



User Guide

AC1350 High Power Wireless Dual Band Router
Archer C58HP

Contents

About This Guide	1
Chapter 1. Get to Know About Your Router	2
1. 1. Product Overview.....	3
1. 2. Panel Layout.....	3
1. 2. 1.Top View	3
1. 2. 2.The Back Panel.....	4
Chapter 2. Connect to the Internet	6
2. 1. Position Your Router	7
2. 2. Connect to the Internet.....	7
2. 2. 1.Install the Antennas	7
2. 2. 2.Router Mode	7
2. 2. 3.Range Extender Mode.....	10
2. 2. 4.Access Point Mode.....	11
Chapter 3. Log In to Your Router.....	13
Chapter 4. Guest Network.....	15
4. 1. Create a Network for Guests	16
4. 2. Customize Guest Network Options.....	16
Chapter 5. Parental Controls	18
Chapter 6. QoS.....	22
6. 1. Prioritize Internet Traffic with QoS.....	23
6. 2. Update the Database	24
Chapter 7. Network Security	26
7. 1. Protect the Network from Cyber Attacks	27
7. 2. Access Control	28
7. 3. IP & MAC Binding	29
Chapter 8. NAT Forwarding.....	31
8. 1. Share Local Resources on the Internet by Virtual Servers.....	32

8. 2.	Open Ports Dynamically by Port Triggering	33
8. 3.	Make Applications Free from Port Restriction by DMZ	34
8. 4.	Make Xbox Online Games Run Smoothly by UPnP	35

Chapter 9. VPN Server 37

9. 1.	Use OpenVPN to Access Your Home Network.....	38
9. 2.	Use PPTP VPN to Access Your Home Network	39

Chapter 10. Customize Your Network Settings..... 45

10. 1.	Change the LAN Settings	46
10. 2.	Configure to Support IPTV Service.....	46
10. 3.	Specify DHCP Server Settings	47
10. 4.	Set Up a Dynamic DNS Service Account	49
10. 5.	Create Static Routes.....	49
10. 6.	Specify Wireless Settings.....	52
10. 7.	Extend Host Network	53
10. 8.	Adjust Wi-Fi Coverage	54
10. 9.	Use WPS for Wireless Connection	54
10. 9. 1.	Use the WPS Wizard for Wi-Fi Connections.....	54
10. 9. 2.	Use the PIN for Wi-Fi connections	55
10. 10.	Schedule Your Wireless Function	55

Chapter 11. Manage the Router 57

11. 1.	Change Operation Mode.....	58
11. 2.	Set Up System Time	58
11. 3.	Control LEDs	59
11. 4.	Test the Network Connectivity	60
11. 5.	Upgrade the Firmware	61
11. 6.	Backup and Restore Configuration Settings	62
11. 7.	Auto Reboot.....	63
11. 8.	Change the Login Password	63
11. 9.	Password Recovery.....	64
11. 10.	Local Management	65
11. 11.	Remote Management.....	66
11. 12.	System Log.....	67
11. 13.	Monitor the Internet Traffic Statistics.....	69

FAQ 70

About This Guide

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

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

Conventions

In this guide the following conventions are used:

Convention	Description
<u>Underlined</u>	Underlined words or phrases are hyperlinks. You can click to redirect to a website or a specific section.
Teal	Contents to be emphasized and texts on the web page are in teal, including the menus, items, buttons, etc.
>	The menu structures to show the path to load the corresponding page. For example, Advanced > Wireless > MAC Filtering means the MAC Filtering function 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	<ul style="list-style-type: none">✎ click to edit the corresponding entry.🗑️ click to delete the corresponding entry.🔌 click to enable or disable the corresponding entry.🔍 click to view more information about items on the page.

More Info

The latest software, management app and utility can be found at [Download Center](http://www.tp-link.com/support) at <http://www.tp-link.com/support>.

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

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

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

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

Chapter 1

Get to Know About Your Router

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

It contains the following sections:

- [Product Overview](#)
- [Panel Layout](#)

1.1. Product Overview

The TP-Link router is designed to fully meet the need of Small Office/Home Office (SOHO) networks and users demanding higher networking performance. The powerful antennas ensure continuous Wi-Fi signal to all your devices while boosting widespread coverage throughout your home, the built-in Ethernet ports supply high-speed connection to your wired devices, and the flexible working modes are capable to meet all your network needs.

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

1.2. Panel Layout

1.2.1. Top View



RE button: This button is located on the top panel of the router. Press and hold it for about 3 seconds to change to the Range Extender mode.

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

LED Explanation

Name	Status	Indication
WPS	On/Off	This light remains on for 5 minutes when a WPS connection is established, and then turns off.
	Blinking	WPS connection is in progress. This may take up to 2 minutes.
LAN	On	At least one LAN port is connected to a powered-on device.
	Off	No LAN port is connected to a powered-on device.
WAN	White on	The internet is available.
	Orange on	The router's WAN port is connected, but the internet is not available.
	Off	The router's WAN port is not connected.
PWR	On	Power is on.
	Blinking	The system is starting up or firmware is being upgraded. Do not disconnect or power off the router.
	Off	Power is off.
2.4G/5G	On	The corresponding wireless function (2.4G/5G) is working normally.
	Off	The corresponding wireless function (2.4G/5G) is disabled.
RE	Blinking	The router is connecting to the host wireless network. This may take up to 2 minutes.
	On	The router is working in Repeater mode and connected to the host wireless network.

1.2.2. The Back Panel



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

Item	Description
PWR Port	For connecting the router to a power socket via the provided power adapter.
Power On/Off Button	For powering on or off the router.

Item	Description
Wi-Fi On/Off Button	Press and hold this button about 2 seconds to enable or disable the wireless function.
Reset Button	Use a pin to press and hold this button until all the LEDs turn on momentarily to reset the router to its factory default settings.
WAN Port	For connecting to a DSL/Cable modem, or an Ethernet jack.
WPS Button	If your devices, such as wireless adapters, that support Wi-Fi Protected Setup, then you can press this button to quickly establish a connection between the router and devices.
Ethernet Ports (1/2/3/4)	For connecting your PCs or other wired network devices to the router.
Antennas	Used for wireless operation and data transmitting. Upright them for the best Wi-Fi performance.

Chapter 2

Connect to the Internet

This chapter contains the following sections:

- [Position Your Router](#)
- [Connect to the Internet](#)

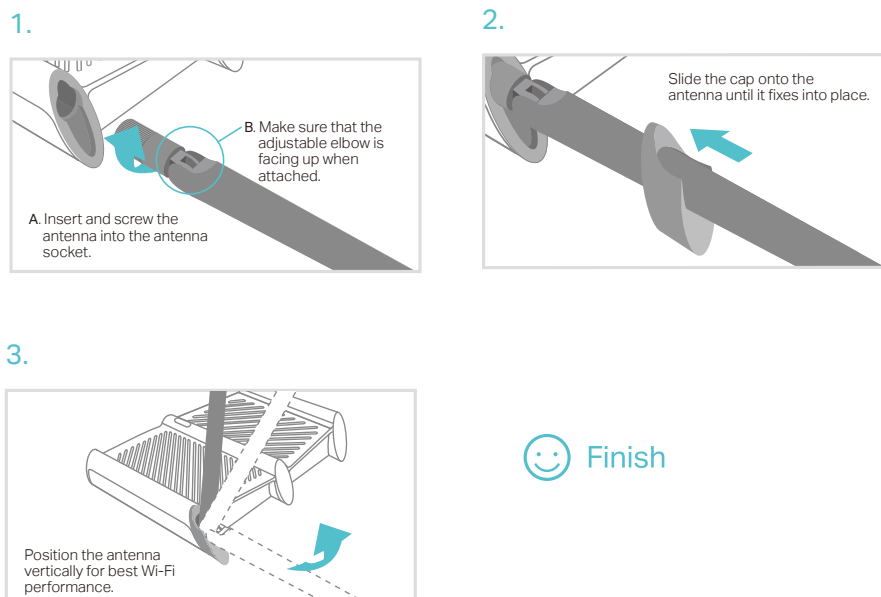
2.1. Position Your Router

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

2.2. Connect to the Internet

2.2.1. Install the Antennas

Please install the antennas first by following the steps shown below before you start.



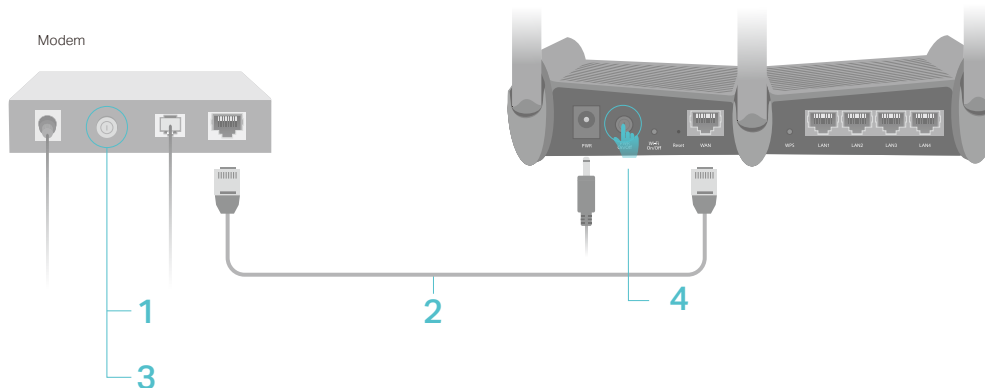
The router provides three working modes: Router, Range Extender and Access Point. You can choose the mode to better suit your network needs and follow the guide to complete the configuration.

2.2.2. Router Mode

This mode enables multiple users to share internet connection via ADSL/Cable Modem.

1. Follow the steps below to connect your router.

If your internet connection is through an Ethernet cable from the wall instead of through a DSL / Cable / Satellite modem, connect the Ethernet cable directly to the router's WAN port, and then follow Step 4 and 5 to complete the hardware connection.



- 1) Turn off the modem, and remove the backup battery if it has one.
- 2) Connect the modem to the WAN port on your router with an Ethernet cable.
- 3) Turn on the modem, and then wait about **2 minutes** for it to restart.
- 4) Connect the power adapter to the router and turn on the router.
- 5) Verify that the hardware connection is correct by checking these LEDs.

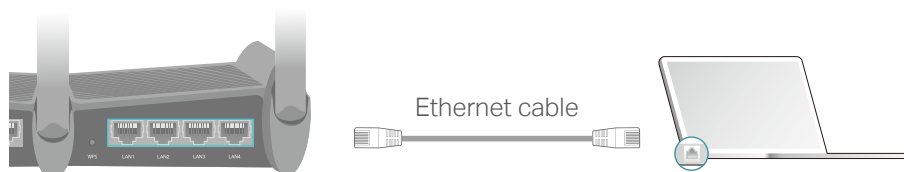


🔗 **Tips:** If the 2.4G or 5G LED is off, press and hold the Wi-Fi On/Off button until it is on.

2. Connect your computer to the router.

• **Method 1: Wired**

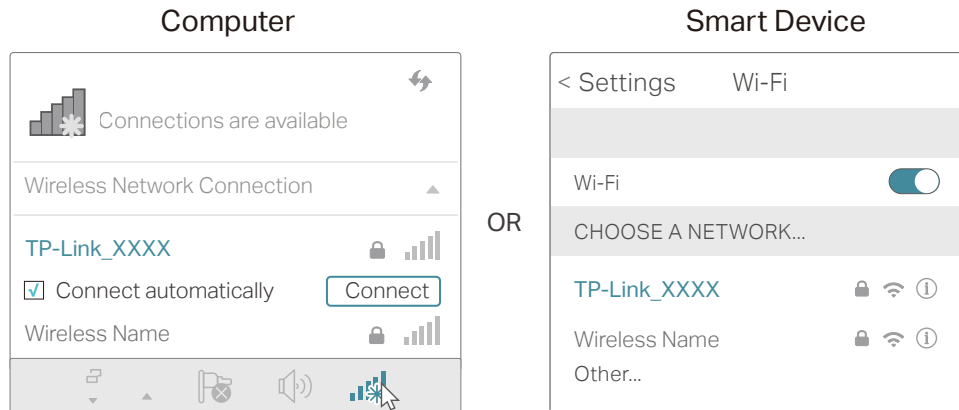
Turn off the Wi-Fi on your computer and connect the devices as shown below.



• **Method 2: Wirelessly**

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

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

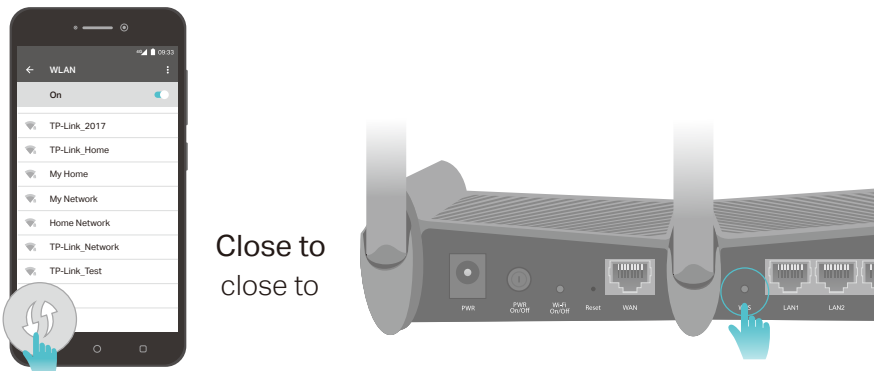


- **Method 3: Use the WPS button**

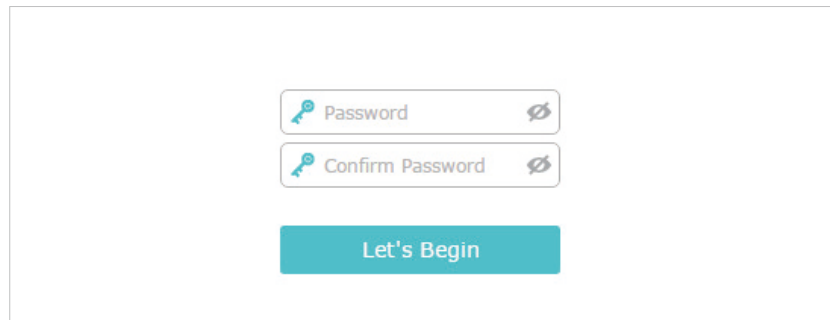
Wireless devices that support WPS, including Android phones, tablets, most USB network cards, can be connected to your router through this method (Not supported by iOS devices).

Note: The WPS function cannot be configured if the wireless function of the router is disabled. Also, the WPS function will be disabled if your wireless encryption is WEP. Please make sure the wireless function is enabled and is configured with the appropriate encryption before configuring the WPS.

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



3. Enter <http://tplinkwifi.net> in the address bar of a web browser and create a password for future logins.



The image shows a login interface with two input fields for passwords. The first field is labeled 'Password' and the second is labeled 'Confirm Password'. Both fields have a key icon on the left and a clear icon on the right. Below the fields is a teal button labeled 'Let's Begin'.




■ Note: If the login page does not appear, please refer to the [FAQ](#) section.

4. After successful login, follow the step-by-step instructions to complete the initial configuration.
5. **Enjoy!** For wireless devices, you may have to reconnect to the wireless network if you have customized the SSID (network name) and password during the configuration.


2. 2. 3. Range Extender Mode

This mode boosts your home wireless coverage.

Step 1: Configure

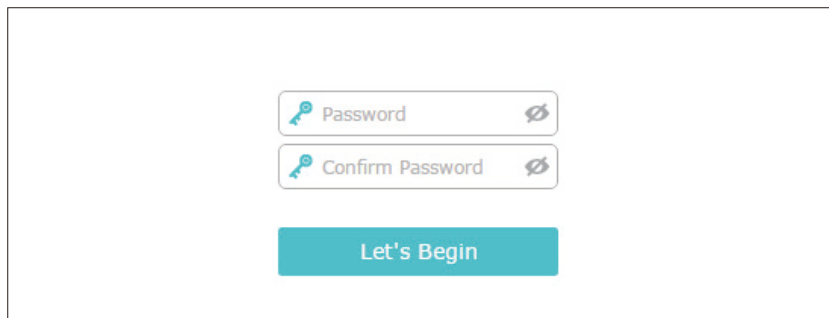
🔗 **Tips:** Using WPS Button is an easy way to extend your host network. We recommend you to use this way if your host router has a WPS button. The button might look like one of these:  |  | .

- **Option One: Using the RE Button**

- 1) Press the WPS button on the host router.
- 2) Press and hold the  (RE button) on the top panel of the router for about 3 seconds within 1 minute. The router will start to connect to the host router. Once connected, the router will reboot.
- 3) Once rebooted, the **RE LED** should change from blinking to a solid state, indicating successful connection.

- **Option Two: Using a Web Browser**

- 1) Connect a computer to the router via an Ethernet cable or wirelessly by using the SSID (Network Name) and password printed on the label at the bottom of the router.
- 2) Enter <http://tplinkwifi.net> in the address bar of a web browser and create a password for future logins.

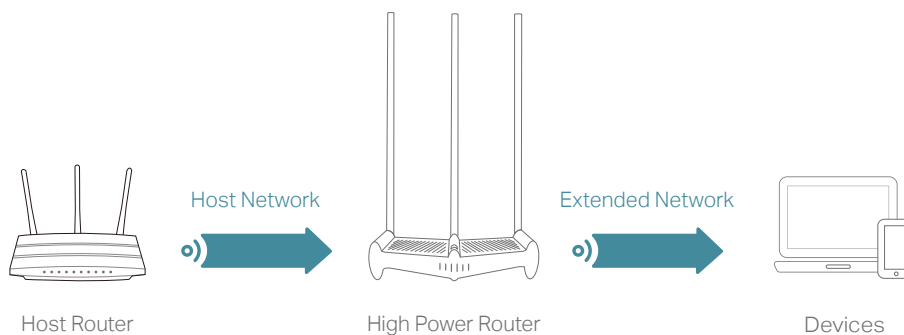


■ Note: If the login page does not appear, please refer to the FAQ section.

- 3) After successful login, follow the step-by-step instructions to complete the initial configuration.

Step 2: Relocate:

Place the router between your host router and the Wi-Fi dead zone. The location you choose must be within the range of your existing host network.

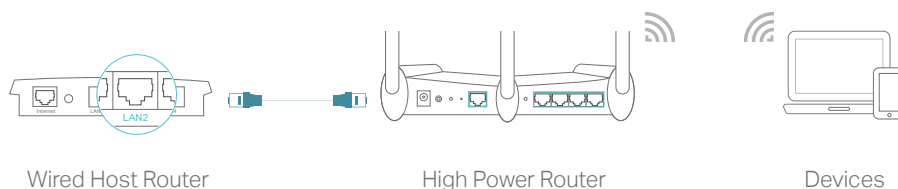


Step 3: Enjoy!

The extended network shares the same password as that of your host network. If you have customized the SSID (network name) of the extended network, connect to the new Wi-Fi.

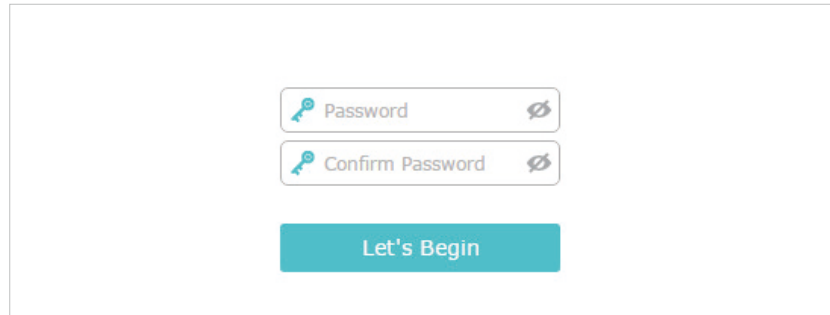
2.2.4. Access Point Mode

This mode transforms your existing wired network to a wireless one.



1. Connect the router to your wired host router's Ethernet port via an Ethernet cable as shown above and turn on the router.

2. Connect a computer to the router via an Ethernet cable or wirelessly by using the SSID (network name) and password printed on the bottom label of the router.
3. Enter <http://tplinkwifi.net> in the address bar of a web browser and create a password for future logins.



The image shows a web browser interface for setting a password. It features two input fields: the first is labeled 'Password' and the second is labeled 'Confirm Password'. Both fields have a key icon on the left and a clear (X) icon on the right. Below these fields is a teal button with the text 'Let's Begin'.

■ Note: If the login page does not appear, please refer to the [FAQ](#) section.

4. After successful login, follow the step-by-step instructions to complete the initial configuration.
5. **Enjoy!** Connect to the wireless network by using the SSID (network name) and password of the router.

Chapter 3

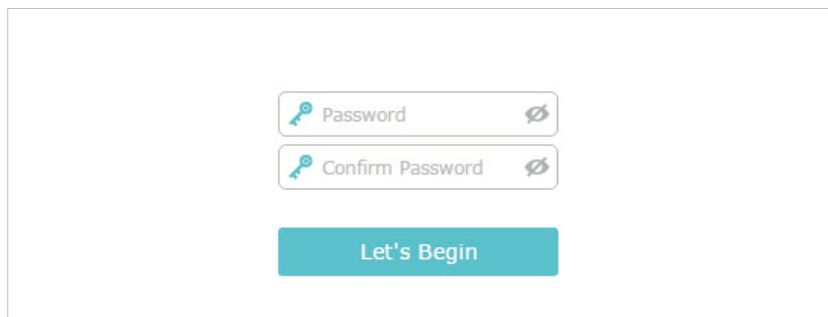
Log In to Your Router

This chapter shows how to log in to the web management page of the router.

With the web-based utility, it is easy to configure and manage the router. The web-based utility 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 router.

1. Set up the TCP/IP Protocol in [Obtain an IP address automatically](#) mode on your computer.
2. Visit <http://tplinkwifi.net> and create a password for future logins.



The image shows a web-based login form for a router. It contains two input fields for passwords, each with a key icon on the left and a toggle icon on the right. The first field is labeled 'Password' and the second is labeled 'Confirm Password'. Below these fields is a teal button with the text 'Let's Begin'.

Note:

- If the login window does not appear, please refer to the [FAQ](#) section.

Chapter 4

Guest Network

This function allows you to provide Wi-Fi access for guests without disclosing your main network. When you have guests in your house, apartment, or workplace, you can create a guest network for them. In addition, you can customize guest network options to ensure network security and privacy. Guest Network is only supported by the Router and Access Point modes.

It contains the following sections:

- [Create a Network for Guests](#)
- [Customize Guest Network Options](#)

4. 1. Create a Network for Guests

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [Guest Network](#) or [Settings](#) > [Guest Network](#). Locate the [Wireless](#) section.
3. Create a guest network as needed.
 - 1) Tick the [Enable Guest Network](#) checkbox for the 2.4GHz/5GHz wireless network.
 - 2) Customize the SSID. Don't select [Hide SSID](#) unless you want your guests to manually input the SSID for guest network access.
 - 3) Set [Security](#) to [WPA/WPA2 Personal](#), keep the default [Version](#) and [Encryption](#) values, and customize your own password.

Wireless

2.4GHz Wireless: Enable Guest Network

Network Name (SSID): Hide SSID

Security: No Security WPA/WPA2-Personal

Version: Auto WPA-PSK WPA2-PSK

Encryption: Auto TKIP AES

Password:

5GHz Wireless: Enable Guest Network

Network Name (SSID): Hide SSID

Security: No Security WPA/WPA2-Personal

Version: Auto WPA-PSK WPA2-PSK

Encryption: Auto TKIP AES

Password:

Save

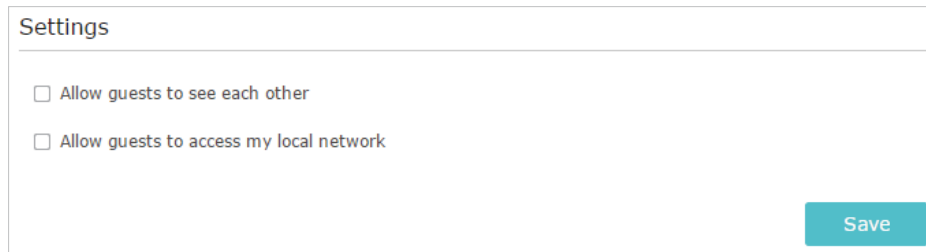
4. Click [Save](#). Now your guests can access your guest network using the SSID and password you set!

Tips: To view guest network information, go to [Advanced](#) > [Status](#) and locate the [Guest Network](#) section.

4. 2. Customize Guest Network Options

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

2. Go to [Advanced](#) > [Guest Network](#) or [Settings](#) > [Guest Network](#). Locate the [Settings](#) section.
3. Customize guest network options as needed.



Settings

Allow guests to see each other

Allow guests to access my local network

Save

- [Allow guests to see each other](#)

Tick this checkbox if you want to allow the wireless clients on your guest network to communicate with each other via methods such as network neighbors and Ping.

- [Allow guests to access my local network \(in Router mode\)](#)

Tick this checkbox if you want to allow the wireless clients on your guest network to communicate with the devices connected to your router's LAN ports or main network via methods such as network neighbors and Ping.

4. Click [Save](#). Now you can ensure network security and privacy!

 **Tips:** To view guest network information, go to [Advanced](#) > [Status](#) and locate the [Guest Network](#) section.

Chapter 5

Parental Controls

This function allows you to block inappropriate, explicit and malicious websites, and control access to specified websites at specified time. Parental Controls are only supported by the Router mode.

I want to:

Control the times of day my children or other home network users are allowed to access the Internet and even types of websites they can visit.

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 (6PM) to 22:00 (10PM) at the weekend and not other times.

How can I do that?

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

3. Click **Add**. And then Click **View Existing Devices**, and select the access device. Or, input the **Device Name** and **MAC Address** manually.

ID	Device Name	MAC Address	Internet Access Time	Description	Status	Modify
--	--	--	--	--	--	--

Device Name: **View Existing Devices**

MAC Address:

Internet Access Time: (Optional)

Enable This Entry

Cancel **OK**

ID	Device Name	MAC Address	Internet Access Time	Description	Status	Modify
1	PC1	C0-4A-00-1A-C3-46				

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

System Time: Sat 25th Jun 2016 02:31:34 undefined

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00:00							
01:00							
02:00							
03:00							
04:00							
05:00							
06:00							
07:00							
08:00							
09:00							
10:00							
11:00							
12:00							
13:00							
14:00							
15:00							
16:00							
17:00							
18:00							
19:00							
20:00							
21:00							
22:00							
23:00							
24:00							

Time

Cancel Reset Save

5. Enter a **Description** for the entry, tick the **Enable This Entry** checkbox, and then click **OK**.

6. Select **Whitelist** as the restriction policy.

Content Restriction

Restriction Policy: Blacklist **Whitelist**

Tips:

- With **Blacklist** selected, the controlled devices cannot access any websites containing the specified keywords during the Internet Access Time period.
- With **Whitelist** selected, the controlled devices can only access websites containing the specified keywords during the Internet Access Time period.

7. Click **+ Add a New Domain Name** . Enter a website and click **Save**.

You can add up to 32 keywords for either Blacklist or Whitelist. Below are some sample entries to allow access.

- **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 (eg. .edu or .org) to block access only to the websites containing that keyword or suffix.

Content Restriction

Restriction Policy: Blacklist Whitelist

[+ Add a New Domain Name](#)

[-](#)

[Save](#)

Done!

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

Chapter 6

QoS

This chapter introduces how to create a QoS (Quality of Service) rule to specify prioritization of traffic and minimize the impact caused when the connection is under heavy load. QoS is only supported by the Router mode.

It contains the following sections:

- [Prioritize Internet Traffic with QoS](#)
- [Update the Database](#)

6. 1. Prioritize Internet Traffic with QoS

QoS (Quality of Service) is designed to ensure the efficient operation of the network when come across network overload or congestion.

I want to: Specify priority levels for some devices or applications.

For example, I have several devices that are connected to my wireless network. I would like to set an intermediate speed on the Internet for my phone.

How can I do that?

1. Enable QoS and set bandwidth allocation.
 - 1) Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
 - 2) Go to **Advanced > QoS > Settings**.
 - 3) Select **Enable QoS**.
 - 4) Input the maximum upload and download bandwidth provided by your internet service provider. 1Mbps equal s to 1000Kbps.
 - 5) Click **Advanced** and drag the scroll bar to set the bandwidth priority percentage.
 - 6) Click **Save**.

The screenshot shows the QoS configuration page. At the top, there's a title 'QoS'. Below it, the 'QoS' section has a checkbox for 'Enable QoS' which is checked. Underneath, there are two rows for bandwidth: 'Upload Bandwidth' and 'Download Bandwidth', both set to '1000' with a unit dropdown menu set to 'Mbps'. Below the bandwidth settings is an 'Advanced' section with a circular icon and the text 'Advanced'. This section contains three horizontal sliders for priority levels: 'High Priority' is set to 60%, 'Middle Priority' is set to 30%, and 'Low Priority' is set to 10%. A 'Save' button is located at the bottom right of the form.

2. Add a middle priority QoS rule for the phone.
 - 1) Select **By Device** and then click **View Existing Devices**.

QoS Rule

Type: By Device By Application

Device Name: [View Existing Devices](#)

MAC Address:

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

2) Choose the respective device from the list.

Access Devices List

ID	Device Name	IP Address	MAC Address	Operation
1	<i>iPhone</i>	192.168.0.175	1C-1A-C0-3B-28-4B	Choose
2	<i>ASUS AC</i>	192.168.0.157	C0-4A-00-1A-C3-45	Choose

3) Click **OK**.

QoS Rule


Type: By Device By Application

Device Name: [View Existing Devices](#)

MAC Address:

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

3. Refer to the steps above to apply other QoS rules if any.

Note: If you want to delete a QoS rule, click  to remove the responding rule from the list.

Done!

Now QoS is implemented to prioritize Internet traffic.

6.2. Update the Database

This function can help to add or update the applications the router supports. If the applications you need are not listed in the Application list, you can try to download the new version and upgrade the database. New database versions are posted at www.tp-link.com and can be downloaded for free.

1. Download the latest QoS database from our website www.tp-link.com.
2. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
3. Go to **Advanced > QoS > Database**. Click **Browse** to select the database upgrade file, and then click **Upgrade**. Wait until the upgrade is completed and do not operate during the process.

Database Upgrade

New Database File: **Browse**

Database Version: Qos database 1.5.0

Upgrade

Chapter 7

Network Security

This chapter guides you on how to protect your home network from cyber attacks and unauthorized users by implementing these three network security functions. You can protect your home network against DoS (Denial of Service) attacks from flooding your network with server requests using DoS Protection, block or allow specific client devices to access your network using Access Control, or you can prevent ARP spoofing and ARP attacks using IP & MAC Binding. Some features are only supported by a certain mode.

It contains the following sections:

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

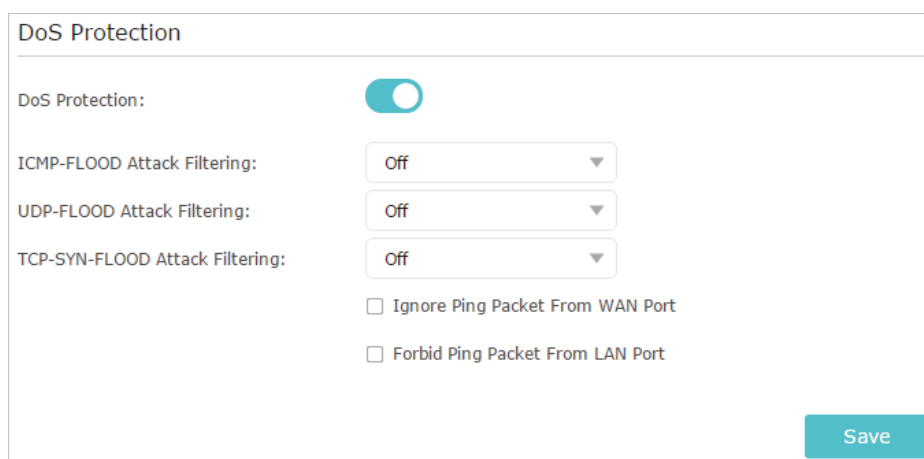
7.1. Protect the Network from Cyber Attacks

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

The SPI Firewall can prevent cyber attacks and validate the traffic that is passing through the router based on the protocol. This function is enabled by default, and it's 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 router.
2. Go to [Advanced](#) > [Security](#) > [Settings](#).



DoS Protection

DoS Protection:

ICMP-FLOOD Attack Filtering:

UDP-FLOOD Attack Filtering:


TCP-SYN-FLOOD Attack Filtering:

Ignore Ping Packet From WAN Port

Forbid Ping Packet From LAN Port

Save

3. Enable [DoS Protection](#).
4. Set the level ([Off](#), [Low](#), [Middle](#) or [High](#)) of protection for [ICMP-FLOOD Attack Filtering](#), [UDP-FLOOD Attack Filtering](#) and [TCP-SYN-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-SYN-FLOOD Attack Filtering](#) - Enable to prevent the TCP-SYN (Transmission Control Protocol-Synchronize) flood attack.

 **Tips:** The level of protection is based on the number of traffic packets. The protection will be triggered immediately when the number of packets exceeds the preset threshold value (the value can be set on [Advanced](#) > [System Tools](#) > [System Parameters](#) > [DoS Protection Level Settings](#)), and the vicious host will be displayed in the [Blocked DoS Host List](#).

Blocked DoS Host List			
Host Number: 0		Refresh Delete	
<input type="checkbox"/>	ID	IP Address	MAC Address
--	--	--	--

- If you want to ignore the ping packets from the WAN port, select [Ignore Ping Packet From WAN Port](#); if you want to ignore the ping packets form the LAN port, select [Ignore Ping Packet From LAN Port](#).
- Click [Save](#).

7.2. Access Control

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

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

How can I do that?

- Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
- Go to [Advanced-Settings](#) > [Access Control](#).
- Enable [Access Control](#).

Access Control	
Access Control:	<input checked="" type="checkbox"/>

- Select the access mode to either block (recommended) or allow the device(s) in the list.

To block specific device(s):

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

Access Mode	
Default Access Mode:	<input checked="" type="radio"/> Blacklist <input type="radio"/> Whitelist
Save	

- Select the device(s) to be blocked in the [Online Devices](#) table by ticking the checkbox(es).

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

Online Devices							
						Refresh	Block
<input checked="" type="checkbox"/>	ID	Device Name	IP Address	MAC Address	Connection Type	Modify	
<input checked="" type="checkbox"/>	1	Roses-iPhone	192.168.0.175	1C-1A-C0-3B-28-4B	Wireless		
<input type="checkbox"/>	2	ADMIN-PC	192.168.0.157	C0-4A-00-1A-C3-45	Wireless		

To allow specific device(s):

- 1) Select **Whitelist** and click **Save**.

Access Mode	
Default Access Mode:	<input type="radio"/> Blacklist <input checked="" type="radio"/> Whitelist
<input type="button" value="Save"/>	

- 2) Click **Add** in the **Devices in Whitelist** section. Enter the **Device Name** and **MAC Address** (You can copy and paste the information from the **Online Devices** list if the device is connected to your network).

Devices in Whitelist					
				+ Add	- Delete
<input type="checkbox"/>	ID	Device Name	MAC Address	Modify	
<input type="checkbox"/>	--	--	--	--	
Device Name:		<input type="text"/>			
MAC Address:		<input type="text"/>			
				<input type="button" value="Cancel"/>	<input type="button" value="OK"/>

- 3) Click **OK**.

Done!

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

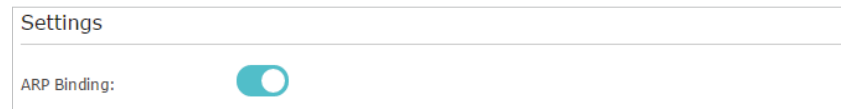
7.3. IP & MAC Binding

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

I want to: Prevent ARP spoofing and ARP attacks.

How can I do that?

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



Settings

ARP Binding:

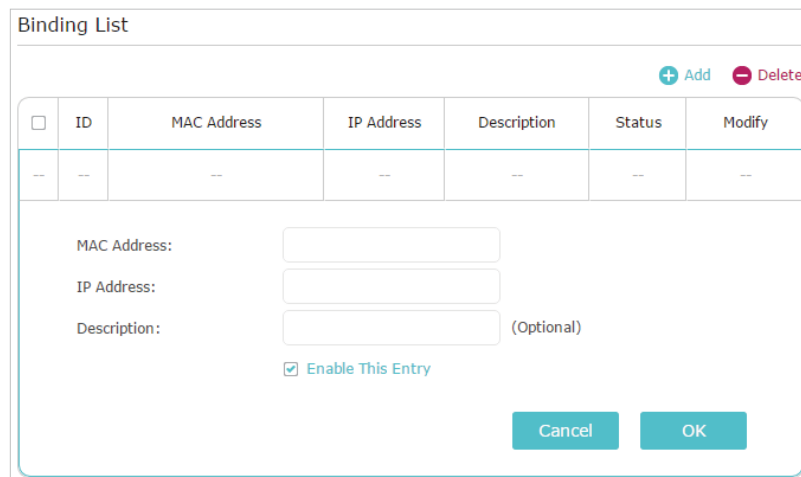
4. Bind your device(s) according to your need.

To bind the connected device(s):

Click  to add the corresponding device to the [Binding List](#).

To bind the unconnected device:

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



Binding List

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

<input type="checkbox"/>	ID	MAC Address	IP Address	Description	Status	Modify
<input type="checkbox"/>	--	--	--	--	--	--

MAC Address:

IP Address:

Description: (Optional)

[Enable This Entry](#)

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

- 2) Enter the [MAC address](#) and [IP address](#) that you want to bind. Enter a [Description](#) for this binding entry.
- 3) Tick the [Enable This Entry](#) checkbox and click [OK](#).

Done!

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

Chapter 8

NAT Forwarding

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

With the forwarding feature the router can penetrate the isolation of NAT and allows devices on the internet to initiatively communicate with devices on the local network, thus realizing some special functions.

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

NAT Forwarding is only supported by the Router mode.

It contains the following sections:

- [Share Local Resources on the Internet by Virtual Servers](#)
- [Open Ports Dynamically by Port Triggering](#)
- [Make Applications Free from Port Restriction by DMZ](#)
- [Make Xbox Online Games Run Smoothly by UPnP](#)

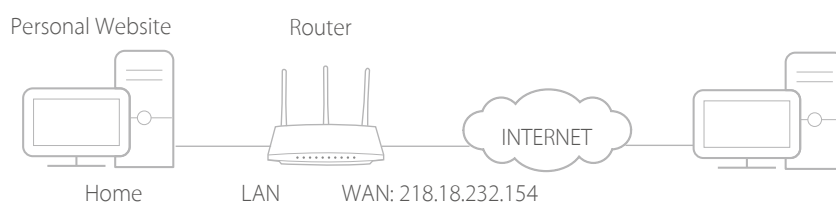
8. 1. Share Local Resources on the Internet by Virtual Servers

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

Virtual Servers can be used for setting up public services on your local network, such as HTTP, FTP, DNS, POP3/SMTP and Telnet. Different services use different service ports. Port 80 is used in HTTP service, port 21 in FTP service, port 25 in SMTP service and port 110 in POP3 service. Please verify the service port number before the configuration.

I want to: Share my personal website I've built on my local network with my friends through the internet.

For example, the personal website has been built on my home PC (192.168.0.100). I hope that my friends on the internet can visit my website in some way. The PC is connected to the router with the WAN IP address 218.18.232.154.



How can I do that?

1. Assign a static IP address to your PC, for example 192.168.0.100.
2. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
3. Go to **Advanced > NAT Forwarding > Virtual Servers**.
4. Click **Add**. Click **View Existing Services** and select **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**.

+ Add - Delete

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

Service Type: View Existing Services

External Port: (XX-XX or XX)

Internal IP:

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

Protocol: ▼

Enable This Entry

Cancel
OK

Tips:

- It is recommended to keep the default settings of **Internal Port** and **Protocol** if you are not clear about which port and protocol to use.
- If the service you want to use is not in the **Service Type**, you can enter the corresponding parameters manually. You should verify the port number that the service needs.
- You can add multiple virtual server rules if you want to provide several services in a router. Please note that the **External Port** should not be overlapped.

Done!

Users on the internet can enter [http:// WAN IP](http://WAN IP) (in this example: [http:// 218.18.232.154](http://218.18.232.154)) to visit your personal website.

Tips:

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

8.2. Open Ports Dynamically by Port Triggering

Port Triggering can specify a triggering port and its corresponding external ports. When a host on the local network initiates a connection to the triggering port, all the external ports will be opened for subsequent connections. The router can record the IP address of the host. When the data from the internet return to the external ports, the router can forward them to the corresponding host. Port Triggering is mainly applied to online games, VoIPs, video players and common applications including MSN Gaming Zone, Dialpad and Quick Time 4 players, etc.

Follow the steps below to configure the Port Triggering rules:

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

3. Click [View Existing Applications](#), and select the desired application. The [Triggering Port](#), [External Port](#) and [Protocol](#) will be automatically filled in. The following picture takes application [MSN Gaming Zone](#) as an example.

4. Click [OK](#).

Port Triggering

+ Add - Delete

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

Application: MSN Gaming Zone [View Existing Applications](#)

Triggering Port: 47624 (XX,1-65535)

Triggering Protocol: ALL

External Port: 2300-2400,28800-29000 (XX or XX-XX,1-65535,at most 5 pairs)

External Protocol: ALL

Enable This Entry

Cancel OK

Tips:

- You can add multiple port triggering rules according to your network need.
- The triggering ports can not be overlapped.
- If the application you need is not listed in the Existing Applications list, please enter the parameters manually. You should verify the external ports the application uses first and enter them into [External Port](#) field according to the format the page displays.

8.3. Make Applications Free from Port Restriction by DMZ

When a PC is set to be a DMZ (Demilitarized Zone) host on the local network, it is totally exposed to the internet, which can realize the unlimited bidirectional communication between internal hosts and external hosts. The DMZ host becomes a virtual server with all ports opened. When you are not clear about which ports to open in some special applications, such as IP camera and database software, you can set the PC to be a DMZ host.

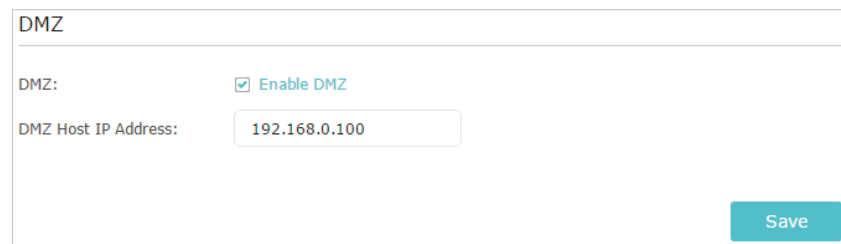
Note: When DMZ is enabled, the DMZ host is totally exposed to the internet, which may bring some potential safety hazards. If DMZ is not in use, please disable it in time.

I want to: Make the home PC join the internet online game without port restriction.

For example, due to some port restriction, when playing the online games, you can login normally but cannot join a team with other players. To solve this problem, set your PC as a DMZ host with all ports open.

How can I do that?

1. Assign a static IP address to your PC, for example 192.168.0.100.
2. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
3. Go to **Advanced > NAT Forwarding > DMZ** and select **Enable DMZ**.
4. Enter the IP address 192.168.0.100 in the **DMZ Host IP Address** field.



DMZ

DMZ: Enable DMZ

DMZ Host IP Address:

Save

5. Click **Save**.

Done!

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

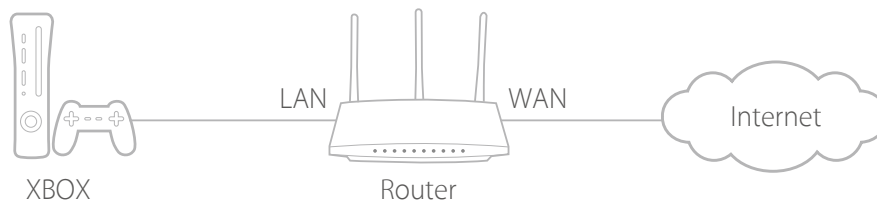
8.4. Make Xbox Online Games Run Smoothly by UPnP

The UPnP (Universal Plug and Play) protocol allows applications or host devices to automatically find the front-end NAT device and send request to it to open the corresponding ports. With UPnP enabled, the applications or host devices on the local network and the internet can freely communicate with each other thus realizing the seamless connection of the network. You may need to enable the UPnP if you want to use applications for multiplayer gaming, peer-to-peer connections, real-time communication (such as VoIP or telephone conference) or remote assistance, etc.

 **Tips:**

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

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




If necessary, you can follow the steps to change the status of UPnP.

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

UPnP

UPnP:

UPnP Service List

Total Clients: 0  Refresh

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

Chapter 9

VPN Server

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

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

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

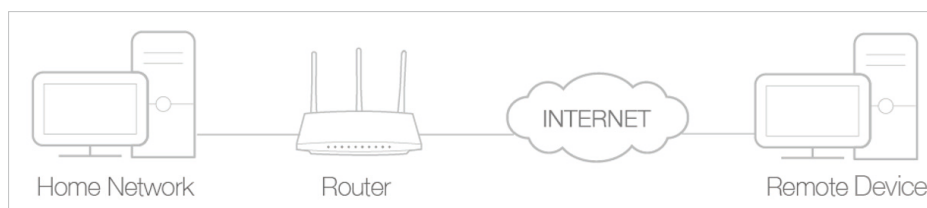
VPN Server is only supported by the Router mode.

It contains the following sections, please choose the appropriate VPN server connection type as needed.

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

9.1. Use OpenVPN to Access Your Home Network

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



Step1. Set up OpenVPN Server on Your Router

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

OpenVPN

Note: No certificate currently, please **Generate** one before enabling VPN Server.

Enable VPN Server

Service Type: UDP TCP

Service Port:

VPN Subnet/Netmask:

Client Access: Home Network Only Internet and Home Network

Note:

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

3. Select the **Service Type** (communication protocol) for OpenVPN Server: UDP, TCP.
4. Enter a VPN **Service Port** to which a VPN device connects, and the port number should be between 1024 and 65535.
5. In the **VPN Subnet/Netmask** fields, enter the range of IP addresses that can be leased to the device by the OpenVPN server.
6. Select your **Client Access** type. Select **Home Network Only** if you only want the remote device to access your home network; select **Internet and Home Network** if you also want the remote device to access internet through the VPN Server.

7. Click **Save**.
8. Click **Generate** to get a new certificate.

Certificate

Generate the certificate.

Generate

Note: If you have already generated one, please skip this step, or click **Generate** to update the certificate.

9. Click **Export** to save the OpenVPN configuration file which will be used by the remote device to access your router.

Configuration File

Export the configuration.

Export

Step 2. Configure OpenVPN Connection on Your Remote Device

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

Note: You need to install the **OpenVPN** client utility on each device that you plan to apply the VPN function to access your router. Mobile devices should download a third-party app from Google Play or Apple App Store.

2. After the installation, copy the file exported from your router to the OpenVPN client utility's "config" folder (for example, `C:\Program Files\OpenVPN\config` on Windows). The path depends on where the OpenVPN client utility is installed.
3. Run the OpenVPN client utility and connect it to OpenVPN Server.

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

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

Step 1. Set up PPTP VPN Server on Your Router

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

PPTP VPN

Enable VPN Server

Client IP Address: -10.0.0. (up to 10 clients)

Advanced

Allow Samba (Network Place) access:

Allow NetBIOS passthrough:

Allow Unencrypted connections:

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

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

Account List (up to 16 users)

<input type="checkbox"/>	ID	Username	Password	Modify
<input type="checkbox"/>	--	--	--	--

Username:

Password:

<input type="checkbox"/>	1	admin	admin	<input checked="" type="checkbox"/> <input type="checkbox"/>
--------------------------	---	-------	-------	--

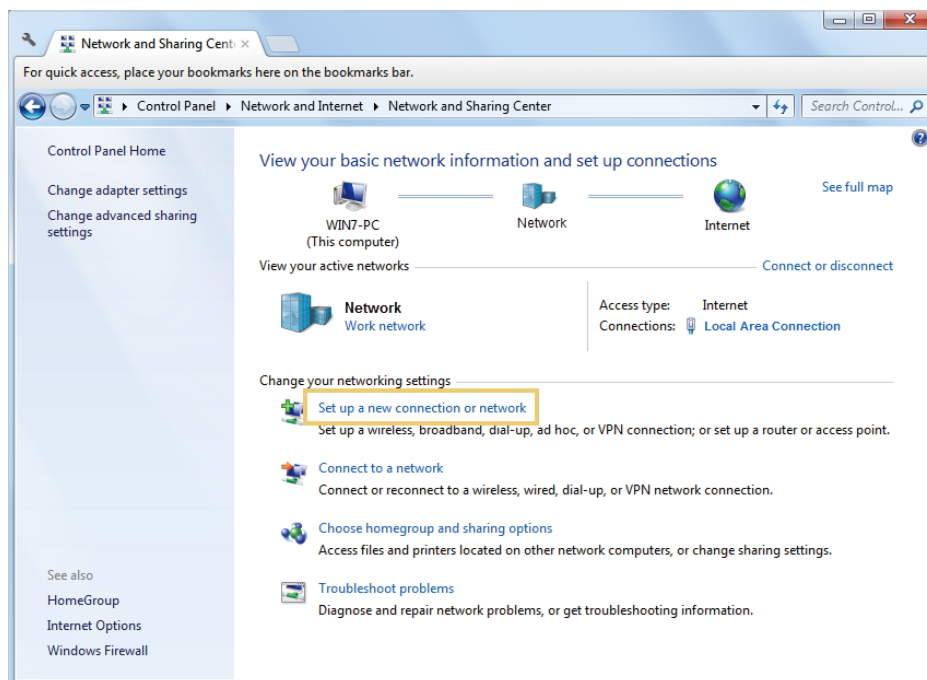
- 1) Click [Add](#).

- 2) Enter the **Username** and **Password** to authenticate devices to the PPTP VPN Server.
- 3) Click **OK**.

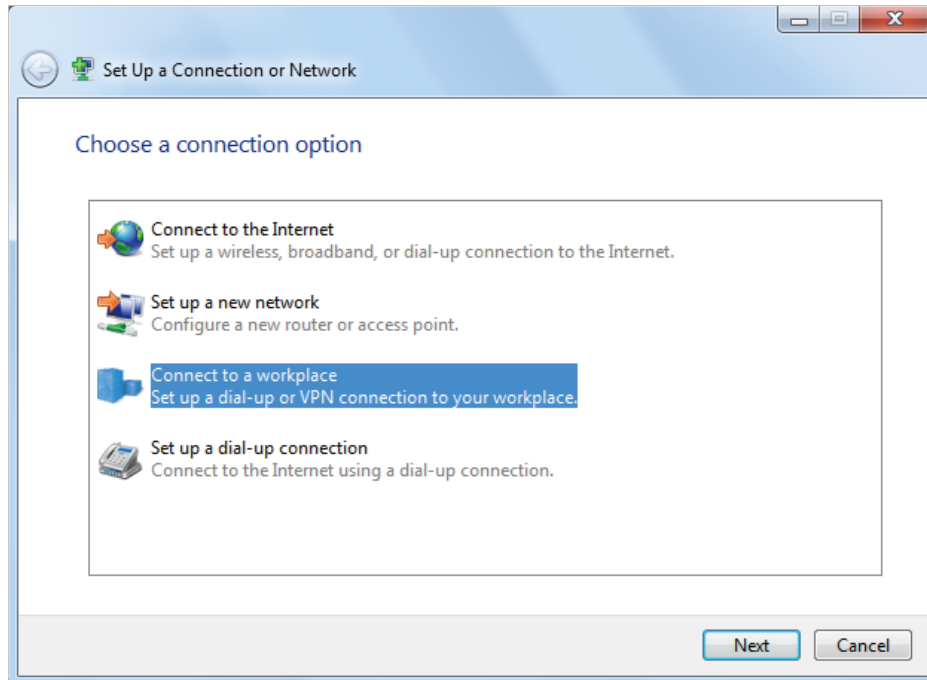
Step 2. Configure PPTP VPN Connection on Your Remote Device

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

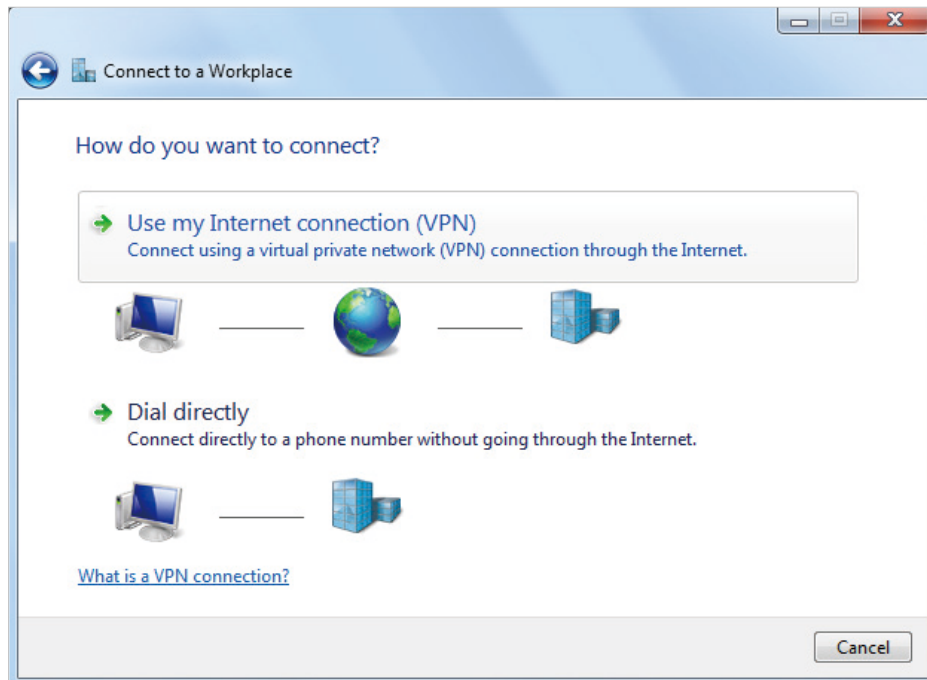
1. Go to **Start > Control Panel > Network and Internet > Network and Sharing Center**.
2. Select **Set up a new connection or network**.



3. Select **Connect to a workplace** and click **Next**.



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



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

Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 218.18.1.73

Destination name: VPN Connection

Use a smart card

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

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

Next Cancel

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

Connect to a Workplace

Type your user name and password

User name: admin

Password: ●●●●●

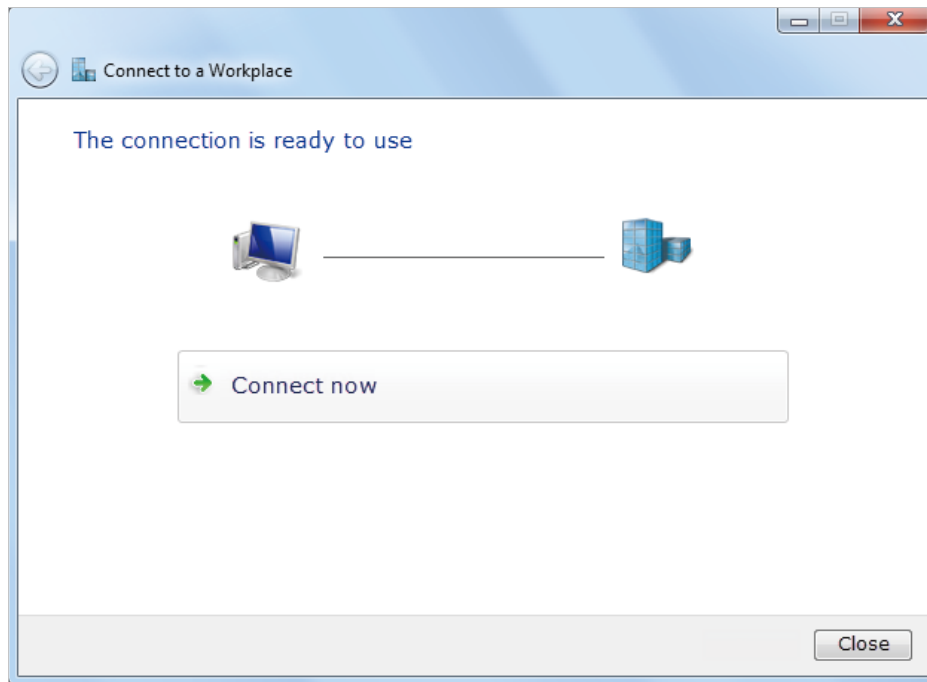
Show characters

Remember this password

Domain (optional):

Connect Cancel

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



Chapter 10

Customize Your Network Settings

This chapter guides you on how to configure advanced network features. Some features are only supported by a certain mode.

It contains the following sections:

- [Change the LAN Settings](#)
- [Configure to Support IPTV Service](#)
- [Specify DHCP Server Settings](#)
- [Set Up a Dynamic DNS Service Account](#)
- [Create Static Routes](#)
- [Specify Wireless Settings](#)
- [Use WPS for Wireless Connection](#)
- [Schedule Your Wireless Function](#)

10.1. Change the LAN Settings

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Network](#) > [LAN](#).
3. Type in a new IP Address appropriate to your needs. And leave the [Subnet Mask](#) as the default settings.

LAN

MAC Address: 50-C7-BF-02-EA-DC

IP Address:

Subnet Mask:

[Save](#)

4. Click [Save](#).

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

10.2. Configure to Support IPTV Service

I want to: Configure IPTV setup to enable Internet/IPTV/Phone service provided by my internet service provider (ISP).

How can I do that?

1. Visit <http://tplinkwifi.net>, and log in the password you set for the router.
2. Go to [Advanced](#) > [Network](#) > [IPTV](#).
3. **If your ISP provides the networking service based on IGMP technology**, e.g., British Telecom(BT) and Talk Talk in UK:
 - 1) Tick the [IGMP Proxy](#) checkbox and select the [IGMP Version](#), either V2 or V3, as required by your ISP.

Settings

IGMP Proxy: [Enable](#)

IGMP Version:

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

If IGMP is not the technology your ISP applies to provide IPTV service:


- 1) Tick [Enable IPTV](#).
- 2) Select the appropriate [Mode](#) according to your ISP.
 - Select [Bridge](#) if your ISP is not listed and no other parameters are required.
 - Select [Custom](#) if your ISP is not listed but provides necessary parameters.

The screenshot shows a configuration panel for IPTV. On the left, there are labels for 'IPTV:', 'Mode:', 'LAN1:', 'LAN2:', 'LAN3:', and 'LAN4:'. To the right of 'IPTV:' is a checked checkbox labeled 'Enable IPTV'. To the right of 'Mode:' is a dropdown menu currently showing 'Bridge'. The dropdown menu is open, displaying a list of options: 'Bridge', 'Singapore-ExStream', 'Malaysia-Unifi', 'Malaysia-Maxis', 'Portugal-MEO', 'Portugal-Vodafone', and 'Custom'. At the bottom right of the panel is a blue 'Save' button.

- 3) After you have selected a mode, the necessary parameters, including the LAN port for IPTV connection, are predetermined. If not, select the LAN type to determine which port is used to support IPTV service.
- 4) Click [Save](#).
- 5) Connect the set-top box to the corresponding LAN port which is predetermined or you have specified in Step 3.

Done!

Your IPTV setup is done now! You may need to configure your set-top box before enjoying your TV.

 **Tips:** Qos and IPTV cannot be enabled at the same time.

10.3. Specify DHCP Server Settings

By default, the DHCP (Dynamic Host Configuration Protocol) Server is enabled and the router acts as a DHCP server; it dynamically assigns TCP/IP parameters to client devices from the IP Address Pool. You can change the settings of the DHCP Server if necessary, and you can reserve LAN IP addresses for specified client devices.

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

2. Go to [Network > DHCP Server](#).

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

Settings

DHCP Server: [Enable DHCP Server](#)

IP Address Pool: -

Address Lease Time: minutes. (1-2880. The default value is 120.)

Default Gateway: (Optional)

Primary DNS: (Optional)

Secondary DNS: (Optional)

[Save](#)

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

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

1. Click [Add](#) in the [Address Reservation](#) section.

Address Reservation

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

<input type="checkbox"/>	ID	MAC Address	Reserved IP Address	Description	Status	Modify
<input type="checkbox"/>	--	--	--	--	--	--

MAC Address:

IP Address:

Description:

Enable This Entry

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

2. Click [View Existing Devices](#) or enter the [MAC address](#) of the client device.
3. Enter the [IP address](#) to reserve for the client device.

4. Enter the [Description](#) for this entry.
5. Tick the [Enable This Entry](#) checkbox and click [OK](#).

10.4. Set Up a Dynamic DNS Service Account

Most ISPs assign a dynamic IP address to the router and you can use this IP address to access your router remotely. However, the IP address can change from time to time and you don't know when it changes. In this case, you might apply the DDNS (Dynamic Domain Name Server) feature on the router to allow you and your friends to access your router and local servers (FTP, HTTP, etc.) using a domain name without checking and remembering the IP address.

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [Network](#) > [Dynamic DNS](#).
3. Select the DDNS [Service Provider](#): NO-IP or DynDNS. If you don't have a DDNS account, you have to register first by clicking [Go to register...](#) Then enter the username, password and domain name of your account.

The screenshot shows the 'Dynamic DNS' configuration page. It includes the following fields and options:

- Service Provider:** Radio buttons for 'NO-IP' (selected) and 'DynDNS', with a link for 'Go to register...'
- Username:** Text input field
- Password:** Text input field
- Domain Name:** Text input field
- Update Interval:** Dropdown menu set to '1 hour'
- WAN IP binding:** Radio buttons for 'Disable' (selected) and 'Enable'

At the bottom, there are three buttons: 'Login and Save' (highlighted in teal), 'Logout', and 'Not launching' (with a red 'x' icon).

4. Click [Login and Save](#).

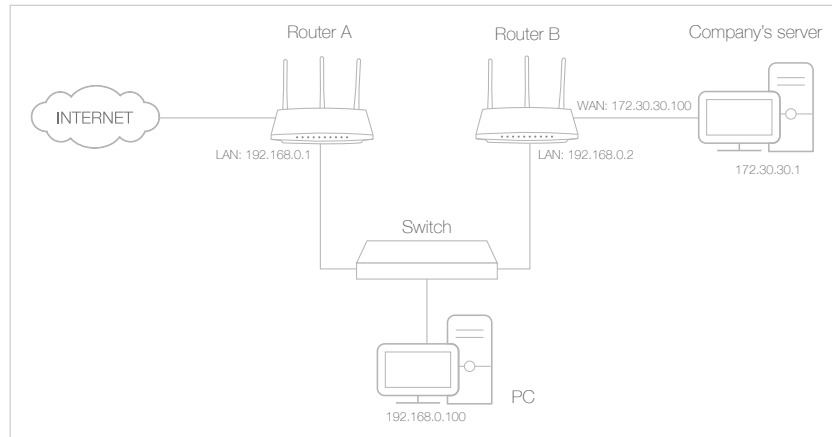
Tips: If you want to use a new DDNS account, please click [Logout](#) first, and then log in with a new account.

10.5. Create Static Routes

Static routing is a form of routing that is configured manually by a network administrator or a user by adding entries into a routing table. The manually-configured routing information guides the router in forwarding data packets to the specific destination.

I want to: Visit multiple networks and servers at the same time.

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



How can I do that?

1. Change the routers' LAN IP addresses to two different IP addresses on the same subnet. Disable Router B's DHCP function.
2. Visit <http://tplinkwifi.net>, and log in with the password you set for Router A.
3. Go to **Advanced > Network > Advanced Routing**.
4. Click **Add** and finish the settings according to the following explanations:

Static Routing

+ Add - Delete

☐	ID	Network Destination	Subnet Mask	Default Gateway	Interface	Description	Status	Modify
--	--	--	--	--	--	--	--	--

Network Destination:

Subnet Mask:

Default Gateway:

Interface: ▾

Description:

Enable This Entry

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


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

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

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

Description: Enter a description for this static routing entry.

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

System Routing Table				
Active Routes Number: 3				 Refresh
ID	Network Destination	Subnet Mask	Gateway	Interface
1	172.30.30.1	255.255.255.255	192.168.0.2	lan
2	192.168.0.0	255.255.255.0	0.0.0.0	lan
3	192.168.0.2	255.255.255.255	0.0.0.0	lan

Done!

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

10.6. Specify Wireless Settings

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

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

➤ To enable or disable the wireless function:

1. Go to [Basic > Wireless](#) or [Settings > Wireless > Wireless Settings](#).
2. The wireless radio is enabled by default. If you want to disable the 2.4GHz/5GHz wireless function of the router, just untick the [Enable Wireless Radio](#) checkbox. 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](#) or [Settings > Wireless > Wireless Settings](#).
2. Create a new SSID for the 2.4GHz/5GHz wireless network in [Network Name \(SSID\)](#) and customize the password in [Password](#). The value is case-sensitive.

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

➤ To hide SSID:

1. Go to [Basic > Wireless](#) or [Settings > Wireless > Wireless Settings](#).
2. Select [Hide SSID](#), and the SSID of the 2.4GHz/5GHz wireless network won't display when you scan for local wireless networks on your wireless device and you need to manually join the network.

➤ To change the security option:

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

2. Select an option from the **Security** of the 2.4GHz/5GHz wireless network. We recommend you don't change the default settings unless necessary. If you select other options, configure the related parameters according to the help page.

In addition

- **Mode** - Select a transmission mode according to your wireless client devices. It is recommended to just leave it as default.
- **Channel Width** - Select a channel width (bandwidth) for the wireless network.
- **Channel** - Select an operating channel for the wireless network. It is recommended to leave the channel to **Auto**, if you are not experiencing the intermittent wireless connection issue.

10.7. Extend Host Network

If you want to extend another host network after Quick Setup when the router works as a range extender, you can refer to this section.

1. Visit <http://tplinkrepeater.net>, and log in with the password you set for the router.
2. Go to **Settings > Wireless > Connect to Network**.
3. Enable **Connect to 2.4GHz Network/Connect to 5GHz Network** and click **Wireless Scanner** to find all available networks.

Connect to Host Network

2.4GHz Network: **Connect to 2.4GHz Network**

Wireless Scanner

Host 2.4GHz SSID:

Host 2.4GHz Security: **No Security** ▼

Channel Width: **Auto** ▼

5GHz Network: **Connect to 5GHz Network**

Wireless Scanner

Host 5GHz SSID:

Host 5GHz Security: **No Security** ▼

Channel Width: **Auto** ▼

Save

4. Select the host network you want to extend.

Note:

If the network you want to extend is on but not listed, please try the following steps.

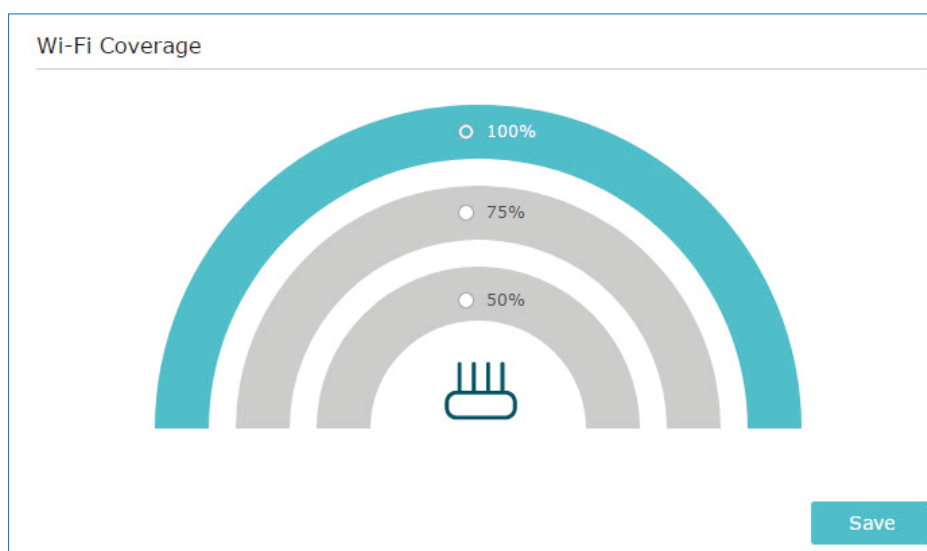
- Move the router closer to your host router, and click **Refresh** in the top-right corner of the list.

- You can manually enter the SSID (network name) and password of the network you want to extend, and click [Save](#).
5. Once a host network is selected, the SSID and security type will be automatically filled in. If the selected network is encrypted, enter the password in the [Password](#) field.
 6. Click [Save](#).

10.8. Adjust Wi-Fi Coverage

Set the router's Wi-Fi coverage depending on how large you want your Wi-Fi area to be.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced - Settings > Wi-Fi Coverage](#).
3. Select [100%](#), [75%](#) or [50%](#) to adjust your Wi-Fi coverage of the router and click [Save](#).



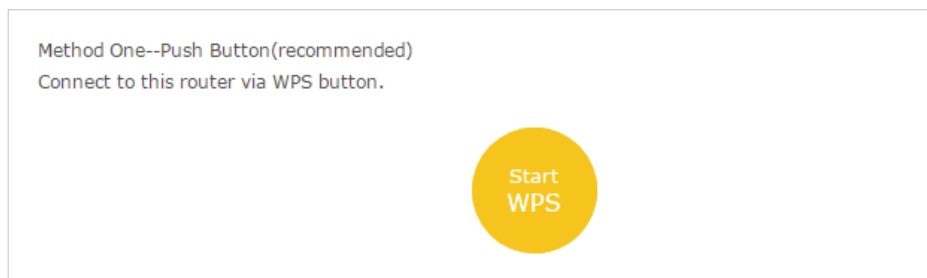
10.9. Use WPS for Wireless Connection

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

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

10.9.1. Use the WPS Wizard for Wi-Fi Connections

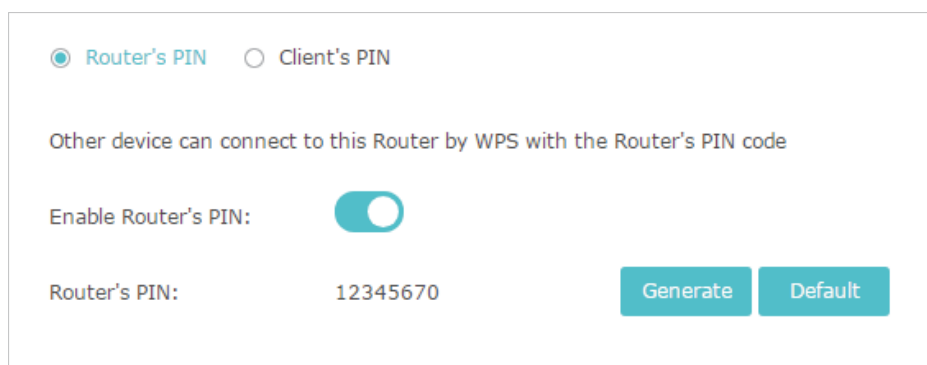
1. Click the [Start WPS](#) button on the screen. Within two minutes, press the WPS button on the client device.



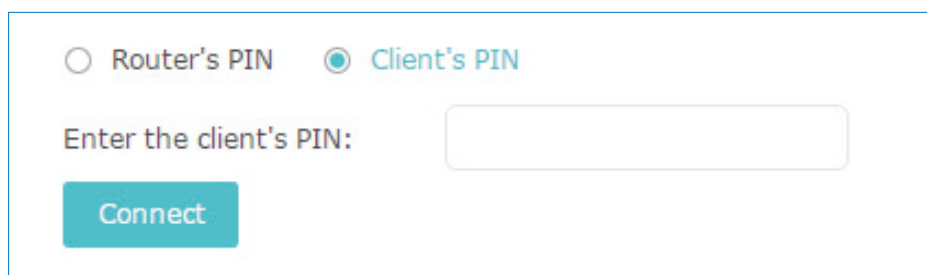
2. **Success** will appear on the above screen and the WPS LED on the router will keep on for five minutes if the client has been successfully added to the network.

10.9.2. Use the PIN for Wi-Fi connections

Router's PIN is enabled by default to allow wireless devices to connect to the router using the PIN. You can use the default one or generate a new one.



You can also enter the PIN of the device you want to connect to the Wi-Fi.



Note:

- If you want to enable/disable the WPS feature, go to [System Tools > System Parameters > WPS](#), tick or untick the [Enable WPS](#) checkbox.
- PIN (Personal Identification Number) is an eight-character identification number preset to each router. WPS supported devices can connect to your router with the PIN. The default PIN is printed on the label of the router.

10.10. Schedule Your Wireless Function

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced > Wireless > Wireless Schedule](#) or [Settings > Wireless > Wireless Schedule](#).
3. Enable [Wireless Schedule](#).
4. Click [Add](#) to set the wireless off time. Specify the time period and days when the wireless network will be off.

Wireless Off Time

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

<input type="checkbox"/>	ID	Wireless Off Time	Repeat	Modify
<input type="checkbox"/>	--	--	--	--

Wireless Off Time:

From:

To:

Repeat: Every Day Selected Day

Note: The rule of repetition days is applied to all time entries.

[Cancel](#) [Save](#)

5. Click [Save](#).

Chapter 11

Manage the Router


This chapter will show you the configuration for managing and maintaining your router. Some features are only supported by a certain mode.

It contains the following sections:

- [Change Operation Mode](#)
- [Set Up System Time](#)
- [Control LEDs](#)
- [Test the Network Connectivity](#)
- [Upgrade the Firmware](#)
- [Backup and Restore Configuration Settings](#)
- [Auto Reboot](#)
- [Change the Login Password](#)
- [Password Recovery](#)
- [Local Management](#)
- [Remote Management](#)
- [System Log](#)
- [Monitor the Internet Traffic Statistics](#)

11.1. Change Operation Mode

The router supports three operation modes: router, access point and range extender. Select one mode as needed.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Click  in the top-right corner of the web page.
3. Select the mode as needed and click [Save](#). The router will reboot to apply the settings.

Mode Selection

Access Point
Transforms your existing wired network to a wireless network.

Router
Provides Internet access for multiple wired and wireless devices simultaneously.

Range Extender
Extends your existing wireless coverage by repeating the wireless signal.

[Cancel](#) [Save](#)

11.2. Set Up System Time

System time is the time displayed while the router is running. The system time you configure here will be used for other time-based functions like Parental Controls.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [System Tools](#) > [Time Settings](#).
 - **To get time from the internet:**
 1. Select your local [Time Zone](#) from the drop-down list.

Time Settings

Current Time: 01/01/1970 00:11:30

Time Zone: -Please Select-

NTP Server I: time.nist.gov

NTP Server II: time-nw.nist.gov (Optional)

Obtain Save

2. In the **NTP Server I** field, enter the IP address or domain name of your desired NTP Server.
3. (Optional) In the **NTP Server II** field, enter the IP address or domain name of the second NTP Server.
4. Click **Obtain** to get the current Internet time and click **Save**.

➤ **To set up Daylight Saving Time:**

1. Select **Enable Daylight Saving Time**.

Daylight Saving Time

Enable Daylight Saving Time

Start: 2016 Mar 2nd Sun 2 AM

End: 2016 Nov First Sun 2 AM

Running Status: Daylight Saving Time is on.

Save

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

11.3. Control LEDs

The router's LEDs indicate the router's activities and status. You can turn on or off the LEDs from the web management page.

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

2. Go to [System Tools > LED Control](#).
3. Tick the [Night Mode](#) checkbox.
4. Specify a time period in the [LED Off Time](#) as needed, and the LEDs will be off during this period.

LED Control

Night Mode

LED Off Time: 21 : 00 - 09 : 00

Note: Before enabling the LED Control, make sure [Time Settings](#) is correct.

Save

5. Click [Save](#).

11.4. Test the Network Connectivity

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

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

Diagnostics

Diagnostic Tool: Ping Traceroute

IP Address/Domain Name:

Start

3. Enter the information with the help of page tips:
 - 1) Choose [Ping](#) or [Traceroute](#) as the diagnostic tool to test the connectivity;
 - [Ping](#) is used to test the connectivity between the router and the tested host, and measure the round-trip time.
 - [Traceroute](#) is used to display the route (path) your router has passed to reach the tested host, and measure transit delays of packets across an Internet Protocol network.
 - 2) Enter the [IP Address](#) or [Domain Name](#) of the tested host.
4. Click [Start](#) to begin the diagnostics.

Tips: Click [Advanced](#), you can modify the ping count, ping packet size or the Traceroute Max TTL. It's recommended to keep the default value.

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

```
PING www.Yahoo.com (116.214.12.74): 64 data bytes
Reply from 116.214.12.74: bytes=64 ttl=50 seq=1 time=51.640 ms
Reply from 116.214.12.74: bytes=64 ttl=50 seq=2 time=53.671 ms
Reply from 116.214.12.74: bytes=64 ttl=50 seq=3 time=56.045 ms
Reply from 116.214.12.74: bytes=64 ttl=50 seq=4 time=57.857 ms

--- Ping Statistic "www.Yahoo.com" ---
Packets: Sent=4, Received=4, Lost=0 (0.00% loss)
Round-trip min/avg/max = 51.640/54.803/57.857 ms
```

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

```
traceroute to www.Yahoo.com (116.214.12.74), 20 hops max, 38 byte packets
 1 219.133.12.1 (219.133.12.1) 19.556 ms 22.274 ms 22.024 ms
 2 113.106.38.77 (113.106.38.77) 30.115 ms 22.649 ms 20.931 ms
 3 * * *
 4 183.56.65.14 (183.56.65.14) 26.210 ms 29.428 ms 28.272 ms
 5 * 202.97.60.25 (202.97.60.25) 29.272 ms 25.461 ms
 6 202.97.60.46 (202.97.60.46) 27.335 ms 27.616 ms 28.272 ms
 7 202.97.60.149 (202.97.60.149) 22.805 ms 24.024 ms 24.711 ms
 8 202.97.6.30 (202.97.6.30) 47.610 ms 54.452 ms 61.137 ms
 9 r4105-s2.tp.hinet.net (220.128.6.110) 51.171 ms 50.515 ms 56.107 ms
10 220.128.11.190 (220.128.11.190) 60.950 ms 60.200 ms 60.419 ms
```

11.5. Upgrade the Firmware

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

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

Note:

- Make sure you remove all attached USB devices from the router before the firmware upgrade to prevent data loss.
- Backup your router configuration before firmware upgrade.
- Do NOT turn off the router during the firmware upgrade.

1. Download the latest firmware file for the router from www.tp-link.com.
2. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
3. Go to [System Tools > Firmware Upgrade](#).
4. Click [Browse](#) to locate the downloaded new firmware file, and click [Upgrade](#).

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

11.6. Backup and Restore Configuration Settings

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

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

➤ To backup configuration settings:

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

➤ To restore configuration settings:

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

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

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

➤ To reset the router to factory default settings:

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

Factory Default Restore

Revert all the configuration settings to their default values.

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

Note:

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

11.7. Auto Reboot

Auto Reboot allows you to specify a time when the router will reboot automatically.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [System Tools](#) > [Auto Reboot](#).
3. Enable [Auto Reboot](#).
4. Select [Every Day](#) or [Selected Day](#). If [Selected Day](#) is selected, then specify the days when you want the router to reboot.
5. Specify the time at which your router will reboot.
6. Click [Save](#).

Auto Reboot

Enable Auto Reboot: [Auto Reboot](#)

Day: [Every Day](#) [Selected Day](#)

Mon Tue Wed Thu Fri Sat Sun

Time: : (HH/MM)

11.8. 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 router.
2. Go to [System Tools](#) > [Administration](#) and focus on the [Account Management](#) section.

The screenshot shows a form titled "Account Management". It contains three input fields: "Old Password:", "New Password:", and "Confirm New Password:". The "New Password:" field has a strength indicator below it with three segments labeled "Low", "Middle", and "High". A "Save" button is located at the bottom right of the form.

3. Enter the old password, then a new password twice (both case-sensitive). Click [Save](#).
4. Use the new password for future logins.

11.9. Password Recovery

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [System Tools](#) > [Administration](#) and focus on the [Password Recovery](#) section.
3. Tick the [Enable Password Recovery](#) checkbox.
4. Specify a [mailbox \(From\)](#) for sending the recovery letter and enter its [SMTP Server](#) address. Specify a [mailbox \(To\)](#) for receiving the recovery letter. If the mailbox (From) to send the recovery letter requires encryption, select [Enable Authentication](#) and enter its username and password.

Tips:

- SMTP server is available for users in most webmail systems. For example, the SMTP server address of Gmail is smtp.gmail.com. You can refer to their Help page to learn the SMTP server address.
- Generally, Enable Authentication should be selected if the login of the mailbox requires username and password.

The screenshot shows a form titled "Password Recovery". It features a checkbox labeled "Enable Password Recovery" which is checked. Below this are input fields for "From:", "To:", and "SMTP Server:". Another checkbox labeled "Enable Authentication" is checked. Below it are input fields for "Username:" and "Password:". At the bottom right, there are two buttons: "Test Email" and "Save".

5. Click [Save](#).

You can click [Test Email](#) to test whether the configuration is successful.

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

11. 10. Local Management

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [System Tools](#) > [Administration](#) and complete the settings In [Local Management](#) section as needed.

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

Toggle on [Access for All LAN Connected Devices](#).

Local Management

Access for All LAN Connected Devices: Toggle On to enable the management for all devices on LAN or keep it Off to enable the management for a specific device.

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

1. Toggle off [Access for All LAN Connected Devices](#).
2. Click [Add](#).

Local Management

Access for All LAN Connected Devices: Toggle On to enable the management for all devices on LAN or keep it Off to enable the management for a specific device.

+ Add - Delete

<input type="checkbox"/>	ID	MAC Address	Description	Status	Modify
--	--	--	--	--	--

MAC Address: View Existing Devices

Description:

Enable This Entry

Cancel
OK

--	1	C0-4A-00-1A-C3-45	Your PC!	💡	📄 🗑️
----	---	-------------------	----------	---	------

3. Click [View Existing Devices](#) and select the device to manage the router from the Existing Devices list, or enter the MAC address of the device manually.
4. Specify a [Description](#) for this entry.
5. Tick the [Enable This Entry](#) checkbox.
6. Click [OK](#).

11. 11. Remote Management

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [System Tools](#) > [Administration](#) and complete the settings in [Remote Management](#) section as needed.

Remote Management

[Disable Remote Management](#)

[Enable Remote Management for All Devices](#)

[Enable Remote Management for Specified Devices](#)

Web Management Port:

Remote Management IP Address:

[Save](#)

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

Select [Disable Remote Management](#) and click [Save](#).

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

1. Select [Enable Remote Management for All Devices](#).
2. Enter [Web Management Port](#) (1024-65535 or 80).
3. Click [Save](#).

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

📌 **Tips:**


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

➤ **Allow specific devices to manage the router remotely:**

1. Select [Enable Remote Management for Specified Devices](#).
2. Enter [Web Management Port](#) (1024-65535 or 80).

3. In **Remote Management IP address**, enter the IP address of the remote device to manage the router.
4. Click **Save**.

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

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

11. 12. System Log



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

➤ To save the system log locally:


1. Visit <http://tplinkwifi.net>, and log in the password you set for the router.
2. Go to **System Tools > System Log**.
3. Choose the type and level of the system logs as needed.
4. Click **Save Log** to save the system logs to a local disk.

System Log

Log Filter: Type= ALL and Level= ALL

 Refresh  Delete All

ID	Time	Type	Level	Log Content
1	2016-06-24 04:28:31	Local Management	NOTICE	[19000] Accessable mode change: Devices in the list.
2	2016-06-24 04:25:12	Locale	INFO	[16605] Language is changed to 'en_US'
3	2016-06-24 04:25:12	Locale	DEBUG	[16605] Explorer language is 'zh_CN'
4	2016-06-24 04:25:02	Locale	INFO	[16435] Language is changed to 'en_US'
5	2016-06-24 04:25:02	Locale	DEBUG	[16435] Explorer language is 'zh_CN'
6	2016-06-24 04:24:58	Locale	INFO	[16283] Language is changed to 'en_US'
7	2016-06-24 04:24:58	Locale	DEBUG	[16283] Explorer language is 'zh_CN'

 Mail Settings

Mail Log
Save Log

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

For example, I want to check my router's working status at a fixed time every day, however, it's too troublesome to log in to the web management page every time I want to go checking. It would be great if the system logs could be sent to my mailbox at 8 a.m. every day.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to **System Tools > System Log**.
3. Click **Mail Settings**.
4. Enter the information required:

The screenshot shows the 'Mail Settings' configuration page. It contains the following elements:

- From:** Text input field.
- To:** Text input field.
- SMTP Server:** Text input field.
- Enable Authentication**
- Username:** Text input field.
- Password:** Text input field.
- Enable Auto Mail**
- Log at** 00 : 00 (HH:MM) everyday
- Log every** 24 hours
- Save** button

- 1) **From:** Enter the email address used for sending the system log.
- 2) **To:** Enter the recipient's email address, which can be the same as or different from the sender's email address.
- 3) **SMTP Server:** Enter the SMTP server address.

Tips: SMTP server is available for users in most webmail systems. For example, the SMTP server address of Hotmail is smtp-mail.outlook.com. You can refer to their Help page to learn the SMTP server address.

- 4) Select **Enable Authentication**.

Tips: Generally, Enable Authentication should be selected if the login of the mailbox requires username and password.

- 5) **Username:** Enter the email address used for sending the system log.
- 6) **Password:** Enter the password to login the sender's email address.
- 7) Select **Enable Auto Mail**.

Tips: The router will send the system log to the designated email address if this option is enabled.

- 8) Set a fixed time. The recipient will receive the system log sent at this time every day.
5. Click [Save](#).

11. 13. 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 router.
2. Go to [Advanced](#) > [System Tools](#) > [Traffic Statistics](#).
3. Toggle on [Traffic Statistics](#), and then you can monitor the traffic statistics in [Traffic Statistics List](#) section.

Traffic Statistics

Traffic Statistics:

Traffic Statistics List

[Refresh](#) [Reset All](#) [Delete All](#)

IP Address/MAC Address	Total Packets	Total Bytes	Current Packets	Current Bytes	Modify
--	--	--	--	--	--

Click [Refresh](#) to update the statistic information on the page.

Click [Reset All](#) to reset all statistic values in the list to zero.

Click [Delete All](#) to delete all statistic information in the list.

Click  to reset the statistic information of the specific device.

Click  to delete the specific device item in the list.

FAQ

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

The default wireless password is printed on the label of the router. If the password has been altered, please connect your computer to the router using an Ethernet cable and follow the steps below:

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

When the router works as a range extender, the passwords of the extended networks are the same as those of your host networks.

Q2. What should I do if I forget my login password of the web management page?

1. With the router powered on, use a pin to press and hold the **Reset** button on the back panel of the router until all the LEDs turn on momentarily.

2. Visit <http://tplinkwifi.net>, and create a new password for future logins.

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

If you have enabled Password Recovery, please follow the steps below to reset the login password without resetting the router:

Note: Make sure the internet access is available before using this method.

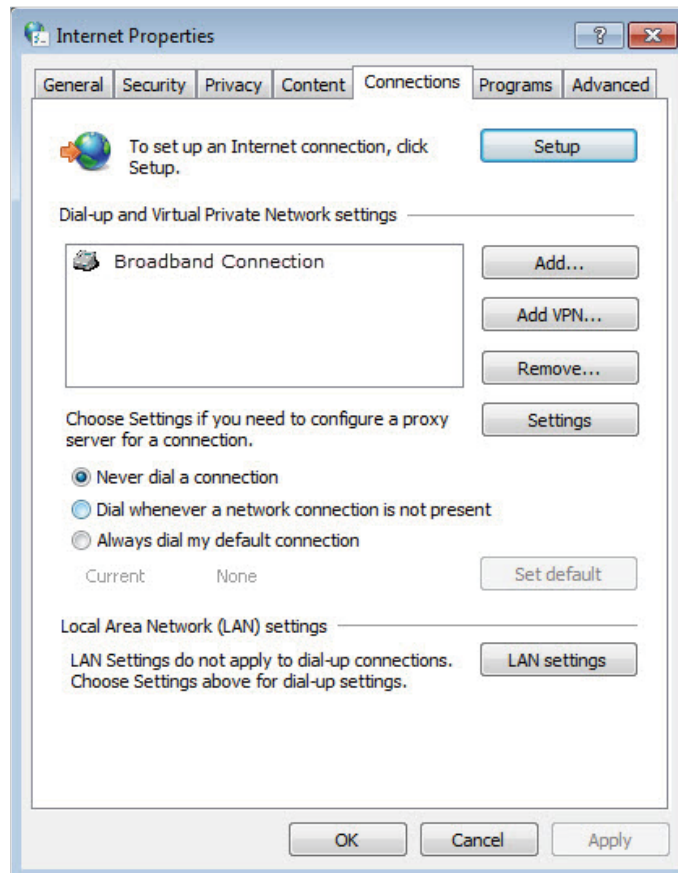
1. Visit <http://tplinkwifi.net>.
2. Click [Forgot Password > Send Code](#). The verification code will be sent to the mailbox you set.
3. Log in to your mailbox and copy the verification code.
4. Paste the verification code on the window which appears in Step 2
5. Click [Confirm](#).
6. Create a new password for future logins.

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

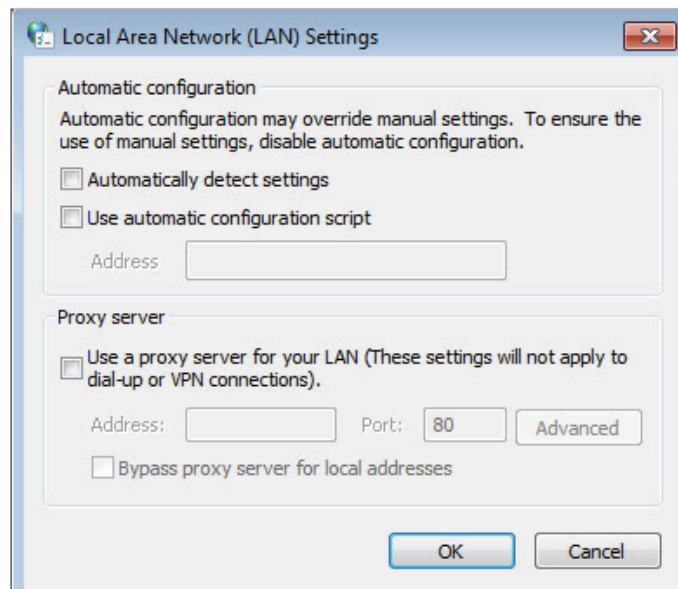
This can happen for a variety of reasons. Please try the following:

- Make sure your computer has connected to the router correctly and the corresponding LED light up.
- Make sure the IP address of your computer is configured as [Obtain an IP address automatically](#) and [Obtain DNS server address automatically](#).

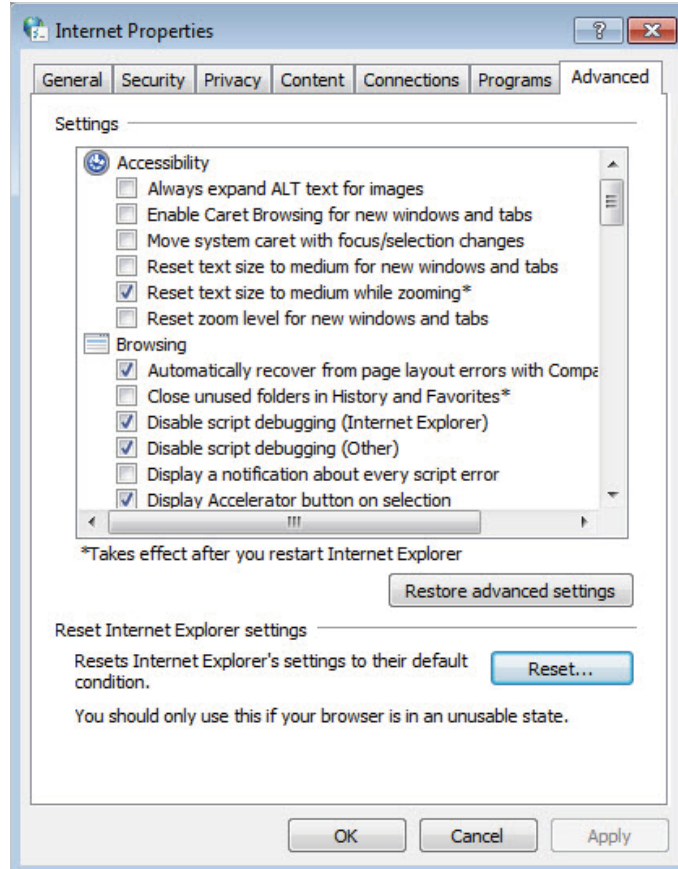
- Verify that <http://tplinkwifi.net> or 192.168.0.1 is correctly entered in the web browser.
- Check your computer's settings: Go to **Start > Control Panel > Network and Internet**, and click **View network status and tasks**.
 - 1) Click **Internet Options** on the bottom left.
 - 2) Click **Connections** and select **Never dial a connection**.



- 3) Click **LAN settings** and deselect the following three options, and click **OK**.



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



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

Q4. What should I do if I can't access the internet after the configuration in router mode?

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

If the IP address is a valid one, please try the following:

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

- 1) Go to [Network](#) > [DHCP](#).
- 2) Enter 8.8.8.8 as Primary DNS, and click [Save](#).

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

Settings

DHCP Server: Enable DHCP Server

IP Address Pool: -

Address Lease Time: minutes. (1-2880. The default value is 120.)

Default Gateway: (Optional)

Primary DNS: (Optional)

Secondary DNS: (Optional)

[Save](#)

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

If the IP address is 0.0.0.0, please try the following:

- Make sure the physical connection between the router and the modem is established.
- Clone the MAC address of your computer.
 - 1) Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
 - 2) Go to [Network > Internet](#) and focus on the [MAC Clone](#) section.
 - 3) Choose an option as needed (enter the MAC address if [Use Custom MAC Address](#) is selected) and click [Save](#).

MAC Clone

Use Default MAC Address

Use Current Computer MAC Address

Use Custom MAC Address

[Save](#)

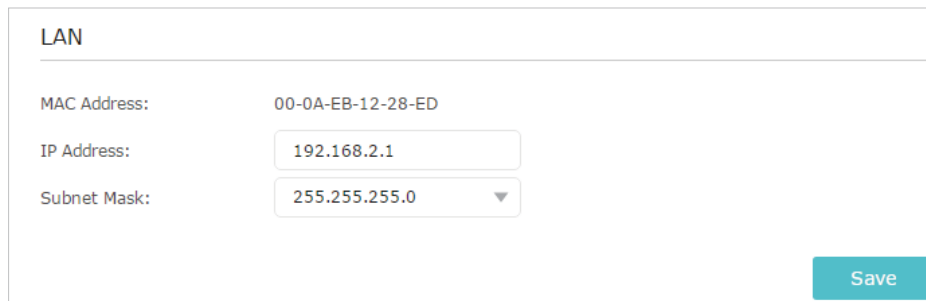
🔗 Tips:

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

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

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

- 1) Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
- 2) Go to **Network > LAN**.
- 3) Modify the LAN IP address as the follow picture shows. Here we take 192.168.2.1 as an example.



The screenshot shows the LAN configuration interface. The MAC Address is 00-0A-EB-12-28-ED. The IP Address is set to 192.168.2.1. The Subnet Mask is set to 255.255.255.0. A Save button is located at the bottom right.

- 4) Click **Save**.
- **Restart the modem and the router.**
 - 1) Power off your modem and the router, and leave them off for 1 minute.
 - 2) Power on your modem first, and wait about 2 minutes.
 - 3) Power on the router, and wait another 1 or 2 minutes and check the internet access.
 - **Double check the WAN Connection Type.**
 - 1) Confirm your WAN Connection Type, which can be got from the ISP.
 - 2) Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
 - 3) Go to **Network > Internet**.
 - 4) Select your **Internet Connection Type** and fill in other parameters.

IPv4

Internet Connection Type: Dynamic IP

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0

Renew Release

Advanced

Save

5) Click [Save](#).

6) Restart the modem and the router.

- Please upgrade the firmware of the router.

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

Q5. What should I do if I can't find my wireless network or I can't 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 a built-in wireless adapter. You can refer to the relevant document or contact the laptop's 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) Clicking [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 network.

- 2) Exit the wireless configuration tool (the TP-Link Utility, for example).
- 3) Select and right click **My Computer** on Desktop, and select **Manage** to open Computer Management window.
- 4) Go to **Services and Applications > Services**, and 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 **Start** and make sure the Service status is **Started**. And then click **OK**.

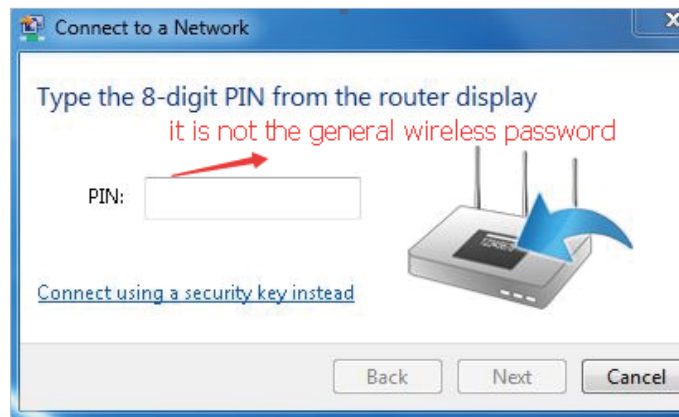
If you can find other wireless network except your own, please follow the steps below:

- Check the WAN LED indicator on your wireless router.
- Make sure your computer/device is still in the range of your router/modem. Move closer if it is currently too far away.

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 when you connect to the wireless network for the first time. This PIN is different from the Wireless Password/ Network Security Key. Usually you can only find it on the label of your router.



- 2) If you can't find the PIN or entering the PIN still does not work, 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 the note **Network Security Key Mismatch**, it is suggested to confirm the wireless password of your wireless router.


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

• Windows unable to connect to XXXX / Can not join this network / Taking longer than usual to connect to this network:

- Check the wireless signal strength of your network. It is weak (1~3 bars), please move the router closer and try again.

- Change the wireless channel of the router to 1, 6, or 11 to reduce interference from other networks.
- Re-install or update the driver for your wireless adapter of the computer.

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice.  is a registered trademark of TP-Link Technologies Co., Ltd. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-Link Technologies Co., Ltd. Copyright © 2017 TP-Link Technologies Co., Ltd. All rights reserved.

FCC STATEMENT



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."

CE Mark Warning



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

OPERATING FREQUENCY(the maximum transmitted power)

2412MHz—2472MHz(20dBm)

5180MHz—5240MHz(23dBm)

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.

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 and 2011/65/EU.

The original EU declaration of conformity may be found at <http://www.tp-link.com/en/ce>.

Restricted to indoor use.

Canadian Compliance Statement

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

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

Le présent appareil est conforme aux CNR d'Industrie 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'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Antenna	Three 9dBi detachable antennas
---------	--------------------------------

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 & BSMI Notice:

注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，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或功能。

第十四條 低功率射頻電機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。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機需忍受合法通信或工業、科學以及醫療用電波輻射性電機設備之干擾。

安全諮詢及注意事項


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






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



Safety Information

- When product has power button, the power button is one of the way to shut off the product; when there is no power button, the only way to completely shut off power is to disconnect the product or the power adapter from the power source.
- Don't disassemble the product, or make repairs yourself. You run the risk of electric shock and voiding the limited warranty. If you need service, please contact us.
- Avoid water and wet locations.
- Adapter shall be installed near the equipment and shall be easily accessible.
- The plug considered as disconnect device of adapter.
-  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.

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.