



User Guide

AC1200 Whole Home Mesh Wi-Fi AP
HC220-G5

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](#) 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:

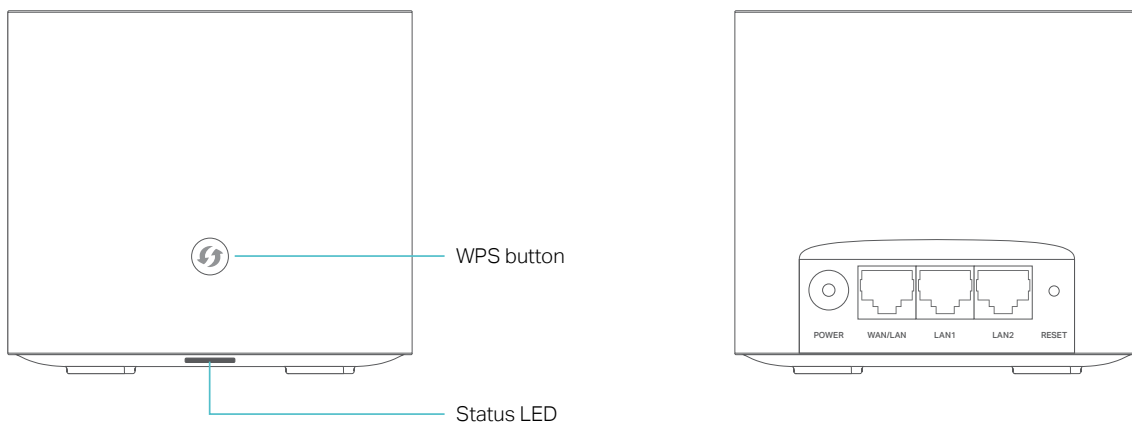
- [Product Overview](#)
- [Appearance](#)

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

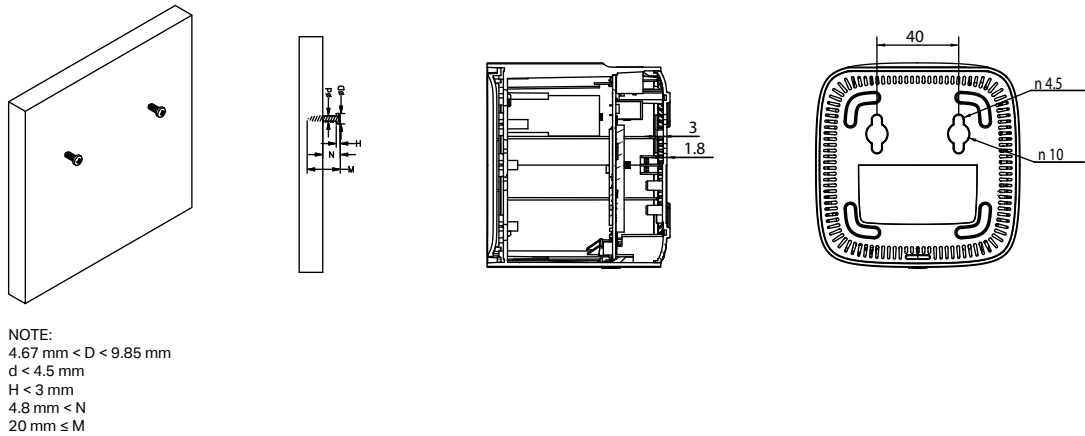
This chapter contains the following sections:

- [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.

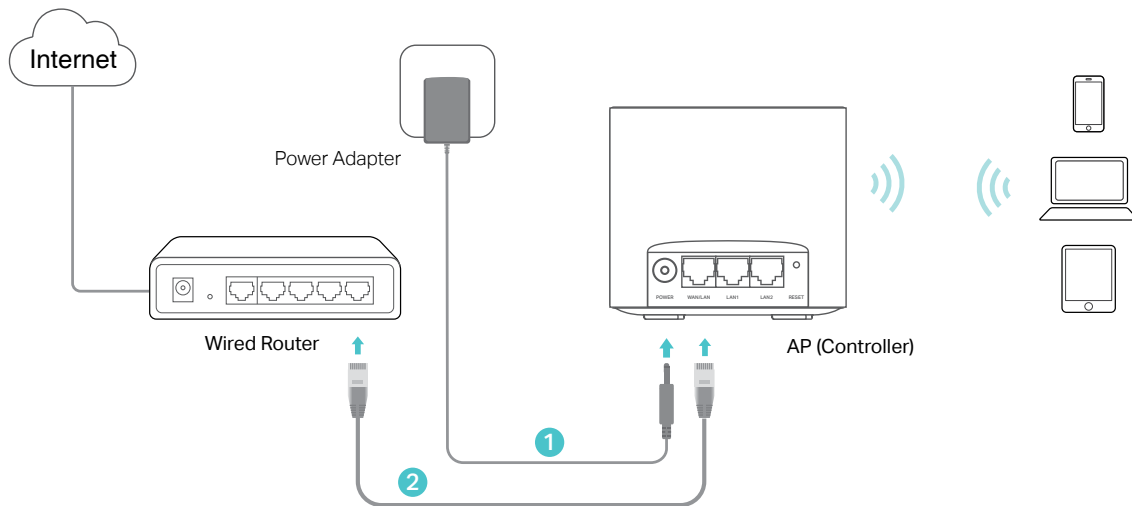
2.2. Connect Your Device

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.

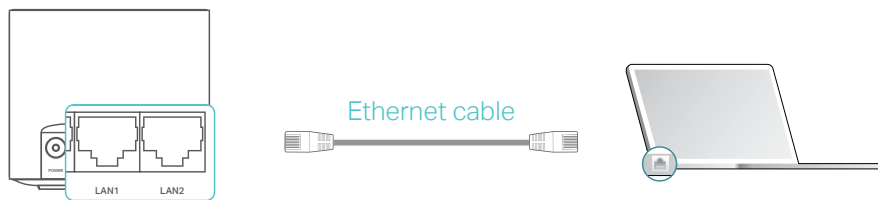
Follow the steps below to connect your device.



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.

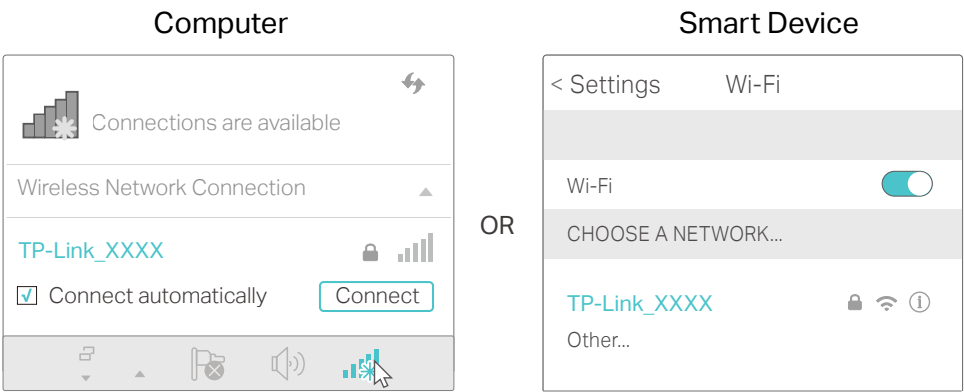
- **Method 1: Wired**

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

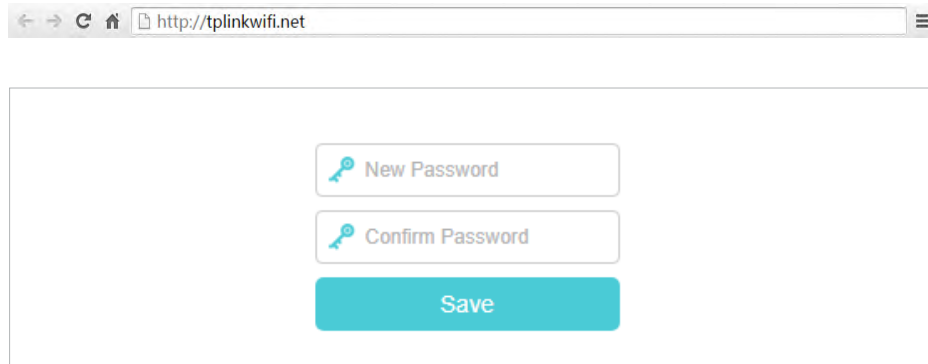
Log In to Your Device

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.

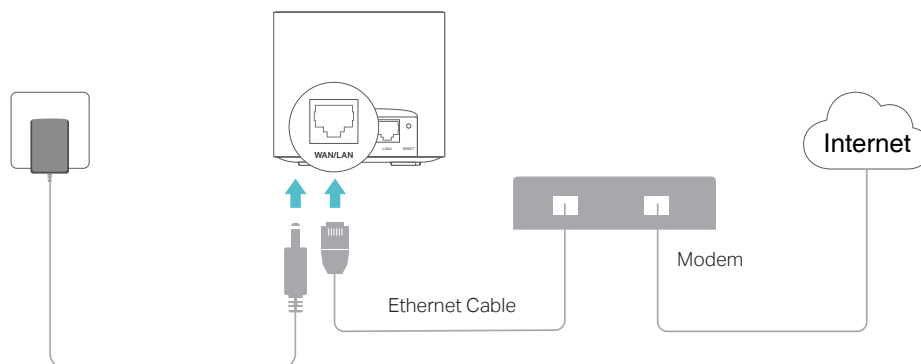
4.2. Configure the Device in Router Mode

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.

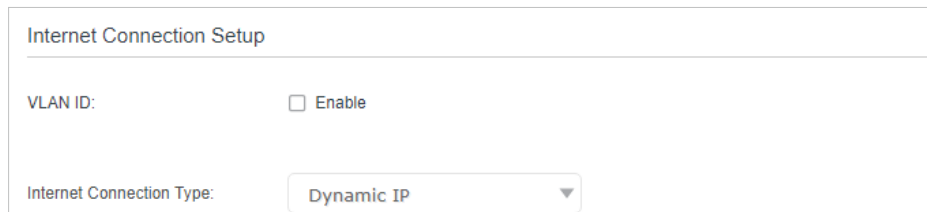
Now, you can set up your network and surf the internet.

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.



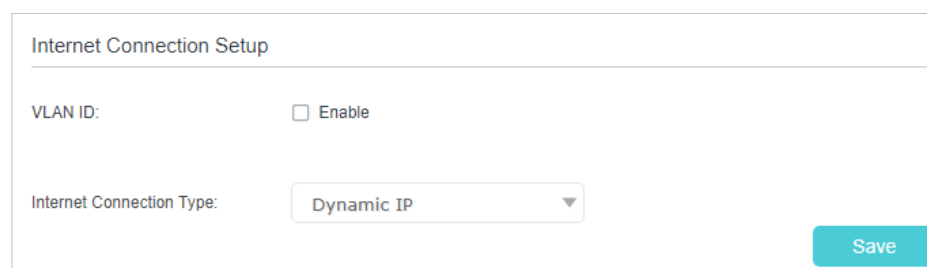
The screenshot shows the 'Internet Connection Setup' page. It has a title bar 'Internet Connection Setup'. Below it, there is a 'VLAN ID' field with an 'Enable' checkbox. Further down, there is an 'Internet Connection Type' dropdown menu currently set to 'Dynamic IP'.

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.

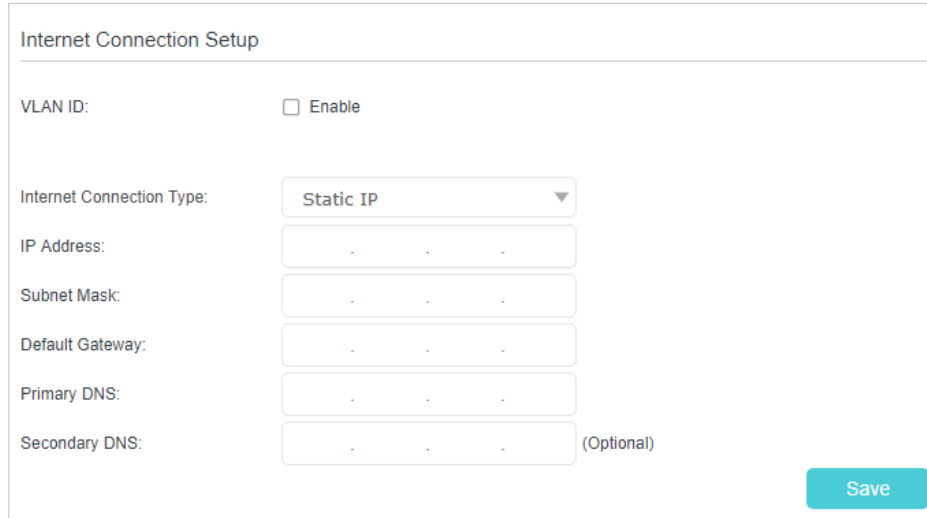
4. Follow the instructions on the page to continue the configuration. Parameters on the images are used for demonstration only.

- 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.



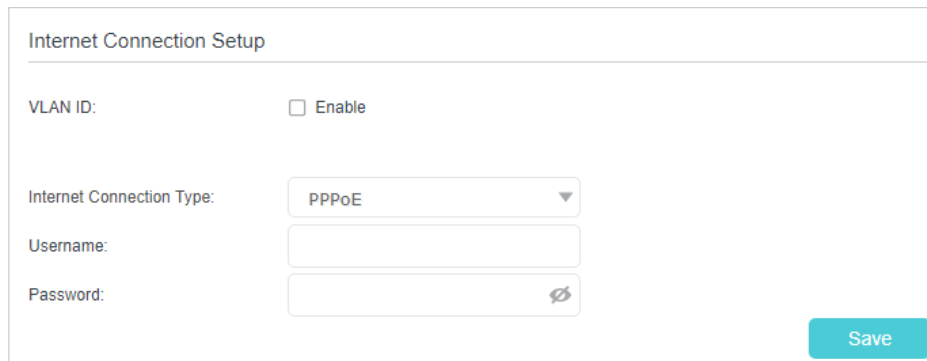
This screenshot is identical to the previous one, showing the 'Internet Connection Setup' page with 'VLAN ID' and 'Internet Connection Type' (Dynamic IP) settings. A teal 'Save' button is visible in the bottom right corner of the form area.

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



The screenshot shows the 'Internet Connection Setup' form. At the top, there is a 'VLAN ID' section with an 'Enable' checkbox. Below this, the 'Internet Connection Type' is set to 'Static IP' in a dropdown menu. The form includes input fields for 'IP Address', 'Subnet Mask', 'Default Gateway', 'Primary DNS', and 'Secondary DNS' (marked as optional). Each of these fields is represented by a box containing three dashes ('-'). A '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 screenshot shows the 'Internet Connection Setup' form. At the top, there is a 'VLAN ID' section with an 'Enable' checkbox. Below this, the 'Internet Connection Type' is set to 'PPPoE' in a dropdown menu. The form includes input fields for 'Username' and 'Password'. The 'Password' field has a toggle icon (an eye with a slash) to the right of it. A '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' field 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' field 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	Edit Delete

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**

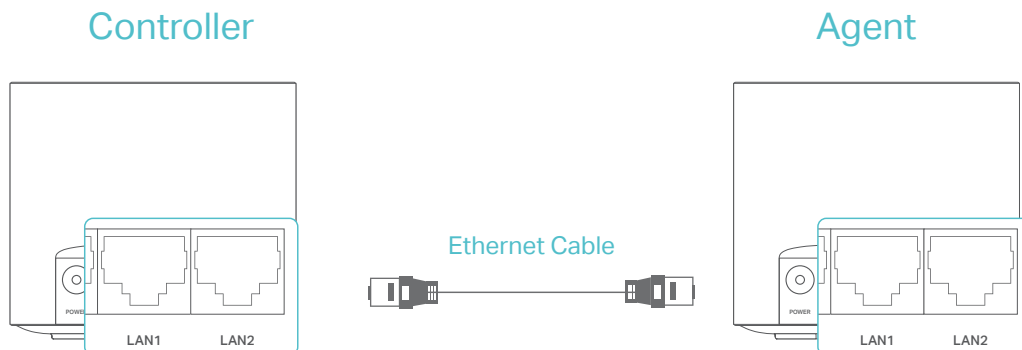
1. Place the agent close to the controller and power it on, wait about two minutes until the status LED turns to flashing blue.
2. Press the WPS button on the controller or the agent in your mesh Wi-Fi system, and within two minutes, press the WPS button on your new agent.



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.

The screenshot shows the 'Multi-SSID' configuration page. It has a title 'Multi-SSID' at the top. Below it, there are three sections for configuring different SSIDs. The first section, 'MSSID1:', has an 'Enable' checkbox checked. Below this, there is a 'Network Name (SSID):' field with the text 'TP-Link_500B_1' and a 'Hide SSID' checkbox. Below that is a 'Security:' dropdown menu with 'No Security' selected. The second section, 'MSSID2:', has an 'Enable' checkbox unchecked. The third section, 'MSSID3:', also has an 'Enable' checkbox unchecked. At the bottom right of the form is a 'Save' button.

- 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.

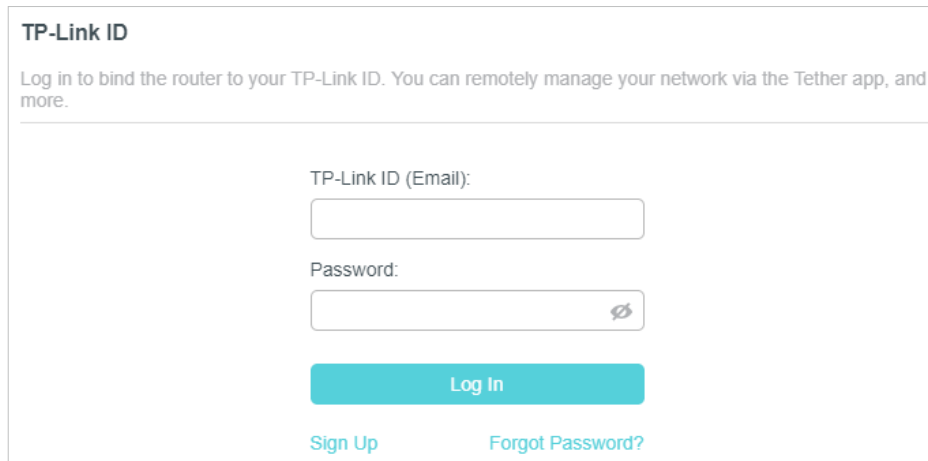
It contains the following sections:

- [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.

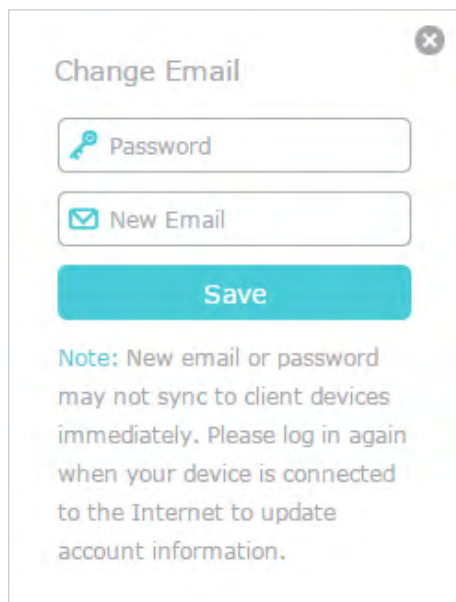
7.2. Change Your TP-Link ID Information

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:**

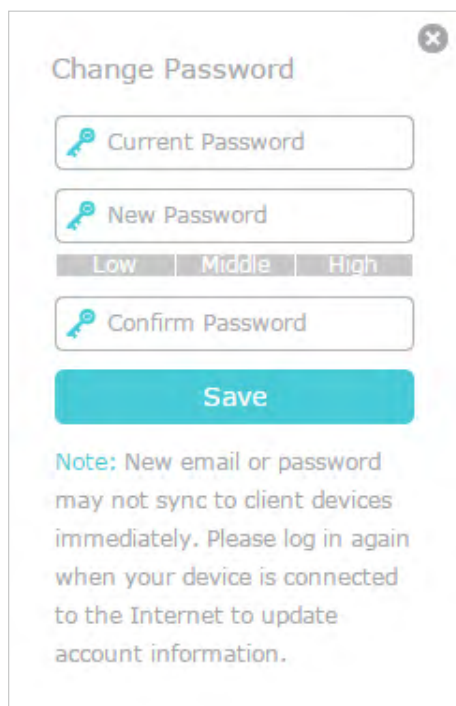
1. Click  behind the Email.
2. Enter the password of your TP-Link ID, then a new email address. And click [SAVE](#).



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

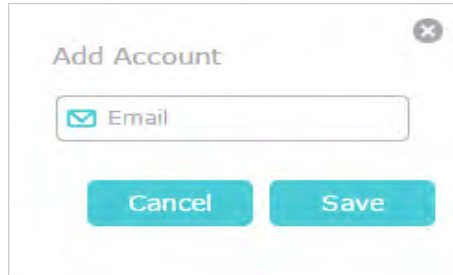
from the same router as **Users**. All accounts can monitor and manage the router locally or remotely, but user accounts cannot:

- 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". It contains a text input field with a blue envelope icon and the placeholder text "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	2020-01-01	Admin		
☐	2	user@tplink.com	2020-01-01	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	example_email@domain.com	2020-01-01	Admin
☒	2	example_email@domain.com	2020-01-01	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.

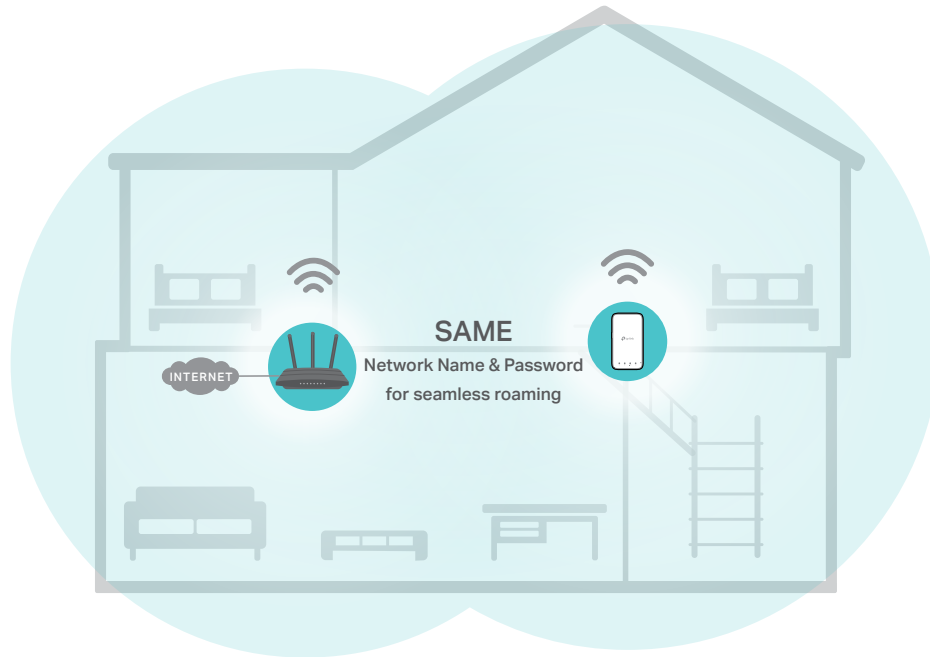
Note: If you need to remotely access your router from your smart devices, you need to:

- 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.

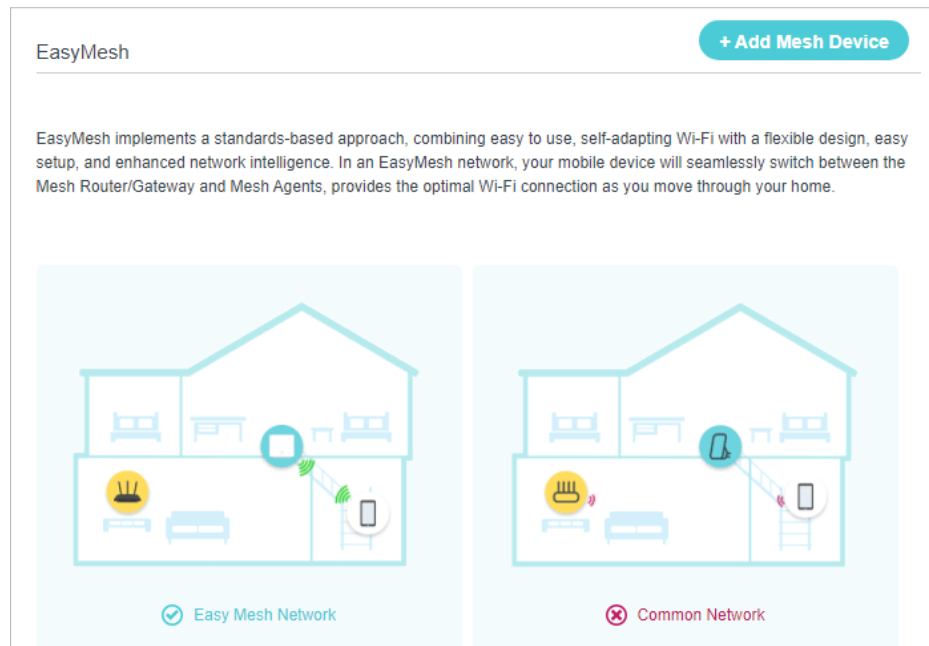


Easy Setup and Management

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?

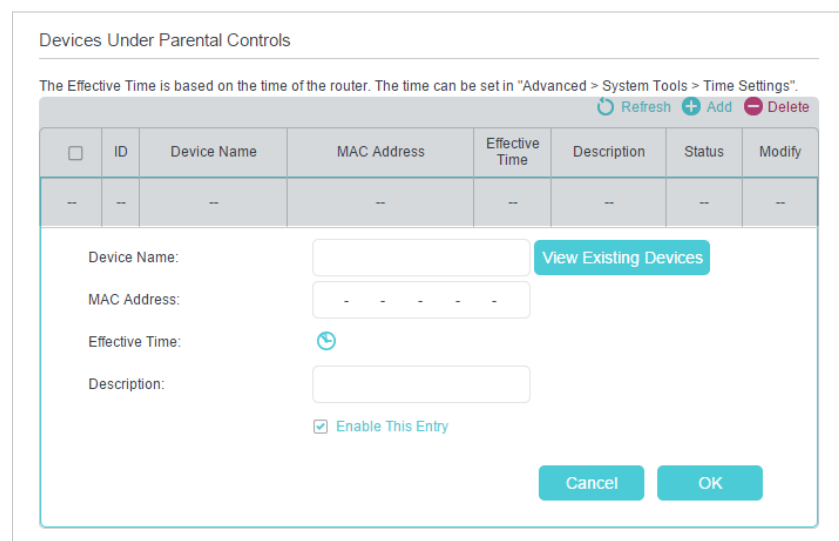
1. Visit <http://tplinkwifi.net>, and log in with the password you set for the controller.
2. Go to [Basic](#) or [Advanced](#) > [Parental Controls](#) and enable [Parental Controls](#).



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

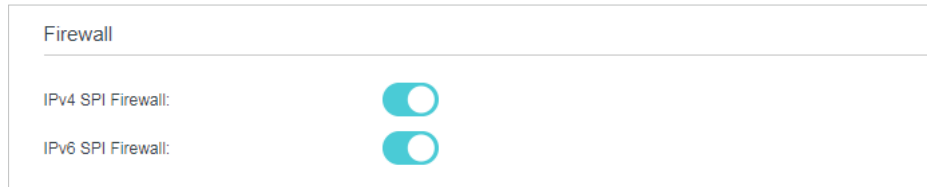
This chapter guides you on how to protect your home network from unauthorized users by implementing network security functions. You can block or allow specific client devices to access your wireless network using MAC Filtering, or using Access Control for wired and wireless networks, or you can prevent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

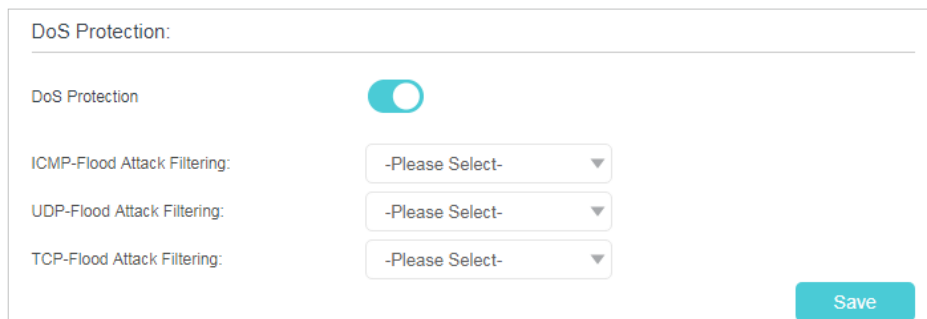
The SPI (Stateful Packet Inspection) Firewall and DoS (Denial of Service) Protection protect the controller from cyber attacks.

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

- 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.

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

Service Filtering

Service Filtering: ☒

- 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 structure:

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

Below the table, there are two input fields:

Device Name:

MAC Address:

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

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:

IP Address:

☒ [Enable This Entry](#)

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

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

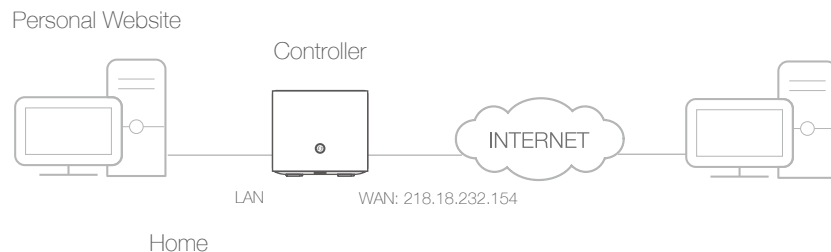
11.2. Share Local Resources over the Internet by Virtual Server

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

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:

ipoe_0_0_d

Service Type:

HTTP

View Existing Applications

External Port:

80

(XX-XX or XX)

Internal IP:

192 . 168 . 0 . 100

Internal Port:

80

(XX or Blank, 1-65535)

Protocol:

TCP

☒ 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

44

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

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:

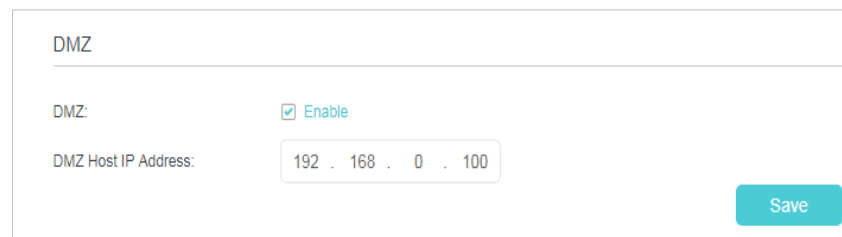
DMZ is most applicable when you don't know which ports to open. When it is enabled, the DMZ host is totally exposed to the internet, which may bring some potential safety hazards. If DMZ is not in use, please disable it in time.

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

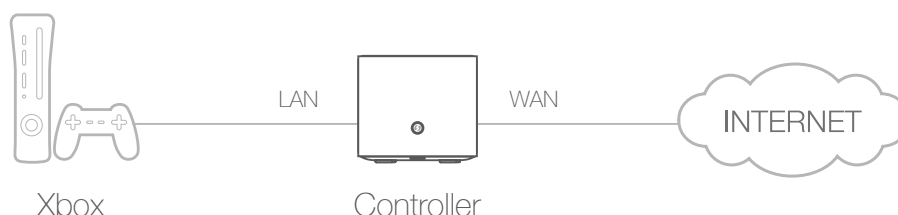
UPnP (Universal Plug and Play) protocol allows the applications or host devices to automatically find the front-end NAT device and send request to it to open the corresponding ports. With UPnP enabled, the applications or host devices in the both sides of NAT device can freely communicate with each other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

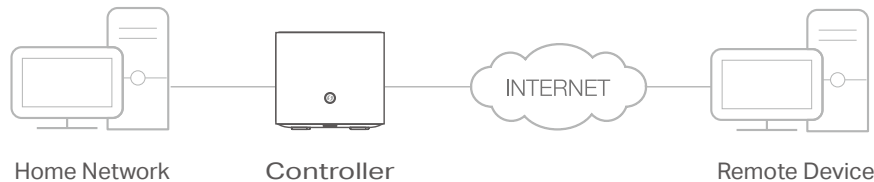
PPTP VPN is more easily used and its speed is faster, it's compatible with most operating systems and also supports mobile devices. Its security is poor and your packets may be cracked easily, and PPTP VPN connection may be prevented by some ISP.

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**.

OpenVPN

Note: No certificate currently, please [Generate](#) one before enabling VPN Server.

☒ Enable VPN Server

Service Type: ☒ UDP ☐ TCP

Service Port:

VPN Subnet/Netmask:

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

[Save](#)

Note:

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. (up to 10 clients)

Username:

Password:

[Save](#)

Note:

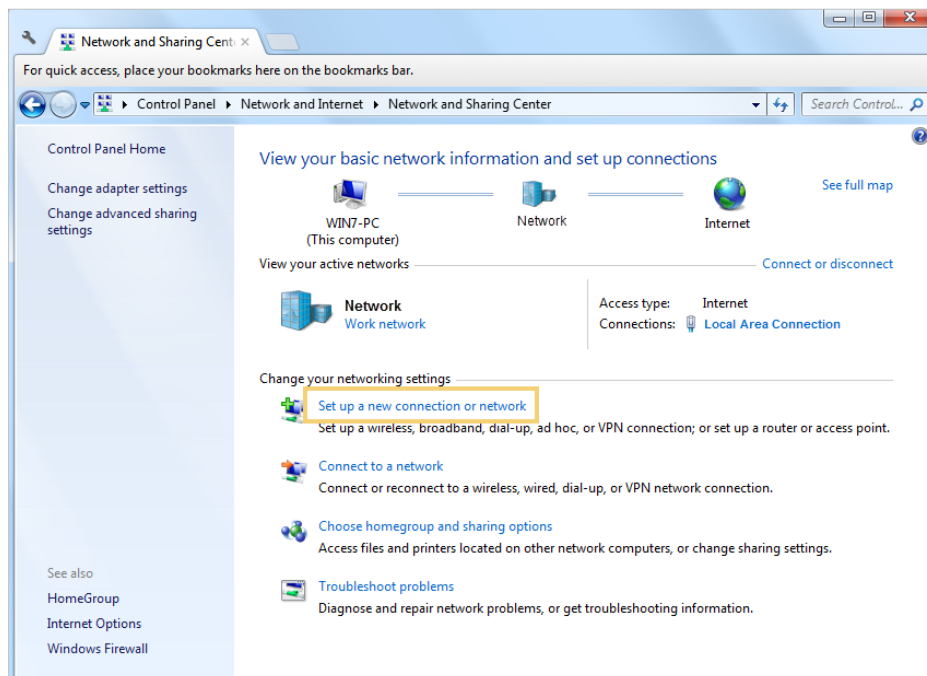
Before you enable [VPN Server](#), we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for controller's WAN port and synchronize your [System Time](#) with internet.

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.

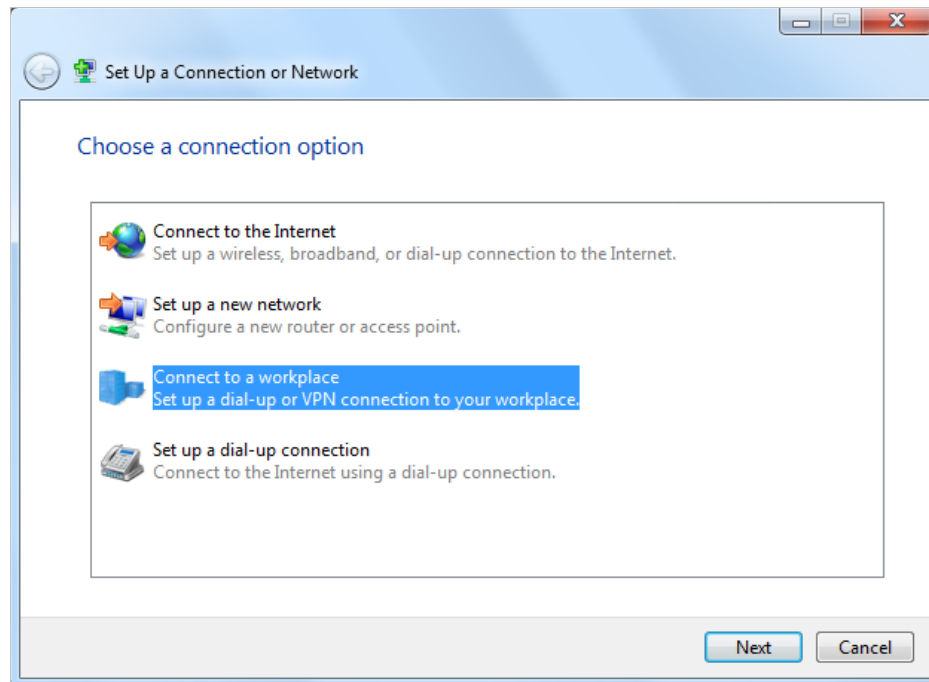
Step 2. Configure PPTP VPN Connection on Your Remote Device

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.

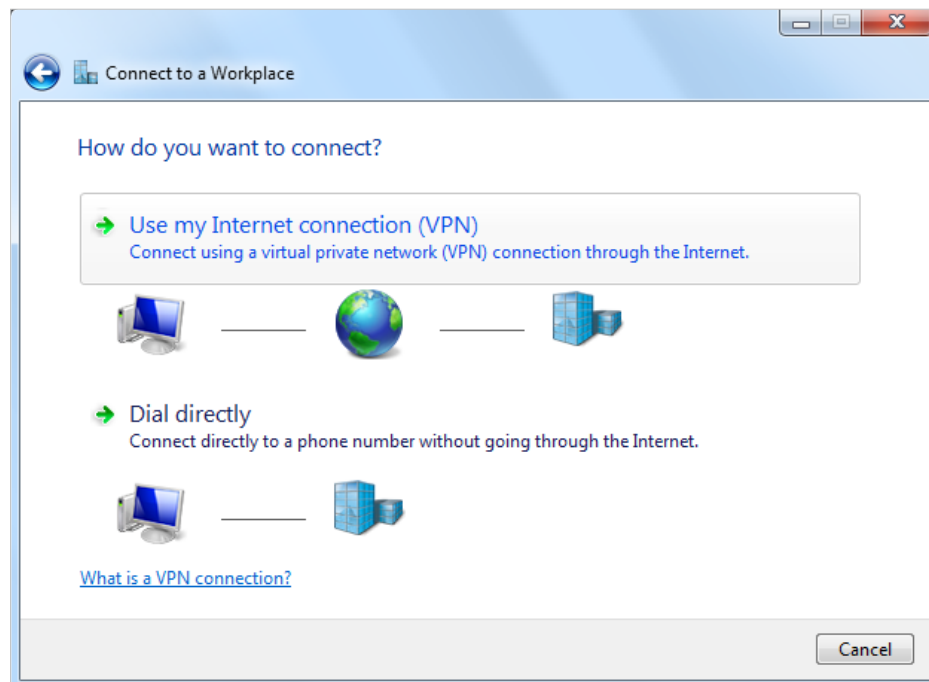
1. Go to [Start > Control Panel > Network and Internet > Network and Sharing Center](#).
2. Select [Set up a new connection or network](#).



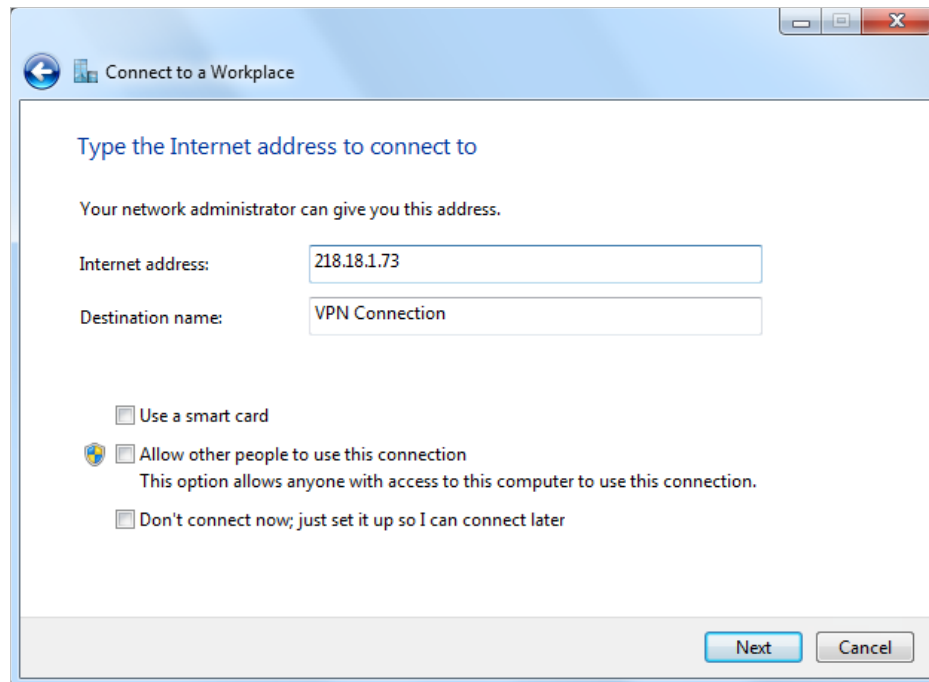
3. Select [Connect to a workplace](#) and click [Next](#).



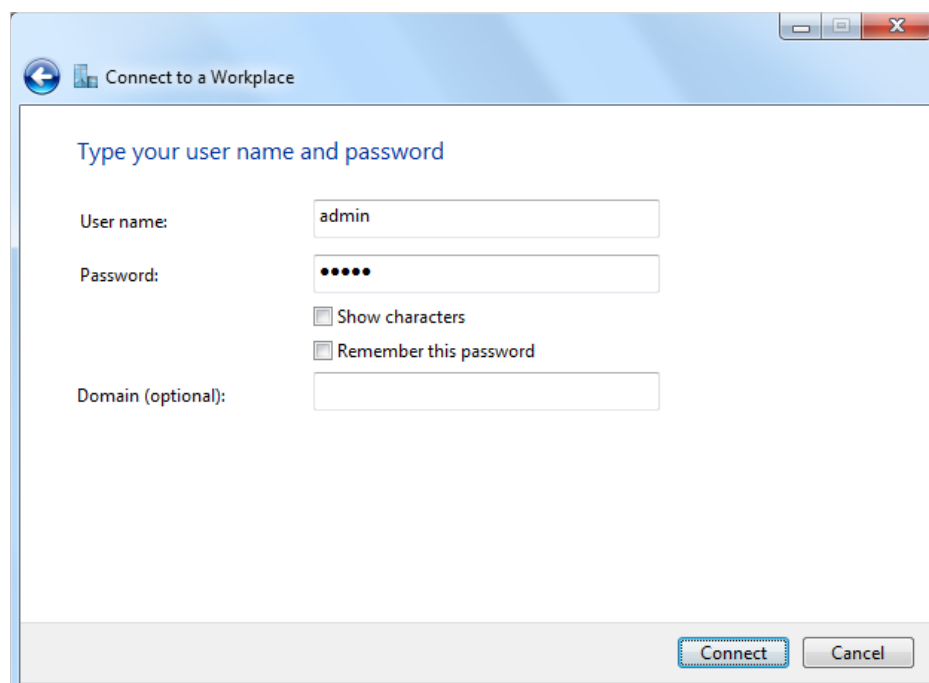
4. Select **Use my Internet connection (VPN)**.



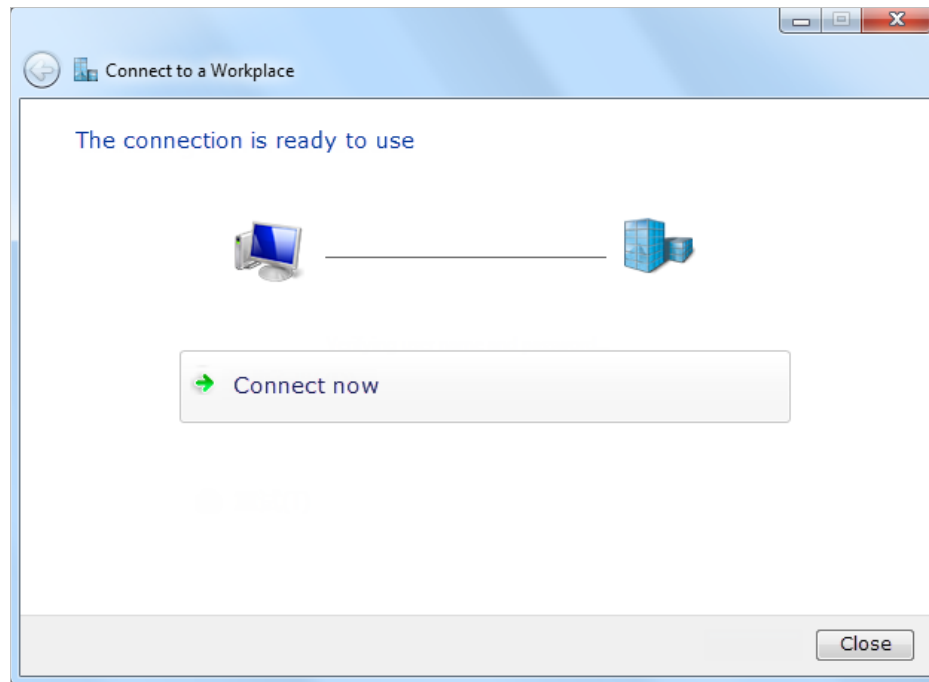
5. Enter the internet IP address of the controller (for example: 218.18.1.73) in the **Internet address** field. Click **Next**.



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



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](#).

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.