



User Guide

AX1800 Whole Home Mesh Wi-Fi AP
HX220-G5
HX220

Contents

About This Guide	1
Chapter 1. Get to Know Your Device	2
1. 1. Product Overview	3
1. 2. Appearance	3
Chapter 2. Connect the Device	5
2. 1. Position the Device	6
2. 2. Connect Your Device	6
Chapter 3. Log In to Your Device	9
Chapter 4. Set Up Internet Connection	11
4. 1. Use Quick Setup Wizard	12
4. 2. Configure the Device in Router Mode	12
4. 2. 1. Connect the Hardware	12
4. 2. 2. Manually Set Up Your Internet Connection	13
4. 2. 3. Set Up an IPv6 Internet Connection	15
Chapter 5. Create Mesh Wi-Fi System	17
Chapter 6. Multi-SSID	20
Chapter 7. TP-Link Cloud Service	22
7. 1. Register a TP-Link ID	23
7. 2. Change Your TP-Link ID Information	23
7. 3. Manage the User TP-Link IDs	24
7. 3. 1. Add TP-Link ID to Manage the Router	25
7. 3. 2. Remove TP-Link ID(s) from Managing the Router	25
7. 4. Manage the Router via the TP-Link Tether App	26
Chapter 8. EasyMesh with Seamless Roaming	27
Chapter 9. Parental Controls	30

Chapter 10. Network Security	34
10. 1. Firewall & DoS Protection	35
10. 2. Service Filtering	36
10. 3. Access Control	37
10. 4. IP & MAC Binding	39
Chapter 11. NAT Forwarding	41
11. 1. Translate Address and Port by ALG	42
11. 2. Share Local Resources over the Internet by Virtual Server	43
11. 3. Open Ports Dynamically by Port Triggering	44
11. 4. Make Applications Free from Port Restriction by DMZ	45
11. 5. Make Xbox Online Games Run Smoothly by UPnP	46
Chapter 12. VPN Server	48
12. 1. Use OpenVPN to Access Your Home Network	49
12. 2. Use PPTP VPN to Access Your Home Network	50
Chapter 13. Customize Your Network Settings	55
13. 1. Change LAN Settings	56
13. 1. 1. Change the LAN IP Address	56
13. 1. 2. Use the Controller as a DHCP Server	56
13. 1. 3. Reserve LAN IP Addresses	57
13. 2. Configure IPv6 LAN Settings	58
13. 2. 1. Configure the RADVD Address Type	58
13. 2. 2. Configure the DHCPv6 Server Address Type	59
13. 3. Set Up a Dynamic DNS Service Account	60
13. 4. Create Static Routes	61
13. 5. Set Up the IPv6 Tunnel	64
13. 5. 1. Use the Public IPv6 Tunnel Service-6to4	64
13. 5. 2. Specify the 6rd Tunnel with Parameters Provided by Your ISP	65
13. 6. Specify Wireless Settings	66
13. 6. 1. Change Basic Wireless Settings	66
13. 6. 2. View Wireless Information	68
13. 6. 3. Advanced Wireless Settings	69
13. 7. Use WPS for Wireless Connection	70
Chapter 14. Manage Your Controller	73
14. 1. Set System Time	74

14. 2.	Control LED	75
14. 3.	Test Internet Connectivity	75
14. 4.	Update the Firmware.....	76
14. 5.	Back Up and Restore Configuration Settings	77
14. 6.	Reboot the Controller.....	78
14. 7.	Administration Management.....	79
14. 7. 1.	Change the Login Password	79
14. 7. 2.	Local Management	79
14. 7. 3.	Remote Management.....	80
14. 7. 4.	ICMP Ping	81
14. 8.	System Log.....	82
14. 9.	CWMP Settings.....	83
14. 10.	SNMP Settings	85
14. 11.	Monitor the Internet Traffic Statistics.....	86
FAQ		88

About This Guide

This guide is a complement to Quick Installation Guide. The Quick Installation Guide provides instructions for quick internet setup, while this guide contains details of each function and demonstrates how to configure them.

Your device supports two operation modes, access point mode and router mode. The access point mode is the default mode, while the router mode has the most functions and features and this guide focus on the router mode trying to give you the whole picture of the functionalities.

When using this guide, please note that features of your device may vary slightly depending on the model and software version you have, and on your location, language, and internet service provider. All screenshots, images, parameters and descriptions documented in this guide are used for demonstration only.

Conventions

In this guide the following conventions are used:

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

More Info

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

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

A Technical Support Forum is provided for you to discuss our products at <http://forum.tp-link.com>.

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

Chapter 1

Get to Know Your Device

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

It contains the following sections:

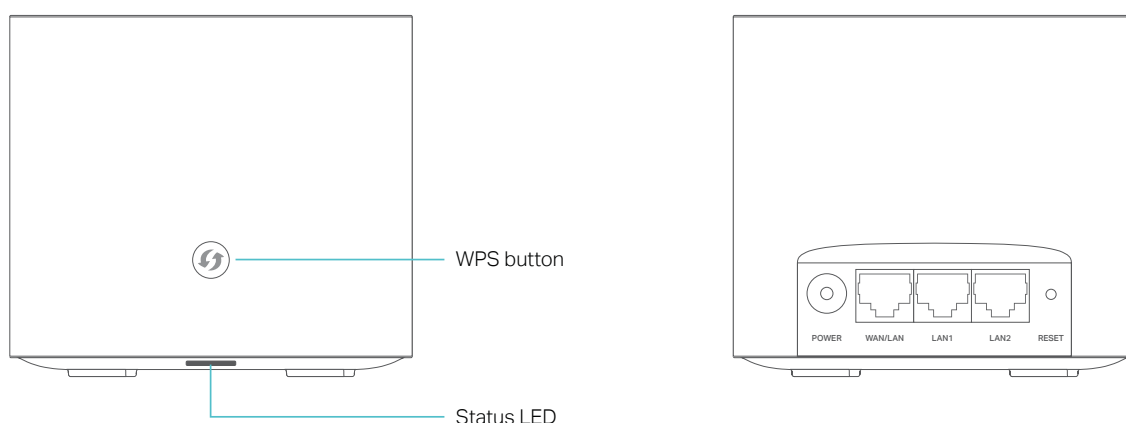
- [Product Overview](#)
- [Appearance](#)

1.1. Product Overview

The Whole Home Mesh Wi-Fi AP is designed to extend your network coverage. You can use multiple devices to create a seamless, intelligent and easy-to-configure mesh network that covers the entire home. The system consists of a controller, and one or more agents. The controller connects to a wired router, or a modem or gateway, the agent extends the wireless coverage of your network.

1.2. Appearance

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



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

LED Explanation	
Status	Indication
Yellow	The device is connected to the controller (For agent only).
Flashing yellow	The device is starting up or resetting.
Flashing blue	The device is ready for configuration.
Fast flashing blue	The device is trying to establish a WPS or mesh connection. This process may take up to two minutes.
Blue	The device has been set up as controller, or its wireless/wired connection with the controller is good, but the internet is unavailable.
Flashing white	The device is upgrading the firmware.
White	The device is ready and the internet is available.
Flashing red	The device has lost connection with the controller. (For agent only).

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

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

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

Chapter 2

Connect the Device

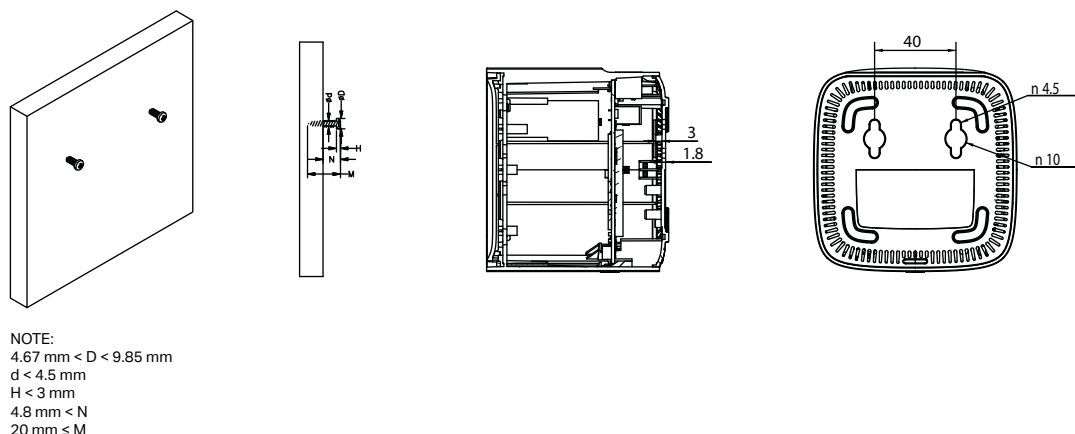
This chapter contains the following sections:

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

2.1. Position the Device

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

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



Note:

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

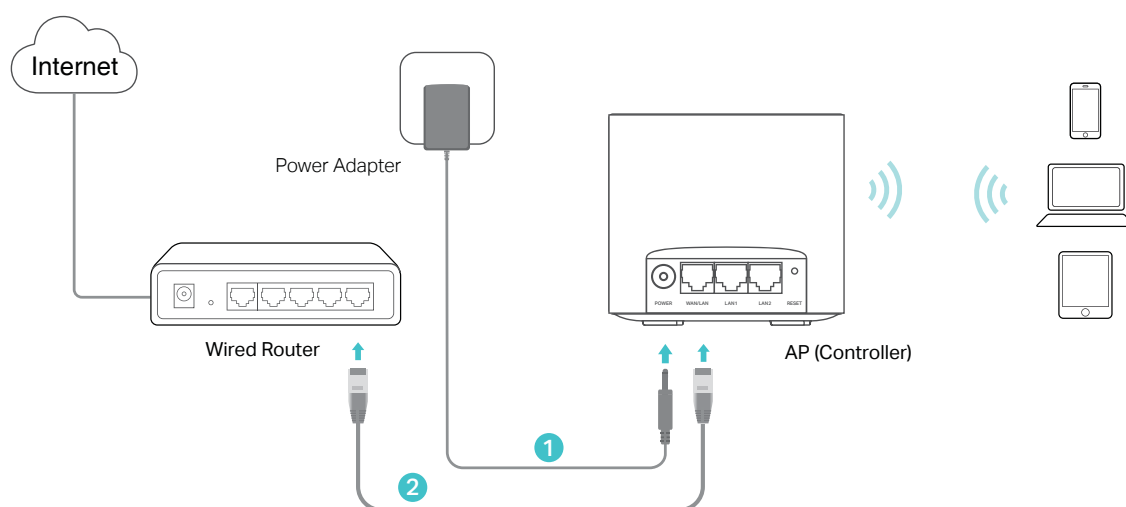
2.2. Connect Your Device

The Whole Home Mesh Wi-Fi AP is designed to extend the Wi-Fi signal and create a mesh wireless network throughout your home.

By default, the AP device is set in access point mode, you can connect the AP device to your existing wired to extend the wireless coverage of your existing network.

If you want to create a new network, the Whole Home Mesh Wi-Fi AP can act as a regular router, refer to [Router Mode Configure the Device in Router Mode](#) section.

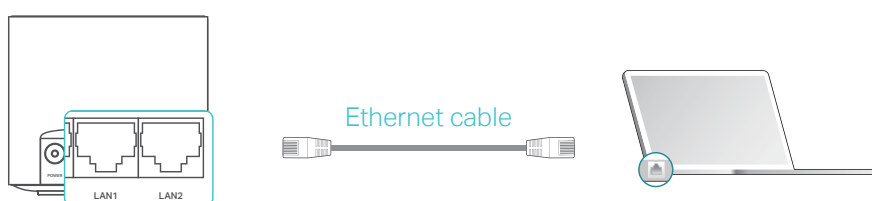
Follow the steps below to connect your device.



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

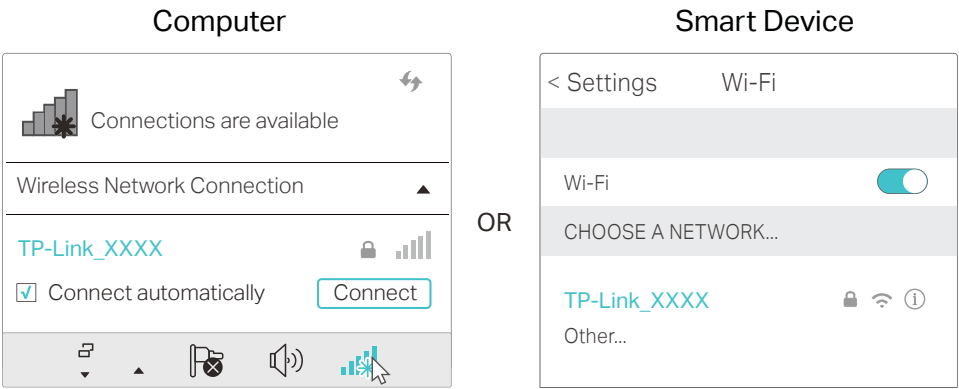
- **Method 1: Wired**

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



- **Method 2: Wireless**

- 1) Find the SSID (Network Name) and Wireless Password printed on the label at the bottom of the 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.



Note:
In access point mode, functions like NAT, Parental Controls are not supported.

Chapter 3

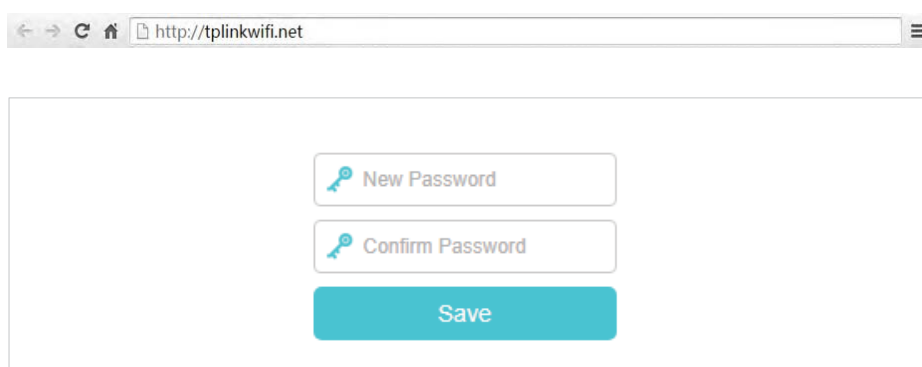
Log In to Your Device

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

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

Follow the steps below to log in to your device.

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



Note:

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

Chapter 4

Set Up Internet Connection

This chapter introduces how to connect your router to the internet. The router is equipped with a web-based Quick Setup wizard. It includes the necessary configuration options of ISP, automates the setup process and verifies whether those settings 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](#)
- [Configure the Device in Router Mode](#)

4. 1. Use Quick Setup Wizard

The Quick Setup wizard will guide you through the process to set up your device.

 Tips:

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

Follow the steps below to set up your router.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for your device.
2. Click **Quick Setup** on the top of the page. Then follow the step-by-step instructions to connect your device to the internet.

 Note:

1. 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.
2. Once you complete the **Quick Setup** process, the device become your mesh Wi-Fi controller, you can add agent to create your mesh Wi-Fi system.

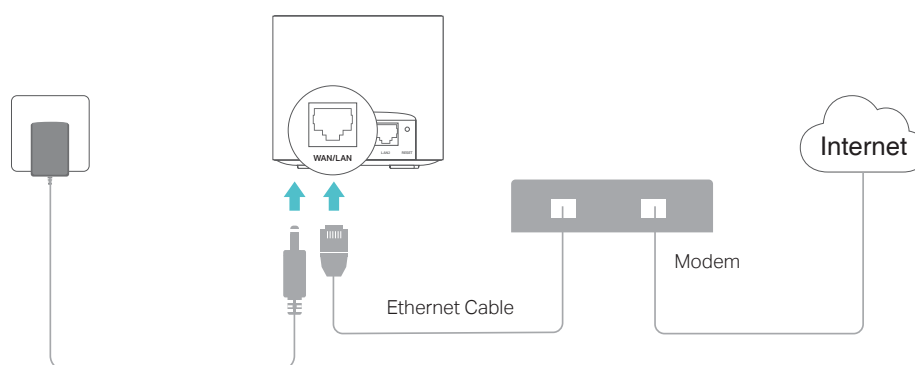
4. 2. Configure the Device in Router Mode

4. 2. 1. Connect the Hardware

If you already have a modem or your internet comes directly from an Ethernet wall outlet, you can set up the device to work as a regular router.

If your internet connection is through an Ethernet cable directly from the wall instead of through a DSL / Cable / Satellite modem, directly connect the Ethernet cable to WAN/LAN port on the AP device, then follow step 4 and 5 to complete the hardware connection.

To switch to router mode:



1. Unplug your modem, and remove the backup battery if it has one.
2. Connect the powered-off modem to the WAN/LAN port on the AP device with an Ethernet cable.
3. Turn on the modem and then wait about 2 minutes for it to restart.

4. Connect the power adapter to the AP device.
5. Connect a computer to the AP device via an Ethernet cable or wirelessly by using the SSID (network name) and Wireless Password.
6. Launch a web browser and enter <http://tplinkwifi.net> in the address bar, and log in to your AP device using the password you set.
7. Go to **Settings > Operation Mode**, select Router and click Save. Wait for the device to reboot, and run the **Quick Setup** and select router mode to set up the internet connection.

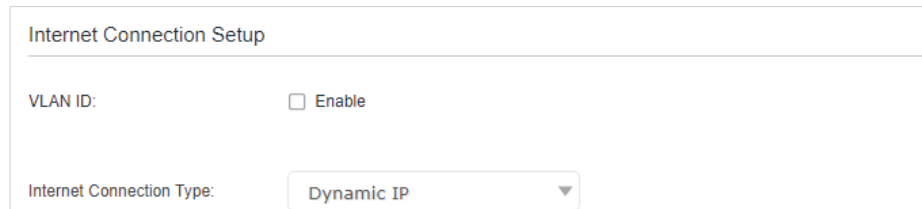
Now, you can set up your network and surf the internet.

4.2.2. 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 the password you set for the router.
2. Go to **Basic > Internet**.
3. Select your internet connection type from the drop-down list.

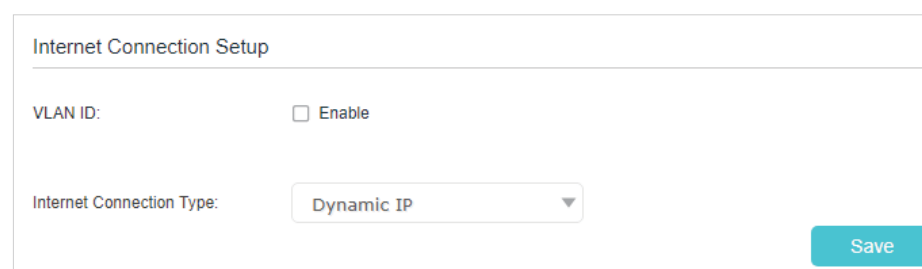


The screenshot shows the 'Internet Connection Setup' page. It has a title bar 'Internet Connection Setup'. Below it, there is a 'VLAN ID:' label followed by an 'Enable' checkbox. Further down, there is an 'Internet Connection Type:' label followed by a dropdown menu currently showing 'Dynamic IP'.

Note:

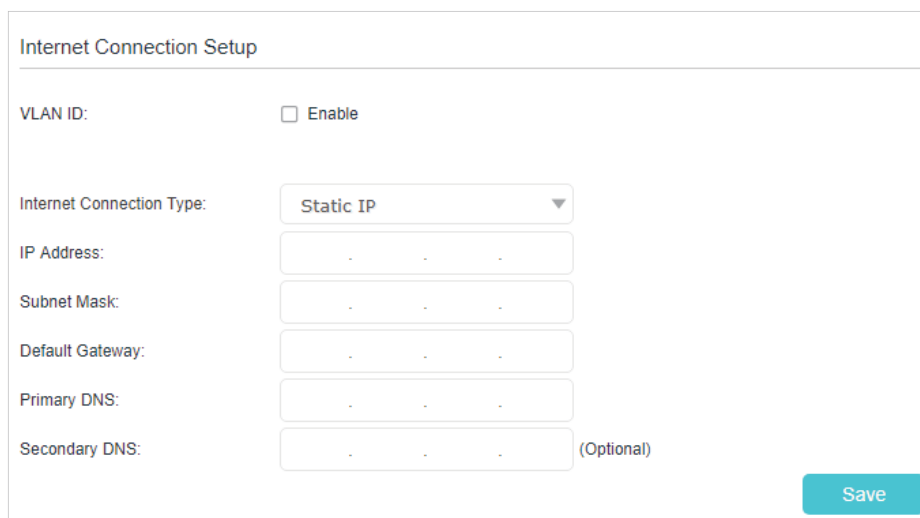
If you are unsure of what your connection type is, please consult your ISP. Since different connection types may require different cables and connection information, please refer to the demonstrations in Step 4 to determine your connection type.

4. Follow the instructions on the page to continue the configuration. Parameters on the images are used for demonstration only.
 - 1) If you choose **Dynamic IP**, you just need to click **Save** to make the settings effective. Dynamic IP users are usually equipped with a cable TV or fiber cable.



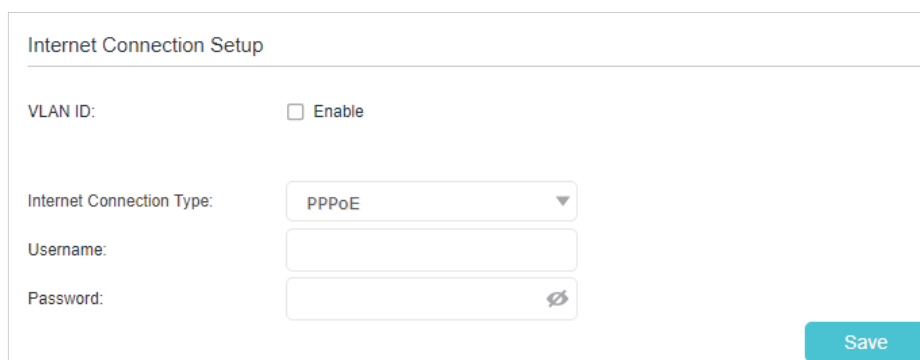
This screenshot is identical to the previous one, showing the 'Internet Connection Setup' page with 'VLAN ID' and 'Dynamic IP' settings. However, a blue 'Save' button is now visible in the bottom right corner of the form area.

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



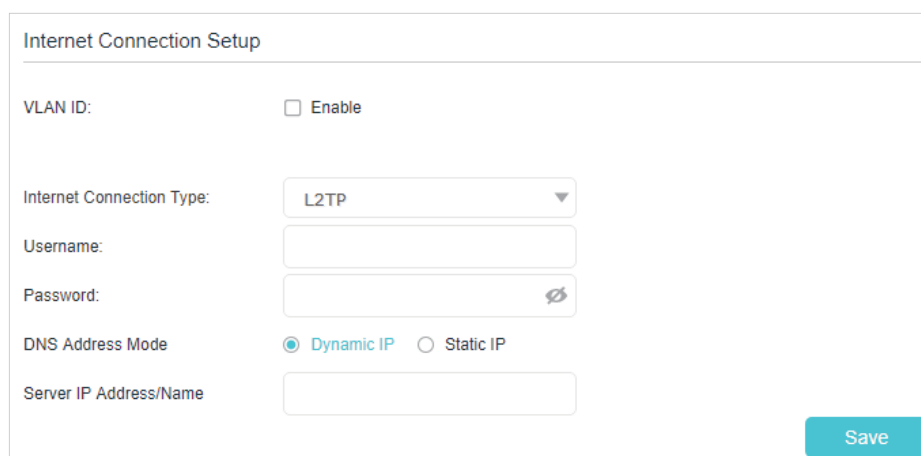
The form is titled "Internet Connection Setup". It contains a "VLAN ID:" label with an "Enable" checkbox. Below this is the "Internet Connection Type:" dropdown menu, which is set to "Static IP". Underneath are five input fields for "IP Address:", "Subnet Mask:", "Default Gateway:", "Primary DNS:", and "Secondary DNS:". Each of these fields contains three dashes "-" as a placeholder. The "Secondary DNS:" field is followed by the text "(Optional)". A teal "Save" button is located at the bottom right of the form.

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



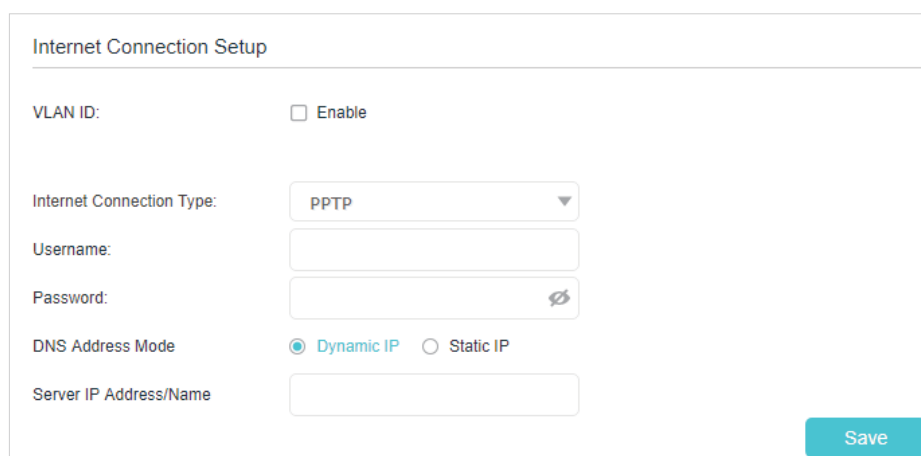
The form is titled "Internet Connection Setup". It contains a "VLAN ID:" label with an "Enable" checkbox. Below this is the "Internet Connection Type:" dropdown menu, which is set to "PPPoE". Underneath are two input fields: "Username:" and "Password:". The "Password:" field has a small icon of two crossed arrows to its right, indicating a password toggle. A teal "Save" button is located at the bottom right of the form.

- 4) If you choose **L2TP**, enter the **Username** and **Password**, and select the **DNS Address Mode** provided by your ISP. Different parameters are needed according to the DNS address mode you selected.



The screenshot shows the 'Internet Connection Setup' form. The 'VLAN ID' section has an 'Enable' checkbox. The 'Internet Connection Type' dropdown is set to 'L2TP'. The 'Username' and 'Password' fields are empty. The 'DNS Address Mode' has 'Dynamic IP' selected with a radio button. The 'Server IP Address/Name' field is empty. A 'Save' button is at the bottom right.

- 5) If you choose [PPTP](#), enter the [Username](#) and [Password](#), and select the [DNS Address Mode](#) provided by your ISP. Different parameters are needed according to the DNS address mode you selected.



The screenshot shows the 'Internet Connection Setup' form. The 'VLAN ID' section has an 'Enable' checkbox. The 'Internet Connection Type' dropdown is set to 'PPTP'. The 'Username' and 'Password' fields are empty. The 'DNS Address Mode' has 'Dynamic IP' selected with a radio button. The 'Server IP Address/Name' field is empty. A 'Save' button is at the bottom right.

5. Click [Save](#) to make the settings effective, and you can refer to [Test Internet Connectivity](#) to test if the internet connection works.

Note:

It may take 1-2 minutes to save the settings.

Tips:

3. You can check your internet connection by clicking [Network Map](#) on the left of the page.
4. 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.
5. If you still cannot access the internet, refer to the [FAQ](#) section for further instructions.

4. 2. 3. Set Up an IPv6 Internet Connection

If your ISP provides information about one of the following IPv6 internet connection types: PPPoE, Dynamic IP(SLAAC/DHCPv6), and Static IP, you can manually set up an IPv6 connection.

If your ISP provides an IPv4-only connection or IPv6 tunnel service, permit IPv6 connection by referring to [Set Up the IPv6 Tunnel](#).

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

Internet Setup				
Refresh Add Delete All				
WAN Interface Name	VLAN ID	Status	Operation	Modify
ipoe_0_0_d	0	Disconnected	Renew	 

3. Select your WAN Interface Name ([Status](#) should be [Connected](#)) and click the  (Edit) icon.
4. Scroll down the page to enable [IPv6](#), and configure the IPv6 parameters.

IPv6:	☒ Enable
Addressing Type:	AUTO
IPv6 Gateway:	pppoe_0_0
 Advanced	

- [Addressing Type](#): Consult your ISP for the addressing type ([DHCPv6](#) or [SLAAC](#)). [SLAAC](#) is the most commonly used addressing type.
- [IPv6 Gateway](#): Keep it as the default setting.

 Note:

If your ISP has provided the IPv6 address, click [Advanced](#) to reveal more settings.

5. Click [OK](#) and IPv6 service is available for your network now.

Chapter 5

Create Mesh Wi-Fi System

This chapter describes how you can add the agent to create a mesh Wi-Fi system and extend the wireless coverage.

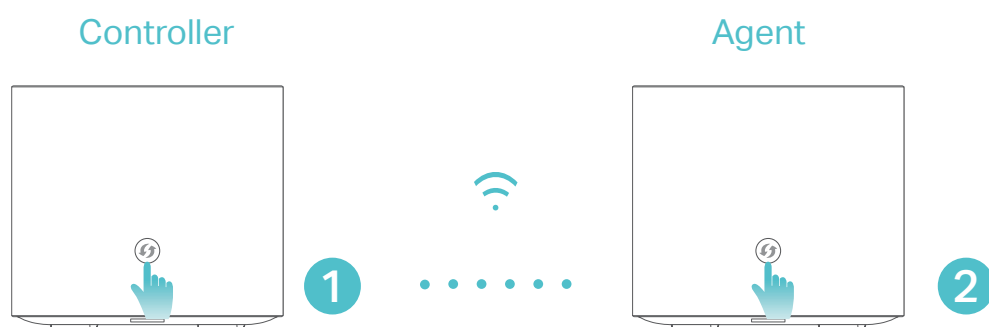
The Whole Home Mesh Wi-Fi System includes a controller, one or more agents. If you have more than one mesh AP devices, you can add the remaining ones as agents to create a mesh Wi-Fi system and extend your Wi-Fi coverage.

Please note that you can only add the AP device as agent when it is in factory default settings.

➤ **To add a agent to your network**

- **Method 1: Wireless Connection**

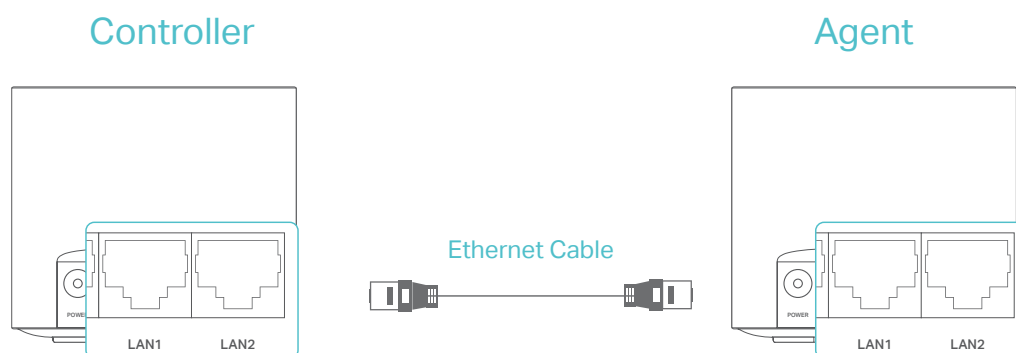
1. Place the agent close to the controller and power it on, wait about two minutes until the status LED turns to flashing blue.
2. Press the WPS button on the controller or the agent in your mesh Wi-Fi system, and within two minutes, press the WPS button on your new agent.



3. The status LED will flash blue fast for about two minutes during the synchronizing process.

- **Method 2: Wired Connection**

1. Place the agent in an open area for best performance and power it on, wait about two minutes for it to get ready for configuration.
2. Connect the LAN ports on the controller and the agent using an Ethernet cable .
3. The agent will automatically synchronize with the controller to extend your network.



 Tips:

1. If the agent's status LED still flashes blue, please repeat the synchronizing process.
2. The agent automatically follows the Wi-Fi settings of the controller.
3. You can also synchronize the add-on agent with the agent in your existing mesh Wi-Fi system.
4. You can log in to the controller if you want to manage your mesh network.

You can place the agent in appropriate places to extend the wireless signal coverage. The specific locations depend on the architectural style, building material, and layout of your house. Please note that the wireless coverage of one agent and the router must be overlapped for synchronization. If you have more than one agent, we recommend that you place the mesh router in the middle of your agents.

You can use the agent's LED status to help you to determine where to place them.

 Tips:

After the placement, if the LED status of agent is flashing red, please move it closer to the controller or the other agent, you can check the satellite's connection status on the web management page by clicking the [Router](#) icon on [Network Map](#).

Chapter 6

Multi-SSID

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

➤ **To create a multi-SSID network:**

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to **Basic > Multi-SSID** or **Advanced > Wireless > Multi-SSID**.
3. Create the multi-SSID network as needed.

Multi-SSID

MSSID1: ☒ Enable

Network Name (SSID): ☐ Hide SSID

Security:

MSSID2: ☐ Enable

MSSID3: ☐ Enable

Save

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

Chapter 7

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.

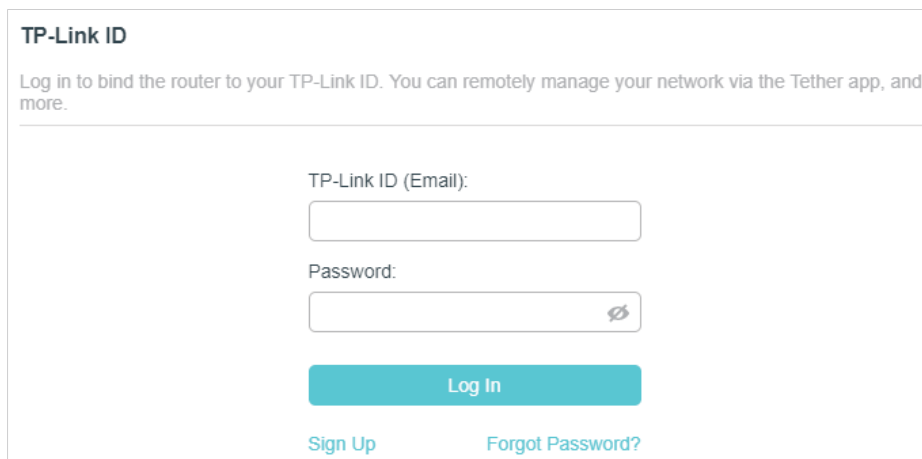
It contains the following sections:

- [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](#)

7.1. Register a TP-Link ID

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to **Advanced > TP-Link ID** or click **TP-Link ID** on the very top of the page.
3. Click **Sign Up** and follow the instructions to register a TP-Link ID.



TP-Link ID

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

TP-Link ID (Email):

Password:

Log In

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

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**, and click **Unbind** in the **Device Information** section.

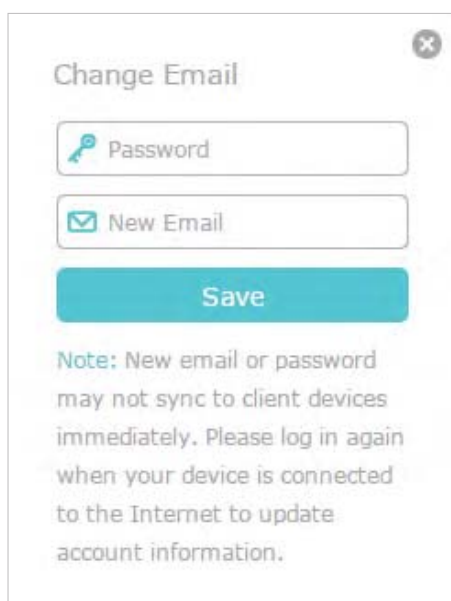
7.2. Change Your TP-Link ID Information

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:**

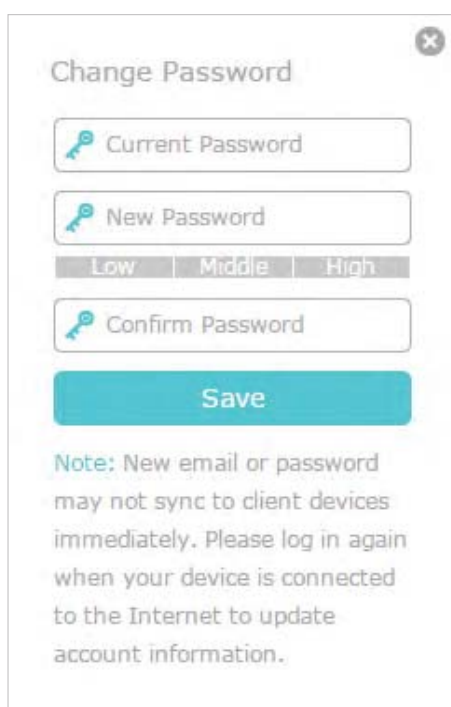
1. Click  behind the Email.
2. Enter the password of your TP-Link ID, then a new email address. And click **SAVE**.



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

- **To change your password:**

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



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

7.3. 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

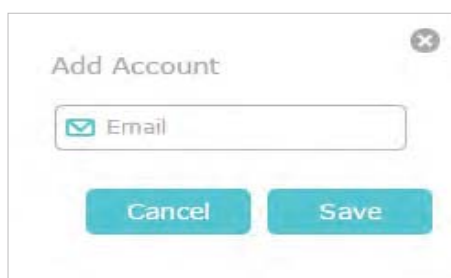
from the same router as [Users](#). All accounts can monitor and manage the router locally or remotely, but user accounts cannot:

- 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.

7.3.1. 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.



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

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

					+ Bind - Unbind	
☐	ID	Email	Binding Date	Role		
☐	1	admin@tplink.com	2023/01/01	Admin		
☐	2	user@tplink.com	2023/01/01	User		

7.3.2. 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](#).

Bound Accounts				
+ Bind - Unbind				
☐	ID	Email	Binding Date	Role
☐	1	shangpu_liang@163.com	2020-08-08	Admin
☒	2	shangpu_liang@163.com	2020-08-08	User

7.4. 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.

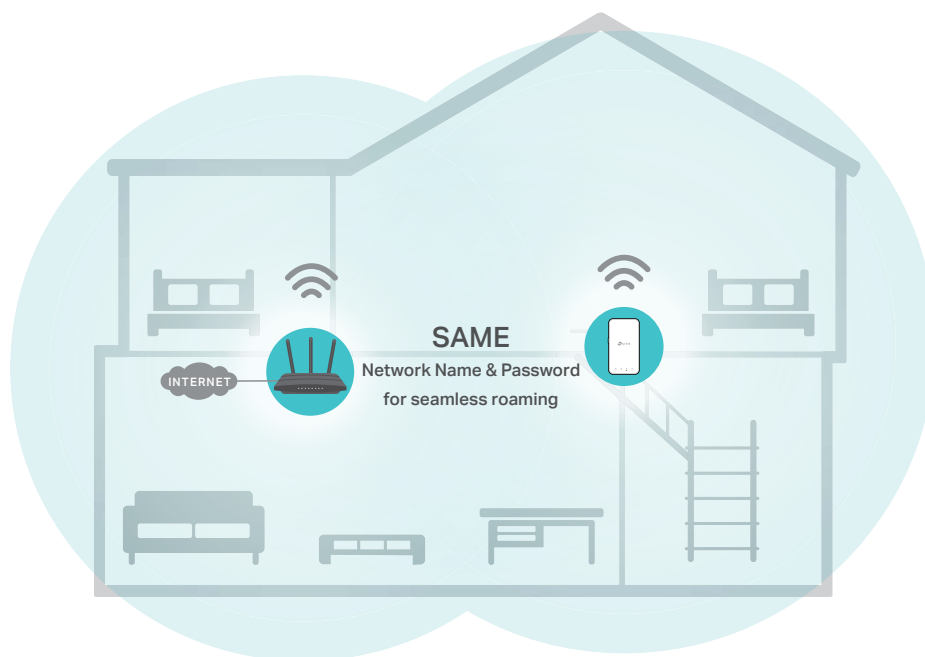
Note: If you need to remotely access your router from your smart devices, you need to:

- 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 8

EasyMesh with Seamless Roaming

TP-Link EasyMesh router and EasyMesh supported routers or extenders work together to form one unified Wi-Fi network. Walk through your home and stay connected with the fastest possible speeds thanks to its seamless coverage.



Unified Wi-Fi Network

Router and extenders share the same wireless settings, including network name, password, access control settings and more.



Seamless Roaming

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

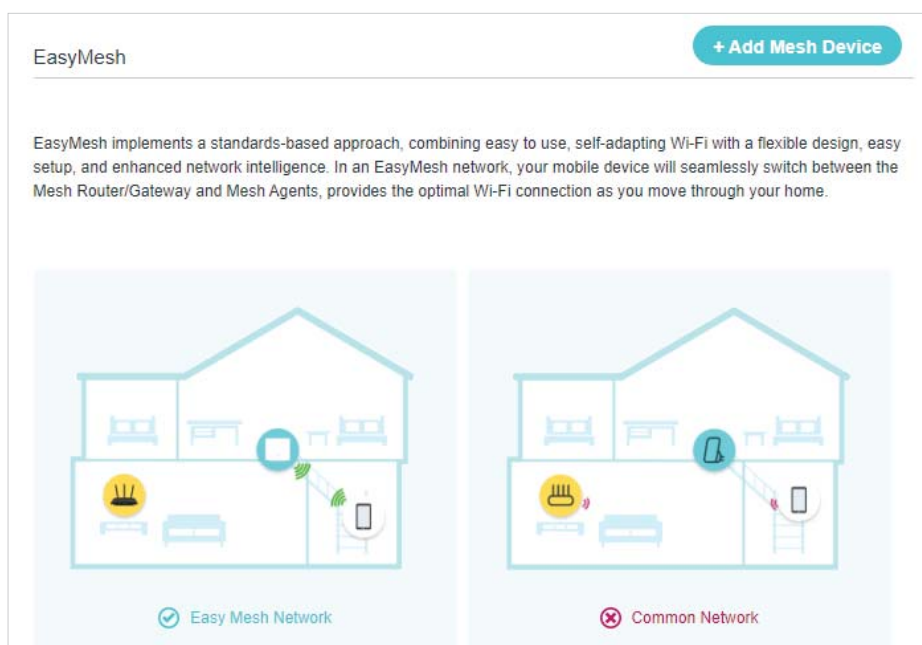


Easy Setup and Management

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

- **To set up a EasyMesh network:**

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



3. Click [Add Mesh Device](#).

4. Follow the setup instructions on the web page to add the new AP device. Or you can follow the setup instructions in the user manual of the new AP.

Note:

Please make sure the new mesh device to be added has not been used in other mesh network.

5. If you have added the mesh device to join the EasyMesh network, it will be listed on the router's [Network Map](#) page.

Chapter 9

Parental Controls

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

I want to:

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

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

How can I do that?

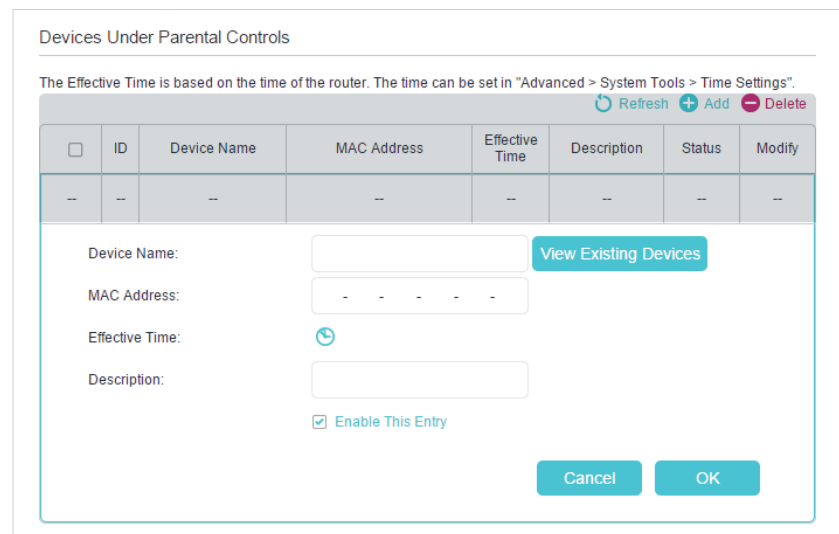
1. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
2. Go to [Basic](#) or [Advanced](#) > [Parental Controls](#) and enable [Parental Controls](#).



Parental Controls

Parental Controls: ☒

3. Click [Add](#), and then click [View Existing Devices](#) to select the connected device(s) to be controlled. Or, input the [Device Name](#) and [MAC Address](#) manually.



Devices Under Parental Controls

The Effective Time is based on the time of the router. The time can be set in "Advanced > System Tools > Time Settings".

Refresh Add Delete

☐	ID	Device Name	MAC Address	Effective Time	Description	Status	Modify
--	--	--	--	--	--	--	--

Device Name: [View Existing Devices](#)

MAC Address:

Effective Time:

Description:

☒ Enable This Entry

Cancel OK

4. Click the  icon to set the Effective Time. Drag the cursor over the appropriate cell(s) and click [OK](#).

5. Enter a [Description](#) for the entry, keep the [Enable This Entry](#) check box selected, and then click [Save](#).
6. Enable [Content Restriction](#), and select [Whitelist](#) as the restriction policy.

Tips:

- With [Blacklist](#) selected, the controlled devices cannot access any websites containing the specified keywords during the Effective Time period.
- With [Whitelist](#) selected, the controlled devices can only access websites containing the specified keywords during the Effective Time period.

7. Click [Add a New Keyword](#) and enter "www.tp-link.com" and "Wikipedia.org" as the keywords and click [Save](#).

8. You can add up to 32 keywords for either Blacklist or Whitelist.

Below are some sample entries for your reference.

- **For Whitelist:** Enter a web address (e.g. wikipedia.org) to allow access only to its related websites. If you wish to block all internet browsing access, do not add any keyword to the **Whitelist**.
- **For Blacklist:** Specify a web address (e.g. wikipedia.org), a web address keyword (e.g. wikipedia) or a domain suffix (e.g. .edu or .org) to block access only to the websites containing that keyword or suffix.

Done!

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

Chapter 10

Network Security

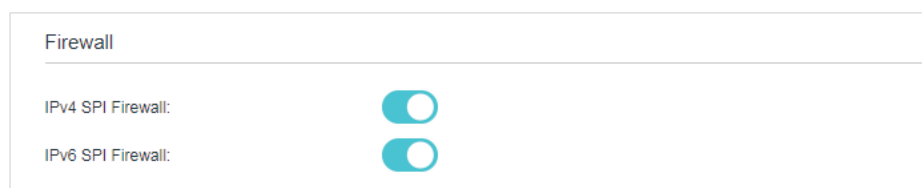
This chapter guides you on how to protect your home network from unauthorized users by implementing network security functions. You can block or allow specific client devices to access your wireless network using MAC Filtering, or using Access Control for wired and wireless networks, or you can prevent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

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

10.1. Firewall & DoS Protection

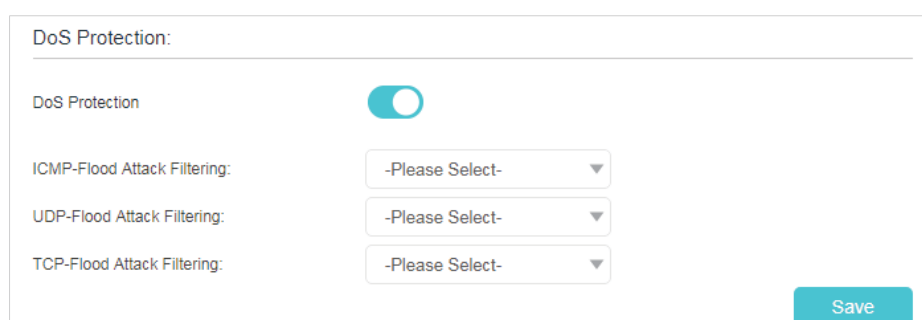
The SPI (Stateful Packet Inspection) Firewall and DoS (Denial of Service) Protection protect the controller from cyber attacks.

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



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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
2. Go to **Advanced > Security > Firewall & DoS Protection**.



Note: [DoS Protection](#) and [Traffic Statistics](#) must be enabled at the same time, you can go to **Advanced > System Tools > Traffic Statistics** to enable traffic statistics function.

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

Tips:

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

Dos Protection Level Settings

ICMP-Flood Protection Level:

Low:

3600

(5-3600) packets/sec

Middle:

2400

(5-3600) packets/sec

High:

1200

(5-3600) packets/sec

UDP-Flood Protection Level:

Low:

3600

(5-3600) packets/sec

Middle:

2400

(5-3600) packets/sec

High:

1200

(5-3600) packets/sec

TCP-SYN-Flood Protection Level:

Low:

3600

(5-3600) packets/sec

Middle:

2400

(5-3600) packets/sec

High:

1200

(5-3600) packets/sec

Save

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

Blocked DoS Host List

Host Number: 0

Refresh

Delete

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

10.2. Service Filtering

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
2. Go to [Advanced](#) > [Security](#) > [Service Filtering](#).
3. Enable [Service Filtering](#).

Service Filtering

Service Filtering: ☒

4. Click [Add](#).

Filtering List

Refresh

Add

Delete

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

Service Type:

Any(ALL)

Protocol:

TCP/UDP

Starting Port:

1

Ending Port:

65535

Service Type:

Any(ALL)

Filter Service For:

☐ Single IP Address

☐ IP Address Range

☒ All IP Addresses

Cancel

OK

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

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

10.3. Access Control

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

I want to:

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

- How can I do that?**

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

2. Go to **Advanced > Security > Access Control** and enable **Access Control**.

Access Control

Access Control:

☒

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

To block specific device(s):

- 1) Select [Blacklist](#) and click [Save](#).

Access Mode

Access Mode:
☒ [Blacklist](#)
☐ [Whitelist](#)

[Save](#)

- 2) Select the device(s) to be blocked in the [Online Devices](#) table (or click the [Add](#) under the [Devices in Blacklist](#) and enter the [Device Name](#) and [MAC Address](#) manually).

- 3) Click [Block](#) above the [Online Devices](#) table. The selected devices will be added to [Devices in Blacklist](#) automatically.

Devices in Blacklist

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

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

Online Devices

[Refresh](#) [Block](#)

☐	ID	Device Name	IP Address	MAC Address	Connection Type
☐	1	W11424	192.168.0.100	84:16:F9:03:E2:D3	Wired
☐	2	Unknown	192.168.0.101	1C:3B:F3:54:51:9B	Wired
☐	3	Unknown	192.168.0.102	1C:3B:F3:54:50:D3	Wired

To allow specific device(s):

- 1) Select [Whitelist](#) and click [Save](#).

Access Mode

Access Mode:
☐ [Blacklist](#)
☒ [Whitelist](#)

[Save](#)

- 2) Click [Add](#) in the [Devices in Whitelist](#) section.

The screenshot shows a web interface titled "Devices in Whitelist". At the top right, there are buttons for "+ Add" and "- Delete". Below this is a table with the following columns: a checkbox, "ID", "Device Name", "MAC Address", and "Modify". The table currently contains one row with dashes "--" in each column. Below the table, there are two input fields: "Device Name:" and "MAC Address:". The "MAC Address" field has a format of "- - - - -". At the bottom right, there are "Cancel" and "OK" buttons.

3) Enter the **Device Name** and **MAC Address**. (You can copy and paste the information from **Online Devices** table if the device is connected to your network.)

4) Click **OK**.

Done!

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

10.4. IP & MAC Binding

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

I want to:

Prevent ARP spoofing and ARP attacks.

How can I do that?

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
2. Go to **Advanced** > **Security** > **IP & MAC Binding** and enable **IP & MAC Binding**.

IP & MAC Binding

IP & MAC Binding:

Binding List

Add

Delete

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

ARP List

Refresh

Bind

☐	ID	Device Name	MAC Address	IP Address	Bound	Modify
☐	1	W11424	84:16:F9:03:E2:D3	192.168.0.100	Unloaded	
☐	2	Unknown	1C:3B:F3:54:51:9B	192.168.0.101	Unloaded	
☐	3	Unknown	1C:3B:F3:54:50:D3	192.168.0.102	Unloaded	

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

To bind the connected device(s):

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

To bind the unconnected device

- 1) Click [Add](#).

Binding List

Add

Delete

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

MAC Address:

84 - 15 - F9 - E2 - D3 -

IP Address:

192 . 168 . 0 . 101

☒ [Enable This Entry](#)

Cancel

OK

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

Done!

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

Chapter 11

NAT Forwarding

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

The router can use a forwarding feature to remove the isolation of NAT and allow external internet hosts to initiatively communicate with the devices in the local network, thus enabling some special features.

TP-Link router includes four forwarding rules. If two or more rules are set, the priority of implementation from high to low is Virtual Servers, Port Triggering, UPnP and DMZ.

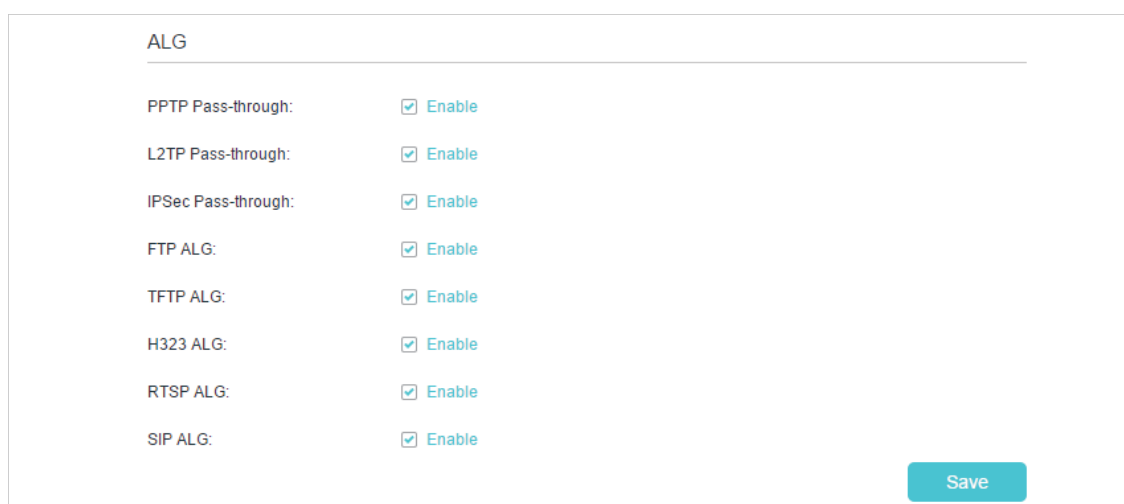
This chapter contains the following sections:

- [Translate Address and Port by ALG](#)
- [Share Local Resources over the Internet by Virtual Server](#)
- [Open Ports Dynamically by Port Triggering](#)
- [Make Applications Free from Port Restriction by DMZ](#)
- [Make Xbox Online Games Run Smoothly by UPnP](#)

11. 1. Translate Address and Port by ALG

ALG (Application Layer Gateway) allows customized NAT (Network Address Translation) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols: FTP, TFTP etc. Enabling ALG is recommended.

Visit <http://tplinkwifi.net>, and log in with the password you set for the controller. Go to **Advanced > NAT Forwarding > ALG**.



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

Save

- **PPTP Pass-through:** If enabled, it allows Point-to-Point sessions to be tunneled through an IP network and passed through the controller.
- **L2TP Pass-through:** If enabled, it allows Layer 2 Point-to-Point sessions to be tunneled through an IP network and passed through the controller.
- **IPSec Pass-through:** If enabled, it allows IPSec (Internet Protocol Security) to be tunneled through an IP network and passed through the controller. IPSec uses cryptographic security services to ensure private and secure communications over IP networks.
- **FTP ALG:** If enabled, it allows FTP (File Transfer Protocol) clients and servers to transfer data via NAT.
- **TFTP ALG:** If enabled, it allows TFTP (Trivial File Transfer Protocol) clients and servers to transfer data via NAT.
- **H323 ALG:** If enabled, it allows Microsoft NetMeeting clients to communicate via NAT.
- **RTSP ALG:** If selected, it allows media player clients to communicate with streaming media servers via NAT.
- **SIP ALG:** If enabled, it allows clients communicate with SIP (Session Initiation Protocol) servers via NAT.

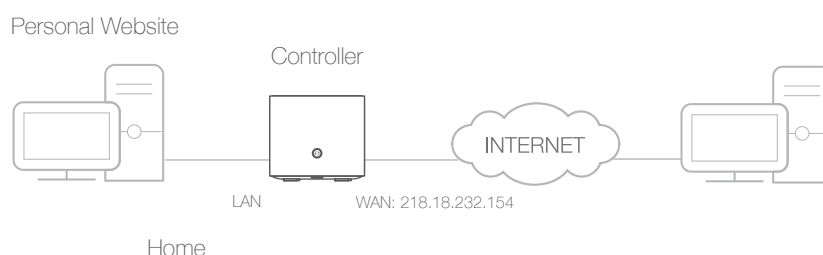
11.2. Share Local Resources over the Internet by Virtual Server

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

Virtual server can be used for setting up public services in your local network, such as HTTP, FTP, DNS, POP3/SMTP and Telnet. Different service uses different service port. 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 configuration.

I want to: Share my personal website I've built in a 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 can visit my website. The PC is connected to the controller 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 the password you set for the controller.
3. Go to **Advanced > NAT Forwarding > Virtual Servers**, click **Add**.

Virtual Servers

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

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

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

Interface Name:

Service Type: [View Existing Applications](#)

External Port: (XX-XX or XX)

Internal IP:

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

Protocol:

☒ Enable This Entry

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

4. Click [View Existing Applications](#), and choose [HTTP](#). The external port, internal port and protocol will be automatically filled in. Enter the PC's IP address 192.168.0.100 in the [Internal IP](#) field.

5. Click [OK](#) to make the settings effective.

[🔗 Tips:](#)

1. 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.
2. If the service you want to use is not in the [Service Type](#), you can enter the corresponding parameters manually. You should verify the port number that the service needs.
3. You can add multiple virtual server rules if you want to provide several services from a controller. Please note that the [External Port](#) cannot be overlapped.

Done!

Internet users can enter [http://WAN IP](#) (in this example: [http://218.18.232.154](#)) to visit your personal website.

[🔗 Tips:](#)

1. For a WAN IP that is assigned dynamically by ISP, it is recommended to apply and register a domain name for the WAN by DDNS, go to [Set Up a Dynamic DNS Service Account](#) for more information. Then you can use [http://domain name](#) to visit the website.
2. 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.

11.3. Open Ports Dynamically by Port Triggering

Port triggering can specify a triggering port and its corresponding external ports. When a host in 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 returns to the external ports, the router can forward them to the corresponding host. Port triggering is mainly applied to online games, VoIPs and video players. Common applications include MSN Gaming Zone, Dialpad, Quick Time 4 players, and so on.

Follow the steps below to configure the port triggering rules:

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
2. Go to **Advanced > NAT Forwarding > Port Triggering**, and click **Add**.

Port Triggering

+ Add - Delete

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

Interface Name:

Application: [View Existing Applications](#)

Triggering Port: (XX, 1-65535)

Triggering Protocol:

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

External Protocol:

☒ Enable This Entry

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

3. Click [View Existing Applications](#), and select the desired application. The triggering port and protocol, the external port and protocol will be automatically filled in. Here we take [MSN Gaming Zone](#) as an example.
4. Click [OK](#) to make the settings effective.

Tips:

1. You can add multiple port triggering rules according to your network needs.
2. If the application you need is not listed in the Existing Applications list, you can 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 suggested.

11.4. Make Applications Free from Port Restriction by DMZ

When a PC is set to be a DMZ (Demilitarized Zone) host in 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, like IP camera and database software, you can set the PC to be a DMZ host.

Note:

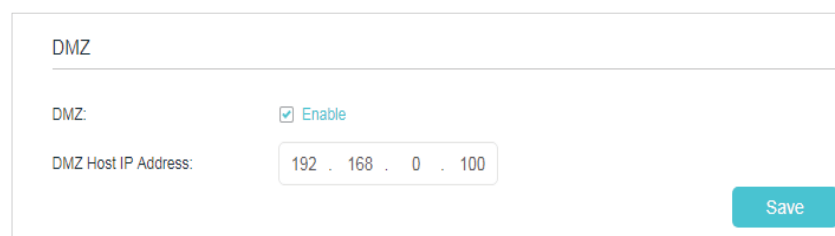
DMZ is most applicable when you don't know which ports to open. When it is enabled, the DMZ host is totally exposed to the internet, which may bring some potential safety hazards. If DMZ is not in use, please disable it in time.

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 with all ports opened.

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 the password you set for your controller.
3. Go to **Advanced > NAT Forwarding > DMZ** and select the **Enable** check box to turn on DMZ.



4. Enter the IP address 192.168.0.100 in the **DMZ Host IP Address** box.
5. Click **Save** to make the settings effective.

Done!

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

11.5. Make Xbox Online Games Run Smoothly by UPnP

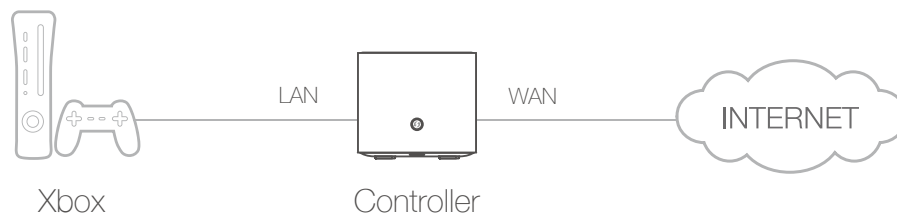
UPnP (Universal Plug and Play) protocol allows the applications or host devices to automatically find the front-end NAT device and send request to it to open the corresponding ports. With UPnP enabled, the applications or host devices in the both sides of NAT device can freely communicate with each other realizing the seamless

connection of the network. You need to enable the UPnP if you want to use applications such as multiplayer gaming, peer-to-peer connections, real-time communication (for example, VoIP or telephone conference), or remote assistance.

 Tips:

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

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



You can follow the steps to change the status of UPnP.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for your controller.
2. Go to **Advanced** > **NAT Forwarding** > **UPnP**, and enable or disable UpnP according to your needs.

UPnP

UPnP:
☒

UPnP Service List

Total Clients: 0
Refresh

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

Chapter 12

VPN Server

The VPN (Virtual Private Networking) Server allows you to access your home network in a secured way through internet when you are out of home. The router offers two ways to setup VPN connection: OpenVPN and PPTP (Point to Point Tunneling Protocol) VPN.

OpenVPN is somewhat complex but with greater security and more stable. It is suitable for restricted environment, such as campus network and company intranet.

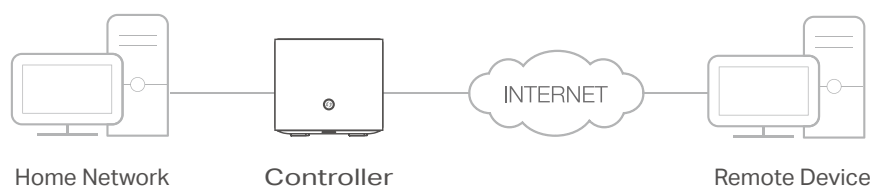
PPTP VPN is more easily used and its speed is faster, it's compatible with most operating systems and also supports mobile devices. Its security is poor and your packets may be cracked easily, and PPTP VPN connection may be prevented by some ISP.

This chapter contains the following sections, you can choose the appropriate VPN server connection type as needed.

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

12.1. Use OpenVPN to Access Your Home Network

In the OpenVPN connection, the home network can act as a server, and the remote device can access the server through the router which acts as an OpenVPN Server gateway. To use the VPN feature, you should enable OpenVPN Server on your router, and install and run VPN client software on the remote device. Please follow the steps below to set up an OpenVPN connection.



Step1. Set Up OpenVPN Server on Your Controller

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
2. Go to **Advanced > VPN > OpenVPN**, and select **Enable VPN Server**.

Note:

1. Before you enable VPN Server, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for controller's WAN port and synchronize your System Time with internet.
2. 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.

Certificate

Generate the certificate.

[Generate](#)

Note:

If you have already generated one, please skip this step, or click [Generate](#) to update the certificate.

9. Click [Export](#) to save the OpenVPN configuration file which will be used by the remote device to access your controller.

Configuration File

Export the configuration.

[Export](#)

Step 2. Configure OpenVPN Connection on Your Remote Device

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

Note:

You need to install the [OpenVPN](#) client utility on each device that you plan to apply the VPN function to access your controller. 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 controller 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.

Tips:

You can go to [Advanced > VPN > VPN Connections](#) to view the clients that are currently connected to the OpenVPN servers.

12.2. Use PPTP VPN to Access Your Home Network

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

Step 1. Set Up PPTP VPN Server on Your Controller

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
2. Go to [Advanced > VPN Server > PPTP VPN](#), and select [Enable VPN Server](#).

PPTP VPN

☒ Enable VPN Server

Client IP Address:

10

.

7

.

0

.

11

-10.7.0.

20

(up to 10 clients)

Username:

admin

Password:

admin

Save

Note:

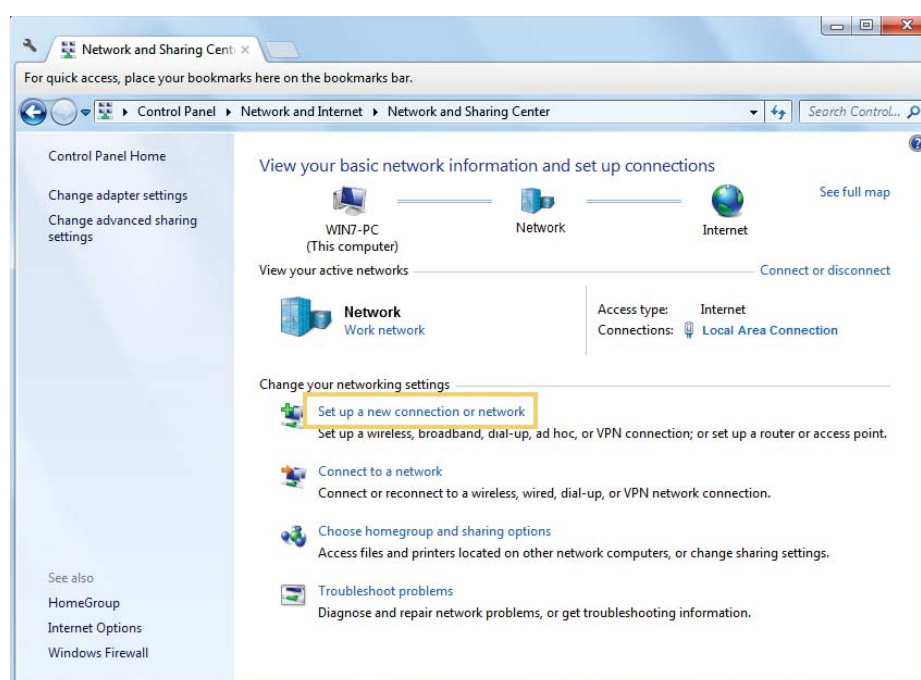
Before you enable [VPN Server](#), we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for controller's WAN port and synchronize your [System Time](#) with internet.

3. In the [Client IP Address](#) field, enter the range of IP addresses (up to 10) that can be leased to the devices by the PPTP VPN server.
4. Enter the [Username](#) and [Password](#) to authenticate clients to the PPTP VPN server.
5. Click [Save](#) to make the settings effective.

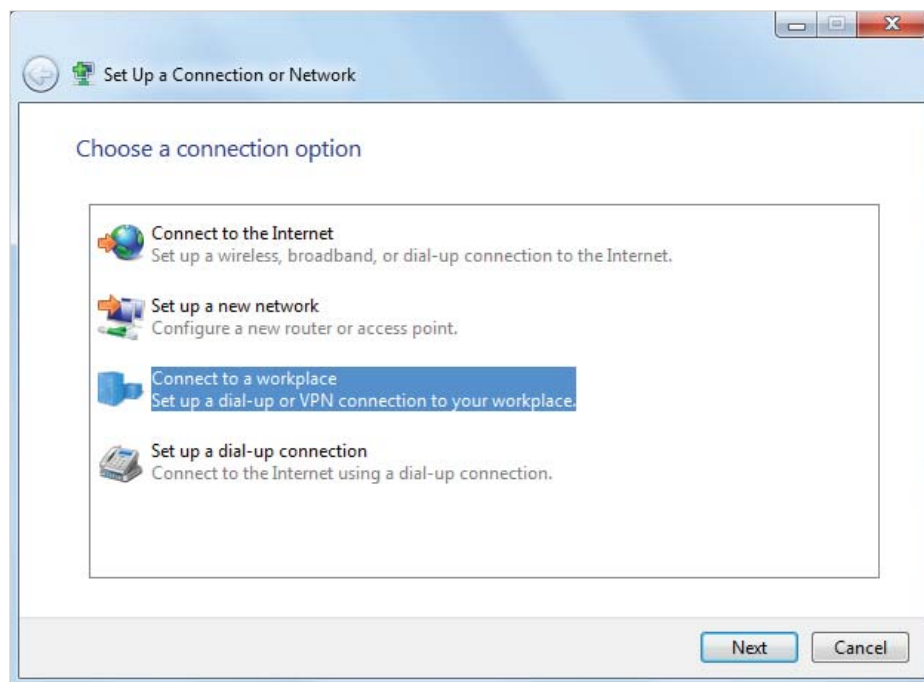
Step 2. Configure PPTP VPN Connection on Your Remote Device

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.

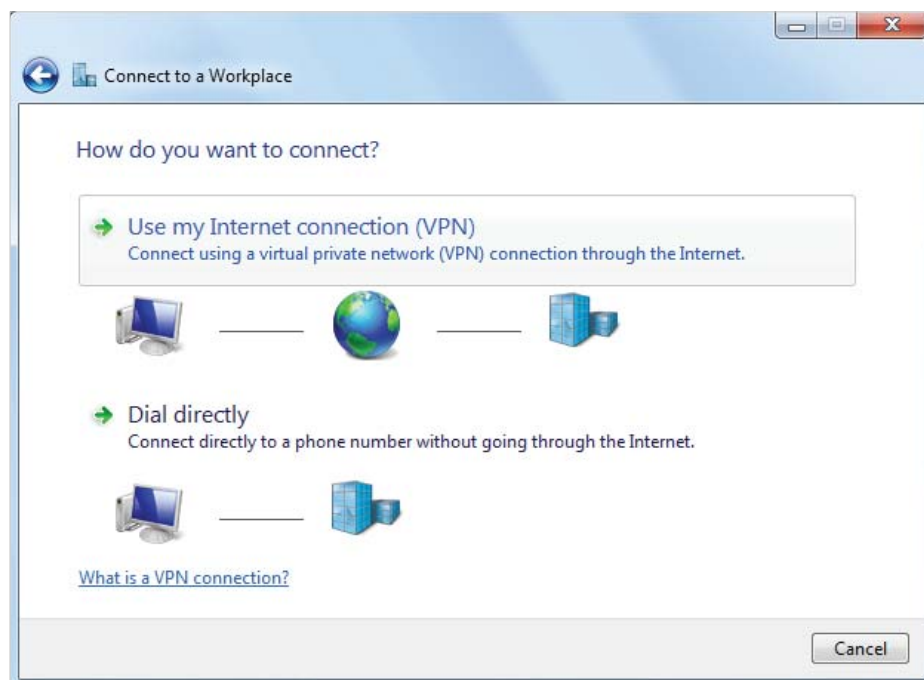
1. Go to [Start > Control Panel > Network and Internet > Network and Sharing Center](#).
2. Select [Set up a new connection or network](#).



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



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



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

Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 218.18.1.73

Destination name: VPN Connection

☐ Use a smart card

☐ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☐ Don't connect now; just set it up so I can connect later

Next Cancel

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

Connect to a Workplace

Type your user name and password

User name: admin

Password: •••••

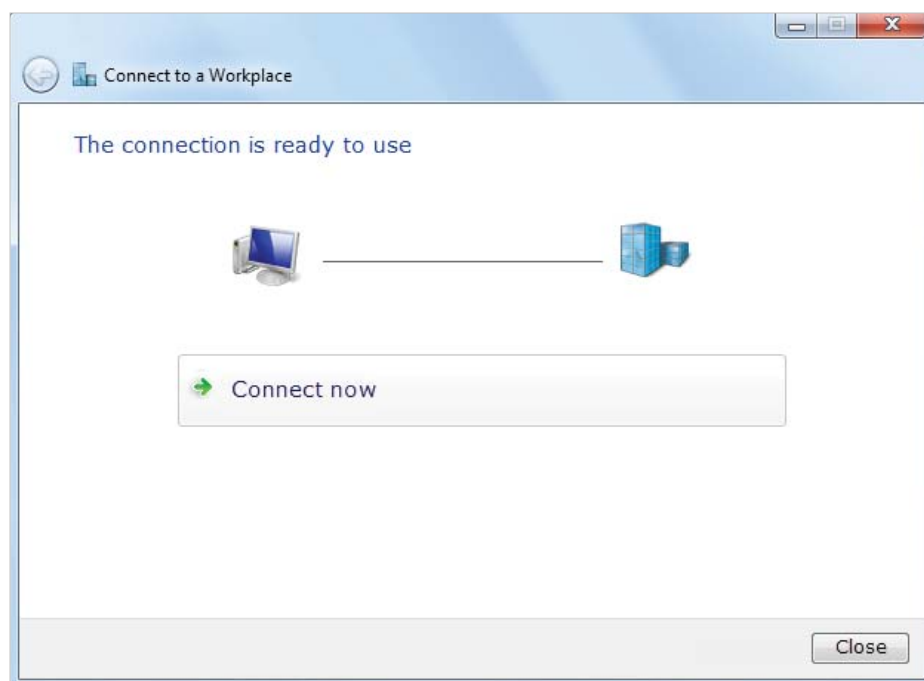
☐ Show characters

☐ Remember this password

Domain (optional):

Connect Cancel

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



 Tips:

You can go to [Advanced > VPN > VPN Connections](#) to view the clients that are currently connected to the PPTP VPN servers.

Chapter 13

Customize Your Network Settings

This chapter introduces how to change the default settings or adjust the basic configuration of the network setting of the controller using the web management page.

It contains the following sections:

- [Change LAN Settings](#)
- [Configure IPv6 LAN Settings](#)
- [Set Up a Dynamic DNS Service Account](#)
- [Create Static Routes](#)
- [Set Up the IPv6 Tunnel](#)
- [Specify Wireless Settings](#)
- [Use WPS for Wireless Connection](#)

13.1. Change LAN Settings

13.1.1. Change the LAN IP Address

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

Follow the steps below to change your IP address.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
2. Go to [Advanced](#) > [Network](#) > [LAN Settings](#), and select [IPv4](#).
3. Click the edit icon in the [Modify](#) column.

MAC Address:	00:0A:EB:12:BB:A1
IP Address:	192 . 168 . 0 . 1
Subnet Mask:	255.255.255.0 ▼
IGMP Snooping:	☒ Enable
Second IP:	☐ Enable

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

13.1.2. Use the Controller as a DHCP Server

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

Follow the steps below to configure DHCP server.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
2. Go to [Advanced](#) > [Network](#) > [LAN Settings](#) page and select [IPv4](#).
3. Enable [DHCP](#) function and select [DHCP Server](#).

DHCP: ☒ Enable

☒ DHCP Server ☐ DHCP Relay

IP Address Pool: 192 . 168 . 0 . 100 - 192 . 168 . 0 . 249

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

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

Default Domain: (Optional)

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

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

Save

4. Specify the [IP Address Pool](#), the start address and end address must be on the same subnet with LAN IP. The controller will assign addresses within this specified range to its clients. It is from 192.168.0.100 to 192.168.0.249 by default.
5. Enter a value for the [Address Lease Time](#). The [Address Lease Time](#) is the amount of time in which a DHCP client can lease its current dynamic IP address assigned by the controller. After the dynamic IP address expires, the user will be automatically assigned a new dynamic IP address. The default is 1440 minutes.
6. Keep the rest settings as default and click [Save](#).

Note:

1. The controller can be configured to work as a [DHCP Relay](#). A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. If it is enabled, the DHCP requests from local PCs will be forwarded to the DHCP server that runs on WAN side.
2. You can also appoint IP addresses within a specified range to devices of the same type by using [Condition Pool](#) feature. For example, you can assign IP addresses within the range (192.168.0.50 to 192.168.0.80) to Camera devices, thus facilitating the network management. Enable DHCP feature and configure the parameters according to your situation on the [Advanced](#) > [Network](#) > [LAN Settings](#) page.

13. 1. 3. Reserve LAN IP Addresses

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

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

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

The screenshot shows the 'Address Reservation' configuration interface. At the top, there are '+ Add' and '- Delete' buttons. Below is a table with the following columns: a checkbox, 'MAC Address', 'Reserved IP Address', 'Group', 'Enable', and 'Modify'. The table currently has one row with dashes in each cell. Below the table, there are input fields for 'MAC Address:', 'IP Address:', and 'Group:'. The 'Group' dropdown is set to 'Default'. There is a 'Scan' button next to the MAC Address field. Below these fields is a checkbox labeled 'Enable This Entry' which is checked. At the bottom right are 'Cancel' and 'OK' buttons.

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

13.2. Configure IPv6 LAN Settings

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

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

13.2.1. Configure the RADVD Address Type

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

DHCP Server IPv4 | IPv6

Group: Default

Address Type: ☒ RADVD ☐ DHCPv6 Server

RDNS: ☐ Enable

Enable ULA Prefix ☐ Enable

Site Prefix Type: ☒ Delegated ☐ Static

WAN Connection: No available interface ▼

Save

- 1) Select the **RADVD** as the address type to make the controller assign IPv6 address prefixes to hosts.

Note:

Do not select the **Enable** check boxes to enable **RDNS** and **ULA Prefix** unless required by your ISP. Otherwise you may not be able to access the IPv6 network. For more information about RDNS and ULA Prefix, contact our technical support.

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

13.2.2. Configure the DHCPv6 Server Address Type

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
2. Go to **Advanced > Network > LAN Settings**.
3. Select **IPv6** to configure IPv6 LAN parameters.

DHCP Server IPv4 | IPv6

Group: Default

Address Type: ☐ RADVD ☒ DHCPv6 Server

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

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

Address Lease Time: 86400 seconds

Site Prefix Type: ☒ Delegated ☐ Static

WAN Connection: No available interface

Save

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

13.3. Set Up a Dynamic DNS Service Account

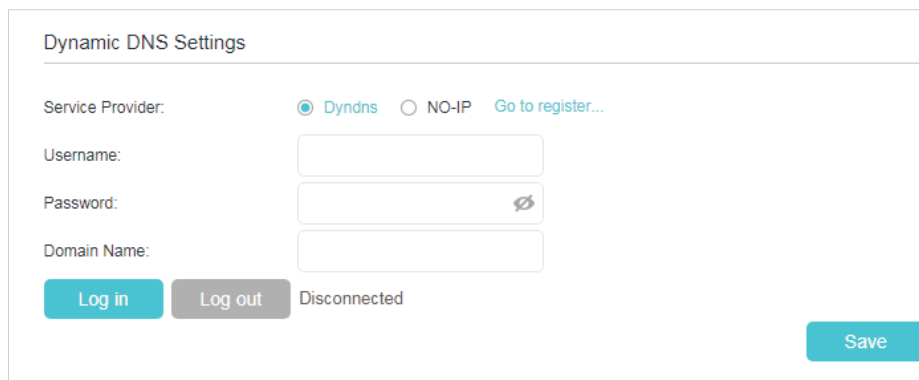
Most ISPs (Internet service providers) assign a dynamic IP address to the router and you can use this IP address to access your router remotely. However, the IP address can change any time and you don't know when it changes. In this case, you might need the DDNS (Dynamic Domain Name Server) feature on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

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

To set up DDNS, please follow the instructions below:

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

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



The screenshot shows a web form titled "Dynamic DNS Settings". It contains the following elements:

- Service Provider:** Two radio buttons, "DynDNS" (selected) and "NO-IP", followed by a link "Go to register...".
- Username:** A text input field.
- Password:** A text input field with a toggle icon on the right.
- Domain Name:** A text input field.
- Buttons:** "Log in" (teal), "Log out" (grey), and "Save" (teal).
- Status:** A label "Disconnected" next to the "Log out" button.

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

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

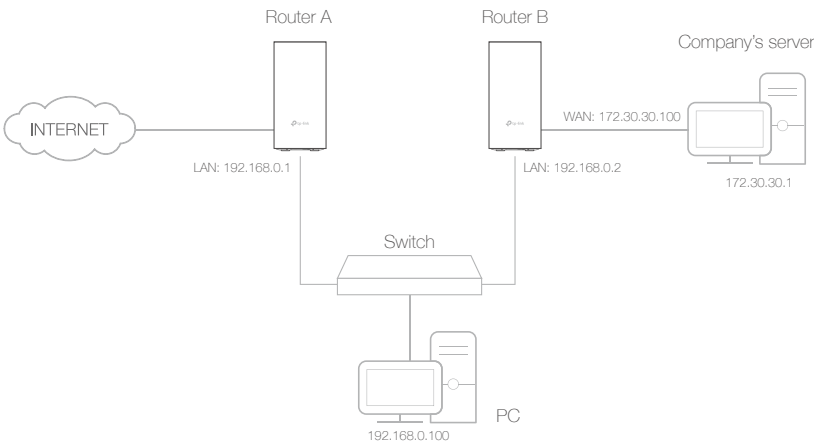
13.4. Create Static Routes

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

I want to:

Visit multiple networks and multiple servers at the same time.

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



How can I do that?

- 1. Make sure the routers use different LAN IP addresses on the same subnet. Disable Router B's DHCP function.
- 2. Visit <http://tplinkwifi.net>, and log in with the password you set for Router A.
- 3. Go to [Advanced > Network > Static Routing](#). Select your current [WAN Interface](#) and click [Save](#).

Default Gateway Settings

IPv4 | IPv6

Select a WAN interface as the system default gateway.

Select WAN Interface:

pppoe_ptm_0_0_d

Save

Static Routing

+ Add - Delete

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

- 4. Click [Add](#) to add a new static routing entry. Finish the settings according to the following explanations:

Static Routing

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

Network Destination: 172 . 30 . 30 . 1
 Subnet Mask: 255 . 255 . 255 . 255
 Gateway: 192 . 168 . 0 . 2
 Interface: LAN

☒ Enable This Entry

Cancel OK

- **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.
 - **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 the data. In the example, the data packets will be sent to the LAN port of Router 2 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 the data packets. In the example, the data is sent to the gateway through the LAN port of Router A, so LAN should be selected.
5. Select the **Enable This Entry** check box to enable this entry.
 6. Click **Save** to save the settings.

Done!

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

13.5. Set Up the IPv6 Tunnel

The IPv6 Tunnel feature helps you obtain IPv6 resources based on an IPv4 WAN connection or vice versa.

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

The controller provides four tunneling mechanisms: [6to4](#), [6rd](#), [DS-Lite](#), and [Map-T](#). The methods of setting up 6rd and DS-Lite tunnel are similar.

13.5.1. Use the Public IPv6 Tunnel Service-6to4

The 6to4 tunnel is a kind of public service. If there are any 6to4 servers on your network, you can use this mechanism to access IPv6 service. If your ISP provides you with an IPv4-only connection but you want to visit IPv6 websites, you can try to set up a 6to4 tunnel.

I want to: Set up the IPv6 tunnel though my ISP doesn't provide me with the tunnel service.

How can I do that?

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
2. Go to [Advanced](#) > [Network](#) > [IPv6 Tunnel](#).
3. Enable [IPv6 Tunnel](#), and select [6to4](#) as the tunneling mechanism and select a WAN connection from the drop-down list, then click [Save](#).

Note:

If there is no available WAN connection to choose, make sure you have connected to the internet and the connection type is not Bridge.

Done! Now you can visit the IPv6 websites with the 6to4 tunnel.

Note:

If you still can't access IPv6 resources, it may mean that no 6to4 public server was found in your network. You can contact your ISP to sign up for IPv6 connection service.

13.5.2. Specify the 6rd Tunnel with Parameters Provided by Your ISP

I want to: Specify the 6rd tunnel with the parameters provided by my 6rd tunnel service provider.

How can I do that?

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
2. Go to [Advanced](#) > [Network](#) > [IPv6 Tunnel](#).
3. Enable [IPv6 Tunnel](#), and select [6rd](#) as the tunneling mechanism and select a WAN connection from the drop-down list.
4. According to the parameters provided by your ISP, choose [Auto](#) or [Manual](#). More parameters are needed if you choose [Manual](#).
5. Click [Save](#).

IPv6 Tunnel

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

IPv6 Tunnel: ☒ Enable

Tunneling Mechanism: 6rd

WAN Connection: ipoe_0_0_d

Configuration Type: ☐ Auto ☒ Manual

IPv4 Mask Length: 0

6rd Prefix: ::

6rd Prefix Length:

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

Save

Note:

If there is no available WAN connection to choose, make sure you have connected to the internet and the connection type is not Bridge.

Done!

Now you can visit the IPv6 websites with the 6rd tunnel.

Tips:

The ways to set up DS-Lite and Map-T tunnel are similar to that of 6rd tunnel. If you are provided with an IPv6-only WAN connection and have signed up for DS-Lite tunnel service, specify the DS-Lite tunnel by referring to the steps above.

13.6. Specify Wireless Settings

13.6.1. Change Basic Wireless Settings

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

Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.

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

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

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

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

■ **Note:**

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

➤ **To hide SSID:**

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

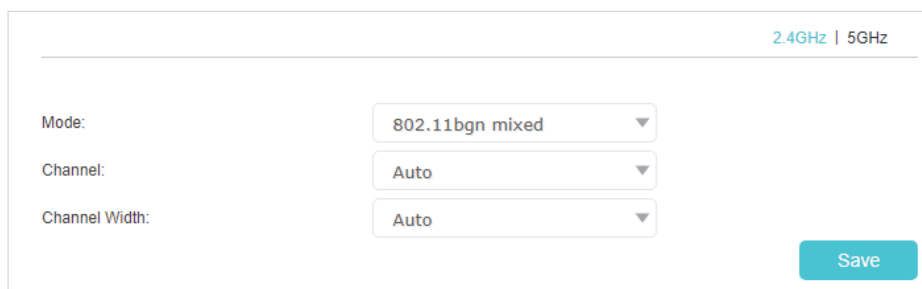
➤ **To enable or disable band steering:**

Band Steering allows each of the device's wireless bands to use the same wireless settings. The device can balance network demand and assign devices to the optimum band.

1. Go to [Advanced](#) > [Wireless](#) > [Wireless Settings](#).
2. Turn on or off the Band Steering.

➤ **To change the mode or channel:**

1. Go to [Advanced](#) > [Wireless](#) > [Wireless Settings](#), and select [2.4GHz](#) or [5GHz](#) you want to change.



The screenshot shows a web interface for configuring wireless settings. At the top right, there is a toggle for '2.4GHz | 5GHz'. Below this, there are three dropdown menus: 'Mode' set to '802.11bgn mixed', 'Channel' set to 'Auto', and 'Channel Width' set to 'Auto'. A blue 'Save' button is located at the bottom right of the settings area.

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

Mode: Select the desired transmission mode.

- 802.11n only: Select only if all of your wireless clients are 802.11n devices.
- 802.11gn mixed: Select if you are using both 802.11g and 802.11n wireless clients.
- 802.11bgn mixed: Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.

Note: When 802.11n only mode is selected, only 802.11n wireless stations can connect to the controller. It is strongly recommended that you select 802.11b/g/n mixed, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the controller.

- 802.11ac only (5GHz): Select only if all of your wireless clients are 802.11ac devices.
- 802.11ac/n mixed (5GHz): Select if you are using a mix of 802.11n and 802.11ac wireless clients.
- 802.11a/n/ac/mixed (5GHz): Select if you are using a mix of 802.11a, 802.11n, and 802.11 ac wireless clients. It is strongly recommended that you select this option.

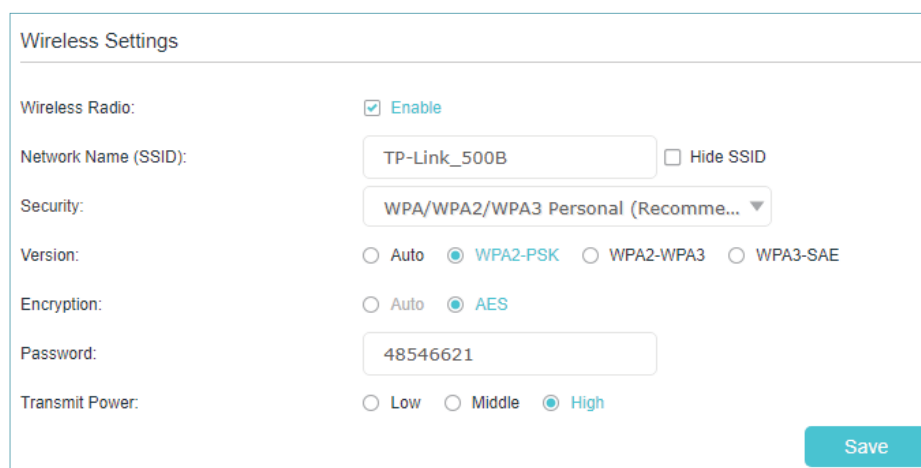
Channel: Select the channel you want to use from the drop-down list. This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

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

Note: These settings are available only when you turned off the Band Steering.

➤ **To change the security option:**

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



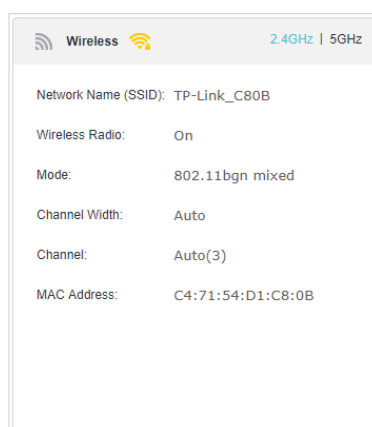
The image shows a 'Wireless Settings' configuration page. It includes fields for 'Wireless Radio' (checked 'Enable'), 'Network Name (SSID)' (TP-Link_500B), 'Security' (WPA/WPA2/WPA3 Personal), 'Version' (WPA2-PSK), 'Encryption' (AES), 'Password' (48546621), and 'Transmit Power' (High). A 'Save' button is at the bottom right.

2. Select an option from the **Security** drop-down list and configure the related parameters. The router provides three options, No Security, WPA/WPA2/WPA3 personal (Recommended), and WPA/WPA2 enterprise. WPA3 is the latest standard and the security level is the highest. We recommend you don't change the default settings unless necessary.
3. Click **Save** to make the settings effective.

13.6.2. View Wireless Information

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

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



The image shows the 'Wireless' status panel with the following details:

Wireless	
Network Name (SSID):	TP-Link_C80B
Wireless Radio:	On
Mode:	802.11bgn mixed
Channel Width:	Auto
Channel:	Auto(3)
MAC Address:	C4:71:54:D1:C8:0B

💡 **Tips:** You can also see the wireless details by clicking the **Online Devices** icon on **Basic** > **Network Map**.

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

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

2. Go to [Advanced](#) > [Wireless](#) > [Statistics](#) page.
3. You can view the detailed information of the wireless clients, including its connection type and security option as well as the packets transmitted.

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

13.6.3. Advanced Wireless Settings

Advanced wireless settings are for those who want more network controls. If you are not familiar with the settings on this page, it's strongly recommended that you keep the provided default values; otherwise it may result in lower wireless network performance.

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

Advanced Settings		2.4GHz 5GHz
Beacon Interval:	100	(25-1000)
RTS Threshold:	2346	(1-2346)
DTIM Interval:	1	(1-255)
Group Key Update Period:	3600	seconds
WMM:	☒ Enable	
Short GI:	☒ Enable	
AP Isolation:	☐ Enable	
AirTime Fairness:	☐ Enable	
		<button>Save</button>

- **Beacon Interval:** Enter a value between 100 and 1000 in milliseconds to determine the duration between which beacon packets are broadcast by the router to synchronize the wireless network. The default 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 sends Request to Send frames to a particular receiving station and negotiates the sending of a data frame, or else the packet will be sent immediately.
- **DTIM Interval:** Enter a value between 1 and 255 to determine the interval of the Delivery Traffic Indication Message (DTIM). 1 indicates the DTIM Interval is the same as [Beacon Interval](#).
- **Group Key Update Period:** Enter the number of seconds to control the time interval for the encryption key automatic renewal. The default is 0, indicating no key renewal.

- **WMM:** This feature guarantees the packets with high-priority messages being transmitted preferentially. WMM is enabled compulsively under 802.11n or 802.11ac mode.
- **Short GI:** This feature is enabled by default and recommended to increase the data capacity by reducing the Guard Interval (GI) time.
- **AP Isolation:** Select this check box to enable the AP Isolation feature that allows you to confine and restrict all wireless devices on your network from interacting with each other, but still able to access the internet. AP isolation is disabled by default.
- **AirTime Fairness:** Enable this feature when you want to sacrifice some of the networking time from the slow devices, so that your faster devices can achieve better quality of service.
- **Fast Roaming (802.11r):** Select the Enable check box to enable the Fast Roaming(802.11r) feature that wireless clients reconnect fast in EasyMesh network. When EasyMesh disabled, this function will not take effect.

13.7. Use WPS for Wireless Connection

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

Method 1: Use the WPS button

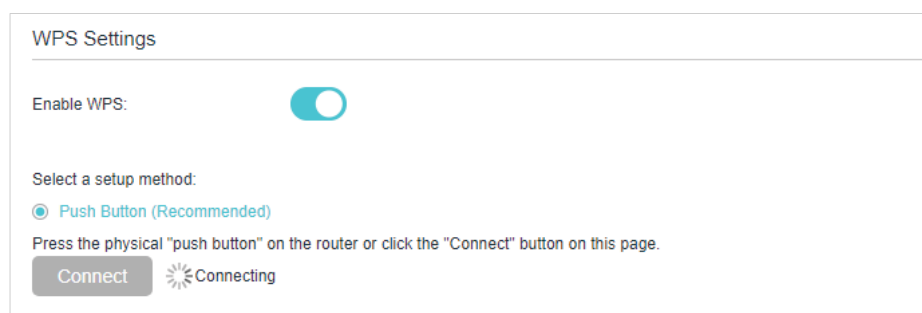
Use this method if your client device has a WPS button.

1. Press the WPS button of the controller.
2. Press the WPS button of the client device directly.
3. The status LED will flash blue fast for about 2 minutes during the WPS process.

Method 2: Use the WPS button on the web management page

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
2. Go to **Advanced > Wireless > WPS**, and locate the **WPS Settings** section.

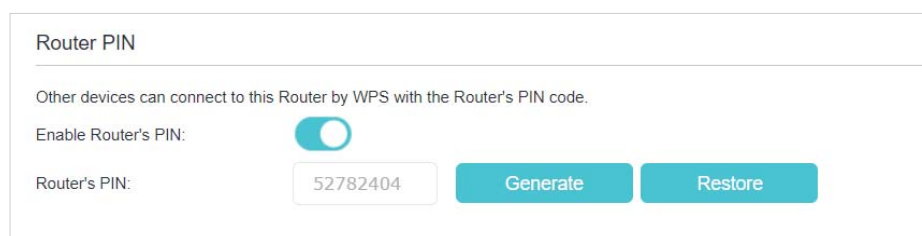


3. Make sure the **Enable WPS** is turned on, and then click **Connect**.
4. Press the WPS button of the client device directly.
5. The status LED may flash blue fast for about 2 minutes during the WPS process.
6. **Connect successfully** will appear after the Connect button, which means the client device has successfully connected to the controller.

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

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
2. Go to **Advanced > Wireless > WPS**, locate the **Router PIN** section and select **2.4GHz** or **5GHz** according to your needs.



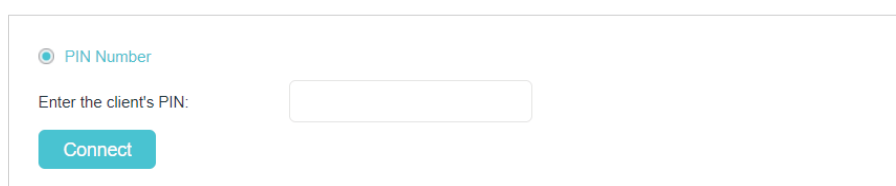
3. Make sure the **Enable Router's PIN** is turned on, and take a note of the current PIN of the controller. You can also click the **Generate** button to get a new PIN.
4. On the client device, enter the controller's PIN. (The default PIN is also printed on the label of the controller.)
5. The status LED may flash blue fast for about 2 minutes during the WPS process.

Note:

The WPS function cannot be configured if the wireless function of the controller is disabled. Please make sure the wireless function is enabled before configuring the WPS.

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
2. Go to **Advanced > Wireless > WPS**, locate the **WPS Settings** section and select **2.4GHz** or **5GHz** according to your needs.
3. Make sure the **Enable WPS** is turned on, and then select **PIN Number**.



4. Enter the client device's PIN, and then click the **Connect** button.

5. **Connect successfully** will appear after the Connect button, which means the client device has successfully connected to the controller.

Chapter 14

Manage Your Controller

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

It contains the following sections:

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

14. 1. Set System Time

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

Follow the steps below to set your system time.

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

System Time

Time Zone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon

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

Time: 7 : 23 : 19

NTP Server I: 0.0.0.0 (Optional)

NTP Server II: 0.0.0.0 (Optional)

Get from PC Get from the Internet Save

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

Daylight Saving Time

Daylight Saving Time: ☒ Enable Daylight Saving Time

Start: 2016 Mar M Last W Sun T 02:00

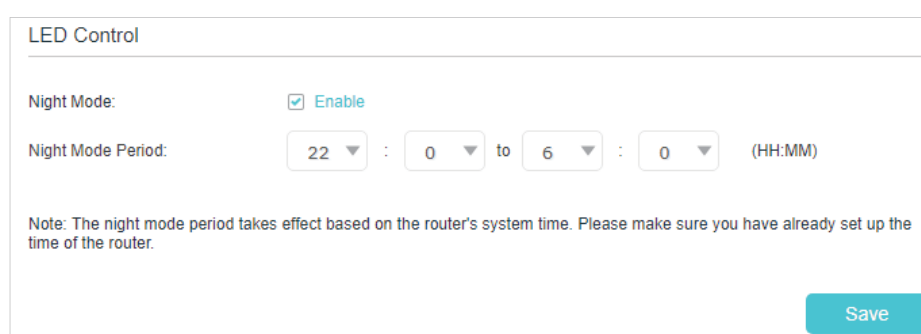
End: 2016 Oct M Last W Sun T 03:00

Save

14.2. Control LED

The controller LED indicates controller activities and behaviors. You can turn on or turn off the controller from the management web-page.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
2. Go to [Advanced](#) > [System Tools](#) > [LED Control](#), and enable [Night Mode](#).
3. Specify the [Night Mode Period](#) according to your need, and the LEDs will be off during this period.
4. Click [Save](#) to make the settings effective.

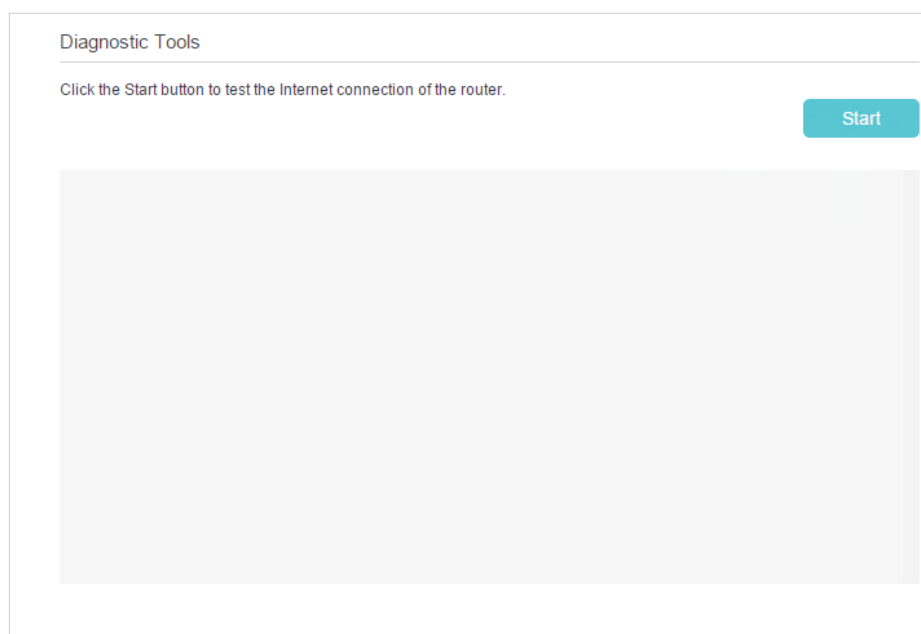


The screenshot shows the 'LED Control' configuration page. It has a title bar 'LED Control'. Below it, 'Night Mode' is checked and labeled 'Enable'. 'Night Mode Period' is set to '22 : 0' to '6 : 0' with a '(HH:MM)' label. A note states: 'Note: The night mode period takes effect based on the router's system time. Please make sure you have already set up the time of the router.' A 'Save' button is at the bottom right.

14.3. Test Internet Connectivity

Diagnostics is used to test the connectivity between the controller and the host or other network devices.

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



3. Click [Start](#) to test the internet connectivity and you will find the test results in the gray box.

14. 4. Update the Firmware

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

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

Note:

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

You can follow the steps below to manually update the firmware.

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

Satellite Version List					
ID	Device Name	Firmware Version	Hardware Version	Status	Synced
1	HX220-G2W	2.0.0.0.9	HX220-G2W v1 00000000	Online	Yes
2	HX220-G2W	2.0.0.0.9	HX220-G2W v1 00000000	Online	Yes

[Upgrade](#)

Note:

The upgrading will also take effect on the synced online satellites. We recommend that you keep the controller and its satellites in the same firmware version. Please do not turn off the controller and its satellites during the firmware upgrading process.

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

14.5. Back Up and Restore Configuration Settings

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

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

➤ **To back up configuration settings:**

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

➤ **To restore configuration settings:**

1. Click [Browse](#) to locate the backup configuration file stored on your computer, and click [Restore](#)

Restore

Restore previous settings from a saved file.

File:

[Browse](#)

[Restore](#)

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

➤ **To reset the controller to factory default settings:**

1. Click [Factory Restore](#) to reset the controller.

Factory Default Restore

Restore all the configuration settings to their default values.

Factory Restore

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

Note:

1. During the resetting process, do not turn off the controller.
2. We strongly recommend you back up the current configuration settings before resetting the controller.
3. If you want to reset the controller into its factory default settings, you need to add the agent again to create a mesh Wi-Fi system.

14.6. Reboot the Controller

The reboot feature cleans the cache to enhance the running performance of the controller. You can schedule the controller to reboot regularly.

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
2. Go to **Advanced > System Tools > Reboot Schedule**, and enable **Auto Reboot**.
3. Specify the **Time** when the controller reboots and the **Auto Reboot Interval** to decide how often it reboots.

Auto Reboot

Auto Reboot: ☒

Time: 03 : 00 (HH:MM)

Auto Reboot Interval: ☒ Three Days ☐ One Week ☐ Thirty Days

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

Save

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

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

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Operation Mode.
- Change the Web Management Port.
- Upgrade the firmware of the controller (system will reboot automatically).
- Restore the controller to its factory defaults (system will reboot automatically).

- Update the configuration with the file (system will reboot automatically).

Note:

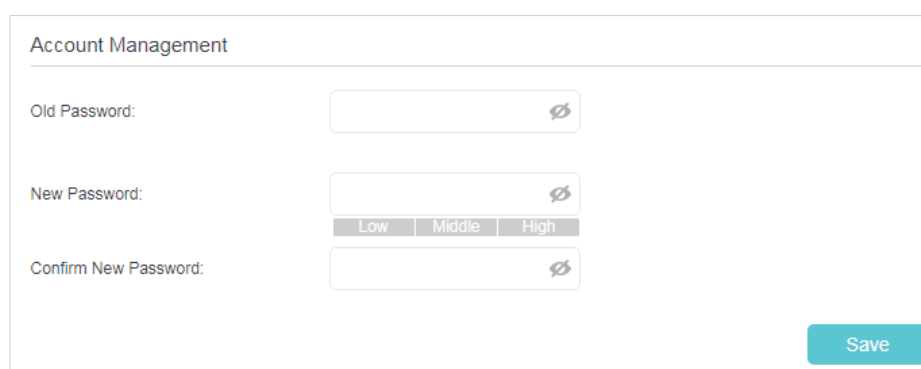
The Auto Reboot feature takes effect based on the controller's system time. Please make sure you have already set the time of the controller.

14.7. Administration Management

14.7.1. Change the Login Password

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
2. Go to **Advanced > System Tools > Administration** page. Locate the **Account Management** section.



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

3. Enter the old password, then a new password twice (both case-sensitive).
4. Click **Save** to make the settings effective.
5. Use the new password for future logins.

14.7.2. Local Management

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

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
2. Go to **Advanced > System Tools > Administration**, and locate the **Local Management** section.

3. Enable **Management over HTTPS** and keep the **Port for HTTP** and **Port for HTTPS** as the default settings. Enter the **IP address** or **MAC address** of the local device to manage the controller.



Local Management

Port for HTTP: 80

Local Management via HTTPS: ☒ Enable

Port for HTTPS: 443

IP/MAC Address: 192.168.0.100

Save

4. Click **Save**.

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

Note:

If you want all local devices can manage the controller, just leave the **IP/MAC Address** field blank.

14.7.3. Remote Management

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

Note:

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

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
2. Go to **Advanced** > **System Tools** > **Administration**, and locate the **Remote Management** section.

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

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

Tips:

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

2. The controller'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 controller through a domain name.

14.7.4. ICMP Ping

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

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

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

- Go to [Advanced](#) > [System Tools](#) > [Administration](#), and locate the [ICMP Ping](#) section.

ICMP Ping

ICMP Ping:

☐ Remote
 ☒ Local

Save

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

14.8. System Log

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

- Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
- Go to [Advanced](#) > [System Tools](#) > [System Log](#) page.

System Log

Type:

ALL

Level:

Notice

Refresh

Delete All

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

Log Settings

Save Log

➤ To view the system logs:

You can view specific system logs by selecting the log type and level.
Click [Refresh](#) to refresh the log list.

➤ To save the system logs:

You can save the system logs to your local computer or a remote server.
Click [Save Log](#) to save the logs in a txt file to your computer.

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

Log Settings

☒ Save Locally

Minimum Level: Information

☒ Save Remotely

Minimum Level: Warning

Server IP: 192.168.1.100

Server Port: 514

Local Facility Name: User

Back Save

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

14.9. CWMP Settings

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

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

CWMP Settings

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

CWMP:

Inform:

Inform DataModel with TR098:

Inform Interval:

300

ACS URL:

ACS Username:

admin

ACS Password:

.....

Interface used by TR-069 client:

Any WAN

☒ Connection Request Authentication

Username:

admin

Password:

.....

Path:

/tr069

Port:

7547

URL:

STUN:

Get RPC Methods

Save

- **CWMP:** Enable or disable the CWMP (CPE WAN Management Protocol) function.
- **Inform:** Enable or disable the function of sending an inform message to the ACS (Auto Configuration Server) periodically.
- **Inform DataModel with TR098:** Enable or disable the function of sending inform complying with the data model defined in TR-098.
- **Inform Interval:** Set the time interval in seconds when the Inform message will be sent to the ACS.
- **ACS URL:** Enter the web address of the ACS which is provided by your ISP.
- **ACS Username/Password:** Enter the username/password to log in to the ACS server.
- **Interface used by TR-069 client:** Select which interface to be used by the TR-069 client.
- **Connection Request Authentication:** Select this check box to enable authentication for the connection request.
- **Username/Password:** Enter the username/password for the ACS server to log in to the controller.

- **Path:** Enter the path for the ACS server to log in to the controller.
- **Port:** Enter the port that connects to the ACS server.
- **URL:** Enter the URL that connects to the ACS server.
- **STUN:** Enable or disable the STUN(Simple Traversal of UDP through NAT) function.
- **STUN Server Address/Port:** Enter the STUN server address and port number provided by your ISP.
- **STUN Username/Password:** Enter the username/password to log in to the STUN server.
- **Minimum/Maximum Keep Alive Period:** Enter the minimum/maximum time for maintaining NAT binding.
- **Get RPC Methods:** Click to get the methods to support CWMP.

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

14. 10. SNMP Settings

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

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

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

SNMP Settings

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

Enable SNMP Agent: ☒

SNMP Agent for WAN: ☐

Read-only Community:

Write Community:

System Name:

System Description:

System Location:

System Contact:

Trap Manager IP:

Save

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

You are suggested to keep the default settings. Click **Save** to make the settings effective.

14. 11. Monitor the Internet Traffic Statistics

The Traffic Statistics page displays the network traffic of the LAN, WAN and WLAN sent and received packets, allowing you to monitor the volume of internet traffic statistics.

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

Traffic Statistics

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

Statistics Interval: seconds

[Save](#)

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

Traffic Statistics List								
Refresh Reset All Delete All								
IP Address/ MAC Address	Total Packets	Total Bytes	Current Packets	Current Bytes	Current ICMP Tx	Current UDP Tx	Current SYN Tx	Modify
--	--	--	--	--	--	--	--	--

FAQ

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

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

1. Connect your computer to the controller using an Ethernet cable.
2. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
3. Go to **Basic** > **Wireless** to retrieve or reset your wireless password.

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

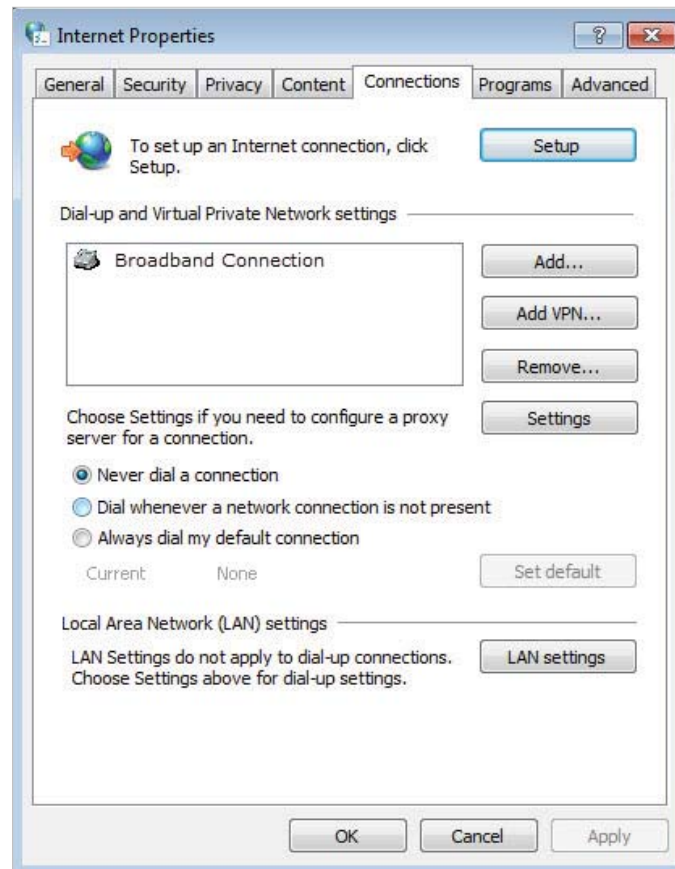
- Press and hold the RESET button on the bottom of the controller for about 5 seconds, and then visit <http://tplinkwifi.net> to create a new login password.

 **Note:** You'll need to reconfigure the controller to surf the internet once the controller is reset, and please mark down your new password for future use.

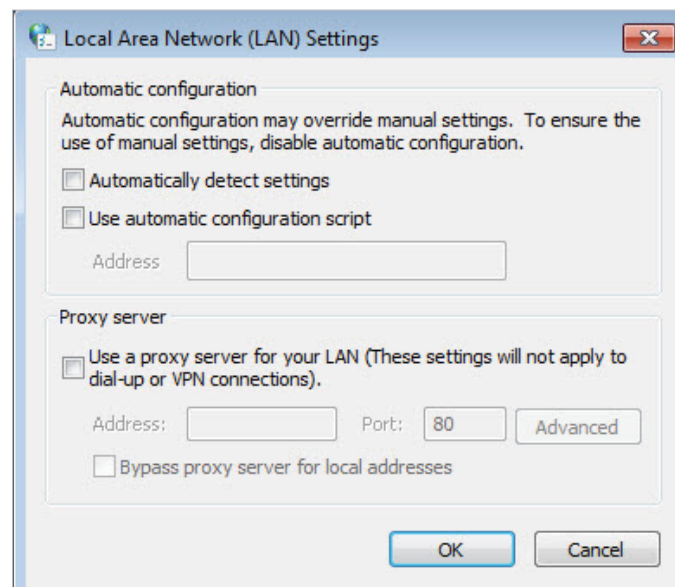
Q3. What should I do if I cannot log in to the controller's web management page?

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

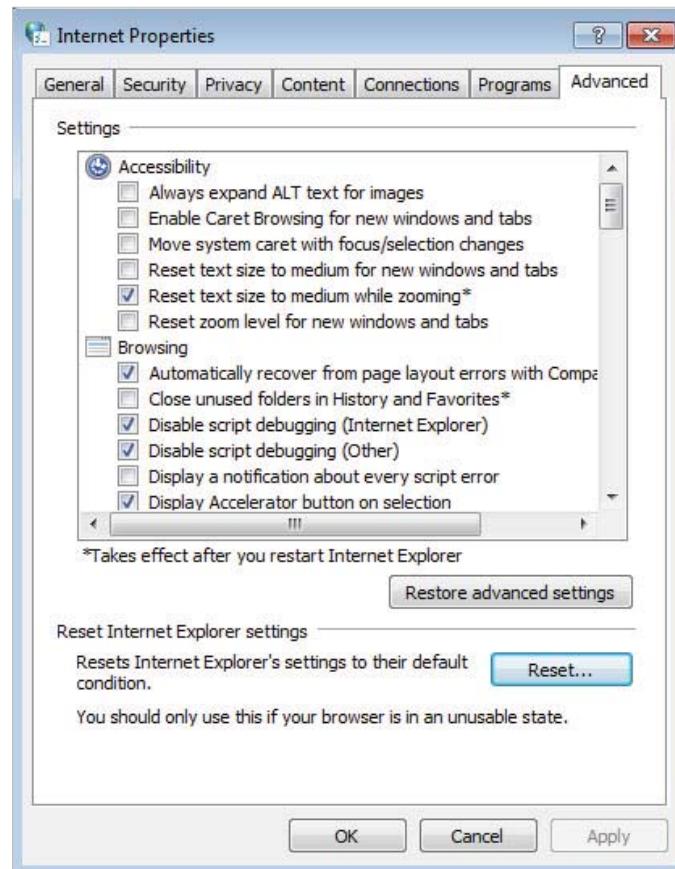
- Make sure your computer is connected to the controller correctly and the corresponding LED indicator(s) light up.
- Make sure the IP address of your computer is configured as **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
- Make sure <http://tplinkwifi.net> 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 clear 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 controller to factory default settings and try again. If login still fails, please contact the technical support.

Note: You'll need to reconfigure the controller to access the internet once the controller is reset.

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
2. Go to **Advanced** > **Status** to check internet status:

As the following image shows, if IP Address is a valid one, please try the methods below:

Internet ✕ IPv4 | IPv6

MAC Address:	50-C7-BF-02-EA-DD
IP Address:	58.61.172.101
Subnet Mask:	255.255.255.255
Default Gateway:	58.61.172.1
Primary DNS:	202.96.134.33
Secondary DNS:	202.96.128.86
Connection Type:	PPPoE

- Your computer might not recognize any DNS server addresses. Please manually configure the DNS server.

- 1) Go to [Advanced](#) > [Network](#) > [LAN Settings](#), and locate the [DHCP](#) section.
- 2) Enter 8.8.8.8 as Primary DNS, click [Save](#).

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

DHCP: ☒ [Enable](#)

☒ [DHCP Server](#) ☐ DHCP Relay

IP Address Pool: 192 . 168 . 0 . 100 - 192 . 168 . 0 . 199

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

Default Gateway: 192 . 168 . 0 . 1 (Optional)

Default Domain: (Optional)

Primary DNS: 8 . 8 . 8 . 8 (Optional)

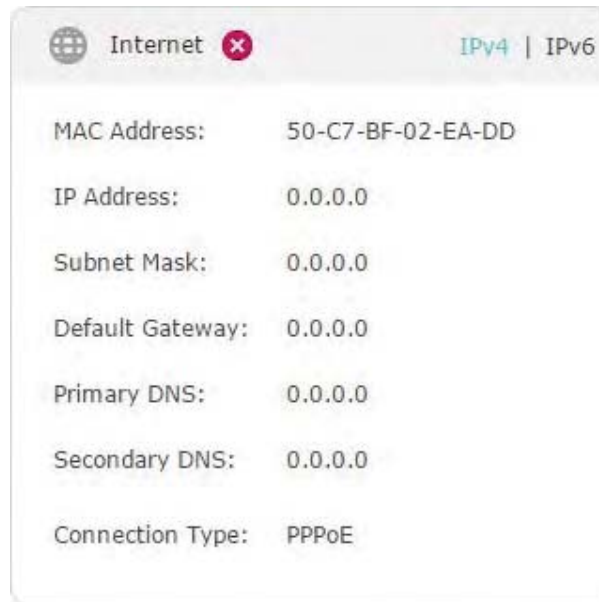
Secondary DNS: 0 . 0 . 0 . 0 (Optional)

[Save](#)

- Restart the modem and the controller.
 - 1) Power off your modem and controller, 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 controller.
 - 4) Wait another 1 or 2 minutes and check the internet access.
- Reset the controller to factory default settings and reconfigure the controller.
- Upgrade the firmware of the controller.

- Check the TCP/IP settings on the particular device if all other devices can get internet from the controller.

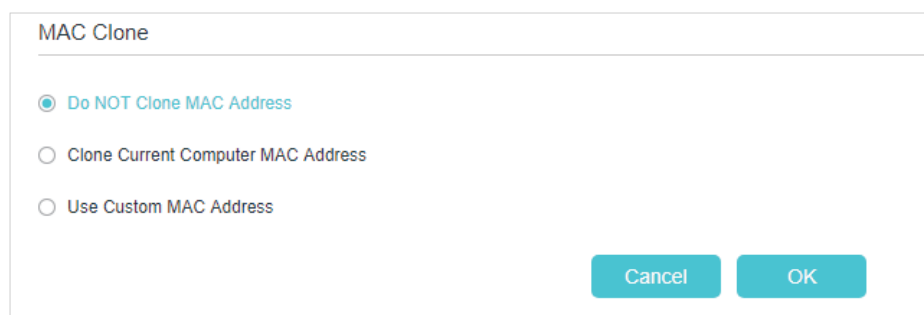
As the following image shows, if the IP Address is 0.0.0.0, please try the methods below:



The screenshot shows a window titled "Internet" with a red "x" icon. It has tabs for "IPv4" and "IPv6". The configuration is as follows:

MAC Address:	50-C7-BF-02-EA-DD
IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Default Gateway:	0.0.0.0
Primary DNS:	0.0.0.0
Secondary DNS:	0.0.0.0
Connection Type:	PPPoE

- Make sure the physical connection between the controller and the modem is proper.
- Clone the MAC address of your computer.
 - 1) Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
 - 2) Go to **Advanced** > **Network** > **Internet** and click the edit icon to find the **MAC Clone** section.
 - 3) Choose an option as needed (enter the MAC address if **Use Custom MAC Address** is selected), and click **OK**.



The screenshot shows a "MAC Clone" dialog box with three radio button options:

- ☒ Do NOT Clone MAC Address
- ☐ Clone Current Computer MAC Address
- ☐ Use Custom MAC Address

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

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 controller into your network to share your internet connection, the ISP will not accept it as the MAC address is changed, so you need to clone your computer's MAC address to the controller.

- The MAC addresses of a computer in wired connection and wireless connection are different.

- **Modify the LAN IP address of the controller.**

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, you 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 the password you set for the controller.
- 2) Go to **Advanced > Network > LAN Settings**, and locate the **DHCP** section.
- 3) Modify the LAN IP address as the following image shows. Here we take 192.168.2.1 as an example.
- 4) Click **Save** to make the settings effective.

MAC Address:	00:0A:EB:12:BB:A1
IP Address:	192 . 168 . 2 . 1
Subnet Mask:	255.255.255.0 ▼

- **Restart the modem and the controller.**
 - 1) Power off your modem and controller, 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 controller.
 - 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 the password you set for the controller.
 - 3) Go to **Basic > Internet**.
 - 4) Select your **Internet Connection Type** and enter other parameters if required.
 - 5) Click **Save**.

Internet Connection Setup

VLAN ID: ☐ Enable

Internet Connection Type: Dynamic IP ▼

- PPPoE
- Dynamic IP
- Static IP
- PPTP
- L2TP

Save

6) Restart the modem and the controller again.

- Please upgrade the firmware of the controller.

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 cannot find my wireless network or I cannot connect the wireless network?

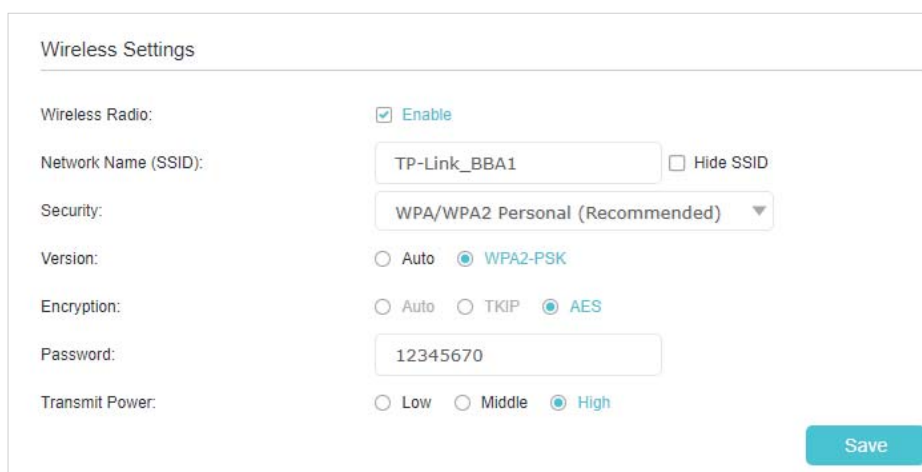
If you fail to find any wireless network, please follow the steps below:

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



The image shows a 'Wireless Settings' configuration window. It includes fields for 'Wireless Radio' (checked 'Enable'), 'Network Name (SSID)' (TP-Link_BBA1), 'Security' (WPA/WPA2 Personal (Recommended)), 'Version' (WPA2-PSK), 'Encryption' (AES), 'Password' (12345670), and 'Transmit Power' (High). There is a 'Save' button at the bottom right.

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 controller.

 **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 controller closer and try again.
 - Change the wireless Channel of the controller to 1, 6 or 11 to reduce interference from other networks.
 - Re-install or update the driver for your wireless adapter of the computer.

Q6. What should I do if the agent's status LED remains flashing red?

- Place the agent close to the controller until the status LED turns solid blue or white, then relocate the agent.
- Reset the agent and try to synchronize the agent with the mesh controller again.

FCC compliance information statement



Product Name: AX1800 Whole Home Mesh Wi-Fi AP

Model Number: HX220-G5/HX220

Component Name	Model	FCC ID
I.T.E. Power	T120100-2B1	2AXJ4HX220

Responsible party:

TP-Link USA Corporation

Address: 10 Mauchly, Irvine, CA 92618

Website: <https://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 20 cm from all persons and must not be colocated or operating in conjunction with any other antenna or transmitter."

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

Issue Date: 2021.10.14

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)

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

Attention: This device may only be used indoors in all EU member states, EFTA countries and Northern Ireland.

Attention: This device may only be used indoors in all EU member states, EFTA countries and Northern Ireland.

	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



UKCA declaration of conformity

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

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

National restrictions

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



Canadian Compliance Statement

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

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

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

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

Caution:

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

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

Avertissement:

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

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

Radiation Exposure Statement:

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

Déclaration d'exposition aux radiations:

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

Industry Canada Statement

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

Korea Warning Statements:

당해 무선설비는 운용중 전파혼신 가능성이 있음.

NCC Notice:

注意！

依據 低功率電波輻射性電機管理辦法

LP0002 低功率射頻器材技術規範_章節 3.8.2

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。

BSMI Notice

安全諮詢及注意事項

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

- 不要私自拆開機殼或自行維修，如產品有故障請與原廠或代理商聯繫。

設備名稱：		型號（型式）：				
Equipment name		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	—	○	○	○	○	○
電源線	○	○	○	○	○	○
網線	○	○	○	○	○	○
其他及 其配件	—	○	○	○	○	○

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



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



Safety Information

- Keep the device away from water, fire, humidity or hot environments.
- Do not attempt to disassemble, repair, or modify the device. If you need service, please contact us.
- Do not use damaged charger or USB cable to charge the device.
- Do not use any other chargers than those recommended.
- Do not use the device where wireless devices are not allowed.
- Adapter shall be installed near the equipment and shall be easily accessible.
- Use only power supplies which are provided by manufacturer and in the original packing of this product. If you have any questions, please don't hesitate to contact us.

Operating Temperature: 0°C~ 40°C (32°F~ 104°F)

Storage Temperature: -40°C~ 70°C (-40°F~ 158°F)

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

Explanations of the symbols on the product label

Symbol	Explanation
	DC voltage
	Indoor use only
	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.
	Alternating current
	Class II equipment
	Caution
	Operator's manual
	Polarity of d.c. power connector