User Guide

Whole Home Mesh Wi-Fi AP

1910020931 REV1.0.0

Contents

About This Guide 1

Chapter 1. Get to Know About 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. Manually Set Up Your Internet Connection 12
4. 3. Set Up the AP as an Access Point 14
4. 4. Set Up an IPv6 Internet Connection 16

Chapter 5. Create Mesh Wi-Fi System 17

Chapter 6. Multi-SSID 21

Chapter 7. TP-Link Cloud Service 23

7. 1. Register a TP-Link ID 24
7. 2. Change Your TP-Link ID Information 24
7. 3. Manage the User TP-Link IDs 25
7. 3. 1. Add TP-Link ID to Manage the AP 26
7. 3. 2. Remove TP-Link ID(s) from Managing the AP 26
7. 4. Manage the AP via the TP-Link Aginet App 27

Chapter 8. Parental Controls 28

Chapter 9. Network Security 32

9. 1. Firewall & DoS Protection 33
9. 2. Service Filtering 34

9. 3. Access Control 35
9. 4. IP & MAC Binding 37

Chapter 10.NAT Forwarding 39

10. 1. Translate Address and Port by ALG 40
10. 2. Share Local Resources over the Internet by Virtual Server 41
10. 3. Open Ports Dynamically by Port Triggering 42
10. 4. Make Applications Free from Port Restriction by DMZ 43
10. 5. Make Xbox Online Games Run Smoothly by UPnP 44

Chapter 11.VPN Server 46

11. 1. Use OpenVPN to Access Your Home Network 47
11. 2. Use PPTP VPN to Access Your Home Network 48
11. 3. Use IPSec VPN to Access Your Home Network 52
11. 4. VPN Connections 55

Chapter 12.Customize Your Network Settings 56

12. 1. Change LAN Settings 57
12. 1. 1. Change the LAN IP Address 57
12. 1. 2. Use the AP as a DHCP Server 57
12. 1. 3. Reserve LAN IP Addresses 58
12. 2. Configure IPv6 LAN Settings 59
12. 2. 1. Configure the RADVD Address Type 59
12. 2. 2. Configure the DHCPv6 Server Address Type 60
12. 3. Set Up a Dynamic DNS Service Account 61
12. 4. Create Static Routes 62
12. 5. Activate RIP 65
12. 6. Set Up the IPv6 Tunnel 66
12. 6. 1. Use the Public IPv6 Tunnel Service-6to4 66
12. 6. 2. Specify the IPV6 Tunnel with Parameters Provided by Your ISP 67
12. 7. Specify Wireless Settings 69
12. 7. 1. Change Basic Wireless Settings 69
12. 7. 2. View Wireless Information 71
12. 7. 3. Advanced Wireless Settings 72
12. 8. Use WPS for Wireless Connection 73

Chapter 13.Manage Your AP 76

13. 1. Set System Time 77
13. 2. Control LED 78

13. 3. Test Internet Connectivity 78
13. 4. Update the Firmware 80
13. 5. Back Up and Restore Configuration Settings 80
13. 6. Reboot the AP 81
13. 7. Administration Management 82
13. 7. 1. Change the Login Password 82
13. 7. 2. Local Management 83
13. 7. 3. Remote Management 83
13. 7. 4. ICMP Ping 85
13. 7. 5. Session ID 85
13. 8. System Log 86
13. 9. CWMP Settings 87
13. 10. SNMP Settings 88
13. 11. Monitor the Internet Traffic Statistics 90

FAQ 91

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.

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
Underlined	Underlined words or phrases are hyperlinks. You can click to redirect to a website or a specific section.
Teal	Contents to be emphasized and texts on the web page are in teal, including the menus, items, buttons 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.

*Maximum wireless signal rates are the physical rates derived from IEEE Standard 802.11 specifications. Actual wireless data throughput and wireless coverage are not guaranteed and will vary as a result of network conditions, client limitations, and environmental factors, including building materials, obstacles, volume and density of traffic, and client location.

*Use of MU-MIMO and 1024-QAM requires clients to also support those functions.

Chapter 1

Get to Know About Your Device

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

It contains the following sections:

- Product Overview
- Appearance

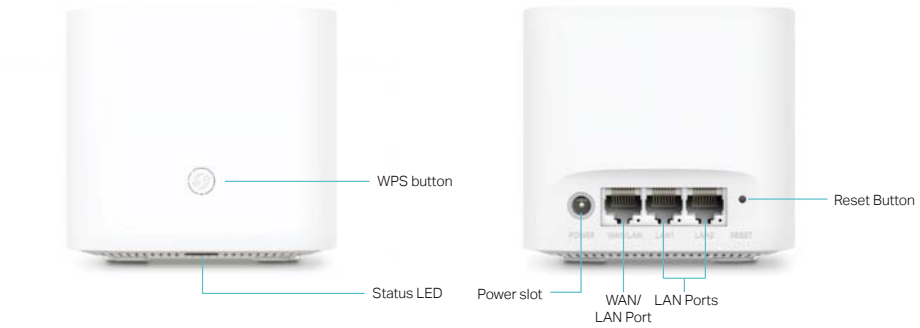
1. 1. Product Overview

The Whole Home Mesh Wi-Fi AP is designed to extend your network coverage. You can use multiple APs to create a seamless, intelligent and easy-to-configure mesh network that covers the entire home.

The Mesh Wi-Fi system consists of a Main AP, one or more agents. The Main AP connects to a wired router, a modem or gateway, the agents extend 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
Flashing yellow	The device is starting up or resetting.
Yellow	The connection quality between the main AP and agent is normal.
Flashing blue	The device is ready for setup.
Fast flashing blue	The device is establishing a WPS or mesh connection.
Blue	The device has been set up, but the internet is unavailable.
Flashing white/green	The device is upgrading the firmware.
White/green	The device works well and the internet is available.
Flashing red	The device has lost connection with the main AP.
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 sync 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(access point 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

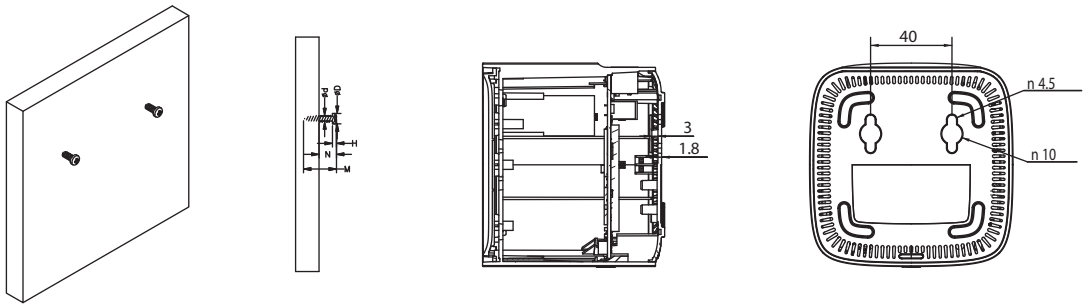
This chapter contains the following sections:

- 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.



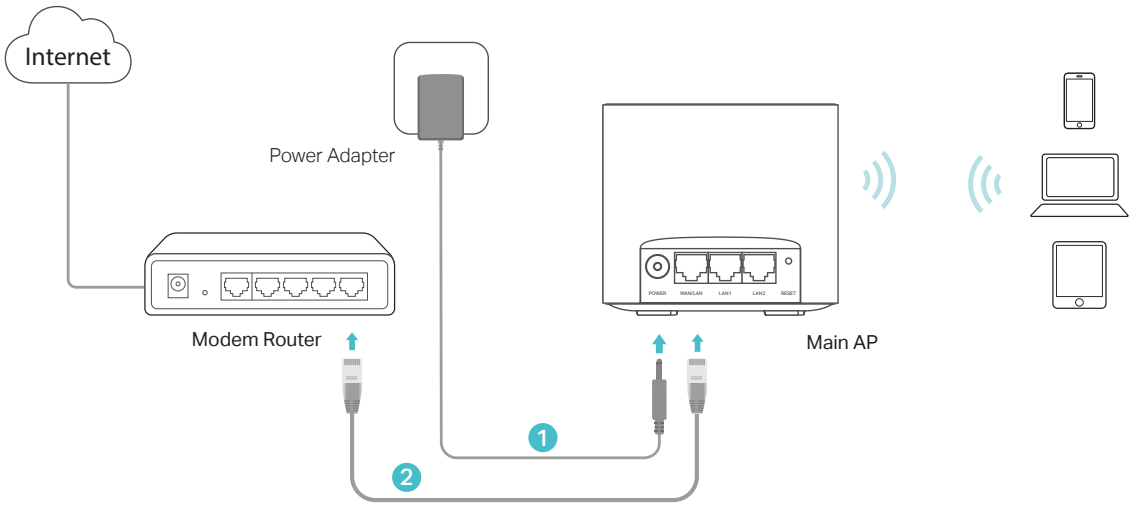
NOTE:
4.67 mm < D < 9.85 mm
d < 4.5 mm
H < 3 mm
4.8 mm < N
20 mm ≤ M

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.

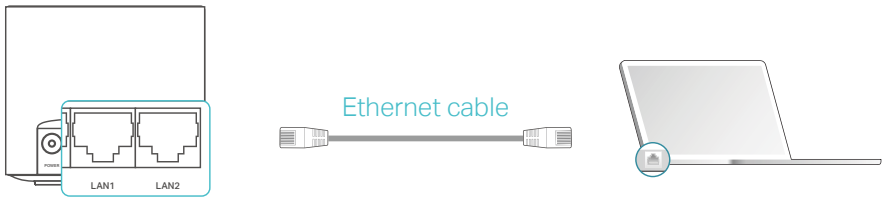
2. 2. Connect Your Device

If you want to set up this device as a regular router or as the Main AP for Mesh Wi-Fi system, follow the steps below to connect your device.



1. Connect the power adapter to the AP.
2. Connect the WAN/LAN port of the AP 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 AP.
   - **Method 1: Wired**

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

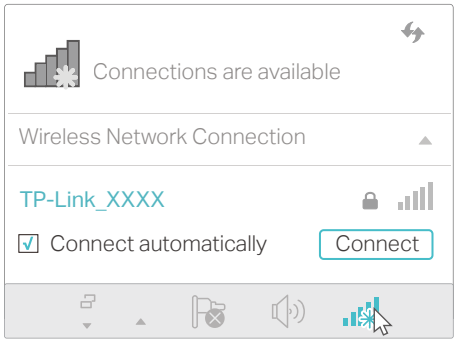


   - **Method 2: Wireless**

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

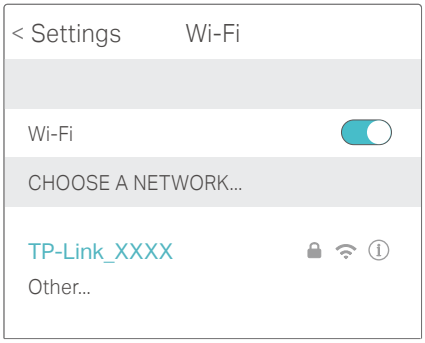
     2) Click the network icon of your computer or go to Wi-Fi Settings of your smart device, and then select the SSID to join the network.

Computer



OR

Smart Device



Chapter 3

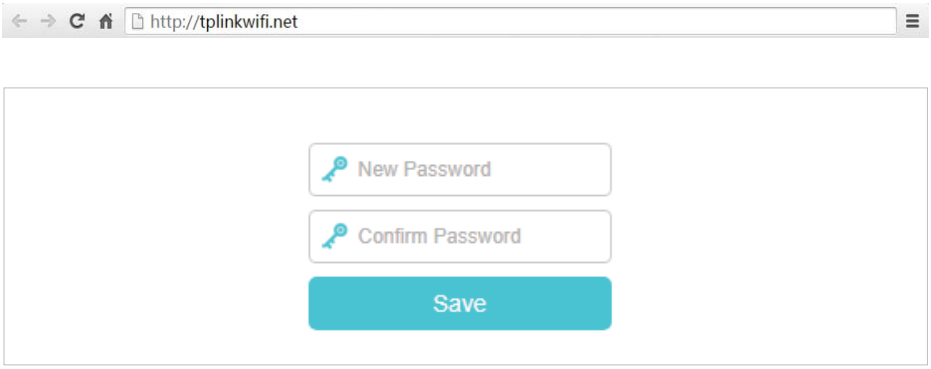
Log In to Your Device

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 AP.



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.
3. If you have registered a TP-Link ID and bound your cloud router to it, the login password you created here will be invalid. Please log in to the cloud router using your TP-Link ID.

Chapter 4

Set Up Internet Connection

This chapter introduces how to connect your device to the internet in Router Mode. The device 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
- Manually Set Up Your Internet Connection
- Set Up the AP as an Access Point
- Set Up an IPv6 Internet Connection

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 AP.

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.

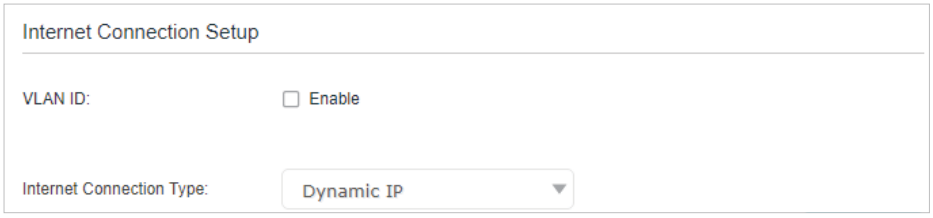
Note:
1. If you have changed the preset wireless network name (SSID) and wireless password during the Quick Setup process, all your wireless devices must use the new SSID and password to connect to the device.
2. Once you complete the Quick Setup process, the device become your mesh Main AP, you can add agents to create your mesh Wi-Fi system.

4. 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.

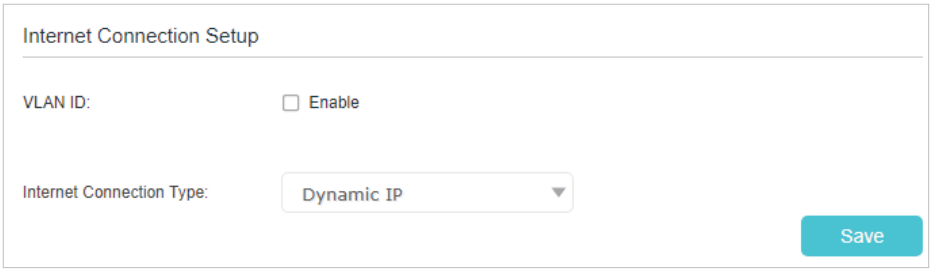
Follow the steps below to check or modify your internet connection settings.

1. Visit http://tplinkwifi.net, and log in with the password you set for the AP.
2. Go to Basic > Internet.
3. Select your internet connection type from the drop-down list.

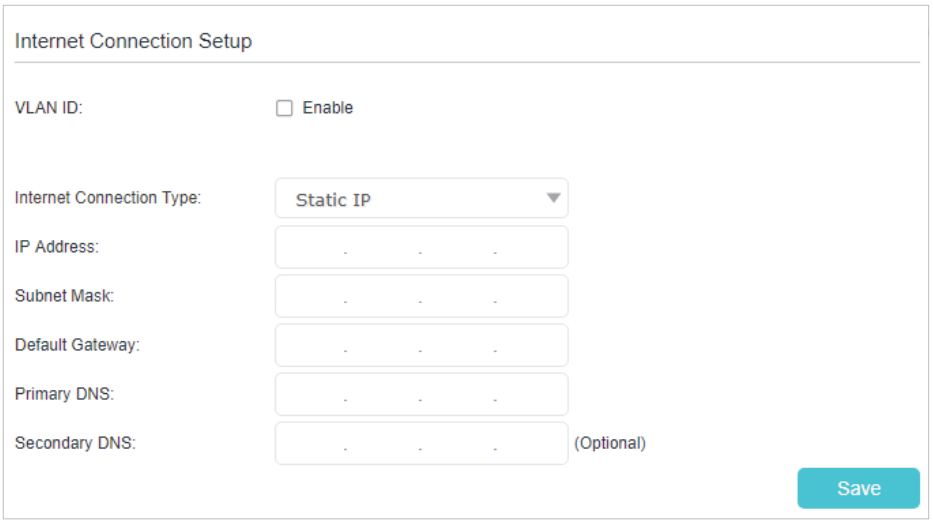


Note:
If you are unsure of what your connection type is, please consult your ISP. Since different connection types may require different cables and connection information, please refer to the demonstrations in Step 4 to determine your connection type.

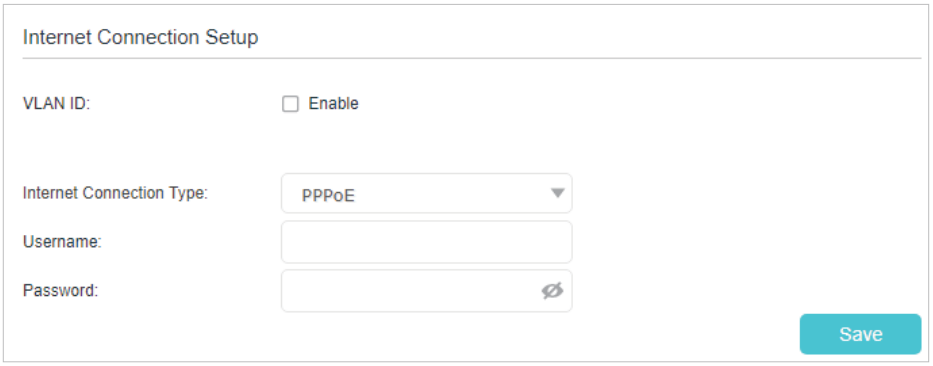
4. Follow the instructions on the page to continue the configuration. Parameters on the images are used for demonstration only.
   1) If you choose Dynamic IP, you just need to click Save to make the settings effective. Dynamic IP users are usually equipped with a cable TV or fiber cable.



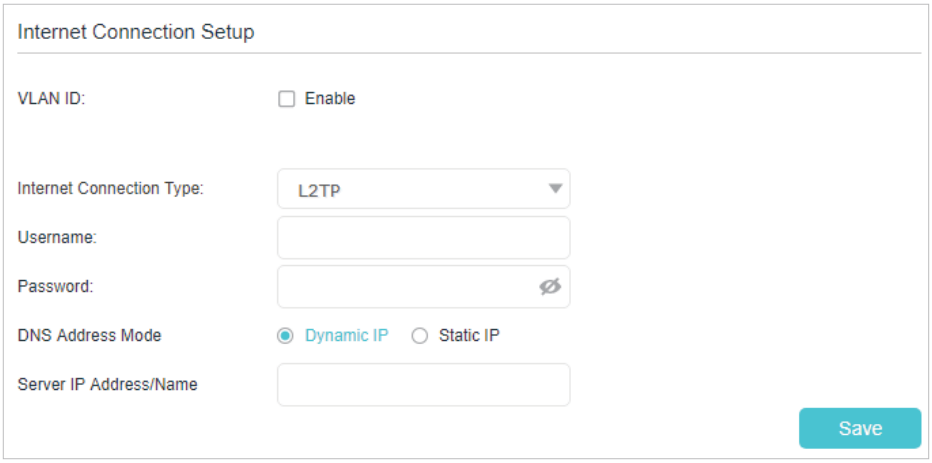
2) If you choose Static IP, enter the information provided by your ISP in the corresponding fields.



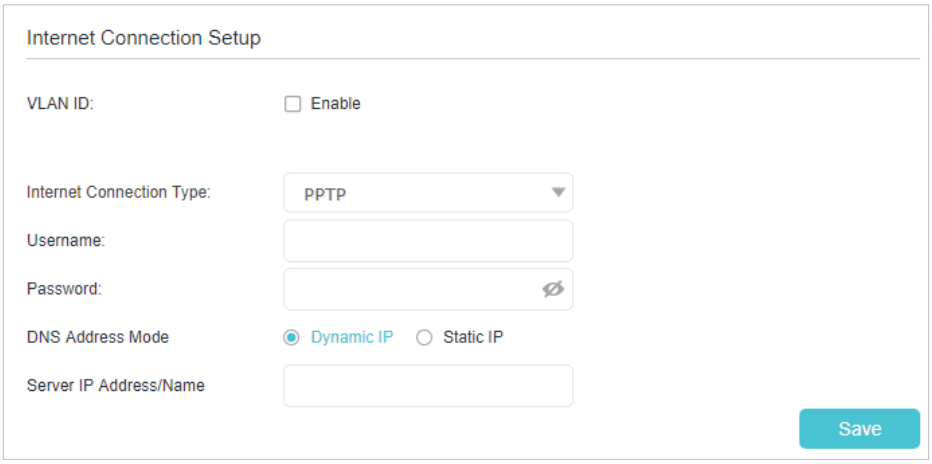
3) If you choose PPPoE, enter the Username and Password provided by your ISP. PPPoE users usually have DSL cable modems.



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



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.



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:

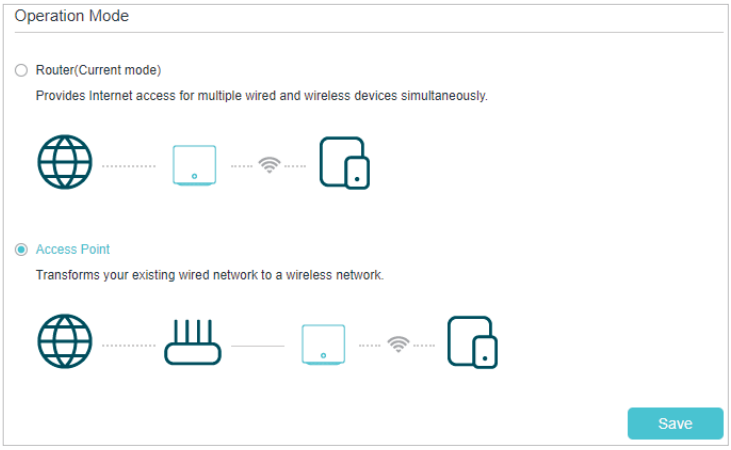
1. You can check your internet connection by clicking Network Map on the left of the page.
2. If you use Dynamic IP and PPPoE and you are provided with any other parameters that are not required on the page, please go to Advanced > Network > Internet to complete the configuration.
3. If you still cannot access the internet, refer to the FAQ section for further instructions.

4. 3. Set Up the AP as an Access Point

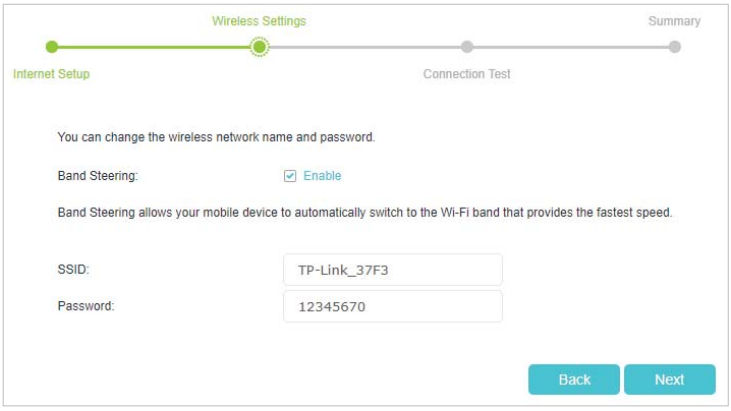
The AP can work as an access point, transforming your existing wired network to a wireless one.

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

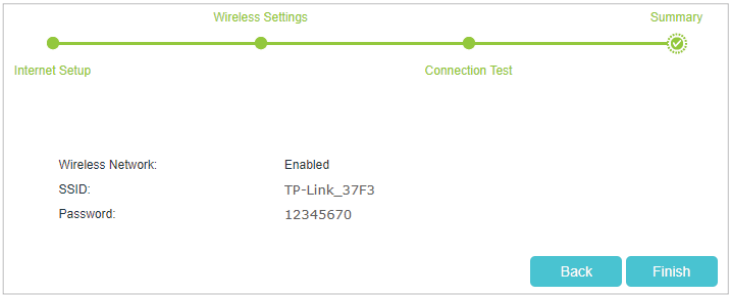
2. Go to Advanced > Operation Mode, select Access Point and click Save. The AP will reboot and switch to Access Point mode.



3. After rebooting, connect the AP to your existing wired router via an Ethernet cable.
4. Log in again to the web management page http://tplinkwifi.net, and click Quick Setup.
5. Configure your wireless settings and click Next.



6. Confirm the information and click Save. Now, you can enjoy Wi-Fi.



Tips:

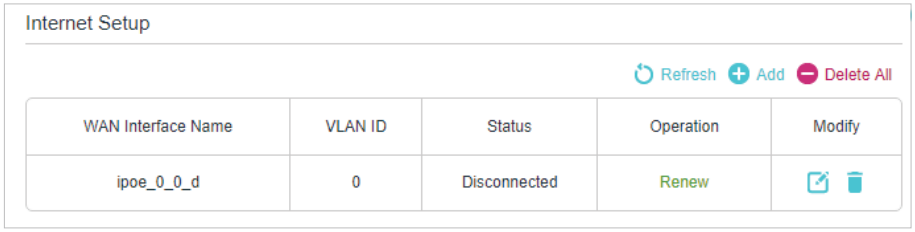
- Functions, such as Parental Controls, VPN Server and NAT Forwarding, are not supported in the Access Point mode.

4. 4. 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), 6to4 tunnel 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 AP.
2. Go to Advanced > Network > Internet.



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.

- Addressing Type: Consult your ISP for the addressing type (DHCPv6, SLAAC or AUTO). 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 agents to create a mesh Wi-Fi system to extend the wireless coverage.

The Whole Home Mesh Wi-Fi System includes a Main AP, 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.

When the Quick Setup process is completed, your AP can be used as a Main AP of the mesh network.

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**

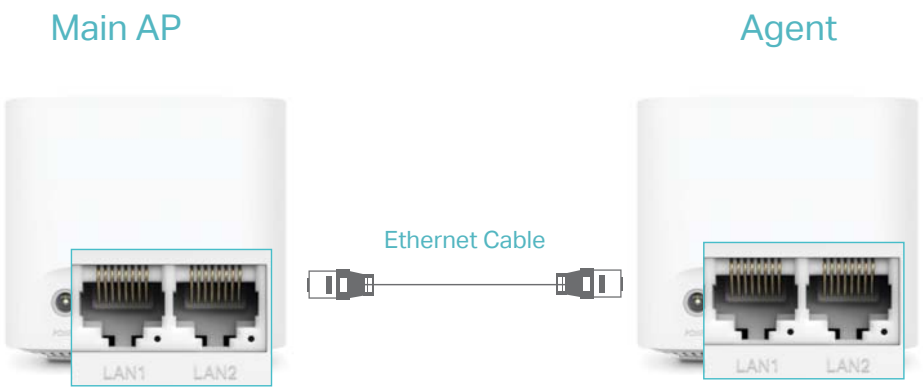
- **Method 1: Wireless Connection**

1. Place the agent close to the Main AP and power it on, wait about two minutes until the status LED turns to flashing blue.
2. Press the WPS button on the Main AP 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.

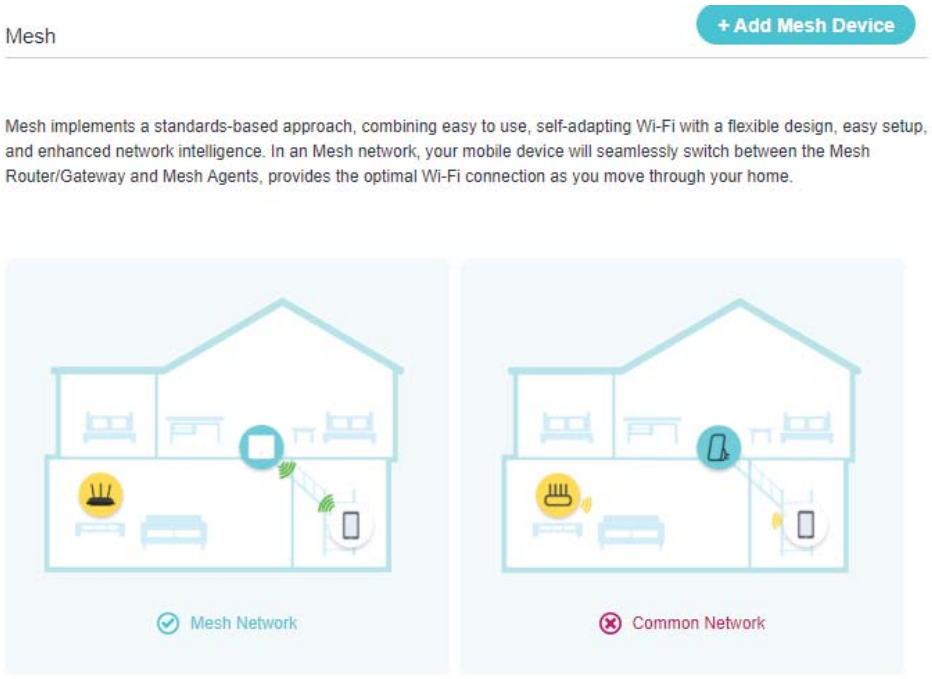
- **Method 2: Wired Connection**

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 Main AP and the agent using an Ethernet cable .
3. The agent will automatically synchronize with the Main AP to extend your network.



- **Method 3: Add mesh device via web management page**

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Basic > Mesh, click + Add Mesh Device and follow the step by step instructions to add more mesh devices.



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 Main AP.
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 Main AP if you want to manage your mesh network.

After the agent is successfully connected to the 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' 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 Main AP or the other agent, you can go to Network Map to check the Main AP and the agent's connection status.

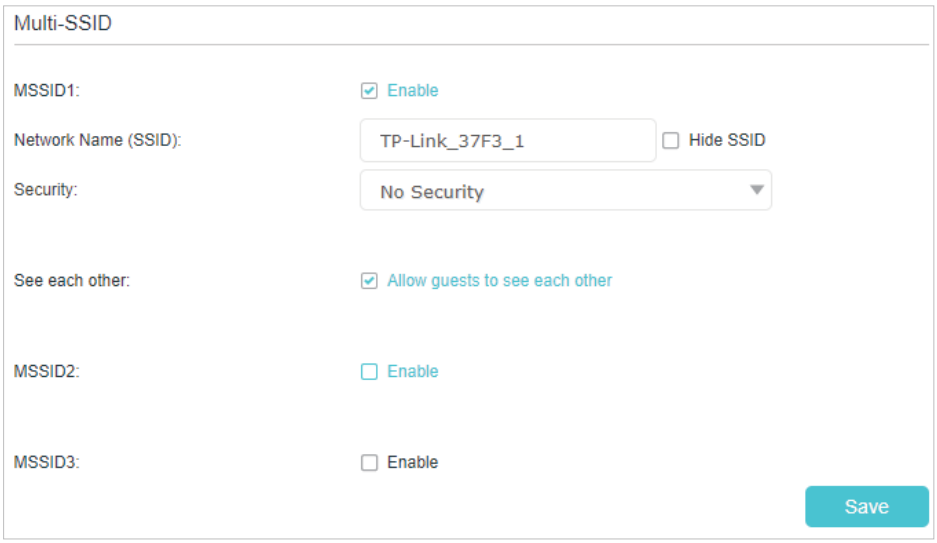
Chapter 6

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 AP.
2. Go to Basic > Multi-SSID or Advanced > Wireless > Multi-SSID.
3. Create the multi-SSID network as needed.



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 AP with a TP-Link ID, and you can easily monitor and manage your home network when you are out and about via the Aginet app. To ensure that your AP 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 AP, and the Aginet app with which you can manage your home network no matter where you may find yourself.

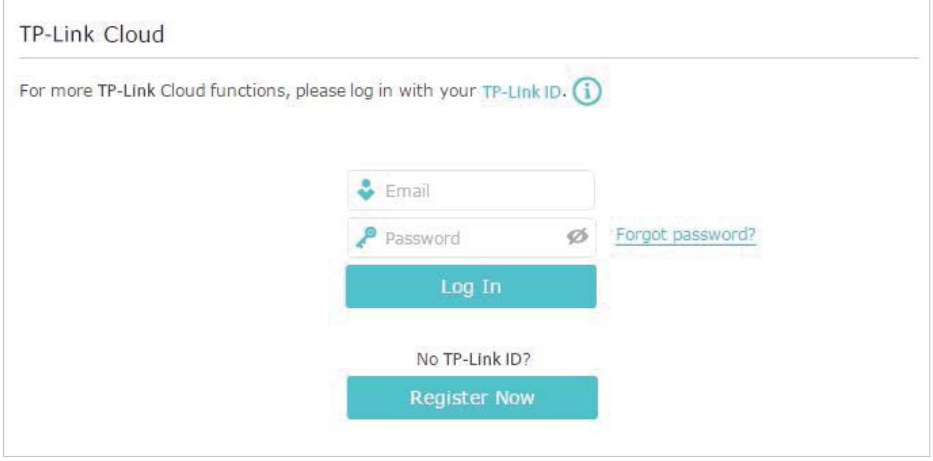
It contains the following sections:

- Register a TP-Link ID
- Change Your TP-Link ID Information
- Manage the User TP-Link IDs
- Manage the AP via the TP-Link Aginet 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 AP.
2. Go to Basic > TP-Link Cloud.
3. Click Register Now and follow the instructions to register a TP-Link ID.



4. After activating your TP-Link ID, come back to the TP-Link ID page to log in. The TP-Link ID used to log in to the AP 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 Aginet APP. Please refer to Manage the AP via the TP-Link Aginet App to install the app.
- If you want to unbind the admin TP-Link ID from your AP, please go to Basic > TP-Link Cloud, an click Unbind in the Device Information section.

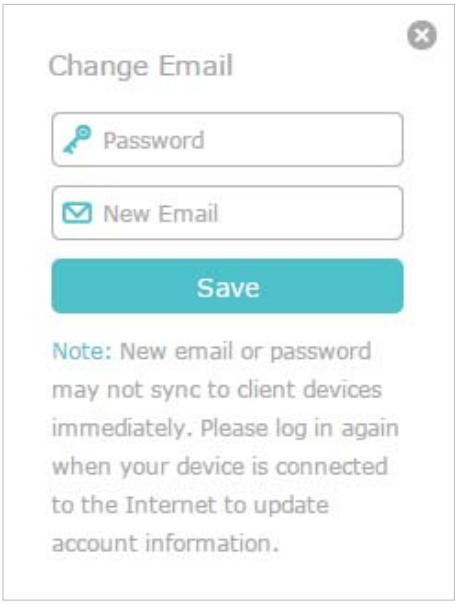
7. 2. Change Your TP-Link ID Information

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 Basic > TP-Link Cloud, and focus on the Account Information section.

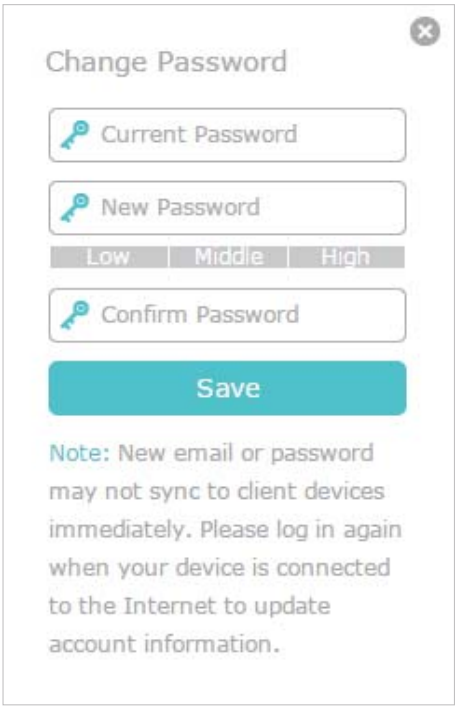
- **To change your email address**:

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



- **To change your password:**

1. Click behind the Password.
2. Enter the current password, then a new password twice. And click Save.



7. 3. Manage the User TP-Link IDs

The TP-Link ID used to log in to the AP 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

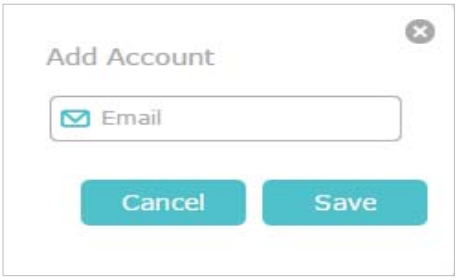
the same AP as Users. All accounts can monitor and manage the AP locally or remotely, but user accounts cannot:

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

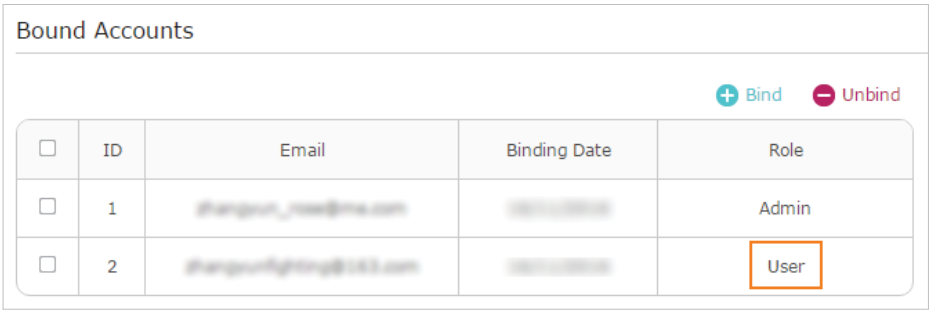
7. 3. 1. Add TP-Link ID to Manage the AP

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID.
2. Go to Basic > TP-Link Cloud, 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 Aginet app. Refer to Manage the AP via the TP-Link Aginet App to install the app and register a new TP-Link ID.

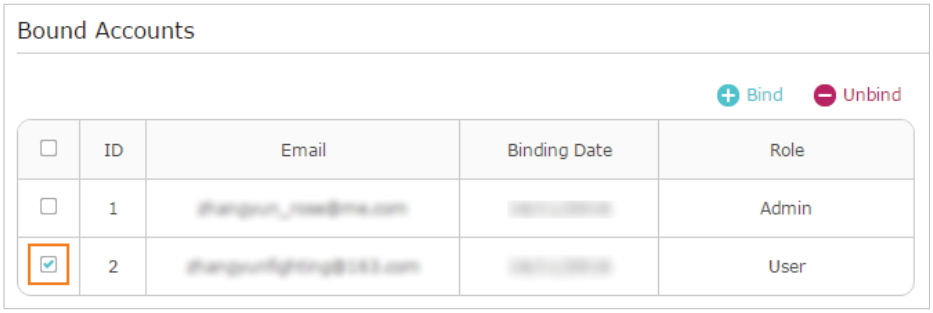


4. The new TP-Link ID will be displayed in the Bound Accounts table as a User.



7. 3. 2. Remove TP-Link ID(s) from Managing the AP

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID.
2. Go to Basic > TP-Link Cloud, 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.



7. 4. Manage the AP via the TP-Link Aginet App

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

2. Launch the Aginet 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 AP's wireless network.
4. Go back to the Aginet app, select the model of your AP and log in with the password you set for the AP.
5. Manage your AP as needed.

Note: If you need to remotely access your AP 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

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:

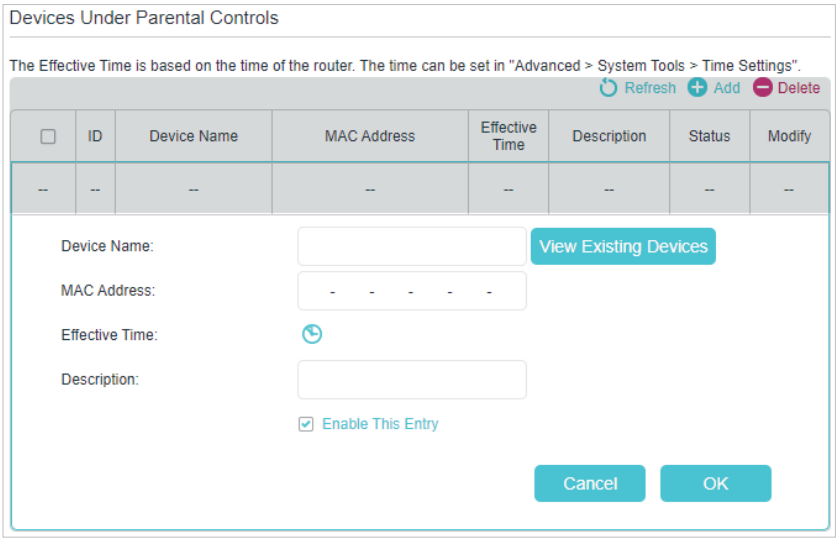
Control what types of websites my children or other home network users can visit and the time of day they are allowed to access the internet.

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.

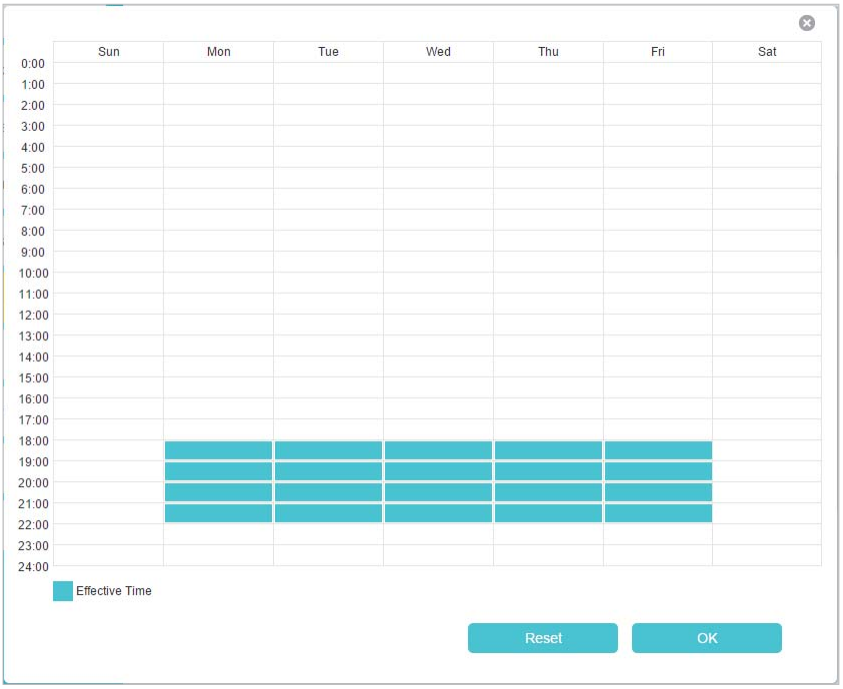
How can I do that?

1. Visit http://tplinkwifi.net, and log in with the password you set for the AP.
2. Go to Basic or Advanced > Parental Controls and enable 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.

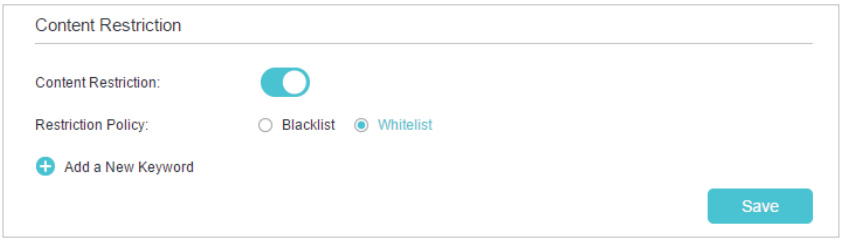


4. Click the icon to set the Effective Time. Drag the cursor over the appropriate cell(s) and click OK.



5. Enter a Description for the entry, keep the Enable This Entry check box selected, and then click Save.

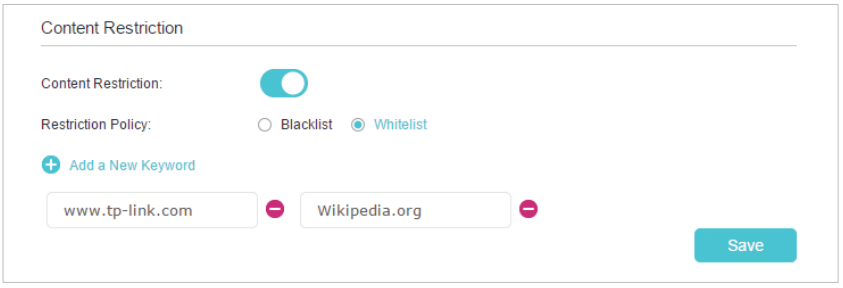
6. Enable Content Restriction, and select Whitelist as the restriction policy.



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 9

Network Security

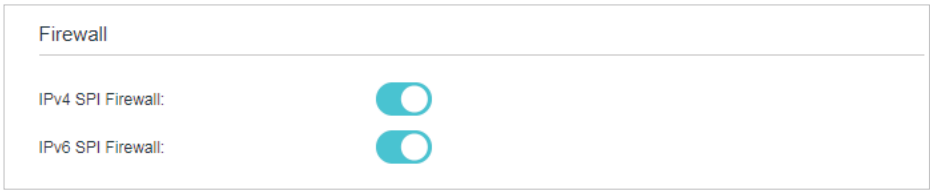
This chapter guides you on how to protect your home network from unauthorized users by implementing network security functions. You can block or allow specific client devices to access your wireless network using MAC Filtering, or using Access Control for wired and wireless networks, or you can prevent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

- Firewall & DoS Protection
- Service Filtering
- Access Control
- IP & MAC Binding

9. 1. Firewall & DoS Protection

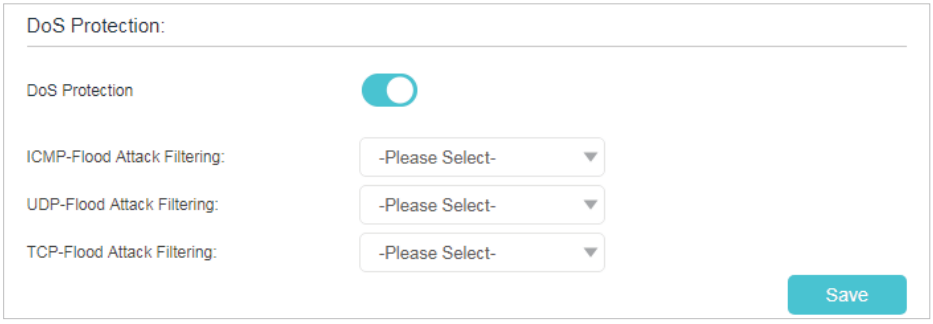
The SPI (Stateful Packet Inspection) Firewall and DoS (Denial of Service) Protection protect the AP from cyber attacks.

The SPI Firewall can prevent cyber attacks and validate the traffic that is passing through the AP 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 AP.
2. Go to Advanced > Security > Firewall & DoS Protection.

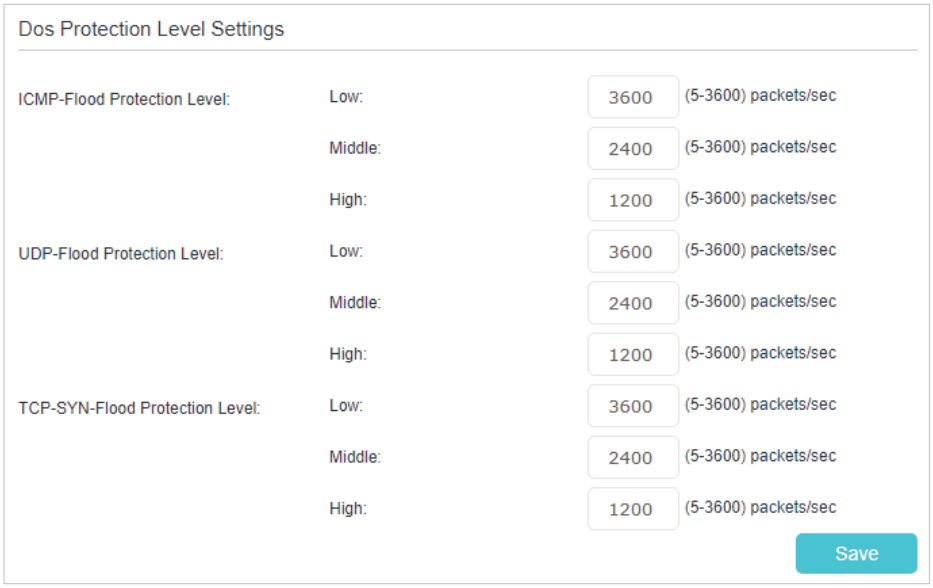


Note: DoS Protection and Traffic Statistics must be enabled at the same time, you can go to Advanced > System Tools > Traffic Statistics to enable traffic statistics function.

3. Enable DoS Protection.
4. Set the pretection 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.

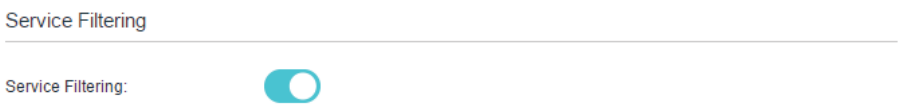


2. The protection will be triggered immediately when the number of packets exceeds the preset threshold value, and the vicious host will be displayed in the Blocked DoS Host List.

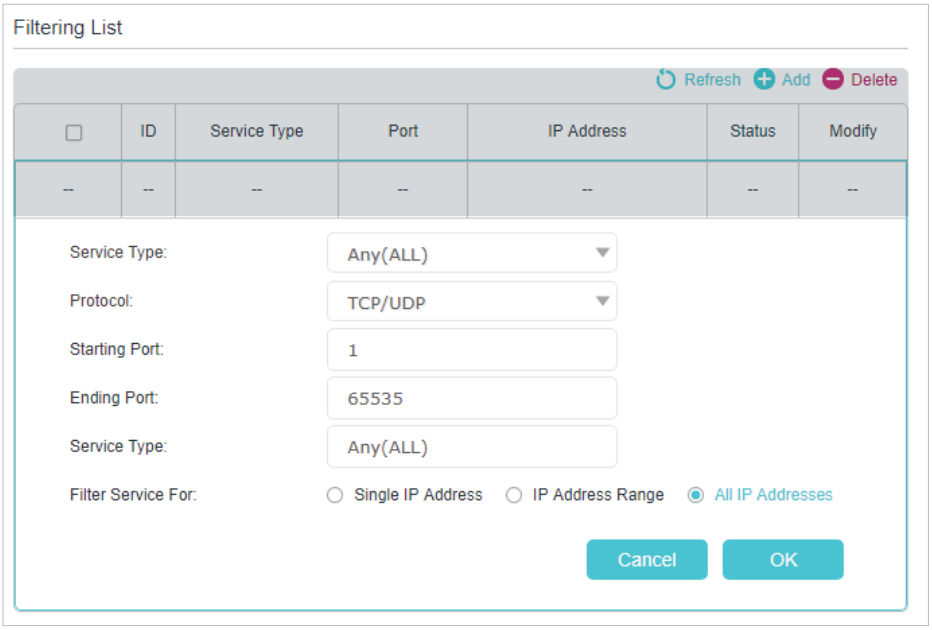
9. 2. Service Filtering

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 AP.
2. Go to Advanced > Security > Service Filtering.
3. Enable Service Filtering.



4. Click Add.



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.

9. 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).

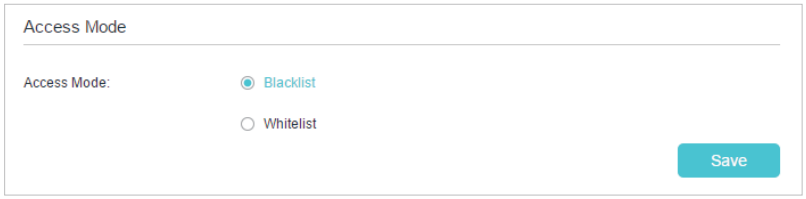
How can I do that?

1. Visit http://tplinkwifi.net, and log in with the password you set for the AP.
2. Go to Advanced > Security > Access Control and enable Access Control.

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

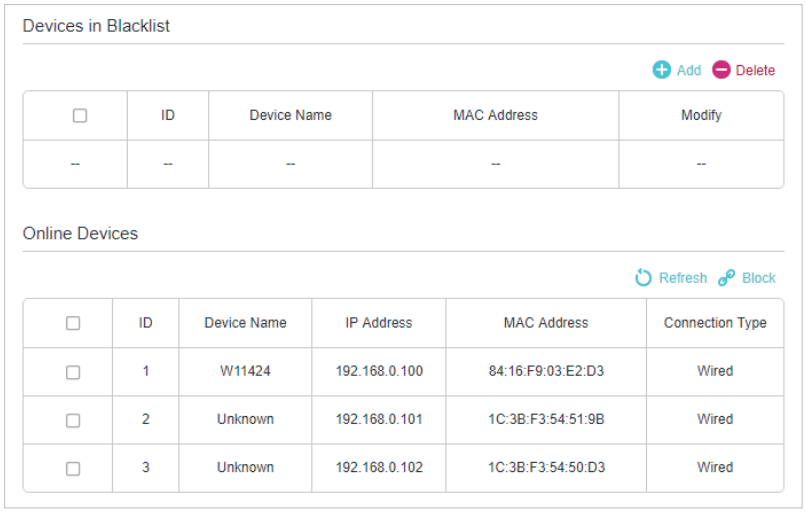
To block specific device(s):

1) Select Blacklist and click Save.



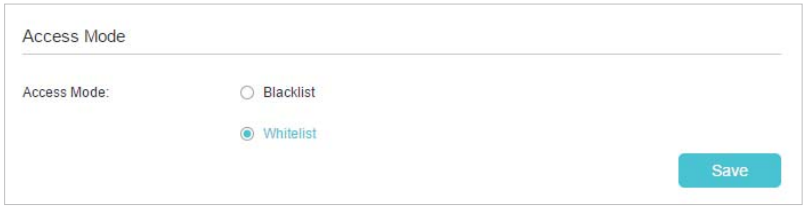
2) Select the device(s) to be blocked in the Online Devices table (or click the Add under the Devices in Blacklist and enter the Device Name and MAC Address manually).

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

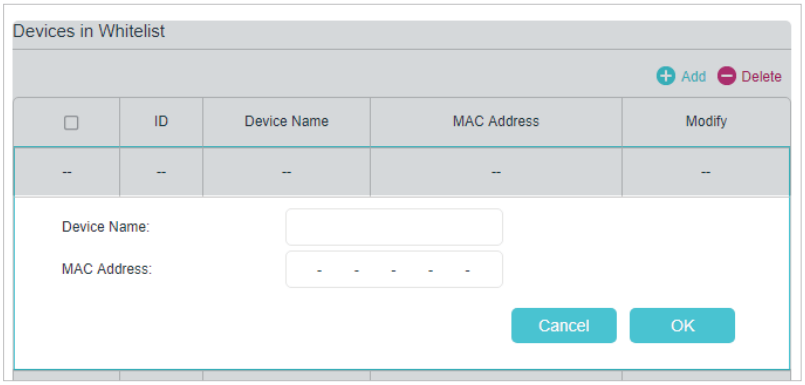


To allow specific device(s):

1) Select Whitelist and click Save.



2) Click Add in the Devices in Whitelist section.



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.

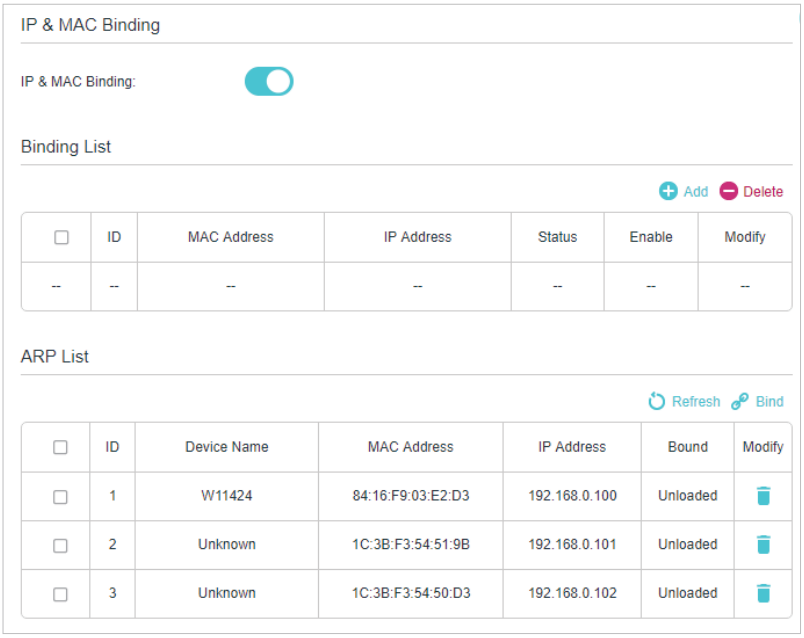
9. 4. IP & MAC Binding

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 AP.
2. Go to Advanced > Security > IP & MAC Binding and enable IP & MAC Binding.



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

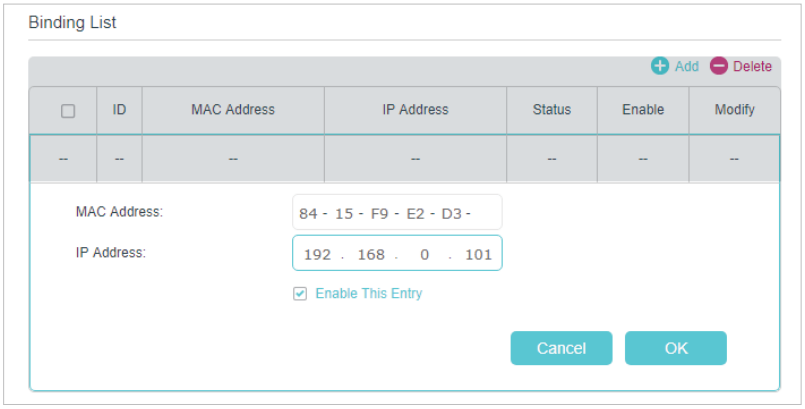
   To bind the connected device(s):

   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.



   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 10

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.

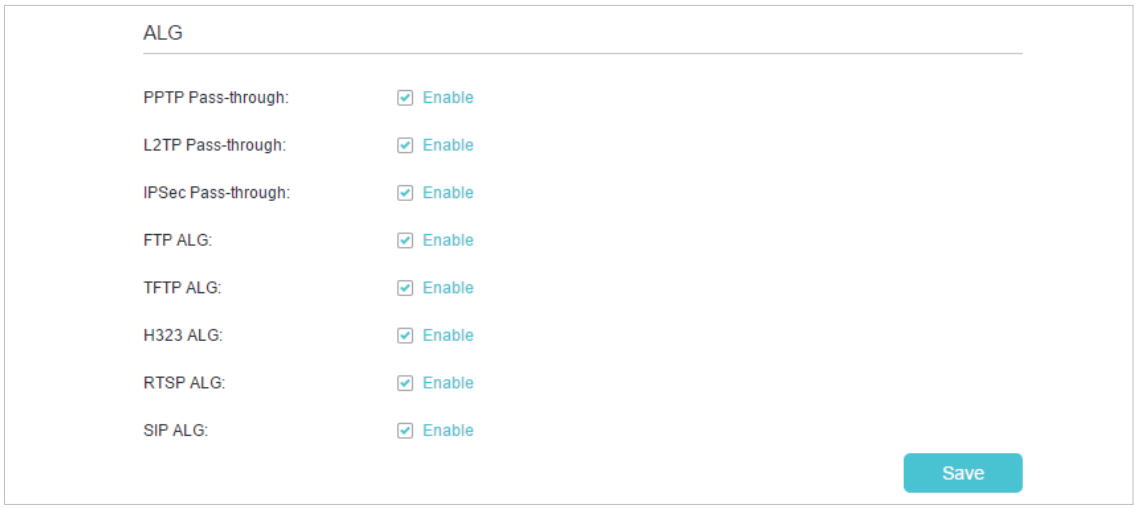
This chapter contains the following sections:

- 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

10. 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 AP. Go to Advanced > NAT Forwarding > ALG.



- PPTP Pass-through: If enabled, it allows Point-to-Point sessions to be tunneled through an IP network and passed through the AP.
- L2TP Pass-through: If enabled, it allows Layer 2 Point-to-Point sessions to be tunneled through an IP network and passed through the AP.
- IPSec Pass-through: If enabled, it allows IPSec (Internet Protocol Security) to be tunneled through an IP network and passed through the AP. 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.

10. 2. Share Local Resources over the Internet by Virtual Server

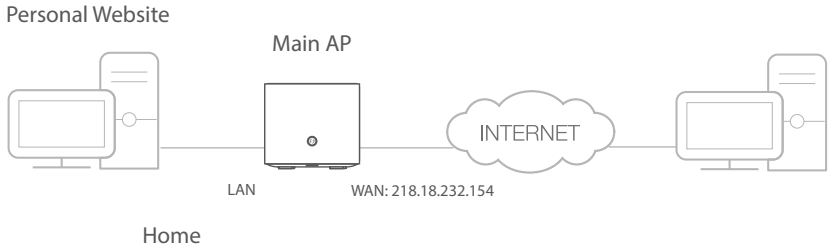
When you build up a server in the local network and want to share it on the internet, Virtual Server can realize the service and provide it to the internet users. At the same time virtual server can keep the local network safe as other services are still invisible from the internet.

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:

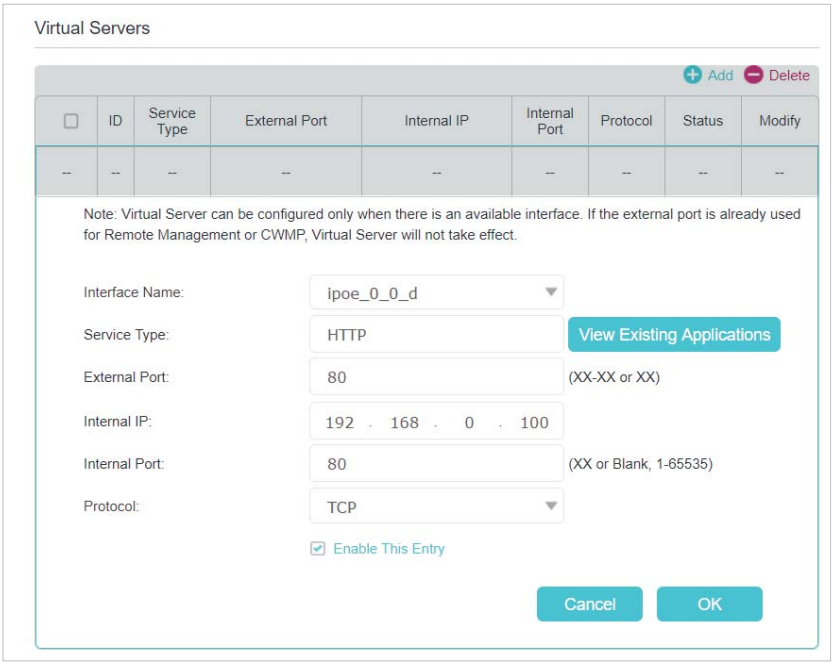
Share my personal website I've built in a local network with my friends through the internet.

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 AP 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 AP.
3. Go to Advanced > NAT Forwarding > Virtual Servers, click Add.



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 AP. 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.

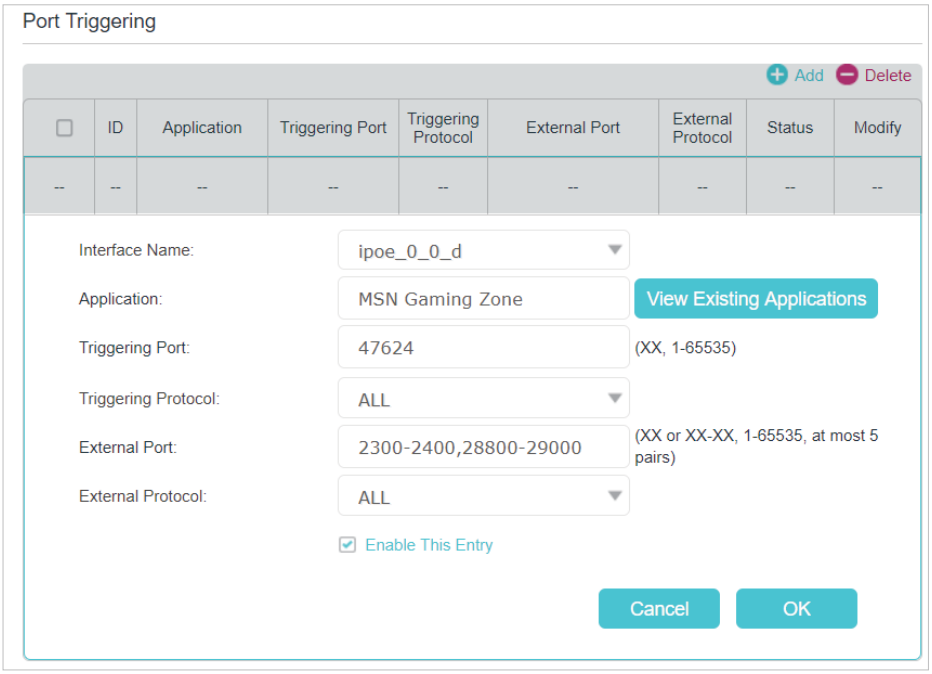
10. 3. Open Ports Dynamically by Port Triggering

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 AP.
2. Go to Advanced > NAT Forwarding > Port Triggering, and click Add.



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.

10. 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 AP.
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.

10. 5. Make Xbox Online Games Run Smoothly by UPnP

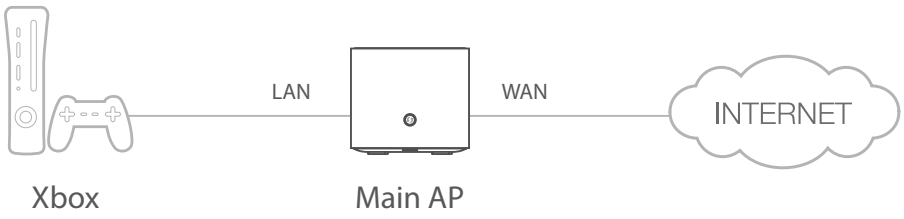
UPnP (Universal Plug and Play) protocol allows the applications or host devices to automatically find the front-end NAT device and send request to it to open the corresponding ports. With UPnP enabled, the applications or host devices in the both sides of NAT device can freely communicate with each other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

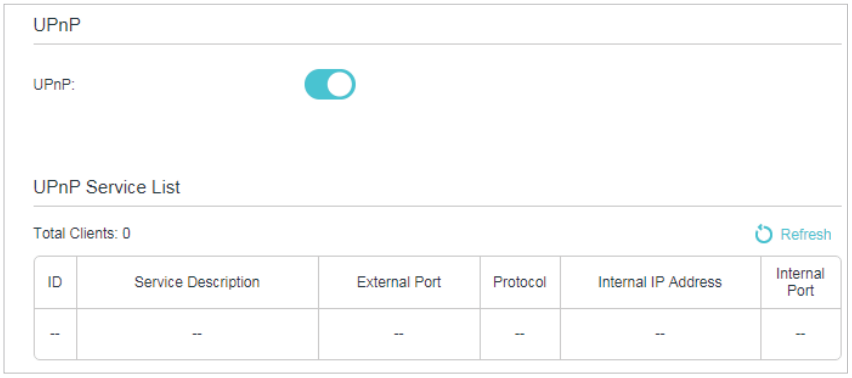
1. UPnP is enabled by default in this device.
2. Only the application supporting UPnP protocol can use this feature.
3. UPnP feature needs the support of operating system (e.g. Windows Vista/ Windows 7/ Windows 8, etc. Some operating systems need to install the UPnP components).

For example, when you connect your Xbox to the AP which has connected to the internet to play online games, UPnP will send request to the AP 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 AP.
2. Go to Advanced > NAT Forwarding > UPnP, and enable or disable UpnP according to your needs.



Chapter 11

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 ISPs.

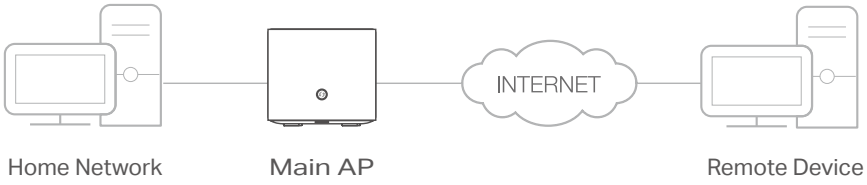
IPSec (IP Security) is a set of services and protocols defined by IETF (Internet Engineering Task Force) to provide high security for IP packets and prevent attacks.

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
- Use IPSec VPN to Access Your Home Network
- VPN Connections

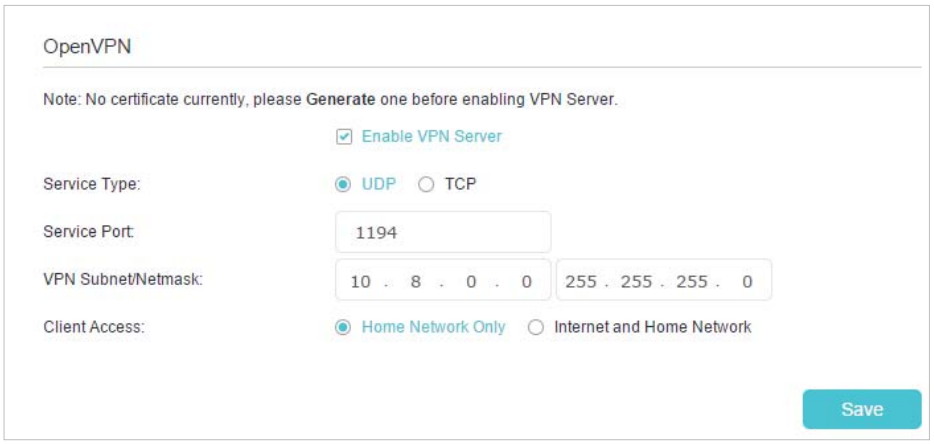
11. 1. Use OpenVPN to Access Your Home Network

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 AP

1. Visit http://tplinkwifi.net, and log in with the password you set for the AP.
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 AP'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.

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 AP.

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 AP. 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 AP 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.

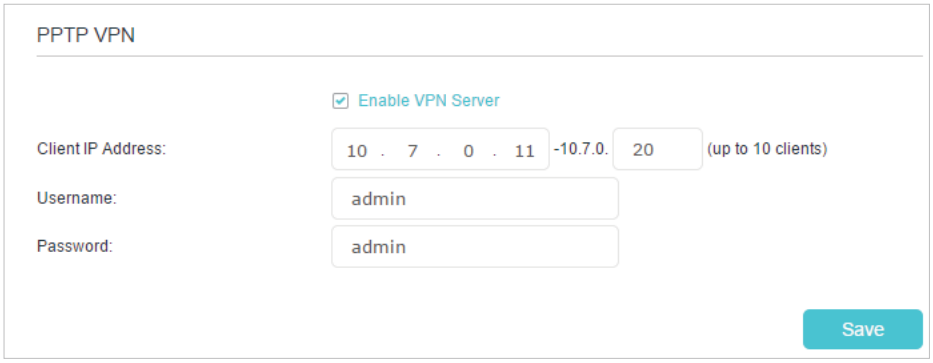
Tips:
You can go to Advanced > VPN > VPN Connections to view the clients that are currently connected to the OpenVPN servers.

11. 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 AP

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



Note:

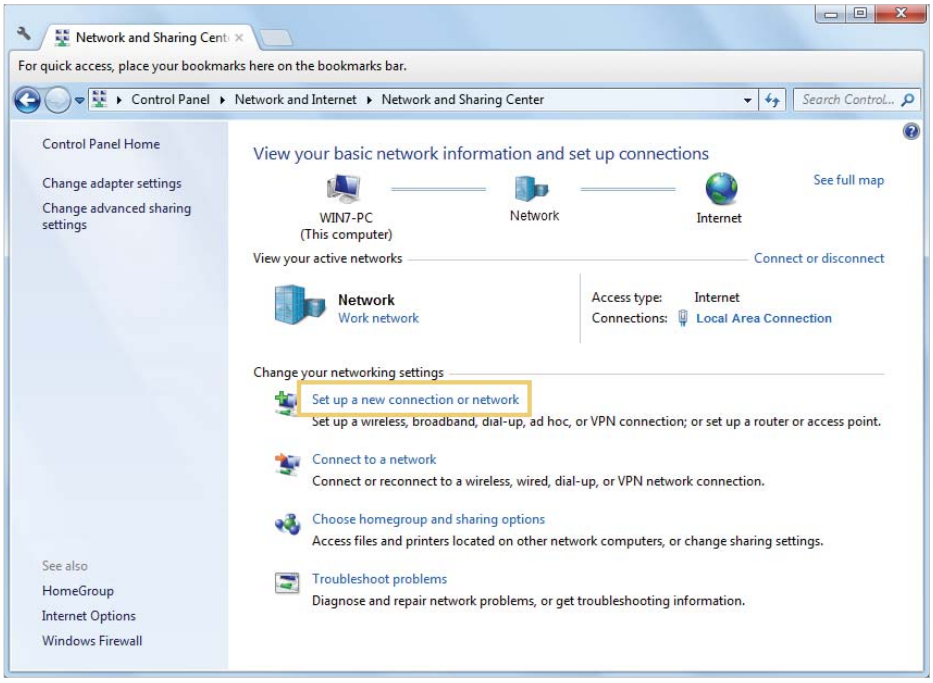
Before you enable VPN Server, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for AP's WAN port and synchronize your System Time with internet.

3. In the Client IP Address filed, 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.

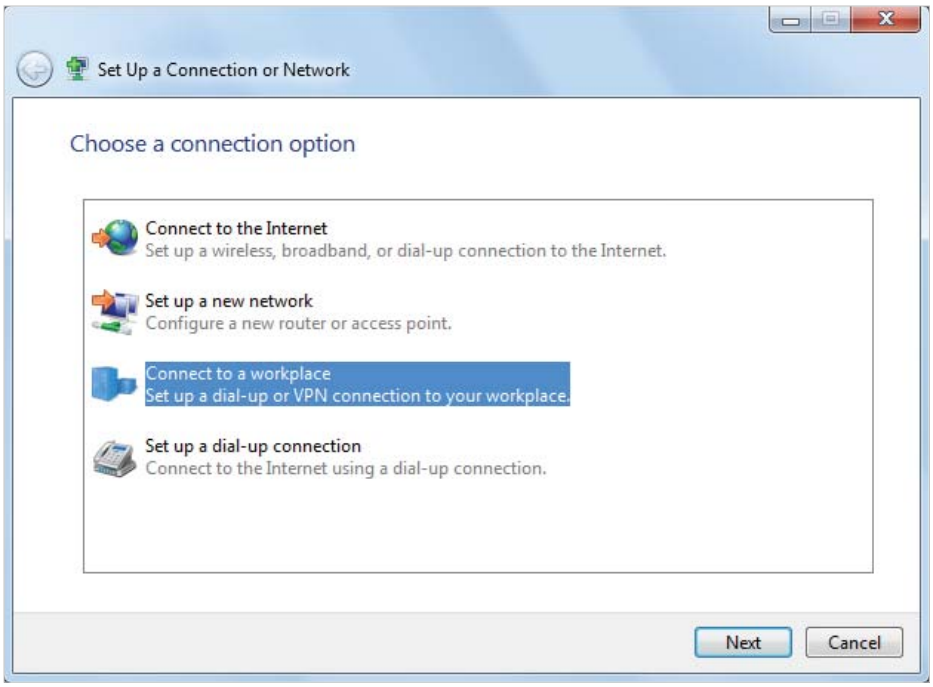
Step 2. Configure PPTP VPN Connection on Your Remote Device

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.

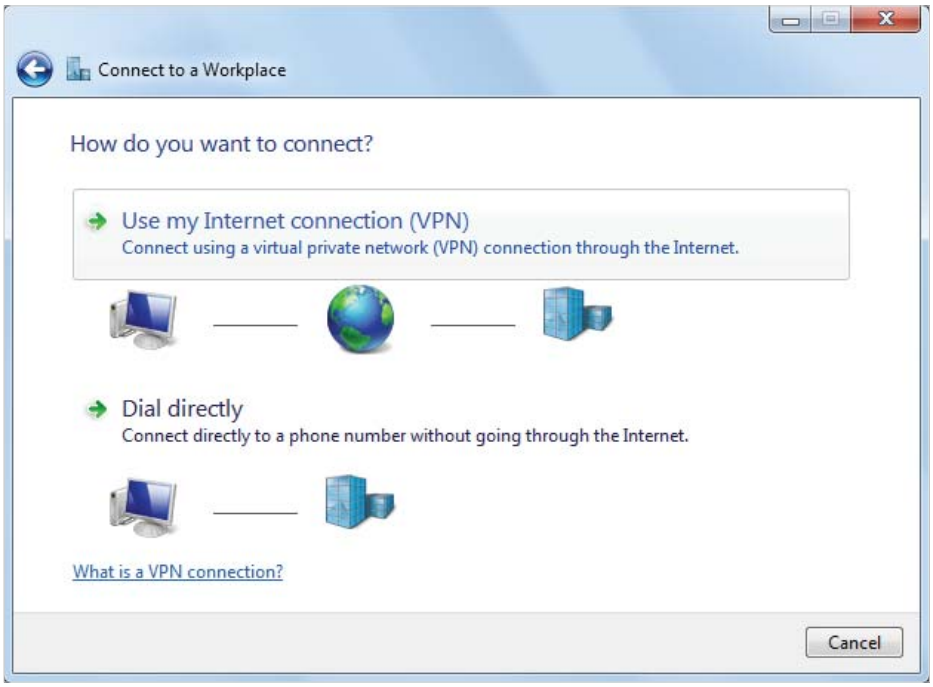
1. Go to Start > Control Panel > Network and Internet > Network and Sharing Center.
2. Select Set up a new connection or network.



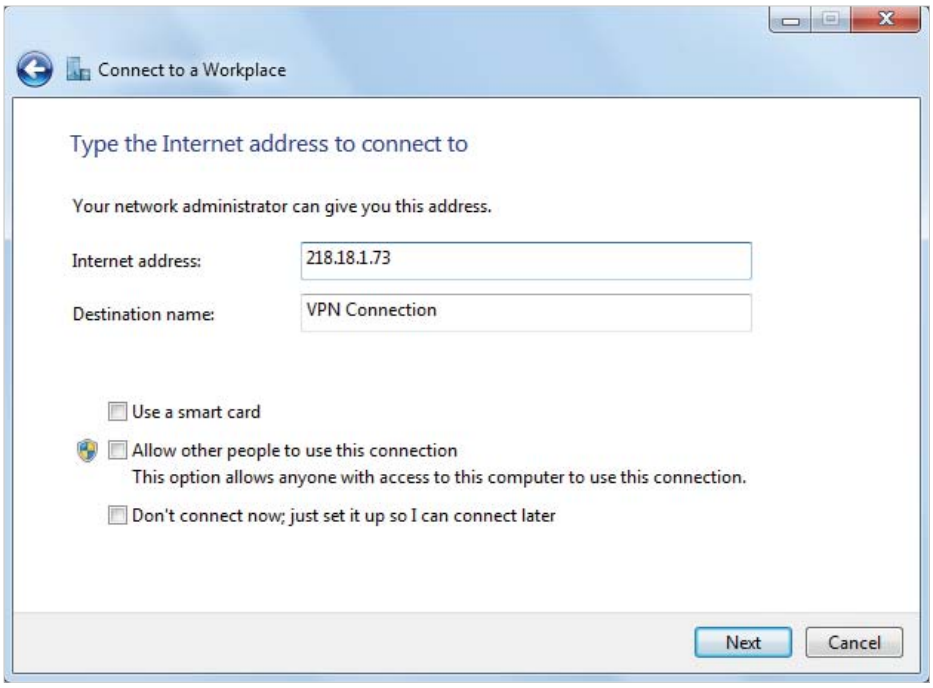
3. Select Connect to a workplace and click Next.



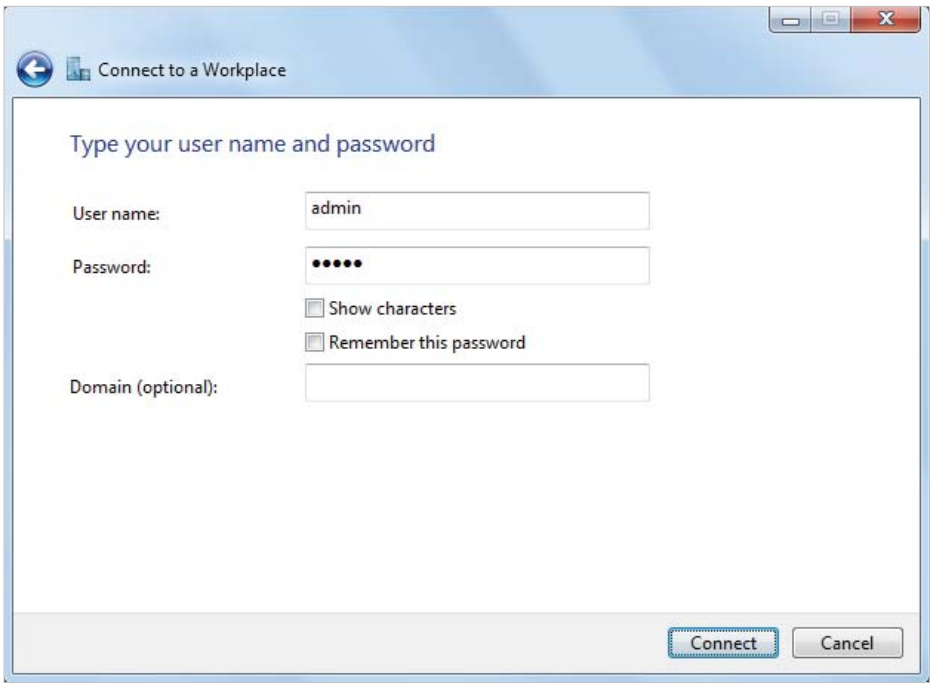
4. Select Use my Internet connection (VPN).



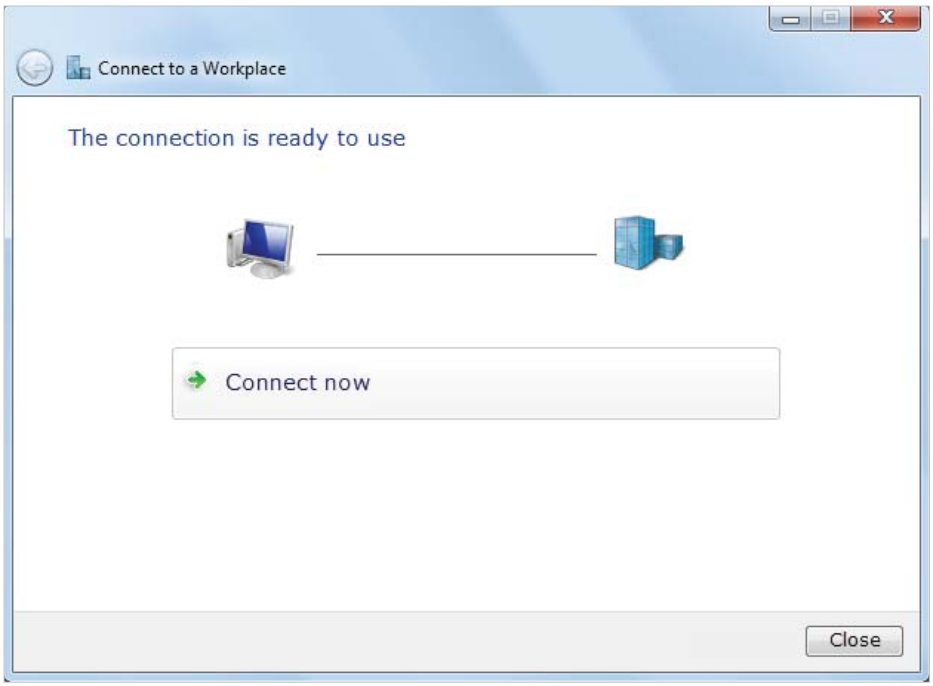
5. Enter the internet IP address of the AP (for example: 218.18.1.73) in the Internet address field. Click Next.



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



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

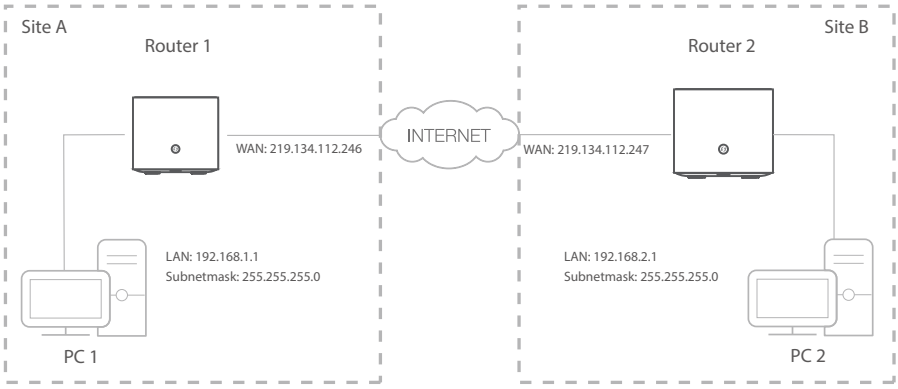


Tips:
You can go to Advanced > VPN > VPN Connections to view the clients that are currently connected to the PPTP VPN servers.

11. 3. Use IPSec VPN to Access Your Home Network

IPSec VPN is used to create a VPN connection between local and remote networks. To use IPSec VPN, you should check that both local and remote routers support IPSec VPN feature. Then, follow the steps below to set up an IPSec VPN connection.

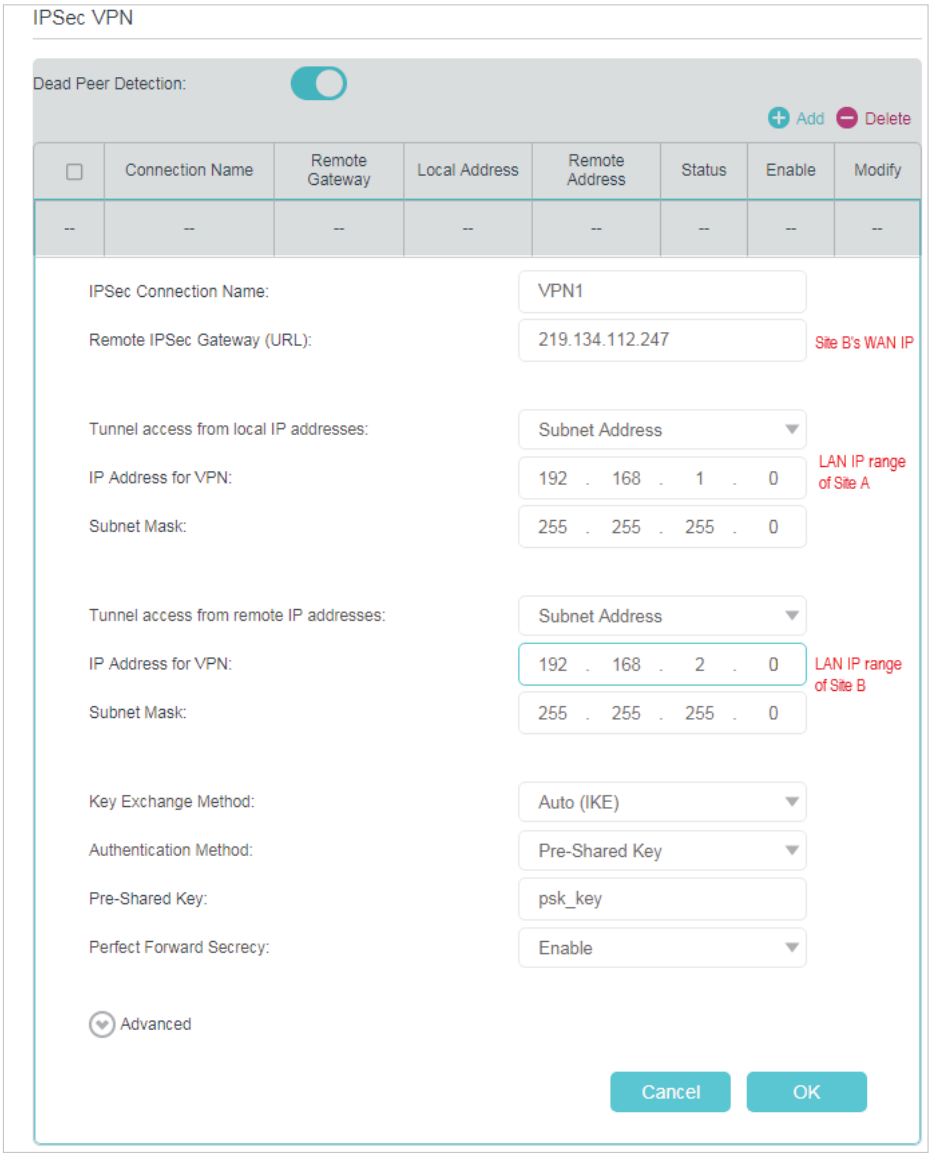
1. The typical VPN topology is here. Site A refers to local network, and Site B refers to the remote network that is to be connected. Record Site A and Site B's LAN and WAN IP addresses before you start configuration.



2. Configuration on Site A (local network).

1) Visit http://tplinkmodem.net, and log in with the password you set for the router.

2) Go to Advanced > VPN > IPSec VPN, and click Add.



3) In the IPSec Connection Name column, specify a name.

4) In the Remote IPSec Gateway (URL) column, Enter Site B's WAN IP address.

5) Configure Site A's LAN.
In the Tunnel access from local IP addresses column, we take Subnet Address as an example. Input the LAN IP range of Site A in the IP Address for VPN column, and input Subnet Mask of Site A.

6) Configure Site B's LAN.
In the Tunnel access from remote IP addresses column, we take Subnet Address as an example. Input the LAN IP range of Site B in the IP Address for VPN column, and input Subnet Mask of Site B.

7) Select the Key Exchange Method for the policy. We select Auto(IKE) here.

8) Enter the Pre-Shared Key for IKE authentication. Then keep Perfect Forward Secrecy enabled.

Note: Make sure Site A and Site B use the same key.

9) Leave the Advanced Settings as default value. Then click OK.

	Connection Name	Remote Gateway	Local Address	Remote Address	Status	Enable	Modify
☐	VPN1	219.134.112.247	192.168.1.0	192.168.2.0	Down		

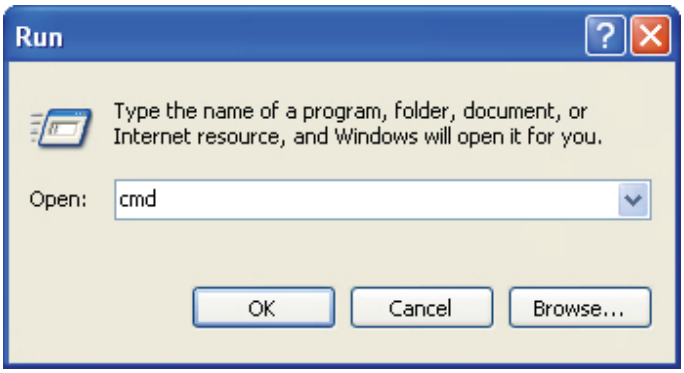
Note: The Status column is Down after the configuration, and it will change to UP only when Site A and Site B are communicating via the VPN connection.

3. Configuration on Site B (remote network). Refer to step 2 configuration on Site A and make sure that Site A and Site B use the same pre-shared keys and Perfect Forward Secrecy settings.

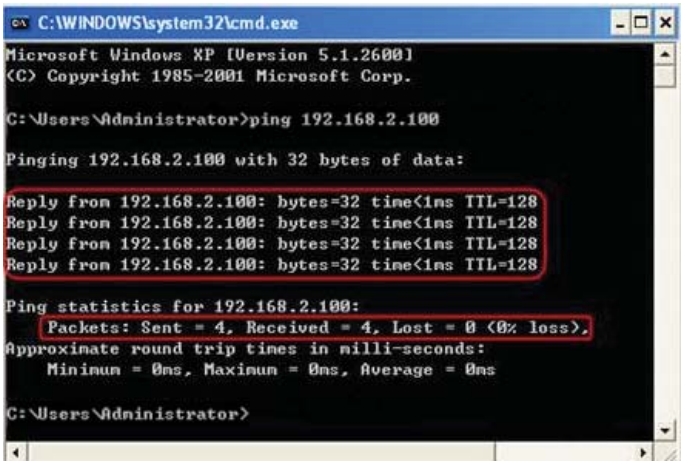
4. Check the VPN connection. You can ping site B' LAN IP from your computer in site A to verify that the IPSec VPN connection is set up correctly.

Tips: To check the VPN connection, you can do the following.

1. On the host in Site A, press [Windows Logo] + [R] to open Run dialog. Input "cmd" and hit OK.



2. In the CLI window, type in "ping 192.168.2.x" ("192.168.2.x" can be IP address of any host in Site B). Then press [Enter].



3. If Ping proceeds successfully (gets replies from host in Site B), the IPSec connection is working properly now.

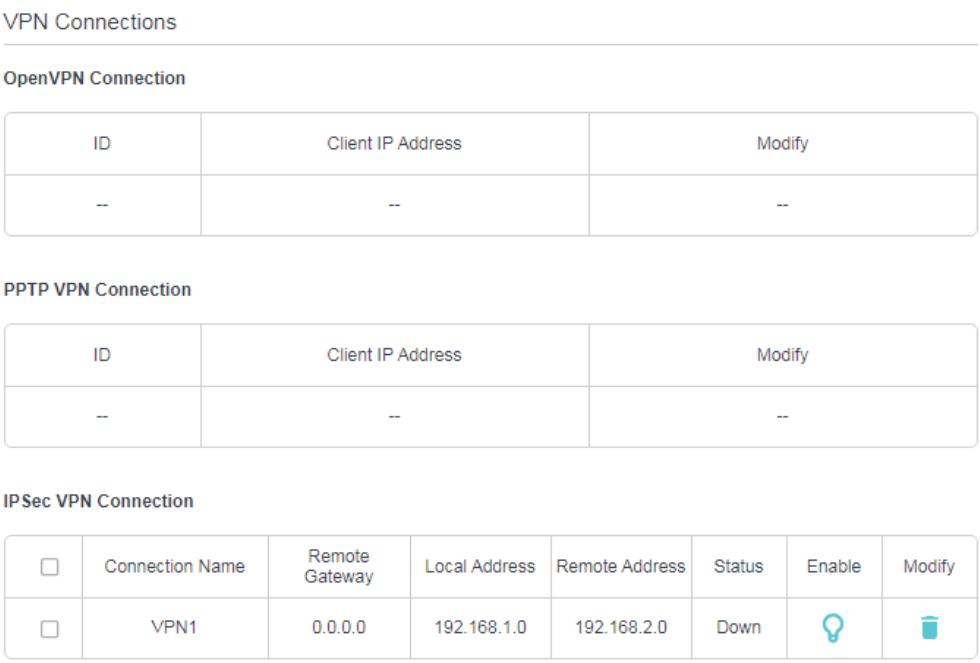
5. Now IPSec VPN is implemented to establish a connection.

Note:

1. The product supports a maximum of ten simultaneous connections.
2. If one of the site has been offline for a while, for example, if Site A has been disconnected, on Site B you need to click Disable and then click Enable after Site A back on line in order to re-establish the IPSec tunnel.

11. 4. VPN Connections

You can view the clients that are currently connected to the OpenVPN servers, PPTP VPN servers and IPSec VPN hosted on the router on the VPN Connection page.



Chapter 12

Customize Your Network Settings

This chapter introduces how to change the default settings or adjust the basic configuration of the network setting of the AP 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
- Activate RIP
- Set Up the IPv6 Tunnel
- Specify Wireless Settings
- Use WPS for Wireless Connection

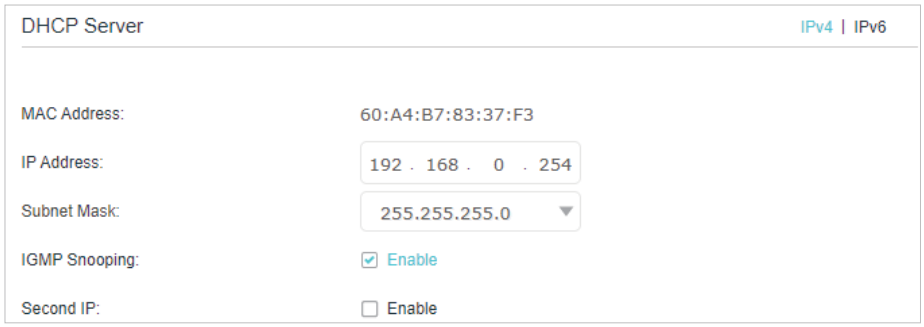
12. 1. Change LAN Settings

12. 1. 1. Change the LAN IP Address

The AP is preset with a default LAN IP 192.168.0.254 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 AP.
2. Go to Advanced > Network > LAN Settings, and select IPv4.



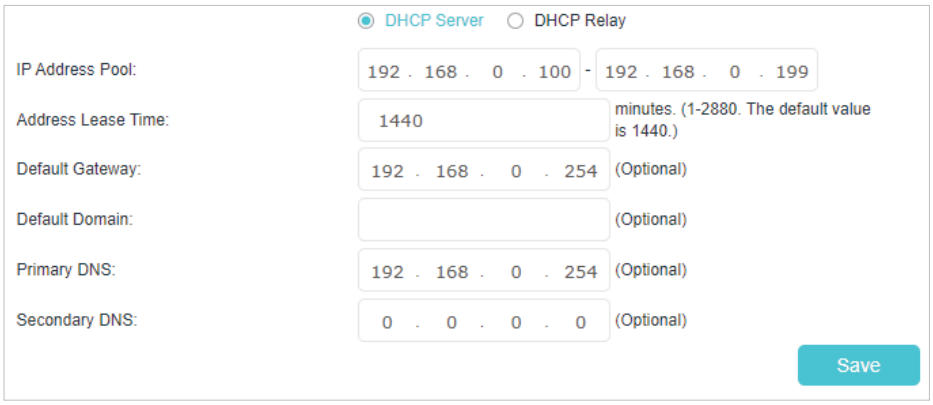
3. Enter a new IP Address appropriate to your needs.
4. Select the Subnet Mask from the drop-down list. The subnet mask together with the IP address identifies the local IP subnet.
5. Keep IGMP Snooping enabled by default. IGMP snooping is the process of listening to IGMP (Internet Group Management Protocol)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

12. 1. 2. Use the AP as a DHCP Server

You can configure the AP to act as a DHCP server to assign IP addresses to its clients. To use the DHCP server function of the AP, 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 AP.
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 AP 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 AP. 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:

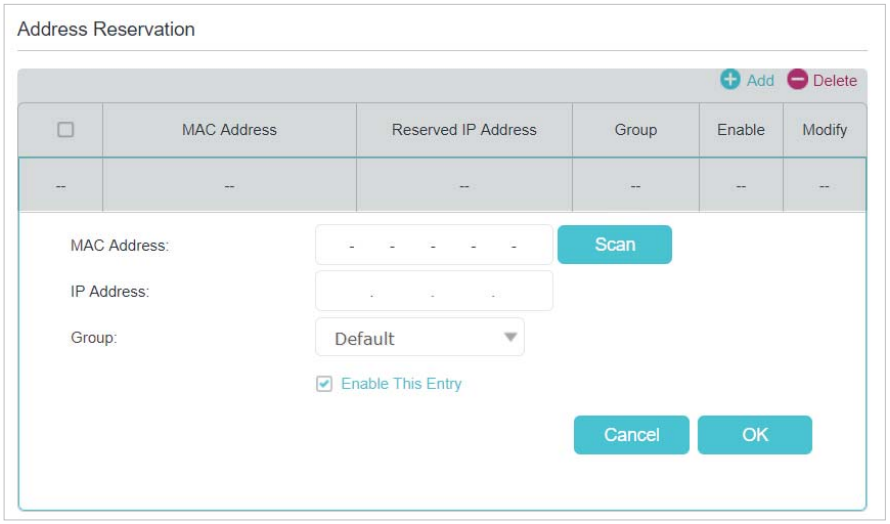
1. The AP can be configured to work as a DHCP Relay. A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. If it is enabled, the DHCP requests from 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 to192.168.0.80) 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.

12. 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 AP 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 AP.
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.



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 AP.
6. Keep the Enable This Entry check box selected and click OK to make the settings effective.

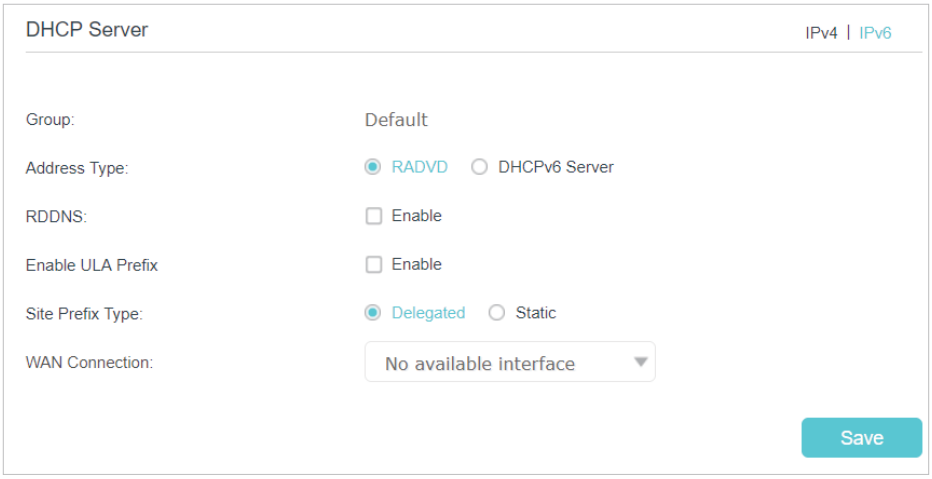
12. 2. Configure IPv6 LAN Settings

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

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

12. 2. 1. Configure the RADVD Address Type

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



1) Select the RADVD as the address type to make the AP assign IPv6 address prefixes to hosts.

Note:

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

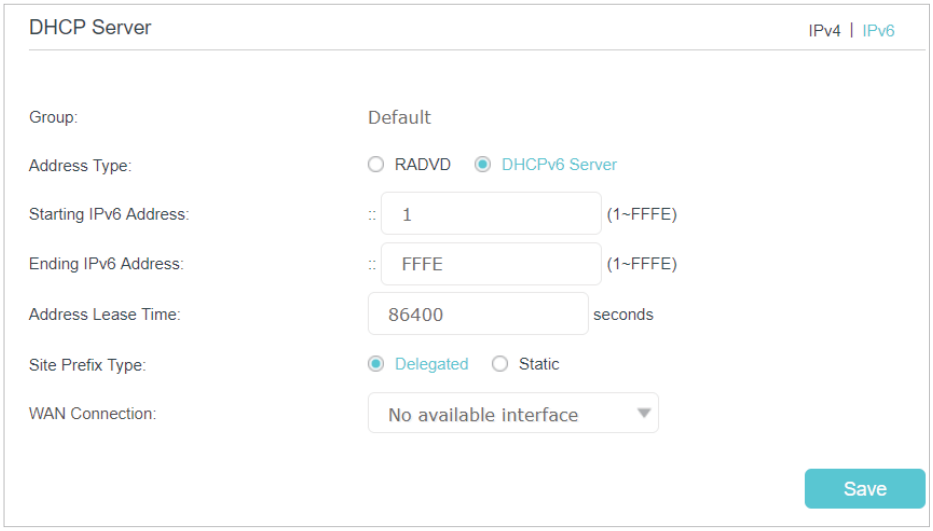
2) Keep Site Prefix Type as the default value Delegated. If your ISP has provided a specific IPv6 site prefix, select Static and enter the prefix.

3) Keep WAN Connection as the default setting.

4. Click Save to make the settings effective.

12. 2. 2. Configure the DHCPv6 Server Address Type

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



1) Select the DHCPv6 Server as the address type to make the AP assign IPv6 addresses to hosts.

2) Specify the Starting/Ending IPv6 Address for the IPv6 suffixes. The AP 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.

12. 3. Set Up a Dynamic DNS Service Account

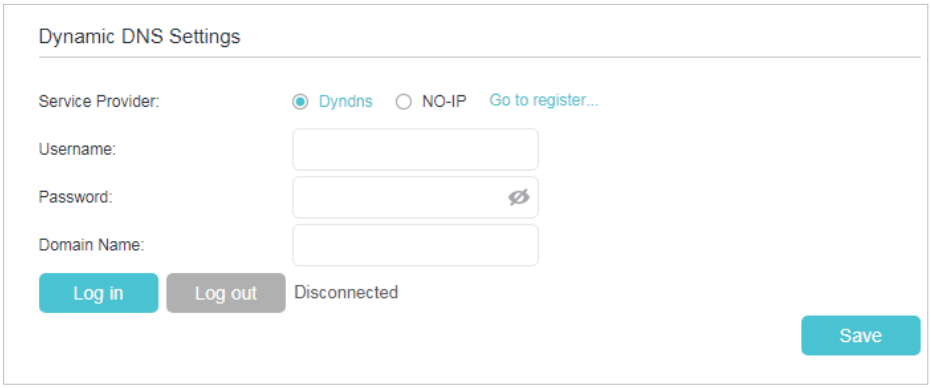
Most ISPs (Internet service providers) assign a dynamic IP address to the router and you can use this IP address to access your router remotely. However, the IP address can change any time and you don't know when it changes. In this case, you might need the DDNS (Dynamic Domain Name Server) feature on 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 AP.

To set up DDNS, please follow the instructions below:

1. Visit http://tplinkwifi.net, and log in with the password you set for the AP.
2. Go to Advanced > Network > Dynamic DNS.
3. Select the Service Provider (Dyndns or NO-IP). Enter the username, password and domain name of the account (such as lisa.ddns.net)

4. If you don't have a DDNS account, you have to register first by clicking click Go to register ... .



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.

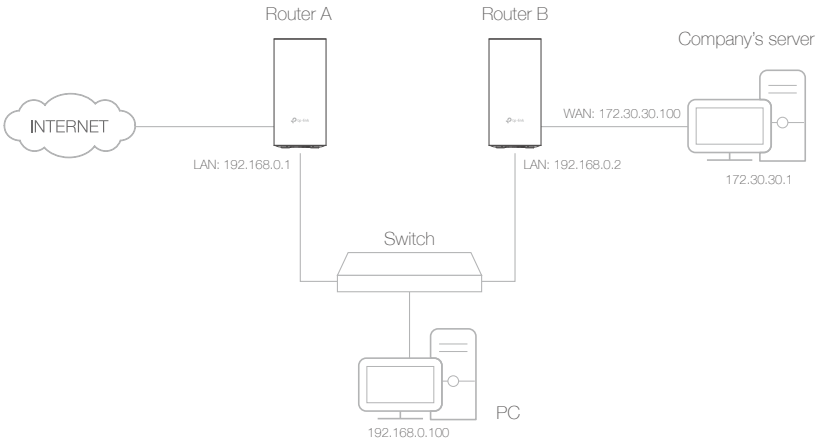
12. 4. Create Static Routes

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:

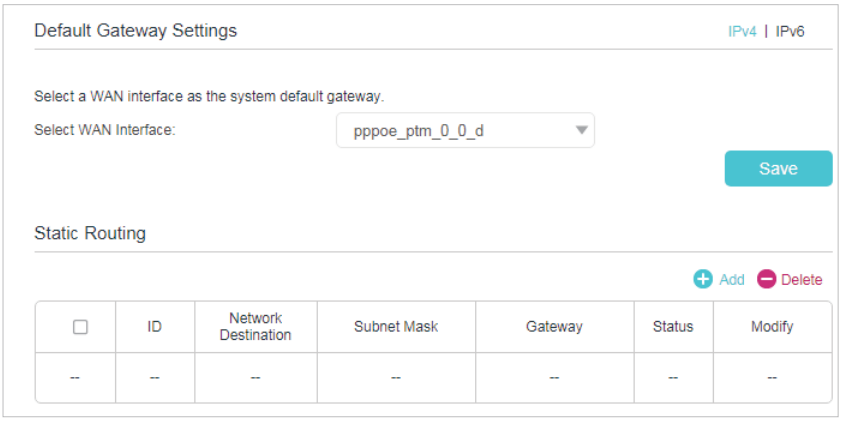
Visit multiple networks and multiple servers at the same time.

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.

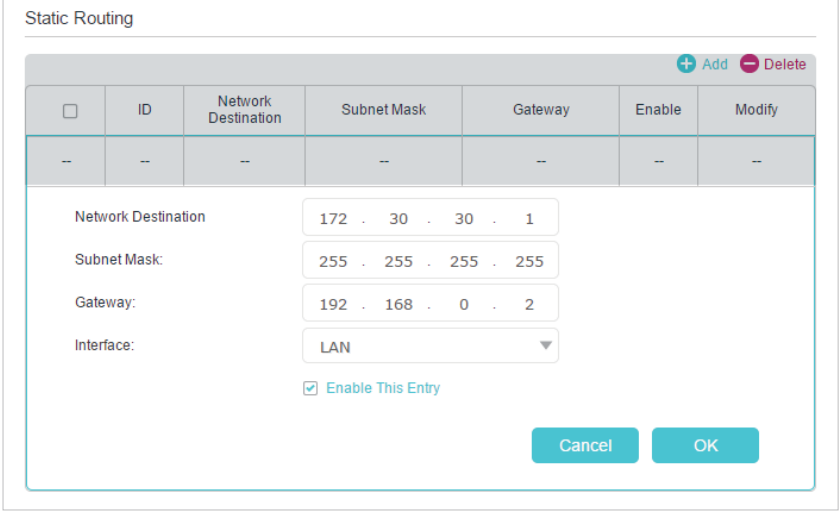


How can I do that?

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.



4. Click Add to add a new static routing entry. Finish the settings according to the following explanations:



- Network Destination: The destination IP address that you want to assign to a static route. This IP address cannot be on the same subnet with the WAN IP or LAN IP of Router A. In the example, the IP address of the company network is the destination IP address, so here enter 172.30.30.1.
- Subnet Mask: Determines the destination network with the destination IP address. If the destination is a single IP address, enter 255.255.255.255; otherwise, enter the subnet mask of the corresponding network IP. In the example, the destination network is a single IP, so here enter 255.255.255.255.
- 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!

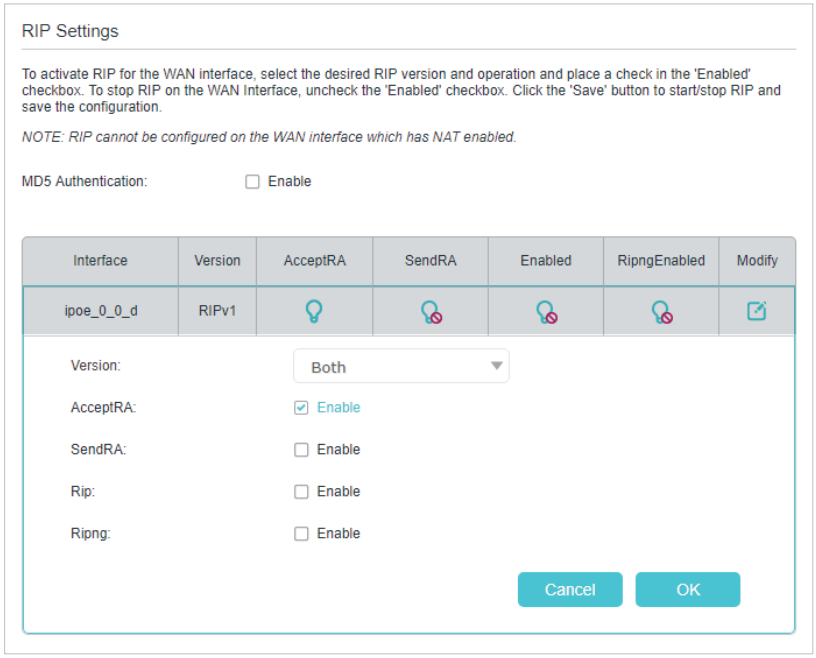
Open a web browser on your PC. Enter the company server's IP address to visit the company network.

12. 5. Activate RIP

RIP (Routing Information Protocol) is a distance-vector routing protocol which can be used to exchange topology information between routers. Generally, it is used in small to medium-sized network as an Interior Gateway Protocol. RIP uses the UDP (User Datagram Protocol) as its transport protocol.

- **To enable RIP**

1. Visit http://tplinkwifi.net, and log in with the password you set for the AP.
2. Go to Advanced > Network > RIP Settings. Click the icon to modify the settings according to your needs.



- Version: Select the RIP protocol version.
- AcceptRA: Enable the router to accept Router Advertisement.
- SendRA: Enable the router to send Router Advertisement.
- Rip: Enable the RIP settings for IPv4.
- Ripng: Enable the RIP settings for IPv6. RIPng is designed for the exchange of routing information through an IPv6-based network.

3. Click OK to make the settings effective.

Note:

NAT does not work on the WAN interface with NAT function enabled. You can go to Advanced > Network > Internet to click the corresponding icon of the WAN Interface to find the advanced option, and then disable the NAT function.

12. 6. 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 AP provides four tunneling mechanisms: 6to4, 6rd, DS-Lite, and Map-T. The methods of setting up 6rd and DS-Lite tunnel are similar.

12. 6. 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 AP.
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:

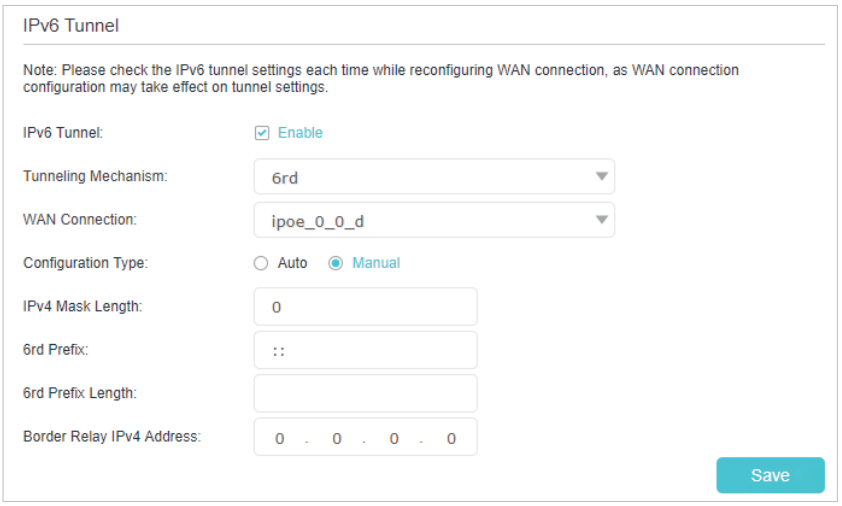
If you still can't access IPv6 resources, it may means that no 6to4 public server was found in your network. You can contact your ISP to sign up for IPv6 connection service.

12. 6. 2. Specify the IPV6 Tunnel with Parameters Provided by Your ISP

➢ To specify the 6rd Tunnel

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

1. Visit http://tplinkwifi.net, and log in with the password you set for the AP.
2. Go to Advanced > Network > IPv6 Tunnel.
3. Tick the check box, 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.



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.

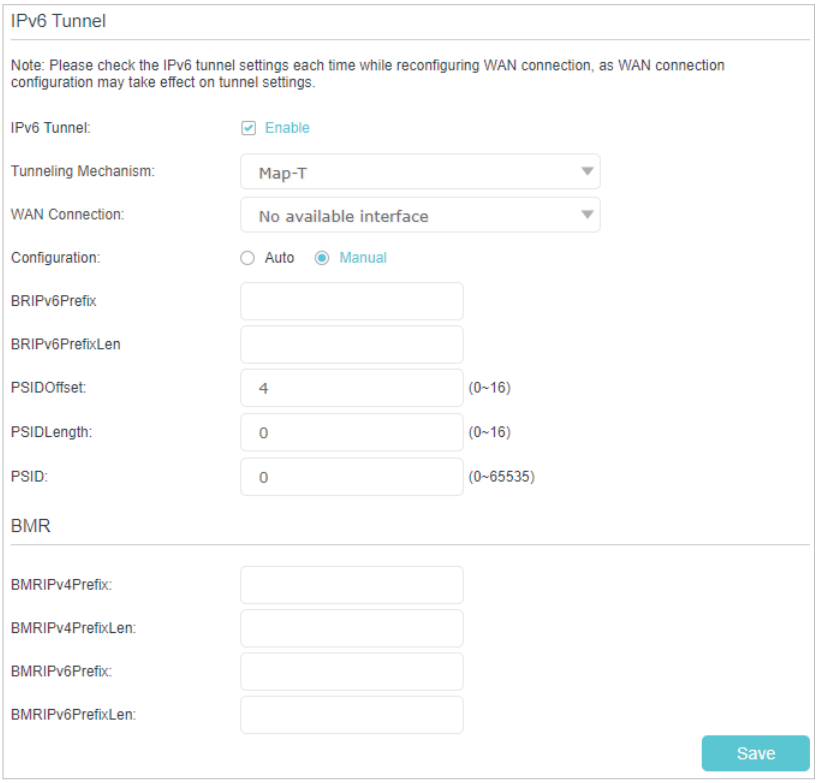
Done! Now you can visit the IPv6 websites with the 6rd tunnel.

Tips:
The way to set up DS-Lite tunnel is 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.

➢ To specify the Map-T Tunnel

I want to: Specify the Map-T tunnel with the parameters provided by my Map-T tunnel service provider.

1. Visit http://tplinkwifi.net, and log in with the password you set for the AP.
2. Go to Advanced > Network > IPv6 Tunnel.
3. Tick the check box, select Map-T 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.



Note:

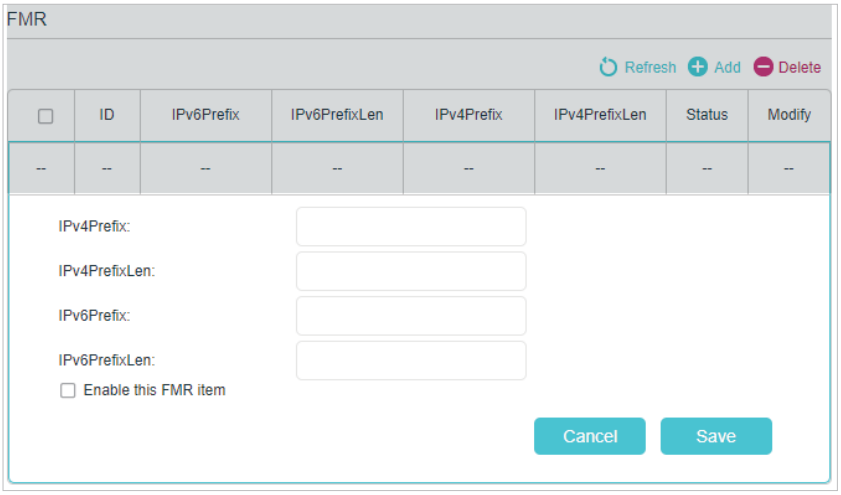
If there is no available WAN connection to choose, make sure you have connected to the internet and the connection type is not Bridge.

Done!

Now you can visit the IPv6 websites with the Map-T tunnel.

Note:

If your ISP provides more parameters for Forwarding Mapping Rules, you can locate to FMR section and click Add to configure and enable a FMR item.



12. 7. Specify Wireless Settings

12. 7. 1. Change Basic Wireless Settings

The AP'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 AP.

➢ **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 AP, 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.

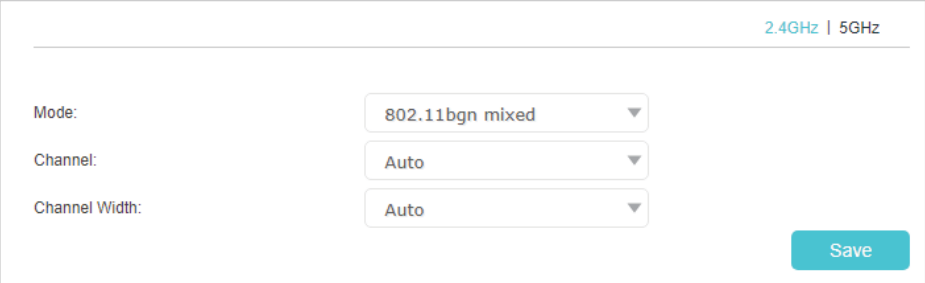
➢ **To enable or disable band steering:**

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.



2. Select the wireless network mode or channel and click Save to make the settings effective.

Mode: Select the desired transmission mode.

Note: It is strongly recommended that you keep the default settings.

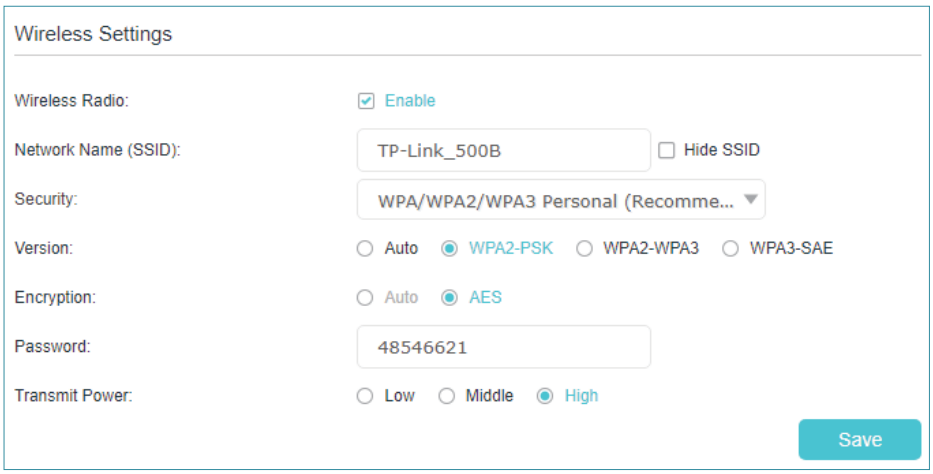
Channel: Select the channel you want to use from the drop-down list. This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

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.

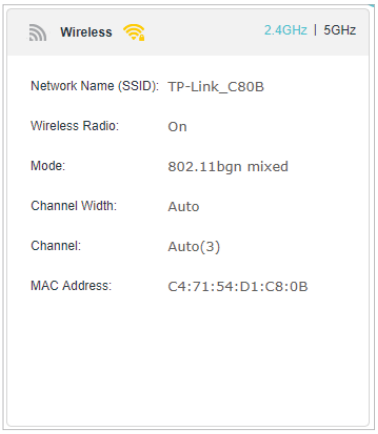


2. Select an option from the Security drop-down list and configure the related parameters. The router provides threr options, No Security, WPA/WPA2/WPA3 personal (Recommended), and WPA/WPA2 enterprise. WPA3 is the latest standard and the security level is the highest. We recommend you don't change the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

12. 7. 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 AP.
2. Go to Advanced > Status page. You will find the Wireless panel.
3. Click 2.4GHz or 5GHz to view the wireless details.



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.

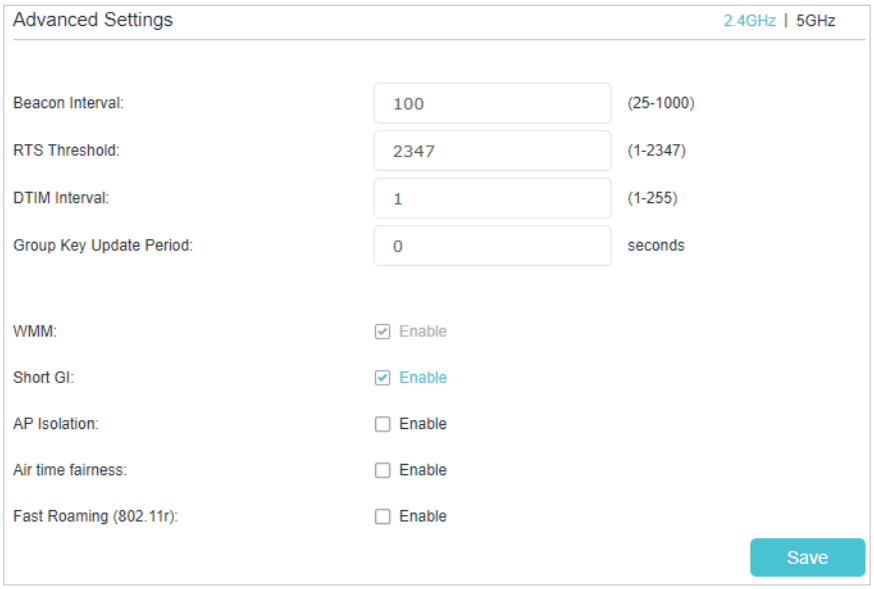
2. Go to Advanced > Wireless > Statistics page.
3. You can view the detailed information of the wireless clients, including its connection type and security option as well as the packets transmitted.

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

12. 7. 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 AP.
2. Go to Advanced > Wireless > Advanced Settings.



- Beacon Interval: Enter a value between 25 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 2347 to determine the packet size of data transmission through the router. By default, the RTS (Request to Send) Threshold size is 2347. 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.

12. 8. 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 AP.
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.

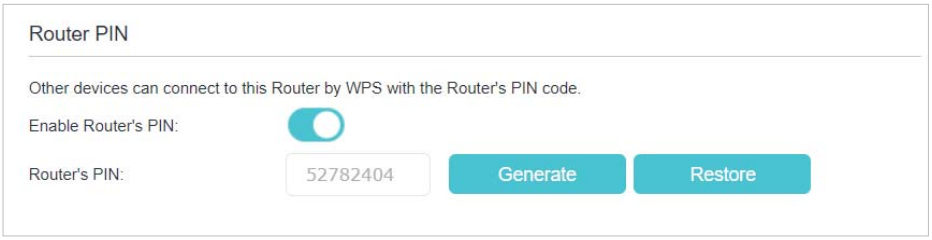
1. Visit http://tplinkwifi.net, and log in with the password you set for the AP.
2. Go to Advanced > Wireless > WPS, and locate the WPS Settings section.

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 AP.

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

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

1. Visit http://tplinkwifi.net, and log in with the password you set for the AP.
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 AP. You can also click the Generate button to get a new PIN.
4. On the client device, enter the AP's PIN. (The default PIN is also printed on the label of the AP.)
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 AP is disabled. Please make sure the wireless function is enabled before configuring the WPS.

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

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

Chapter 13

Manage Your AP

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

It contains the following sections:

- Set System Time
- Control LED
- Test Internet Connectivity
- Update the Firmware
- Back Up and Restore Configuration Settings
- Reboot the AP
- Administration Management
- System Log
- CWMP Settings
- SNMP Settings
- Monitor the Internet Traffic Statistics

13. 1. Set System Time

System time is the time displayed while the AP 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 AP.
2. Go to Advanced > System Tools > Time Settings page.

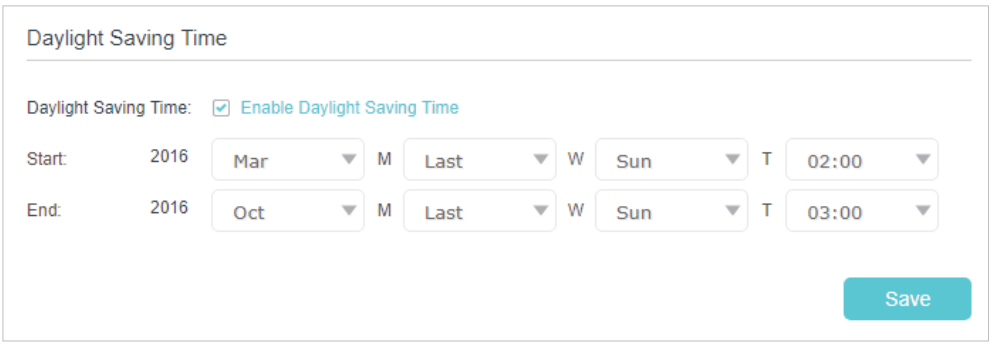
3. Configure the system time using the following methods:

   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 AP can access the internet before you select this way to get system time.

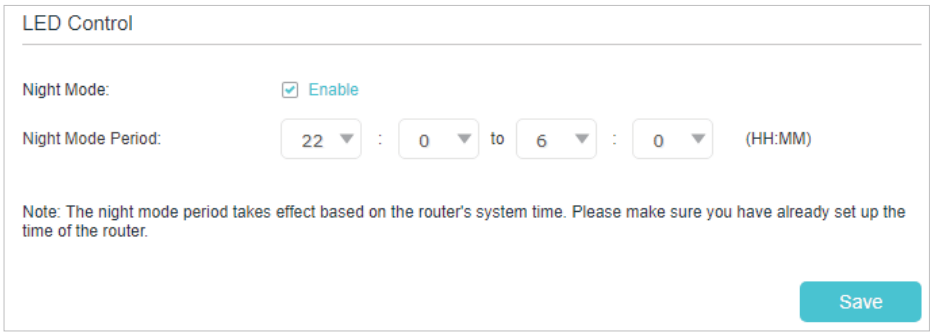
4. Click Save to make the settings effective.
5. After setting the system time, you can set Daylight Saving Time according to your needs. Select the Enable Daylight Saving Time check box to enable daylight saving, set the start and end time, and then click Save to make the settings effective.



13. 2. Control LED

The LEDs indicate the AP activities and behaviors. You can turn on or turn off the AP from the management web-page.

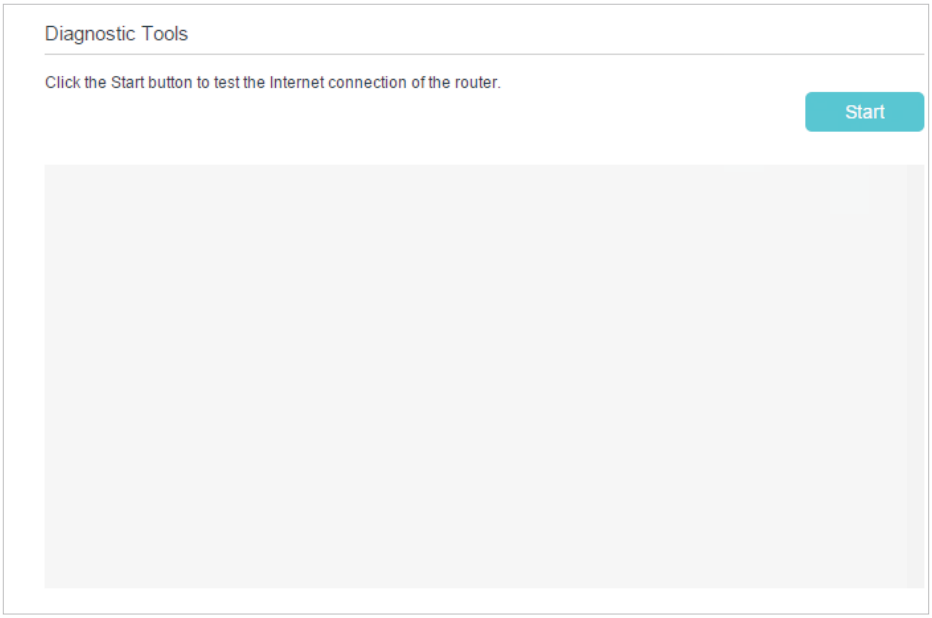
1. Visit http://tplinkwifi.net, and log in with the password you set for the AP.
2. Go to Advanced > System Tools > LED Control, and enable Night Mode.
3. Specify the Night Mode Period according to your need, and the LEDs will be off during this period.
4. Click Save to make the settings effective.



13. 3. Test Internet Connectivity

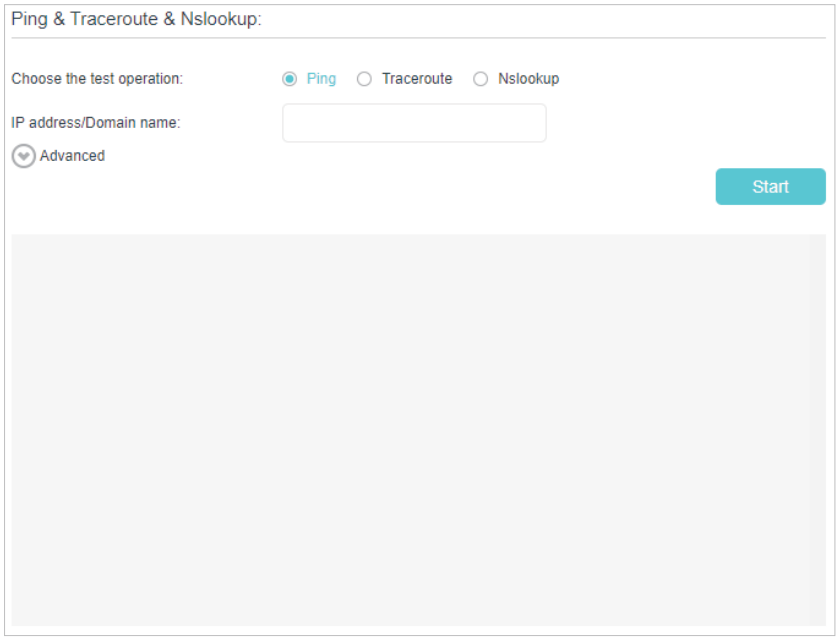
Diagnostics is used to test the connectivity between the AP and the host or other network devices.

1. Visit http://tplinkwifi.net, and log in with the password you set for your AP.
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.

Locate to Ping & Traceroute & Nslookup, you can test the internet by using Ping, Traceroute or Nslookup method.



Ping: Enter the IP address of host, you can send ICMP ECHO_REQUEST packets to network host and the diagnostic result will be display. Ping is used to test the connectivity between the router and the tested host, and measure the round-trip time.

Traceroute: Enter the IP address of host, you can print the route packets trace to network host and the diagnostic result will be display. Traceroute is used to display the route

(path) your router has passed to reach the tested host, and measure transit delays of packets across an Internet

Protocol network.

Nslookup: Enter the Domain name, you can check whether DNS is resolving domain name normally and the diagnostic result will be display.

Note:

Click Advanced, you can modify the ping count, ping packet size or the Traceroute Max TTL. It's recommended to keep the default value.

13. 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 AP. 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 AP and your computer. It is NOT recommended to upgrade the firmware wirelessly.
2. Back up your AP configuration before upgrading the firmware.
3. DO NOT turn off the AP during the firmware upgrade.

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

1. Download the latest firmware file for the AP from our website www.tp-link.com.
2. Visit http://tplinkwifi.net, and log in with the password you set for the AP.
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.

Note:

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

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

13. 5. Back Up and Restore Configuration Settings

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

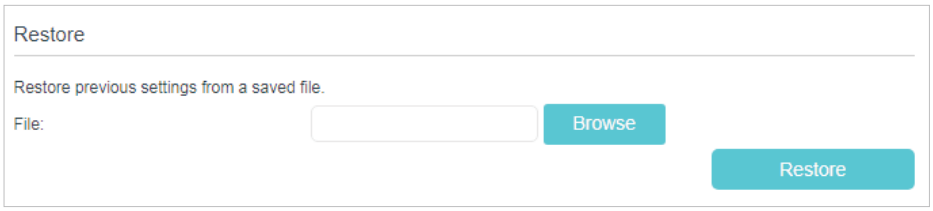
1. Visit http://tplinkwifi.net, and log in with the password you set for the AP.
2. Go to Advanced > System Tools > Backup & Restore.

➢ **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:**

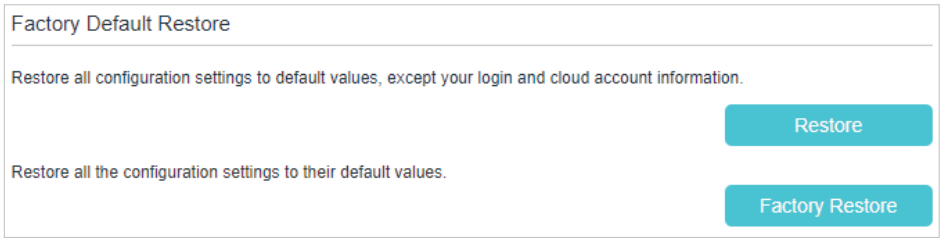
1. Click Browse to locate the backup configuration file stored on your computer, and click Restore



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

➢ **To reset the AP to factory default settings:**

1. Click Restore under the Factory Default Restore session to reset all configuration settings to default values, except your login and cloud account information.
2. Click Factory Restore to restore all the configuration settings to their default values.



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

Note:

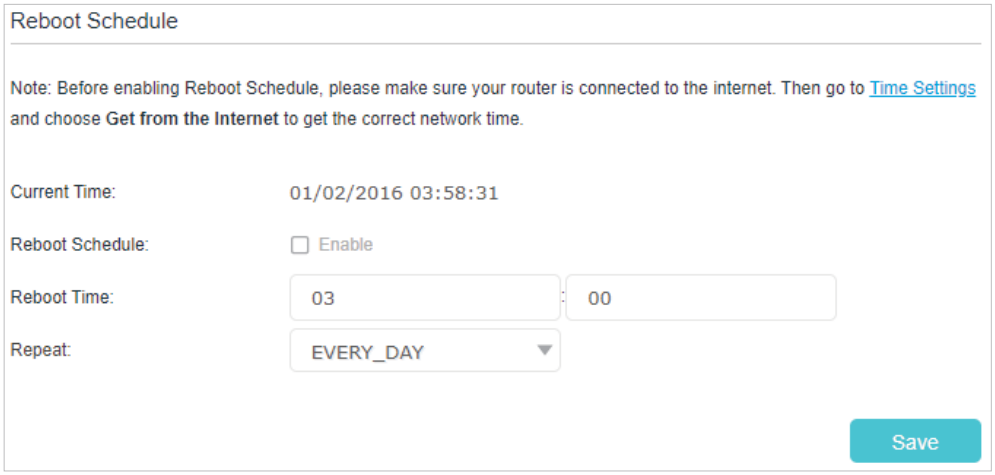
1. During the resetting process, do not turn off the AP.
2. We strongly recommend you back up the current configuration settings before resetting the AP.
3. If you want to reset the AP into its factory default settings, you need to add the agent again to create a mesh Wi-Fi system.

13. 6. Reboot the AP

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

➢ **To schedule the AP to reboot at a specific time:**

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



4. Click Save to make the settings effective.

Note:

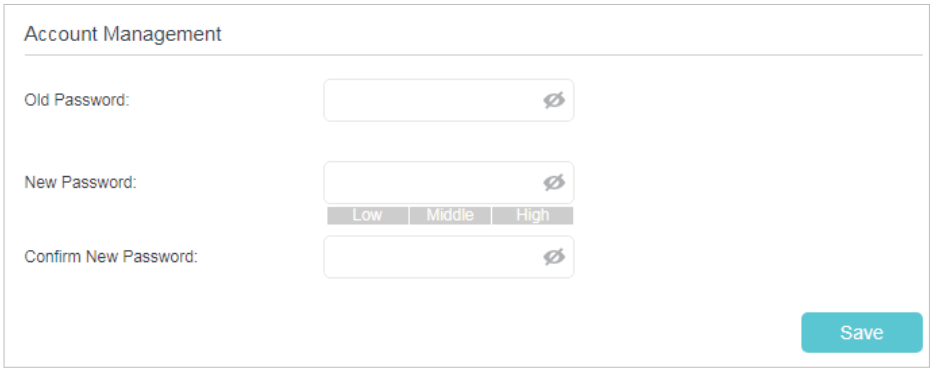
The Auto Reboot feature takes effect based on the AP's system time. Please make sure you have already set the time of the AP.

13. 7. Administration Management

13. 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 AP.
2. Go to Advanced > System Tools > Administration page. Locate the Account Management section.



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.

13. 7. 2. Local Management

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

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

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

4. Click Save.

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

Note:
If you want all local devices can manage the AP, just leave the IP/MAC Address field blank.

13. 7. 3. Remote Management

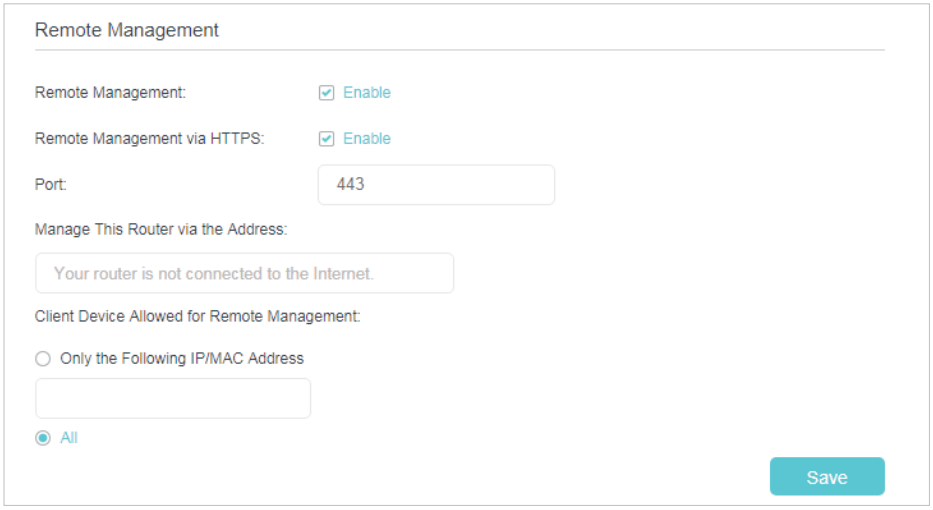
By default, the remote devices are not allowed to manage the AP from the internet. You can enable remote management over HTTP and/or HTTPS if needed. HTTPS is a more secure way to access the AP.

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 AP over HTTPS.

1. Visit http://tplinkwifi.net, and log in with the password you set for the AP.
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 AP. If you just want to allow a specific device to manage the AP, 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 AP using the address displayed on the Manage This Router via the Address field to manage the AP.

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 AP's web management page at Advanced > System Tools > Administration.

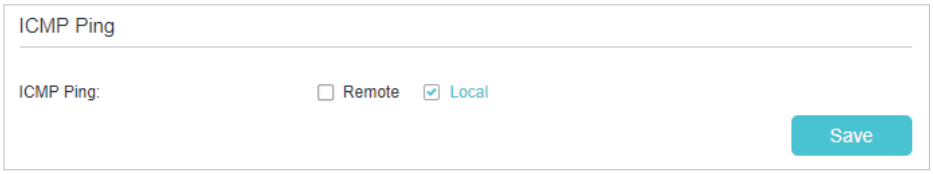
2. The AP's WAN IP is usually a dynamic IP. Please refer to Set Up a Dynamic DNS Service Account if you want to log in to the AP through a domain name.

13. 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 AP's replies to ICMP Ping requests.

1. Visit http://tplinkwifi.net, and log in with the password you set for the AP.
2. Go to Advanced > System Tools > Administration, and locate the ICMP Ping section.

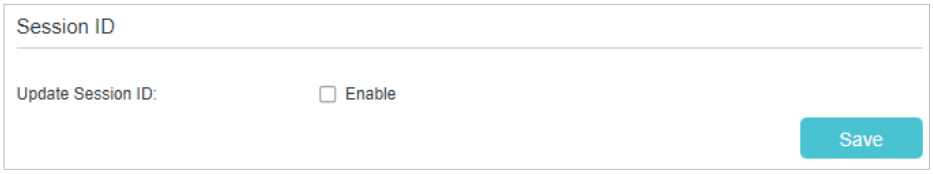


3. Specify the ICMP Ping reply options.
   - Remote: Select it if you want the computers on a public network to ping the AP's WAN IP address.
   - Local: Enabled by default, if enabled, the computers on a private network can ping the AP's LAN IP address.
4. Click Save to make the settings effective.

13. 7. 5. Session ID

When Session ID function is enabled, it will be saved into Flash every time the PPP connection is updated. This can prevent some problems of PPPoE/L2TP/PPTP connection being rejected to reconnect to servers when the device is powered off or the network disconnect accidentally.

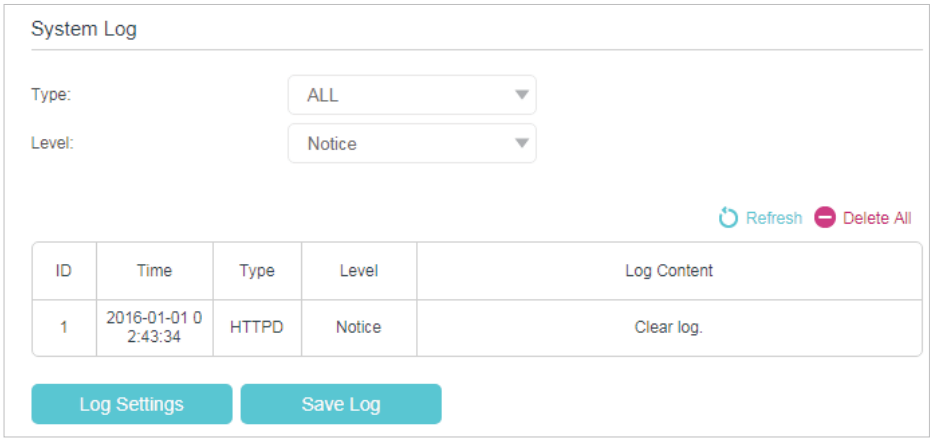
1. Visit http://tplinkwifi.net, and log in with the password you set for the AP.
2. Go to Advanced > System Tools > Administration, and locate the Session ID section.
3. Select the checkbox to update the Session ID,



13. 8. System Log

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

1. Visit http://tplinkwifi.net, and log in with the password you set for the AP.
2. Go to Advanced > System Tools > System Log page.



➢ **To view the system logs:**

You can view specific system logs by selecting the log type and level.

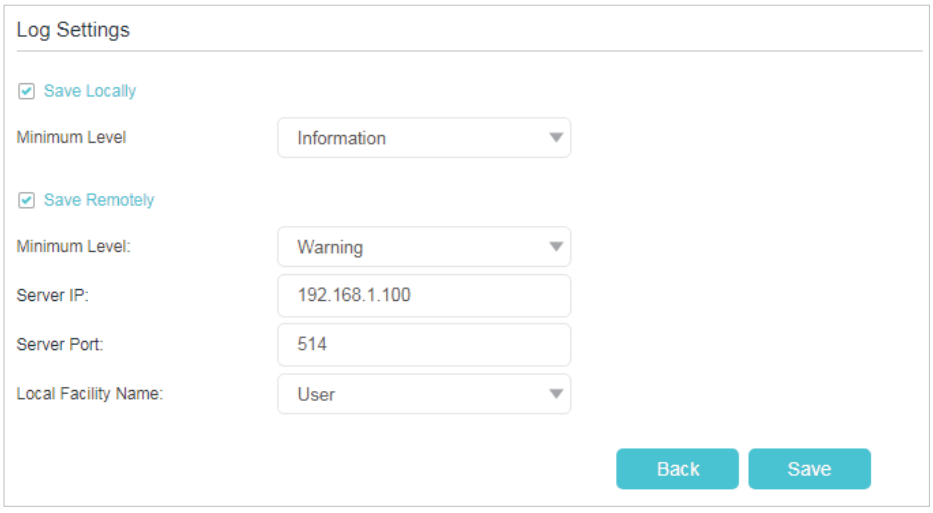
Click Refresh to refresh the log list.

➢ **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.

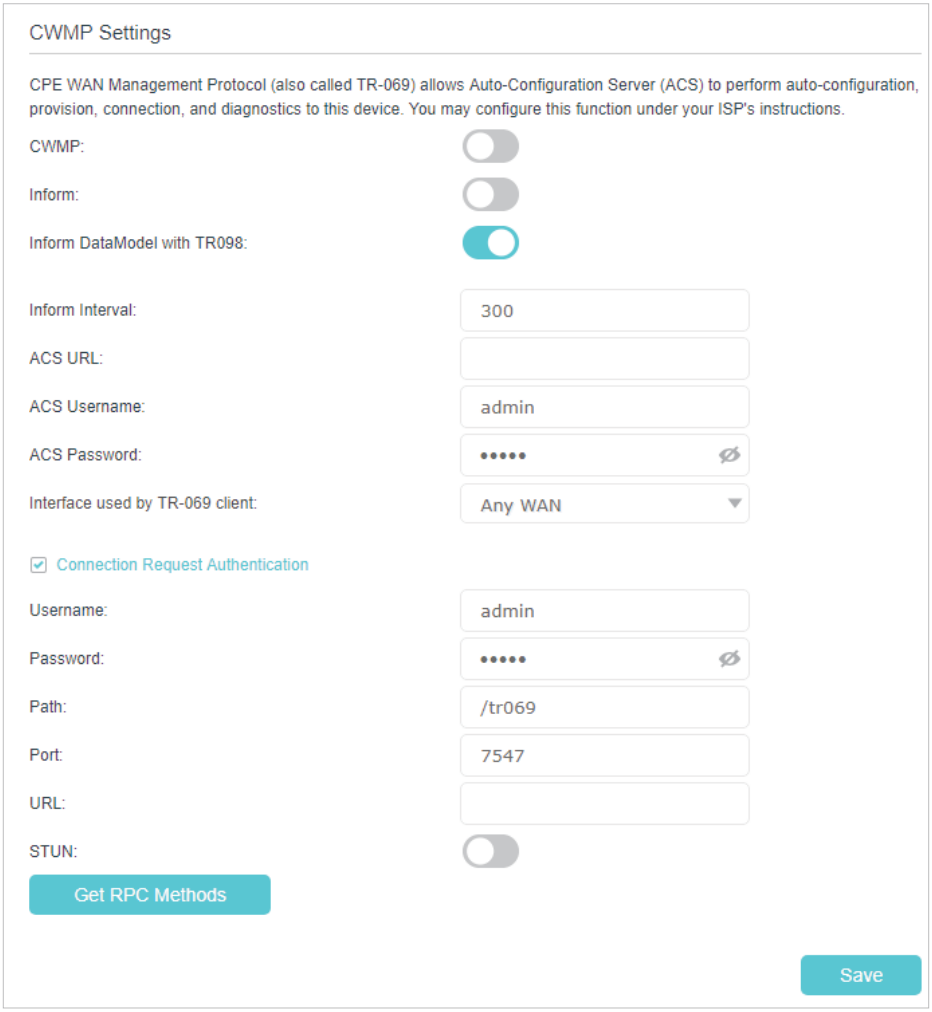


- Save Locally: Select this option to cache the system log to the AP's local memory, select the minimum level of system log to be saved from the drop-down list. The logs will be shown in the table in descending order on the System Log page.
- Save Remotely: Select this option to send the system log to 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.

13. 9. CWMP Settings

The AP 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 AP.
2. Go to Advanced > System Tools > CWMP Settings.



- 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 AP.
- Path: Enter the path for the ACS server to log in to the AP.
- 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.

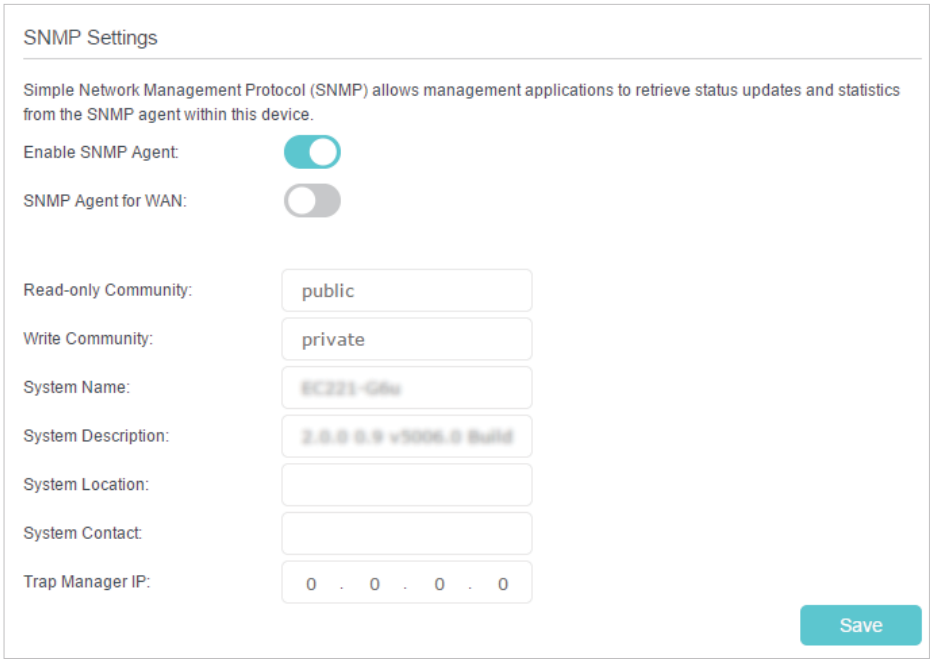
13. 10. SNMP Settings

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 AP.
2. Go to Advanced > System Tools > SNMP Settings.



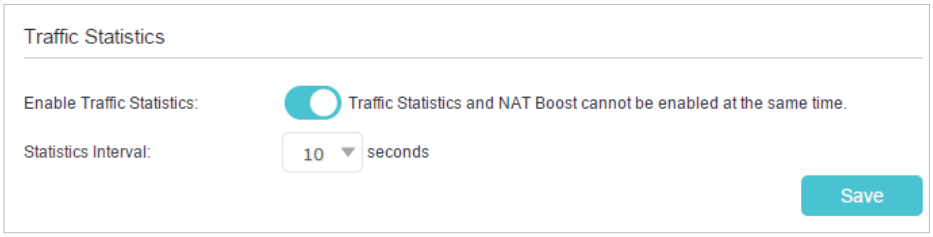
- Enable SNMP Agent/SNMP Agent for WAN: Turn on to enable the built-in SNMP agent that allows the AP to operate as the operational role in receiving and processing of SNMP messages, sending responses to the SNMP manager, and triggering SNMP traps when an event occurs.
- Read-only Community: Displays the default public community string that protects the AP from unauthorized access.
- Write Community: Displays the default write community string that protects the AP 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.

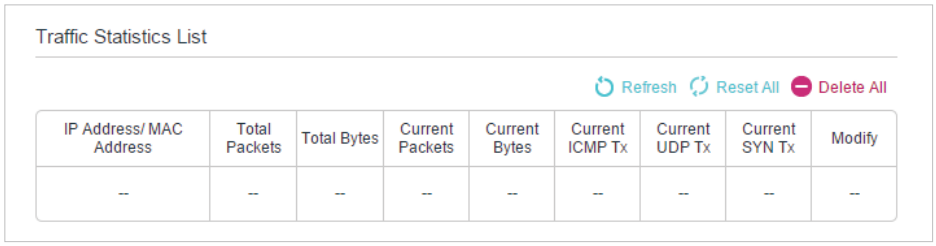
13. 11. Monitor the Internet Traffic Statistics

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 AP.
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 AP within the selected Statistics Interval. This function is disabled by default.



4. You can refer to Traffic Statistics List for the detailed information about the traffic usage of all devices.



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

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

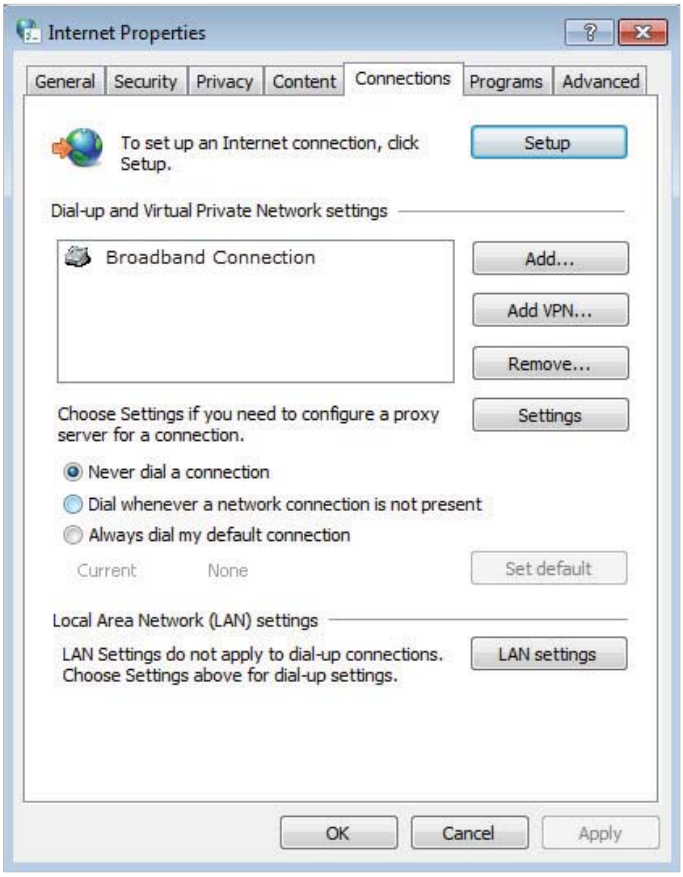
- Press and hold the RESET button of the AP for about 5 seconds, and then visit http://tplinkwifi.net to create a new login password.

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

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

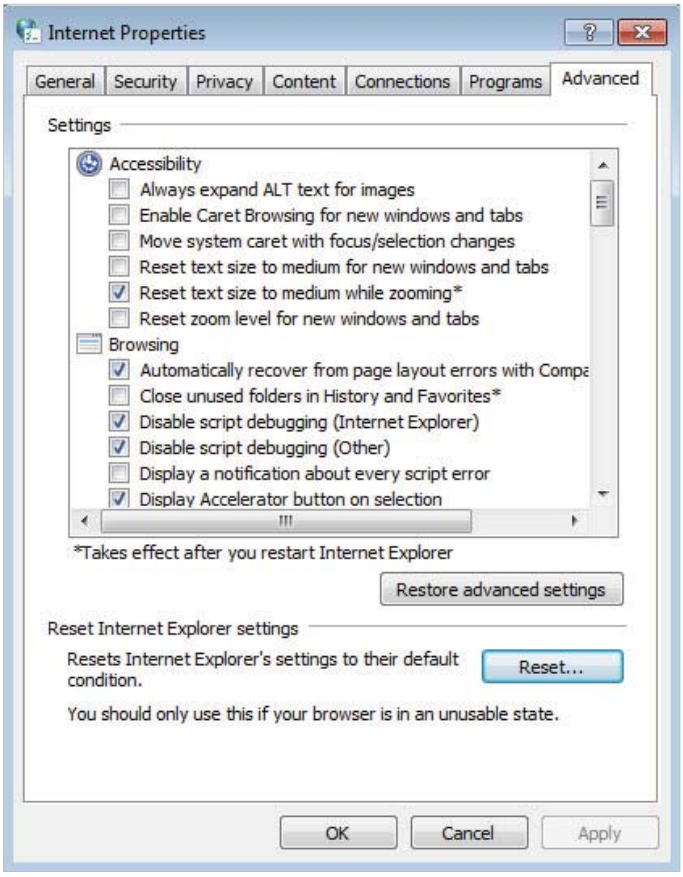
This can happen for a variety of reasons. Please try the methods below to log in again.

- Make sure your computer is connected to the AP 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 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.



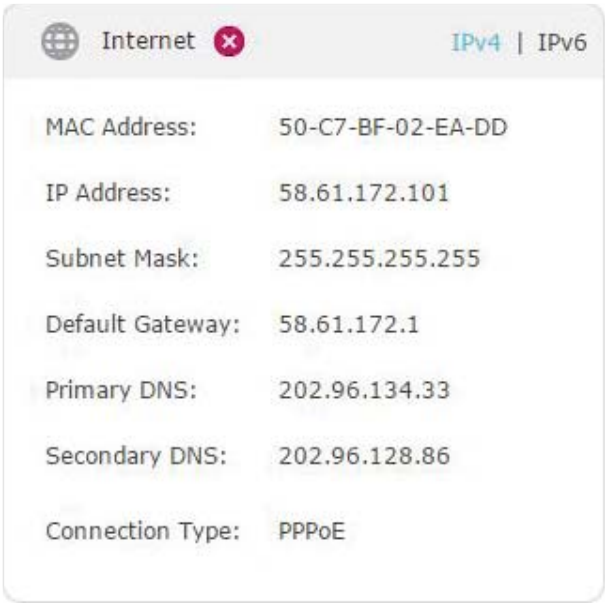
- Use another web browser or computer to log in again.
- Reset the AP to factory default settings and try again. If login still fails, please contact the technical support.

Note: You'll need to reconfigure the AP to access the internet once the AP 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 AP.
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:

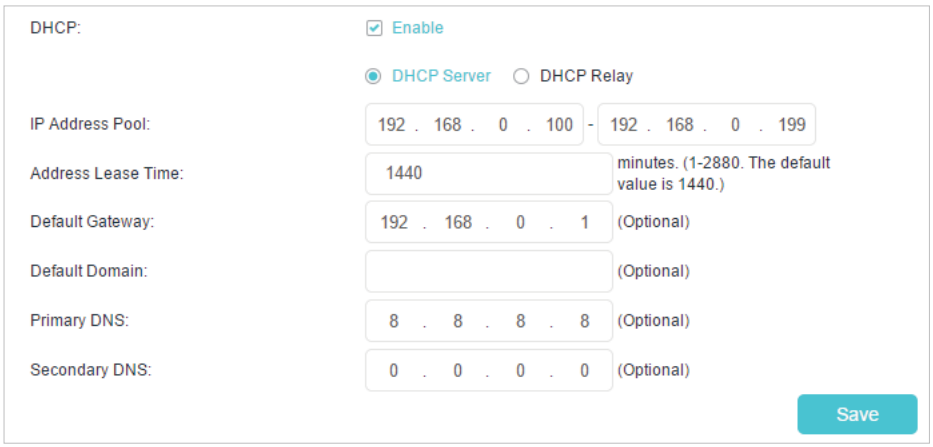


- Your computer might not recognize any DNS server addresses. Please manually configure the DNS server.

  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.



- Restart the modem and the AP.

  1) Power off your modem and AP, 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 AP.

  4) Wait another 1 or 2 minutes and check the internet access.

- Reset the AP to factory default settings and reconfigure the AP.
- Upgrade the firmware of the AP.

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

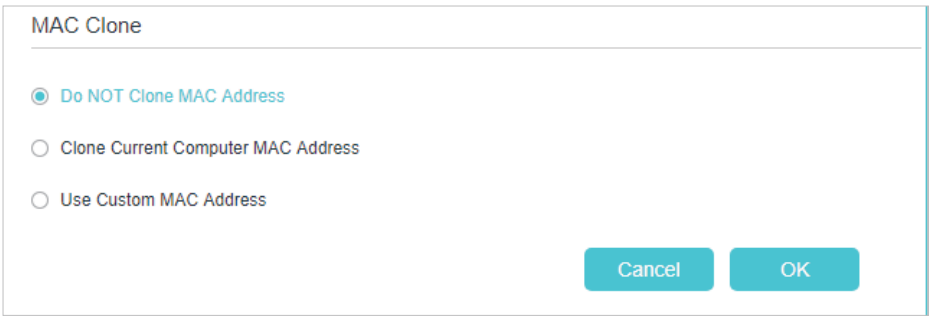
As the following image shows, if the IP Address is 0.0.0.0, please try the methods below:

- Make sure the physical connection between the AP 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 AP.

  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.



Tips:

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

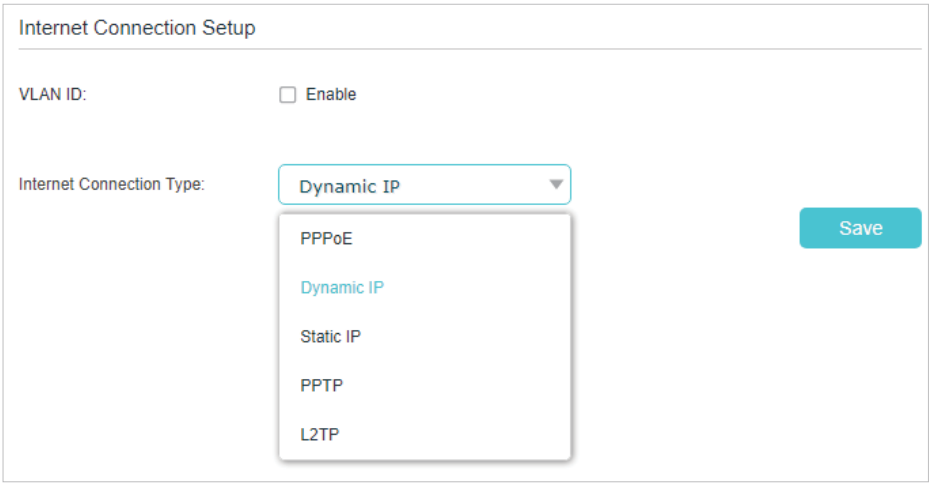
- Modify the LAN IP address of the AP.

  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 AP.
  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.

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



6) Restart the modem and the AP again.

- Please upgrade the firmware of the AP.

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.

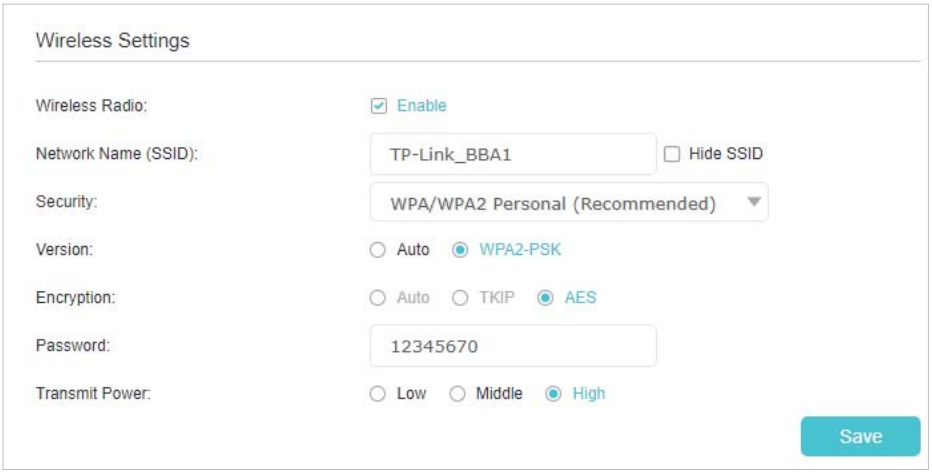
  4) Expand Services and Applications > Services, find and locate Wireless Zero Configuration in the Services list on the right side.

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 AP/modem.
- Make sure your computer/device is still in the range of your AP/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.



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 AP.

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 AP closer and try again.
  - Change the wireless Channel of the AP 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 Main AP until the status LED turns solid blue or white, then relocate the agent.
- Reset the agent and try to synchronize the agent with the Main AP again.

FCC compliance information statement

Product Name: Whole Home Mesh Wi-Fi AP

Model Number: HC220/HX220/HX510...

Component Name	Model	FCC ID
I.T.E. Power	T120100-2B1REV4.0.0	XXXXXXXX

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 6803

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

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

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

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

1) This device may not cause harmful interference.

2) This device must accept any interference received, including interference that may cause undesired operation.

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

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

FCC RF Radiation Exposure Statement

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

"To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located 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: 2021.11.30

CE Mark Warning

CE

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.

UKCA Mark

UK
CA

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.

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;

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： Equipment name				型號（型式）： 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.

EAC

Safety Information

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

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

Storage Temperature: -40˚C~ 60˚C (-40˚F~ 140˚F)

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

Explanations of the symbols on the product label

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
	Operator's manual
⚠	Caution
	Dangerous voltage