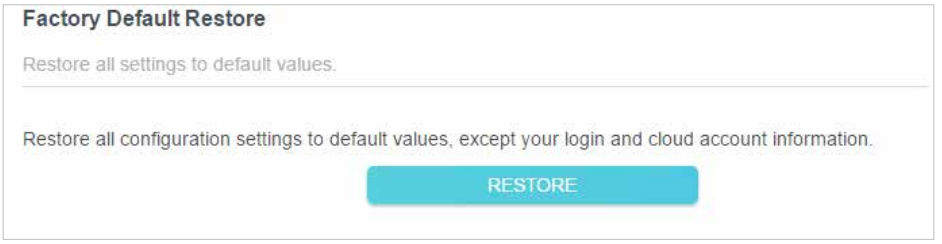


2. Wait a few minutes for the restoring and rebooting.

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.

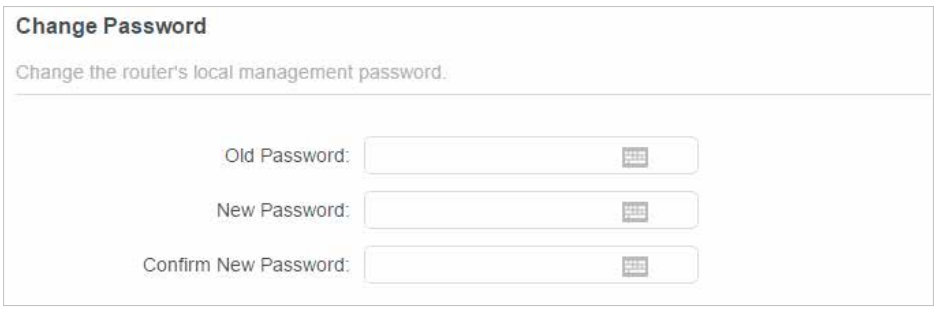
Note:
- During the resetting process, do not turn off or reset the router.
- We strongly recommend you backup the current configuration settings before resetting the router.

18. 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.



3. Enter the old password, then a new password twice (both case-sensitive). Click SAVE.

4. Use the new password for future logins.

18. 4. Password Recovery

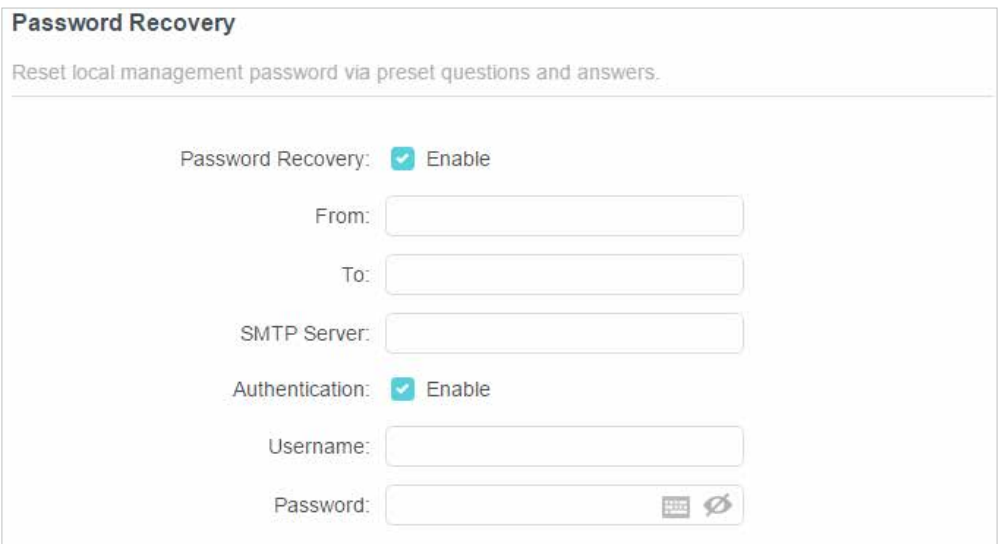
This feature allows you to recover the login password you set for you router in case you forget it.

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.
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.

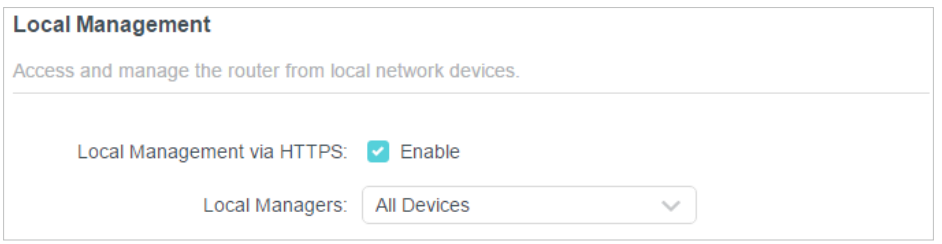
18. 5. Local Management

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.

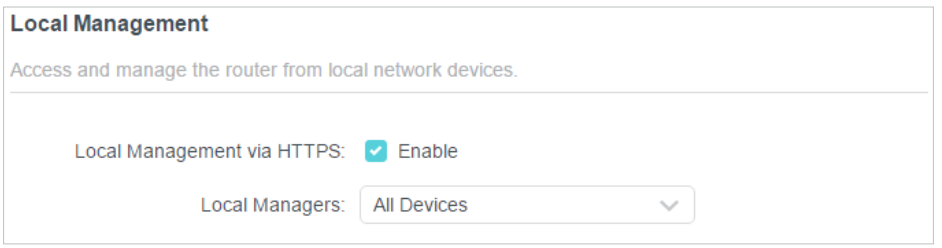
- **Access the router via HTTPS and HTTP:**

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.



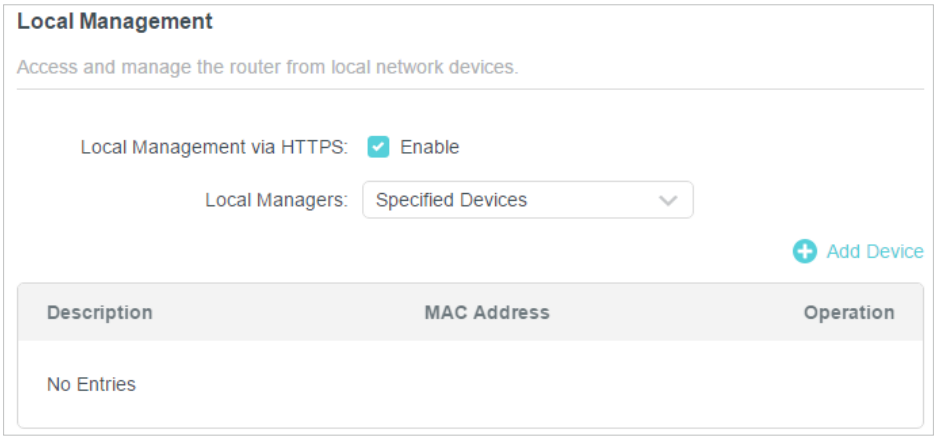
- **Allow all LAN connected devices to manage the router:**

Select All Devices for Local Managers.

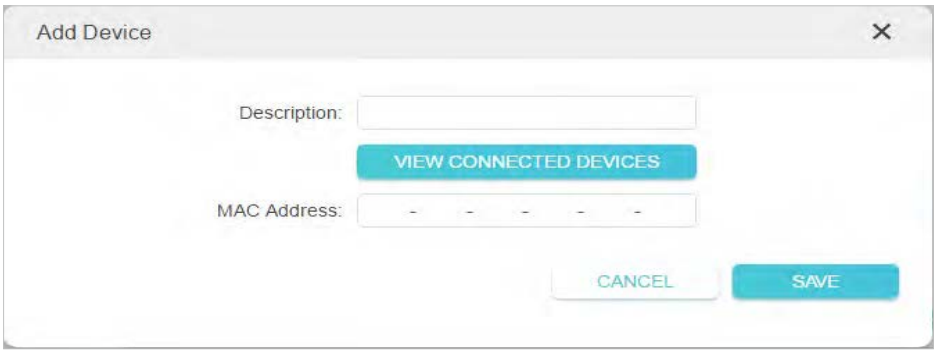


- **Allow specific devices to manage the router:**

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



2. Click Add Device.



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.

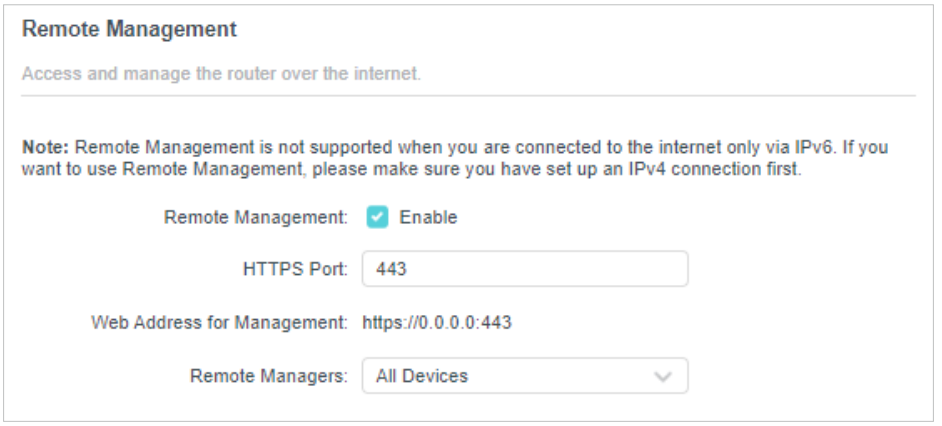
18. 6. Remote Management

This feature allows you to control remote devices' authority to manage the router.

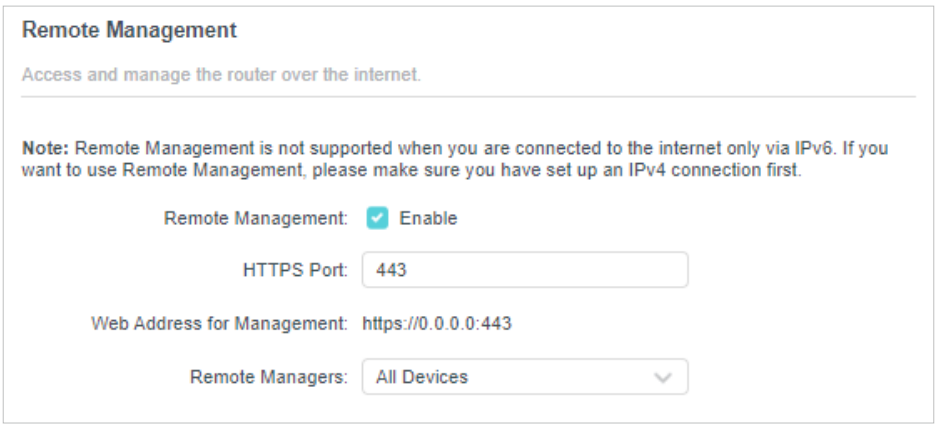
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > System > Administration and complete the settings in Remote Management section as needed.

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

Do not tick the Enable checkbox of Remote Management.



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



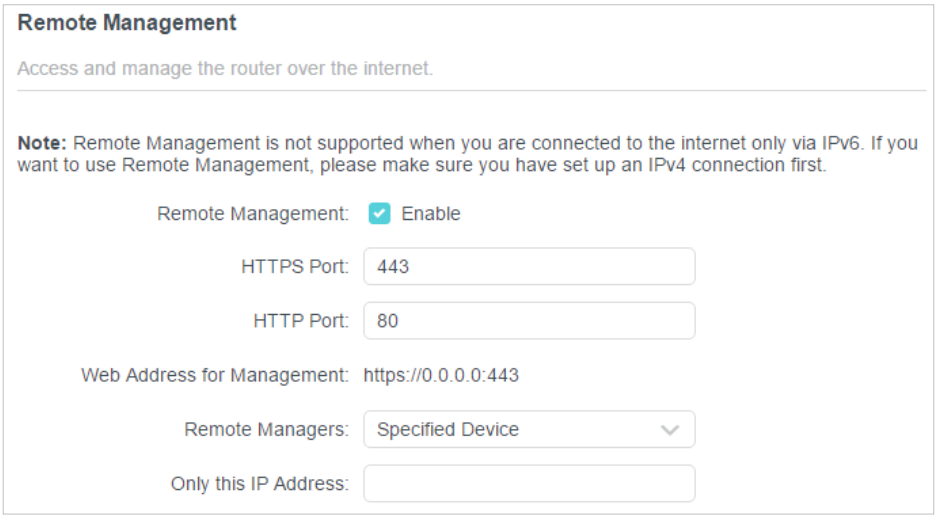
1. Tick the Enable checkbox of Remote Management.
2. Keep the HTTPS port as default settings (recommended) or enter a value between 1024 and 65535.
3. Select All Devices for Specified Devices.
4. Click SAVE.

Devices on the internet can log in to https://Router's WAN IP address:port number (such as https://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:**



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).

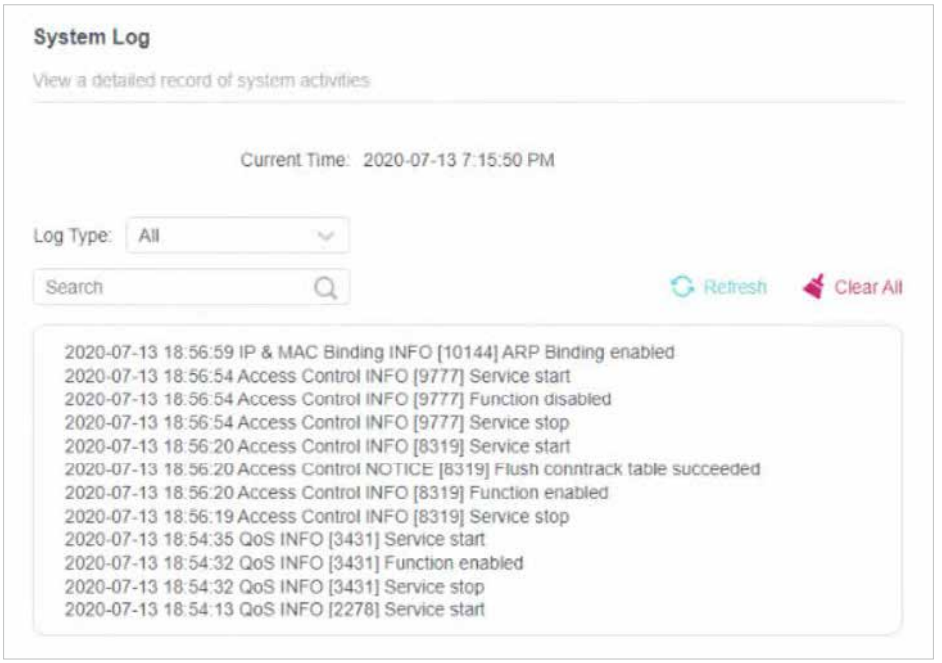
Tips: The router's WAN IP is usually a dynamic IP. Please refer to Set Up a Dynamic DNS Service Account if you want to log in to the router through a domain name.

18. 7. System Log

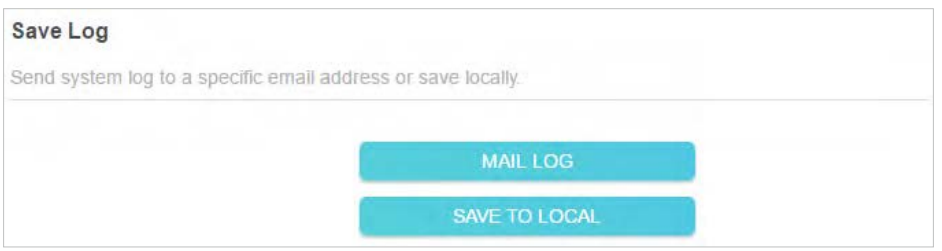
When the router does not work normally, you can save the system log and send it to the technical support for troubleshooting.

- **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.



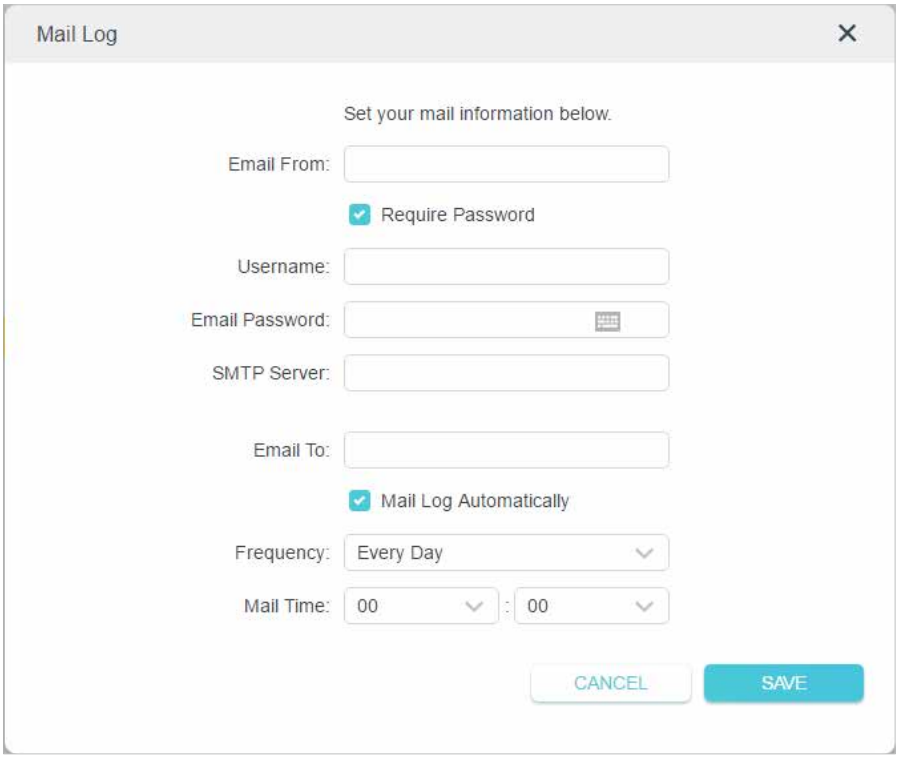
4. In the Save Log section, click SAVE TO LOCAL to save the system logs to a local disk.



- **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:



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.

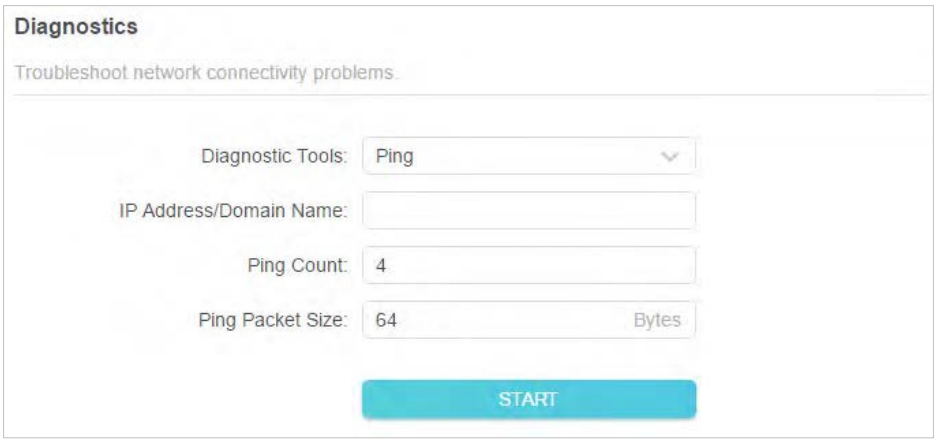
8) Frequency: This determines how often the recipient will receive the system log .

5. Click SAVE.

18. 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.



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.

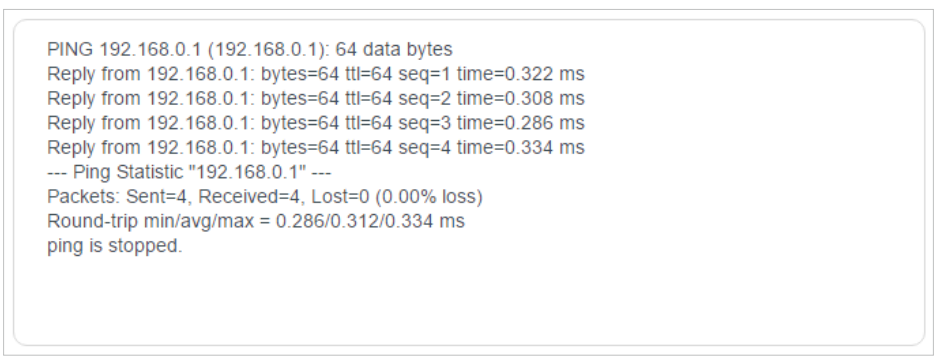
2) Enter the IP Address or Domain Name of the tested host.

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.



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

18. 9. Set System Time and Language

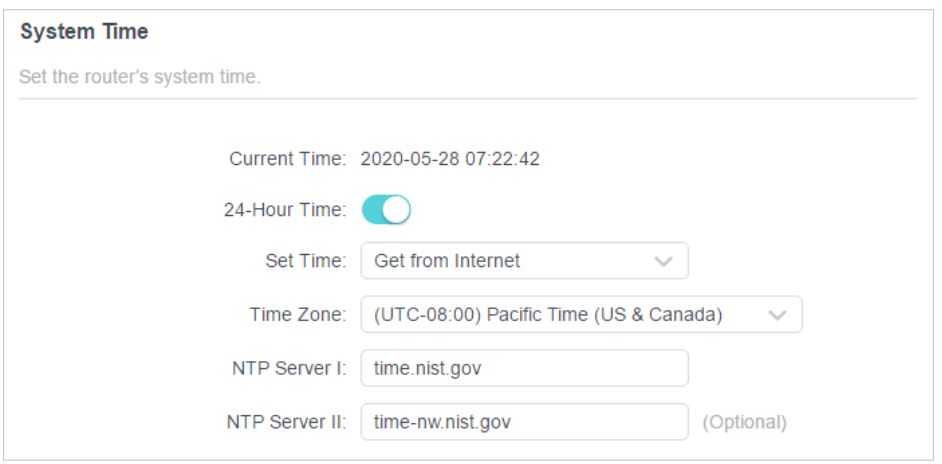
System time is the time displayed while the router is running. The system time you configure here will be used for other time-based functions like Parental Controls. You can choose the way to obtain the system time as needed.

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.

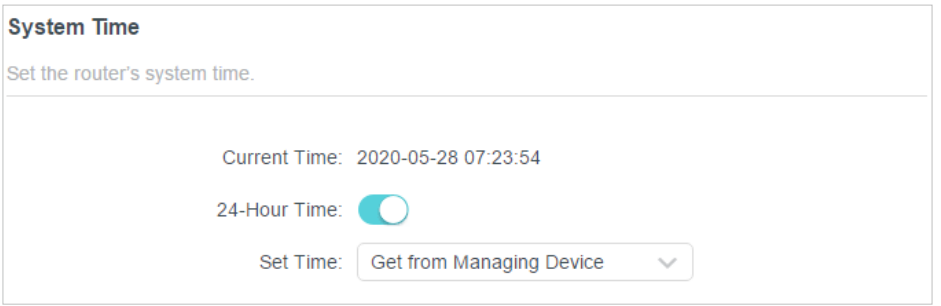


3. Select your local Time Zone from the drop-down list.

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:**

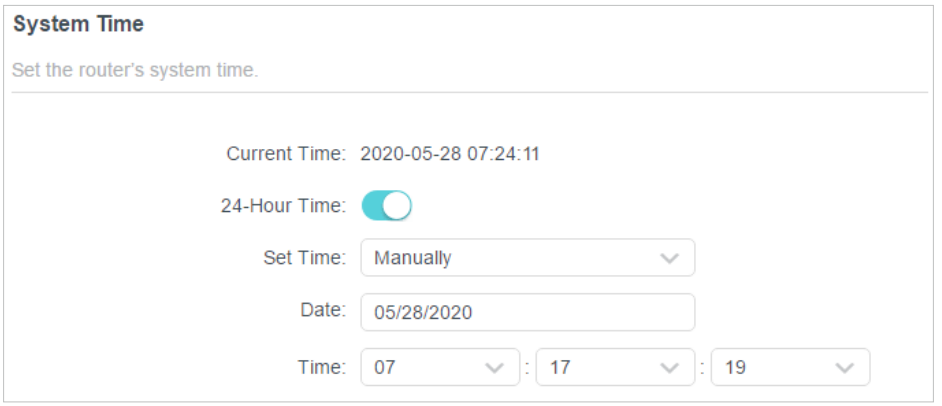
1. In the Set Time field, select Get from Managing Device.



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

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

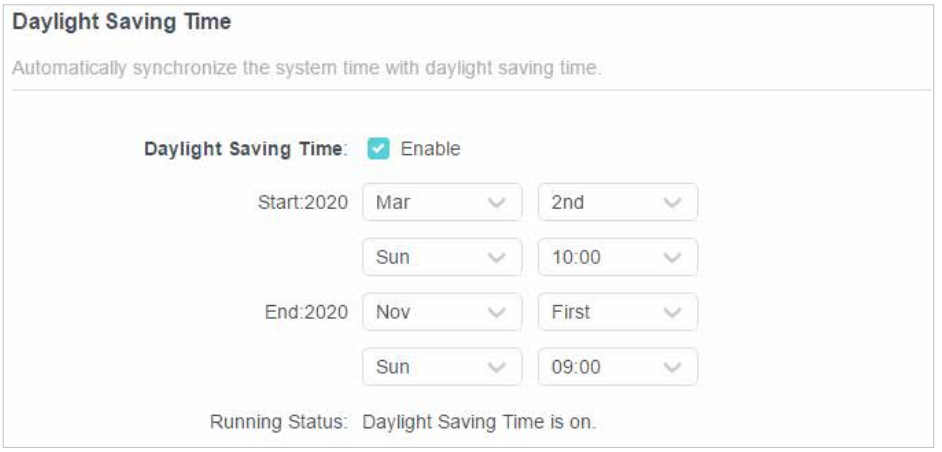
1. In the Set Time field, select Manually.



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.



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.

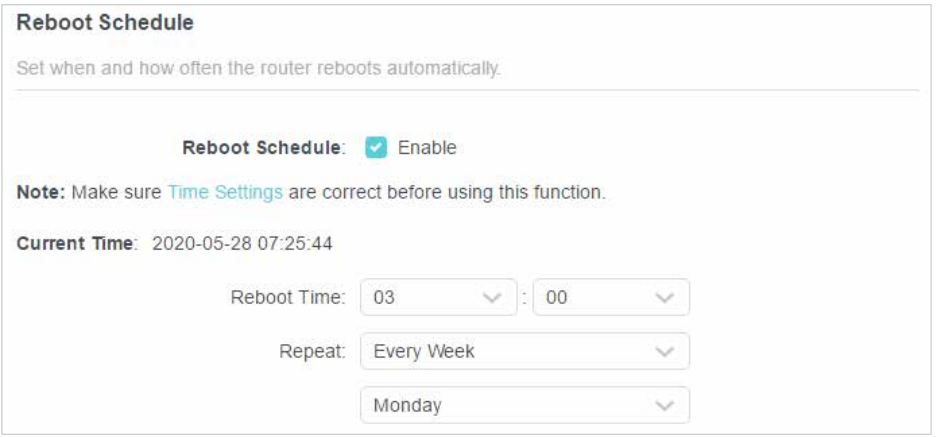
- **To set system language:**

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

18. 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.

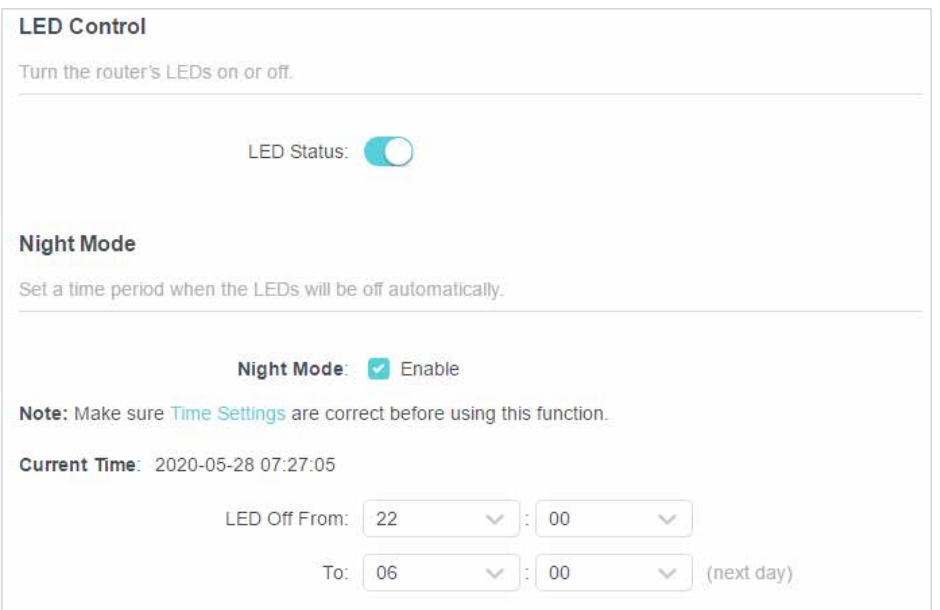


4. Specify the Reboot Time when the router reboots and Repeat to decide how often it reboots.
5. Click SAVE.

18. 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.



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.

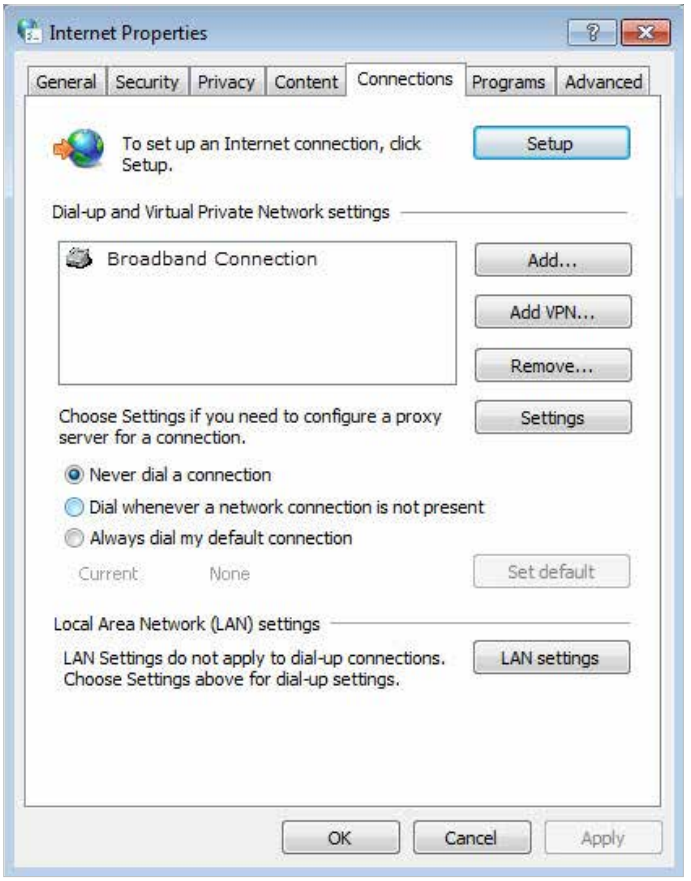
Note:

- 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?

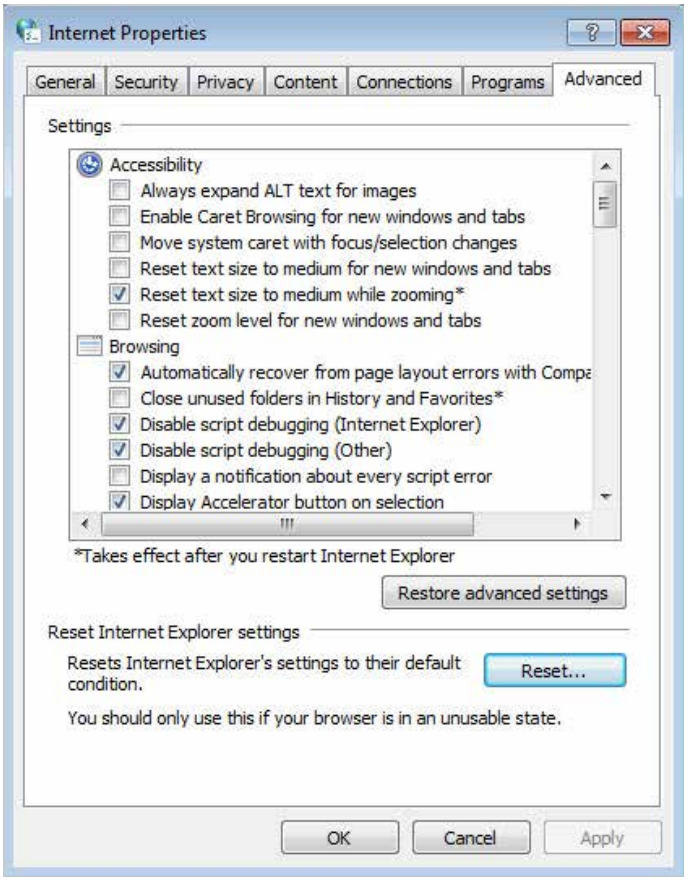
This can happen for a variety of reasons. Please try the methods below to log in again.

- 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.

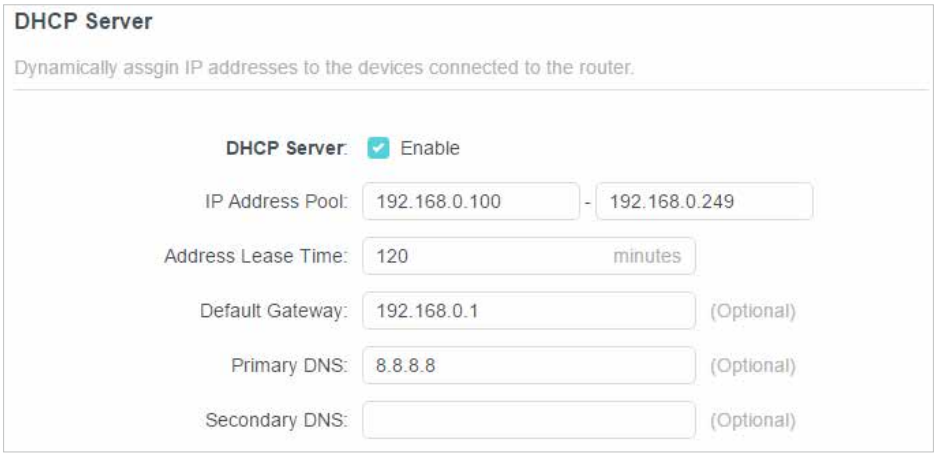
Q4. What should I do if I can't access the internet even though the configuration is finished?

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:

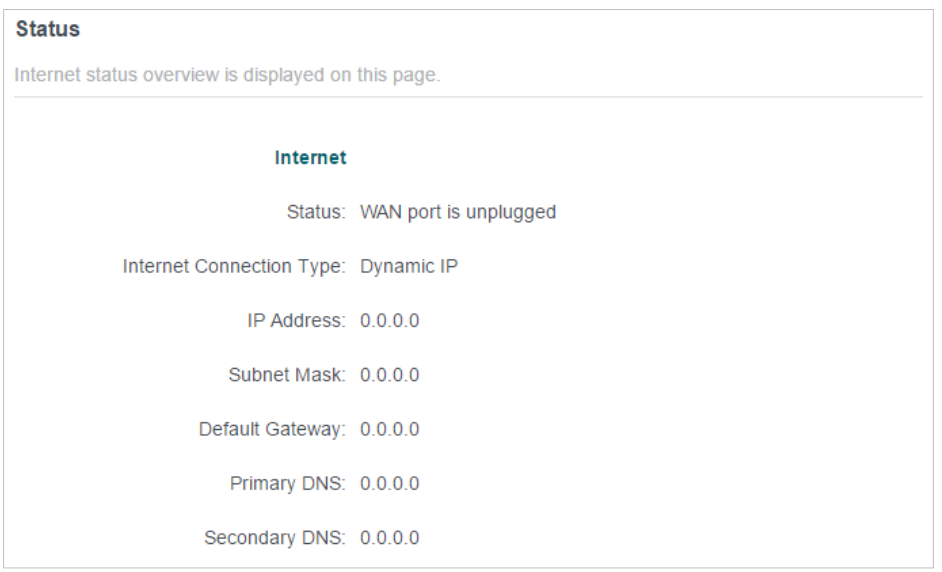
- Your computer might not recognize any DNS server addresses. Please manually configure the DNS server.
  1) Go to Advanced > Network > DHCP Server.
  2) Enter 8.8.8.8 as Primary DNS, click SAVE.

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



- 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:

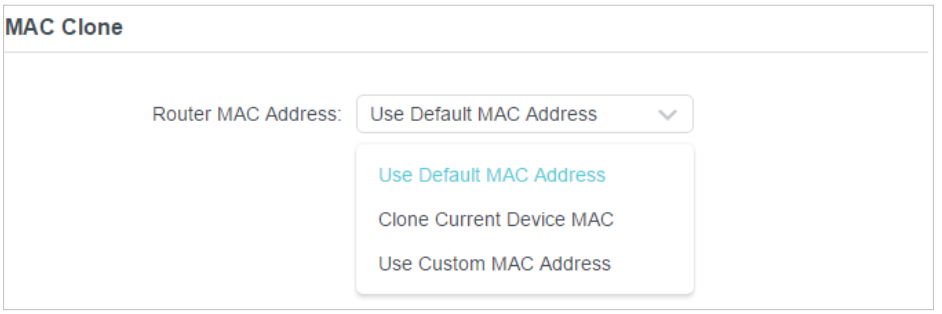


- Make sure the physical connection between the router and the modem is proper.
- Clone the MAC address of your computer.

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:

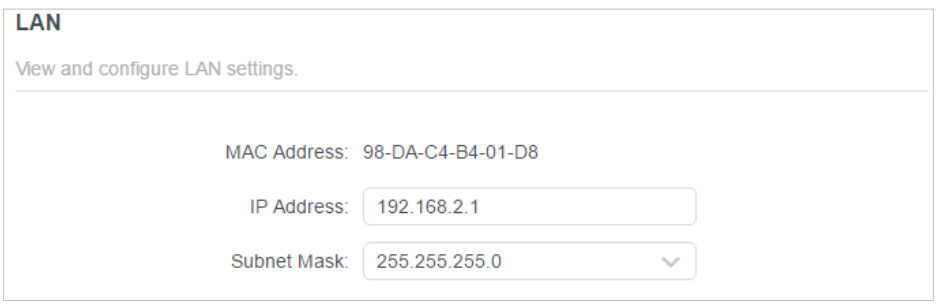
Most TP-Link routers use 192.168.0.1/192.168.1.1 as their default LAN IP address, which may conflict with the IP range of your existing ADSL modem/router. If so, the router is not able to communicate with your modem and you can't access the internet. To resolve this problem, we need to change the LAN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

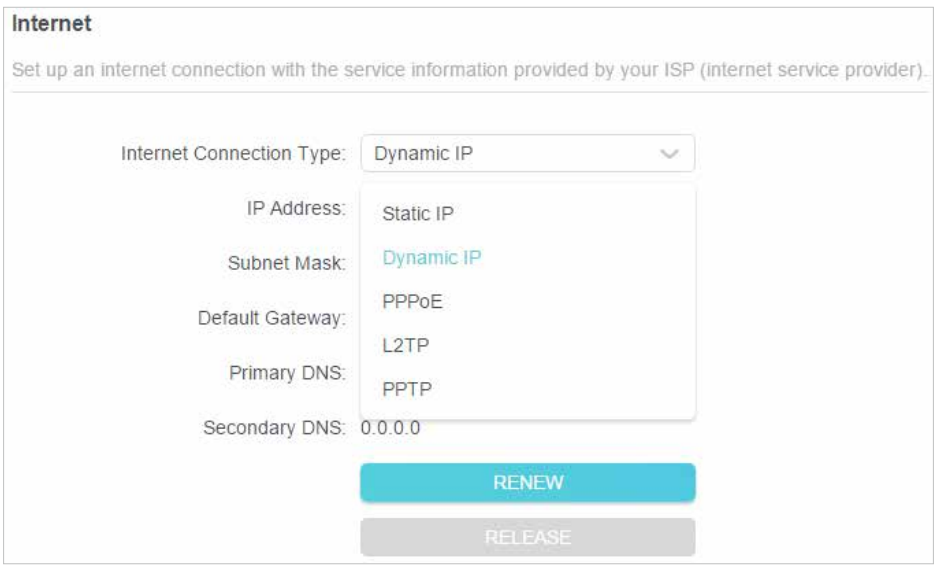
1) Confirm your internet connection type, which can be learned from the ISP.

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.



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: BE24000 Quad-Band Wi-Fi 7 Router
Model Number: Archer BE900

Component Name	Model
I.T.E. Power Supply	T150500-2-DT

Responsible party:
TP-Link USA Corporation
Address: 10 Mauchly, Irvine, CA 92618
Website: http://www.tp-link.com/us/
Tel: +1 626 333 0234
Fax: +1 909 527 6804
E-mail: sales.usa@tp-link.com

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

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

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

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

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

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

FCC RF Radiation Exposure Statement

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

To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 63 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC regulations restrict operation of this device to indoor use only. The operation of this device is prohibited on oil platforms, cars, trans, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10000 feet. Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

FCC compliance information statement

Product Name: I.T.E. Power Supply
Model Number: T150500-2-DT
Responsible party:
TP-Link USA Corporation
Address: 10 Mauchly, Irvine, CA 92618
Website: http://www.tp-link.com/us/
Tel: +1 626 333 0234
Fax: +1 909 527 6804
E-mail: sales.usa@tp-link.com

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

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

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

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

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

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

Issue Date: 2023-12-13

CE Mark Warning

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

OPERATING FREQUENCY(the maximum transmitted power)

2400 MHz -2483.5 MHz (20dBm)

5150 MHz -5250 MHz (23dBm)

5250 MHz -5350 MHz (23dBm)

5470 MHz -5725 MHz (30dBm)

5945MHz -6425 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.

National Restrictions

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.

Frequency band: 5250 - 5350 MHz:

Indoor use: Inside buildings only. Installations and use in road vehicles, trains and aircraft are not permitted. Outdoor use is not permitted.

Frequency band: 5470 - 5725 MHz:

Installations and use in road vehicles, trains and aircraft and use for unmanned aircraft systems (UAS) are not permitted.

	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
CA

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.

	UK

FR
ÉLÉMENTS D'EMBALLAGE
À SÉPARER ET À DÉPOSER
DANS LE BAC DE TRI
BAC DE TRI

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:

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

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

Avertissement:

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

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

ISED regulations restrict operation of this device to indoor use only. The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10000 feet. Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

Les réglementations ISED limitent le fonctionnement de cet appareil à une utilisation en intérieur uniquement. L'utilisation de cet appareil est interdite sur les plates-formes pétrolières, les voitures, les trains, les bateaux et les avions, sauf que l'utilisation de cet appareil est autorisée dans les avions long courrier en vol au-dessus de 10 000 pieds. L'exploitation d'émetteurs dans la bande

5,925-7,125 GHz est interdite pour le contrôle ou les communications avec des systèmes d'avions sans pilote.

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 33 cm 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 33 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。

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：BE24000 Quad-Band Wi-Fi 7 Router Equipment name				型號（型式）：Archer BE900 Type designation (Type)		
單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛 Lead (Pb)	汞 Mercury (Hg)	鎘 Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
PCB	○	○	○	○	○	○
外殼	○	○	○	○	○	○
電源供應器	—	○	○	○	○	○
天線	○	○	○	○	○	○

備考1.〝超出0.1 wt %〞及〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值。

Note 1："Exceeding 0.1 wt %" and "exceeding 0.01 wt %" indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2.〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。

Note 2："○" indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3.〝—〞係指該項限用物質為排除項目。

Note 3：The "—" indicates that the restricted substance corresponds to the exemption.

Продукт сертифіковано згідно с 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)
- This product uses radios and other components that emit electromagnetic fields. Electromagnetic fields and magnets may interfere with pacemakers and other implanted medical devices. Always keep the product and its power adapter more than 15 cm (6 inches) away from any pacemakers or other implanted medical devices. If you suspect your product is interfering with your pacemaker or any other implanted medical device, turn off your product and consult your physician for information specific to your medical device.

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 back 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)