



User Guide

AC2600 MU-MIMO Wi-Fi Router
Archer A10

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.The Front Panel	3
1. 2. 2.The Side Panel	5
1. 2. 3.The Back Panel.....	5
Chapter 2. Connect the Hardware	7
2. 1. Position Your Router	8
2. 2. Connect Your Router.....	8
Chapter 3. Log In to Your Router.....	11
Chapter 4. Set Up Internet Connection	13
4. 1. Use Quick Setup Wizard	14
4. 2. Manually Set up Your Internet Connection	14
4. 3. Set Up an IPv6 Internet Connection	17
Chapter 5. Set Up the Router as an Access Point	21
Chapter 6. TP-Link Cloud Service	24
6. 1. Register a TP-Link ID.....	25
6. 2. Change Your TP-Link ID Information.....	25
6. 3. Manage the User TP-Link IDs	26
6. 3. 1.Add TP-Link ID to Manage the Router.....	27
6. 3. 2.Remove TP-Link ID(s) from Managing the Router.....	27
6. 4. Manage the Router via the TP-Link Tether App	28
Chapter 7. Guest Network.....	29
7. 1. Create a Network for Guests	30
7. 2. Customize Guest Network Options.....	30
Chapter 8. Parental Controls	32

8. 1.	Setting Up Access Restrictions	33
8. 2.	Monitoring Internet Usage	35
Chapter 9. QoS.....		36
Chapter 10.Network Security		38
10. 1.	Protect the Network from Cyber Attacks	39
10. 2.	Access Control	40
10. 3.	IP & MAC Binding	41
Chapter 11.NAT Forwarding.....		43
11. 1.	Share Local Resources on the Internet by Virtual Servers.....	44
11. 2.	Open Ports Dynamically by Port Triggering.....	45
11. 3.	Make Applications Free from Port Restriction by DMZ	46
11. 4.	Make Xbox Online Games Run Smoothly by UPnP	47
Chapter 12.VPN Server		49
12. 1.	Use OpenVPN to Access Your Home Network.....	50
12. 2.	Use PPTP VPN to Access Your Home Network	51
Chapter 13.Customize Your Network Settings.....		56
13. 1.	Change the LAN Settings	57
13. 2.	Configure to Support IPTV Service.....	57
13. 3.	Specify DHCP Server Settings	58
13. 4.	Set Up a Dynamic DNS Service Account	60
13. 5.	Create Static Routes.....	62
13. 6.	Specify Wireless Settings.....	64
13. 7.	Use WPS for Wireless Connection	66
13. 7. 1.	Method 1: Use the WPS Button.....	66
13. 7. 2.	Set the Router's PIN.....	66
13. 7. 3.	Use the WPS Wizard for Wi-Fi Connections.....	67
13. 8.	Set Wireless MAC Filtering	67
13. 9.	Schedule Your Wireless Function	68
Chapter 14.Manage the Router		70
14. 1.	Set Up System Time	71
14. 2.	Test the Network Connectivity	72
14. 3.	Upgrade the Firmware	73
14. 3. 1.	Online Upgrade	73

14. 3. 2.Local Upgrade	74
14. 3. 3.Restore Interrupted Upgrade after Power Failure	75
14. 4. Backup and Restore Configuration Settings	75
14. 5. Set the Router to Reboot Regularly.....	77
14. 6. Change the Administrator Account.....	77
14. 7. Local Management	78
14. 8. Remote Management.....	78
14. 9. System Log.....	79
14. 10. Monitor the Internet Traffic Statistics.....	81
14. 11. System Parameters.....	82
14. 11. 1.Wireless Advanced	82
14. 11. 2.WDS	83
14. 11. 3.LEDs Control	84
14. 11. 4.DoS Protection Settings	84
FAQ	86

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.

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

*Use of MU-MIMO requires clients to also support MU-MIMO.

More Info

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

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

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

Our Technical Support contact information can be found at the [Contact Technical Support](#) page at <https://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, and the built-in Ethernet ports supply high-speed connection to your wired devices.

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. The Front Panel



The router's LEDs are located on the front with an LED On/Off button. You can check the router's working status by following the LED Explanation table.

LED & Button Explanation

Name	Status	Indication
 (Power)	On	The system has started up successfully.
	Flashing	The system is starting up or the firmware is being upgraded. Do not disconnect or power off your router.
	Off	Power is off.
 (2.4GHz Wireless)	On	The 2.4GHz wireless band is enabled.
	Off	The 2.4GHz wireless band is disabled.
 (5GHz Wireless)	On	The 5GHz wireless band is enabled.
	Off	The 5GHz wireless band is disabled.
 (Internet)	Blue On	Internet service is available.
	Orange On	The router's Internet port is connected, but the internet service is not available.
	Off	The router's Internet port is unplugged.
 (Ethernet)	On	At least one powered-on device is connected to the router's LAN port.
	Off	No powered-on device is connected to the router's LAN port.
 (WPS)	On/Off	This light remains on for 5 minutes when a WPS connection is established, then turns off, or WPS connection failed.
	Flashing	WPS connection is in progress. This may take up to 2 minutes.
 (LED On/Off)	On/Off	Press this button to turn on or off the LED.

1.2.2. The Side Panel



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

Item	Description
Wi-Fi On/Off Button	Press and hold the WiFi button for about 2 seconds to turn on or off the wireless function of your router.
Reset Button	Press and hold this button for more than 5 seconds to reset the router to its factory default settings.
WPS Button	Press this button to enable the WPS function.

1.2.3. The Back Panel



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

Item	Description
Power Port	For connecting the router to a power socket via the provided power adapter.
Power On/Off Button	Press this button to power on or off the router.
Internet Port	For connecting to a DSL/Cable modem, or an Ethernet jack.
LAN Ports (1/2/3/4)	For connecting your PC or other Ethernet network devices to the router.
Antennas	Used for wireless operation and data transmit. Upright them for the best Wi-Fi performance.

Chapter 2

Connect the Hardware

This chapter contains the following sections:

- [Position Your Router](#)
- [Connect Your Router](#)

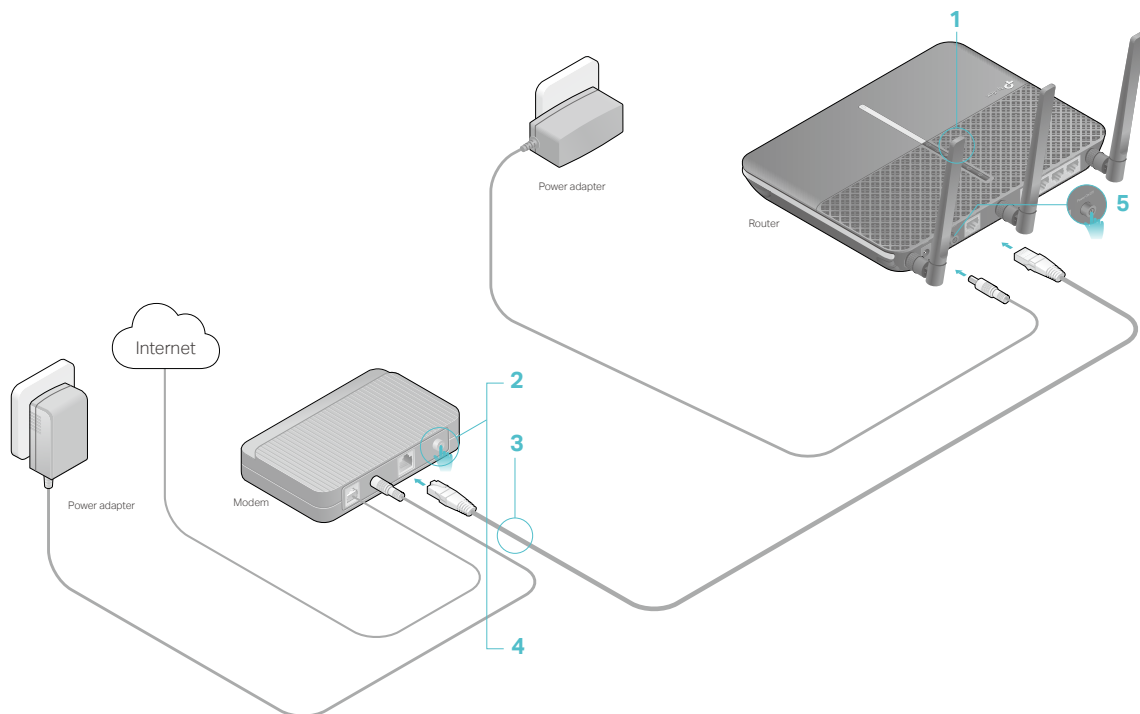
2.1. Position Your Router

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

2.2. Connect Your Router

Follow the steps below to connect your router.

If your internet connection is through an Ethernet cable directly from the wall instead of through a DSL / Cable / Satellite modem, connect the Ethernet cable to the router's Internet port, and then follow Step 1, 5 and 6 to complete the hardware connection.





1. Install the antennas.
2. Turn off the modem, and remove the backup battery if any.
3. Connect the modem to your router's Internet port with an Ethernet cable.

4. Turn on the modem, and then wait about **2 minutes** for it to restart.
5. Connect the power adapter to the router and turn on the router.
6. Verify that the following LEDs are on and solid to confirm the hardware is connected correctly.



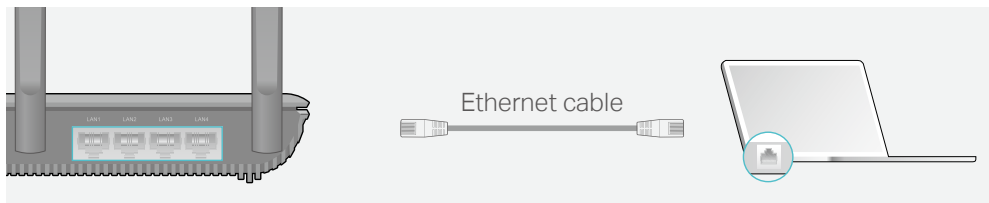
Note:

If the 2.4GHz LED  and 5GHz LED  are off, press and hold the Wi-Fi On/Off button on the side panel for about 2 seconds. Within a few seconds, both the LEDs should turn solid on.

7. Connect your computer to the router.

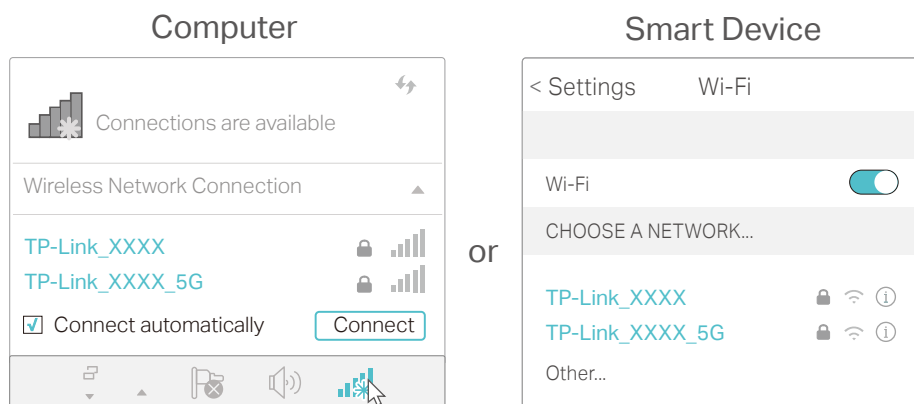
• **Method 1: Wired**

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**

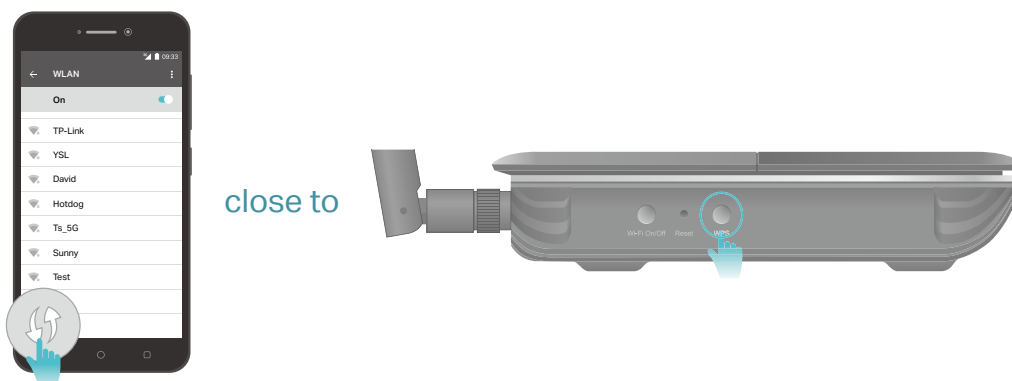
Wireless devices that support WPS, including Android phones, tablets, and most USB network adapters, can be connected to your router through this method.

Note:

- WPS is not supported by iOS devices.
- 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) Tab the WPS icon on the device's screen. Here we take an Android phone for instance.

2) Within two minutes, press the Reset/WPS button on your router.



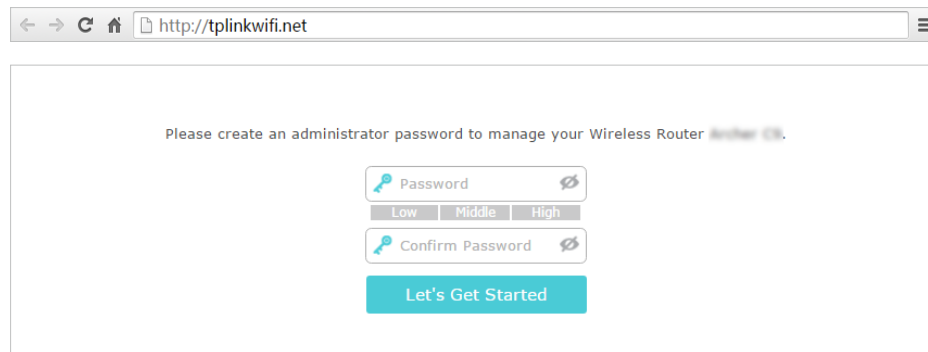
Chapter 3

Log In to Your Router

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

Follow the steps below to log in to your router.

1. Set up the TCP/IP Protocol in [Obtain an IP address automatically](#) mode on your computer.
2. Visit <http://tplinkwifi.net>, and create a login password for secure management purposes. Then click [Let's Get Started](#) to log in.



The screenshot shows a web browser window with the address bar containing <http://tplinkwifi.net>. The main content area displays the instruction: "Please create an administrator password to manage your Wireless Router Router OS." Below this instruction are two password input fields. The first field is labeled "Password" and has a strength indicator below it with three buttons: "Low", "Middle", and "High". The second field is labeled "Confirm Password". Both fields have a toggle icon to the right. At the bottom of the form is a teal button labeled "Let's Get Started".

Note:

- If the login window does not appear, please refer to the [FAQ](#) Section.
- If you have registered a TP-Link ID and bound your cloud router to it, the login password you created here will be invalid. Please log in to the cloud router using your TP-Link ID.

Chapter 4

Set Up Internet Connection

This chapter introduces how to connect your router to the internet. The router is equipped with a web-based Quick Setup wizard. It has necessary ISP information built in, automates many of the steps and verifies that those steps have been successfully completed. Furthermore, you can also set up an IPv6 connection if your ISP provides IPv6 service.

It contains the following sections:

- [Use Quick Setup Wizard](#)
- [Manually Set up Your Internet Connection](#)
- [Set Up an IPv6 Internet Connection](#)

4.1. Use Quick Setup Wizard

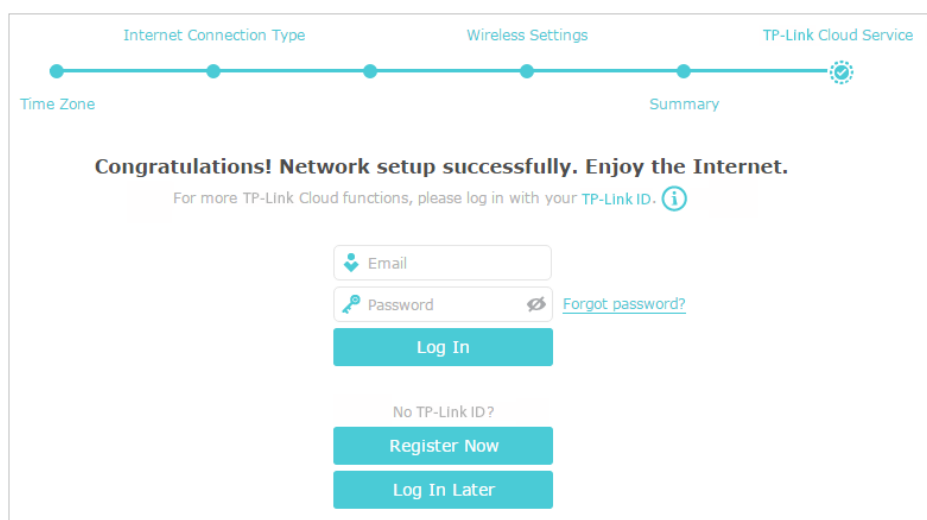
The Quick Setup Wizard will guide you through the process to set up your router.

☞ **Tips:**

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

Follow the steps below to set up your router.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Click **Quick Setup** on the top of the page. Then follow the step-by-step instructions to connect your router to the internet.
3. To enjoy a more complete service from TP-Link (remote management, TP-Link DDNS, etc.), log in with your TP-Link ID or click **Resigter Now** to get one. Then follow the instructions to bind the cloud router to your TP-Link ID.



■ **Note:**

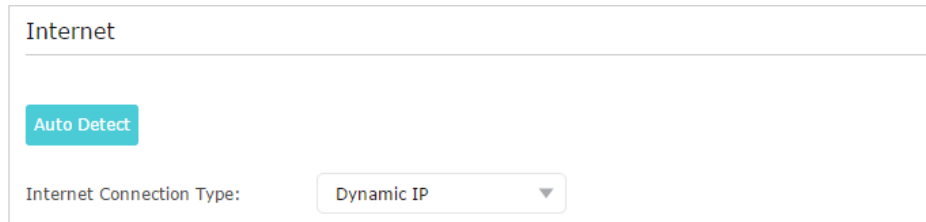
- To learn more about the TP-Link Cloud service, please refer to the [TP-Link Cloud Service](#) section.
- If you do not want to register a TP-Link ID now, you may click [Log In Later](#) to proceed.
- If you have changed the preset wireless network name (SSID) and wireless password during the Quick Setup process, all your wireless devices must use the new SSID and password to connect to the router.

4.2. Manually Set up Your Internet Connection

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

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

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



Internet

Auto Detect

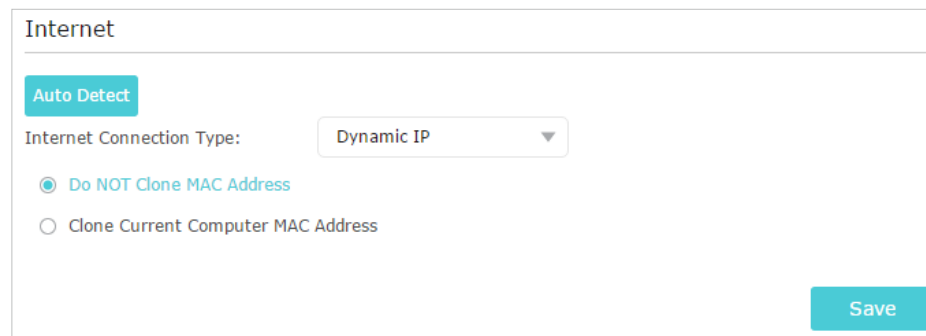
Internet Connection Type: Dynamic IP

Note:

If you are unsure of what your connection type is, click [Auto Detect](#). Since different connection types require different cables and connection information, you can also refer to the demonstrations in Step 4 to determine your connection type.

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

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



Internet

Auto Detect

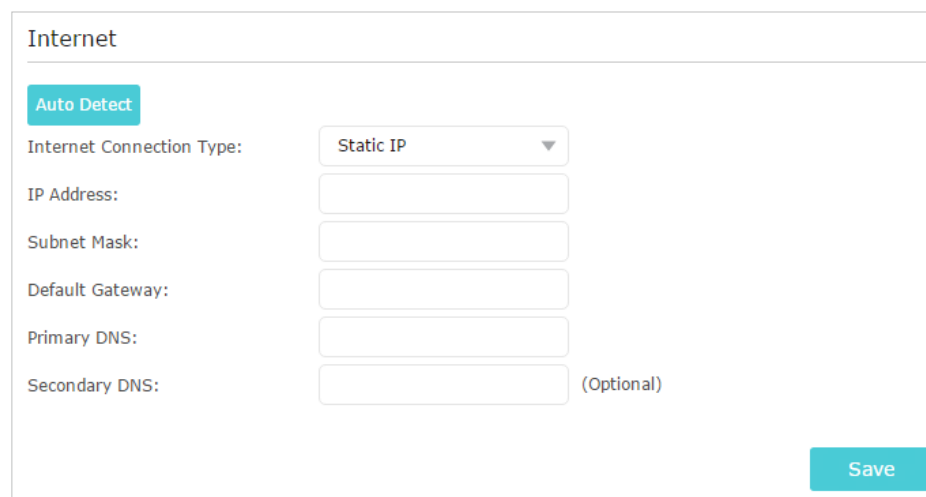
Internet Connection Type: Dynamic IP

Do NOT Clone MAC Address

Clone Current Computer MAC Address

Save

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



Internet

Auto Detect

Internet Connection Type: Static IP

IP Address:

Subnet Mask:

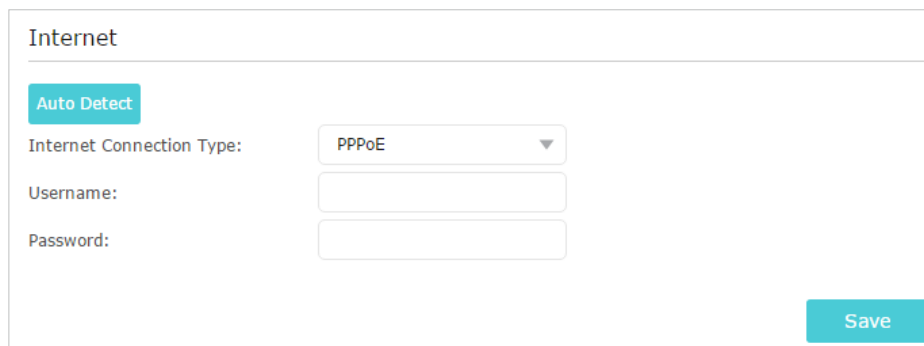
Default Gateway:

Primary DNS:

Secondary DNS: (Optional)

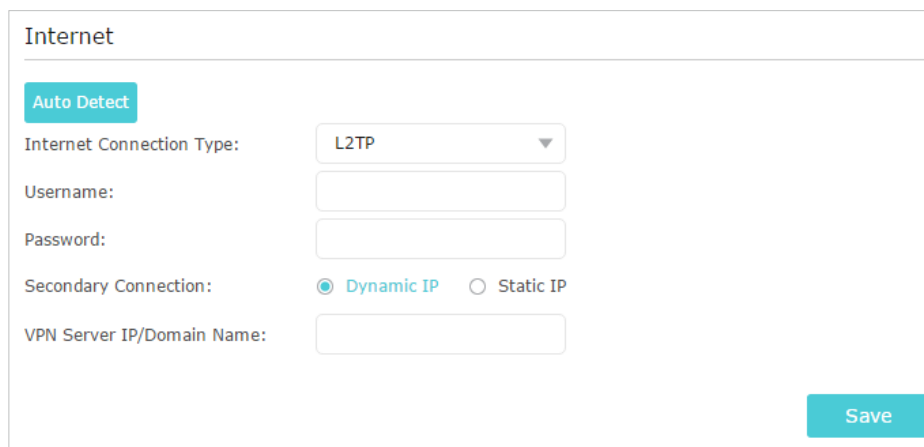
Save

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



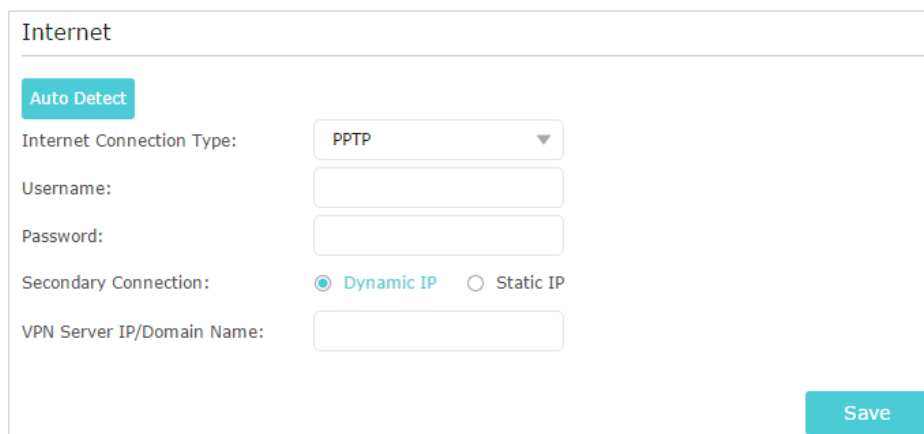
The screenshot shows the 'Internet' configuration page. At the top left is a teal 'Auto Detect' button. Below it, the 'Internet Connection Type' dropdown menu is set to 'PPPoE'. There are two empty text input fields for 'Username:' and 'Password:'. A teal 'Save' button is located at the bottom right of the form.

- 4) If you choose **L2TP**, enter the **username** and **password** and choose the **Secondary Connection** provided by your ISP. Different parameters are needed according to the Secondary Connection you have chosen.



The screenshot shows the 'Internet' configuration page. The 'Internet Connection Type' dropdown menu is set to 'L2TP'. Below the 'Password:' field, there are two radio button options for 'Secondary Connection': 'Dynamic IP' (which is selected) and 'Static IP'. There is an empty text input field for 'VPN Server IP/Domain Name:'. A teal 'Save' button is located at the bottom right of the form.

- 5) If you choose **PPTP**, enter the **username** and **password**, and choose the **Secondary Connection** provided by your ISP. Different parameters are needed according to the Secondary Connection you have chosen.



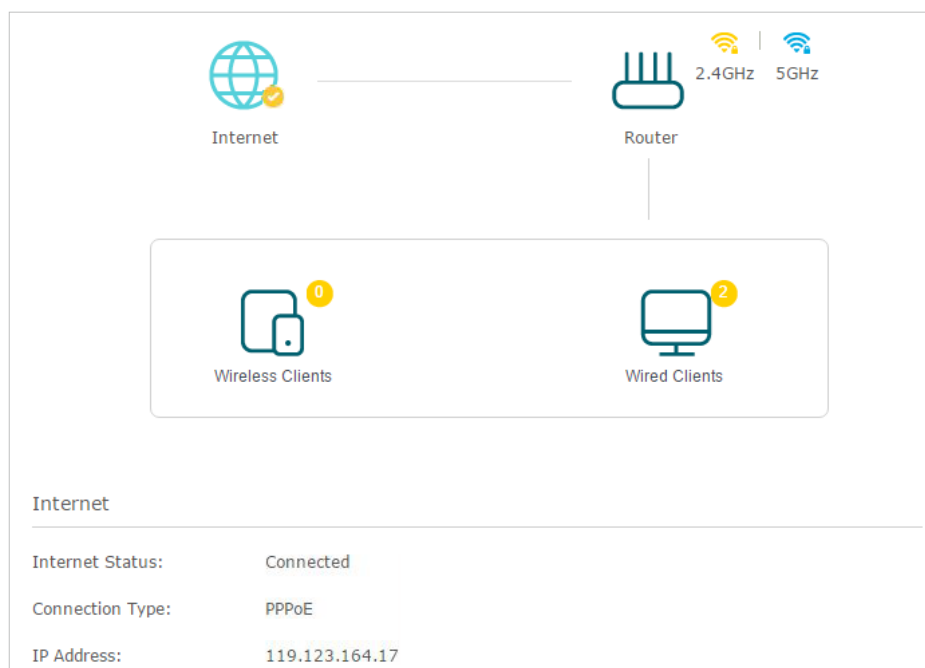
The screenshot shows the 'Internet' configuration page. The 'Internet Connection Type' dropdown menu is set to 'PPTP'. Below the 'Password:' field, there are two radio button options for 'Secondary Connection': 'Dynamic IP' (which is selected) and 'Static IP'. There is an empty text input field for 'VPN Server IP/Domain Name:'. A teal 'Save' button is located at the bottom right of the form.

5. Click **Save**.

6. To check your internet connection, click [Network Map](#) on the left of the page. After the connection succeeds, the screen will display as follows. Here we take PPPoE as an example.

Note:

It may take 1-2 minutes to make the settings valid.



Tips:

- If your internet connection type is [BigPond Cable](#), please go to [Advanced > Network > Internet](#) to set your router.
- If you use [Dynamic IP](#) and [PPPoE](#) and you are provided with any other parameters that are not required on the page, please go to [Advanced > Network > Internet](#) to complete the configuration.
- If you still cannot access the internet, refer to the [FAQ](#) section for further instructions.

4.3. Set Up an IPv6 Internet Connection

Your ISP provides information about one of the following IPv6 internet connection types: PPPoE, Dynamic IP(SLAAC/DHCPv6), Static IP, 6to4 tunnel and Pass-Through (Bridge).

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

Tips:

If you do not know what your internet connection type is, contact your ISP or judge according to the already known information provided by your ISP. Click [?](#) on the management interface to know more about items.

4. Fill in information as required by different connection types. Red blanks must be filled in.

- 1) **Static IP:** Select this type if your ISP uses Static IPv6 address assignment. Fill in blanks and click [Save](#).

The screenshot shows the 'IPv6 Internet' configuration window. At the top, 'Enable IPv6' is checked with a blue toggle switch. Below it, 'Internet Connection Type:' is set to 'Static IP' in a dropdown menu. There are four input fields for IPv6 Address, IPv6 Gateway, IPv6 DNS Server, and Secondary IPv6 DNS Server, each containing '::'. The IPv6 Gateway, IPv6 DNS Server, and Secondary IPv6 DNS Server fields are marked as '(Optional)'. An 'Advanced' section is collapsed, indicated by an upward-pointing arrow. Below it, 'MTU Size(in bytes):' is set to '1500', with a note '(1500 by default, do not change unless necessary)'. A blue 'Save' button is located at the bottom right.

- 2) **Dynamic IP(SLAAC/DHCPv6):** Select this type if your ISP uses Dynamic IPv6 address assignment. Click [Advanced](#) to input further information if your ISP requires. Click [Save](#).

The screenshot shows the 'IPv6 Internet' configuration window. 'Enable IPv6' is checked with a blue toggle switch. 'Internet Connection Type:' is set to 'Dynamic IP' in a dropdown menu. There are two input fields for IPv6 Address and IPv6 Gateway, both containing '::'. An 'Addressing Type:' dropdown menu is set to 'Auto'. An 'Advanced' section is expanded, indicated by a downward-pointing arrow. A blue 'Save' button is located at the bottom right.

- 3) **PPPoE:** Select this type if your ISP uses PPPoEv6, and provides you with a username and password. By default, the router uses the IPv4 account to connect to the IPv6 server. Click [Advanced](#) to input further information if your ISP requires. Click [Save](#).

Note:

If your ISP provides two separate accounts for the IPv4 and IPv6 connections, please uncheck the box for [Use the IPv4 connection's PPPoE session](#) and manually enter the username and password for the IPv6 connection.

The screenshot shows the 'IPv6 Internet' configuration window. At the top, there is a title bar 'IPv6 Internet'. Below it, the 'Enable IPv6' toggle is turned on. The 'Internet Connection Type' dropdown is set to 'PPPoE'. There is a checkbox labeled 'Use the IPv4 connection's PPPoE session' which is currently unchecked. Below this are three input fields: 'Username:', 'Password:', and 'Confirm Password:'. The 'Addressing Type' dropdown is set to 'Auto'. At the bottom left, there is a collapsed 'Advanced' section. A 'Save' button is located at the bottom right.

- 4) **6to4 Tunnel:** An IPv4 internet connection type is a prerequisite for this connection type ([Manually Set up Your Internet Connection](#)). Select this type if your ISP uses 6to4 deployment for assigning address. Click [Save](#).

The screenshot shows the 'IPv6 Internet' configuration window. The 'Enable IPv6' toggle is turned on. The 'Internet Connection Type' dropdown is set to '6to4 Tunnel'. Below this are three input fields: 'IPv4 Address:', 'IPv4 Subnet Mask:', and 'IPv4 Gateway:', all of which are currently set to '0.0.0.0'. A 'Save' button is located at the bottom right.

- 5) **Pass-Through (Bridge):** Select this type if your ISP uses Pass-Through (Bridge) network deployment. No configuration is required for this type of connection. Click [Save](#) and skip to step 6.

The screenshot shows the 'IPv6 Internet' configuration window. The 'Enable IPv6' toggle is turned on. The 'Internet Connection Type' dropdown is set to 'Pass-Through (Bridge)'. A 'Save' button is located at the bottom right.

5. Configure LAN ports. Select the appropriate Address Type and Site Prefix Type according to your ISP. Click [Save](#).

Tips:

Click  on the management interface to know more about items.

IPv6 LAN

Addressing Type: RADVD DHCPv6 Server


Enable RDNSS

Enable ULA Prefix

Site Prefix Type: Delegated Static

[Save](#)

6. Click [Status](#) to check whether you have successfully set up an IPv6 connection. The following figure is an example of a successful PPPoE configuration.

Internet 		IPv4 IPv6
MAC Address:	00-0A-EB-AC-25-01	
IP Address:	2001:c68:202:2111::120/64	
Default Gateway:	fe80::edd0:80d2:7f5e:6be7	
Primary DNS:	2001:c68:202:2111::1	
Secondary DNS:	2001:c68:202:2111::2	
Connection Type:	PPPoE	

 **Tips:**

Visit the [FAQ](#) section if there is no internet connection.

Chapter 5

Set Up the Router as an Access Point

In the Access Point mode, your router connects to a wired or wireless router via an Ethernet cable and extends the wireless coverage of your existing network.


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

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

Switch Mode


Router(Current mode)

In this mode,your router connects to internet directly via Dynamic IP,Static IP,PPPoE,L2TP or PPTP,and shares internet access to multiple wired or wireless devices. NAT and DHCP server are enabled by default.



Access Point

In this mode,your router connects to a wired or wireless router via an Ethernet cable and extends the wireless coverage of your existing network.Functions like NAT,Parental Controls and QoS are not supported in this mode.



Save

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

Summary

Wireless Settings

2.4GHz Wireless: Enable Wireless Radio

Network Name (SSID): Hide SSID

Password:

5GHz Wireless: Enable Wireless Radio

Network Name (SSID): Hide SSID

Password:

Exit **Next**

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

Summary

Wireless Settings

2.4GHz Wireless

Network Name (SSID): TP-LINK_5053

Password: 66378365

5GHz Wireless

Network Name (SSID): TP-LINK_5053_5G

Password: 66378365

Back Save

Tips:

- Functions, such as Parental Controls, Qos and NAT Forwarding, are not supported in the Access Point mode.
- Functions, such as Guest Network, is the same as those in the Router mode.

Chapter 6

TP-Link Cloud Service

TP-Link Cloud service provides a better way to manage your cloud devices. Log in to your router with a TP-Link ID, and you can easily monitor and manage your home network when you are out and about via the Tether app on your smartphone or tablet. To ensure that your router stays new and gets better over time, the TP-Link Cloud will notify you when an important firmware upgrade is available. Surely you can also manage multiple TP-Link Cloud devices with a single TP-Link ID.

This chapter introduces how to register a new TP-Link ID, bind or unbind TP-Link IDs to manage your router, and the Tether app with which you can manage your home network no matter where you may find yourself.

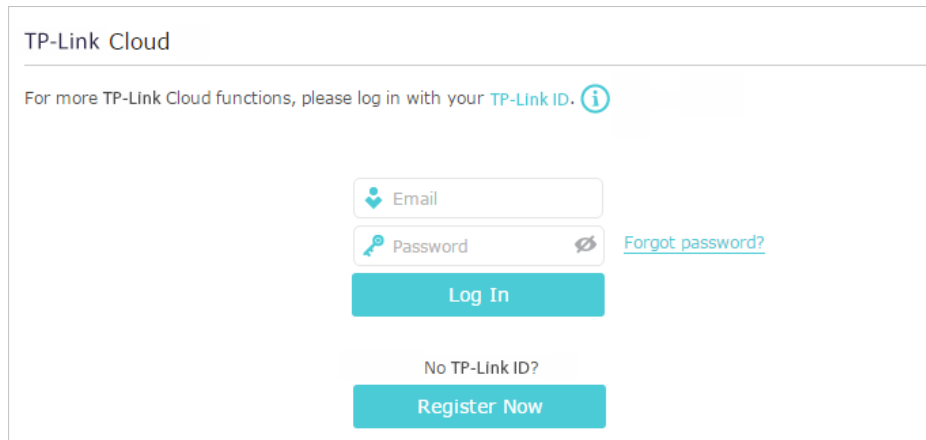
It contains the following sections:

- [Register a TP-Link ID](#)
- [Change Your TP-Link ID Information](#)
- [Manage the User TP-Link IDs](#)
- [Manage the Router via the TP-Link Tether App](#)

6.1. Register a TP-Link ID

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Basic > TP-Link Cloud](#).
3. Click [Register Now](#) and follow the instructions to register a TP-Link ID.



4. After activating your TP-Link ID, come back to the TP-Link Cloud page to log in. The TP-Link ID used to log in to the router for the first time will be automatically bound as an [Admin](#).

■ Note:


- To learn more about the Admin and User TP-Link ID, refer to [Manage the User TP-Link IDs](#).
- Once the router is bound to your TP-Link ID, you need to log in to the router with the TP-Link ID.
- You can register another TP-Link ID via the Tether APP. Please refer to [Manage the Router via TP-Link Tether App](#) to install the app and register a new one
- If you want to unbind the admin TP-Link ID from your router, please go to [Basic > TP-Link Cloud](#), click [Unbind](#) in the [Device Information](#) section.

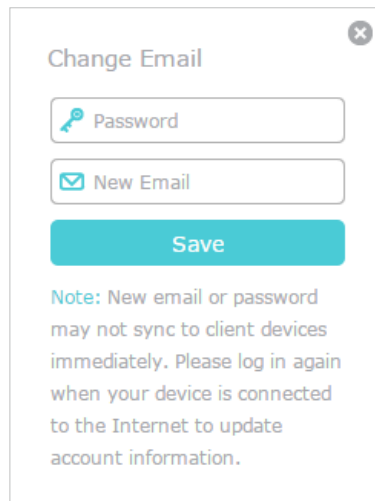
6.2. Change Your TP-Link ID Information

Follow the steps below to change your email address and password of your TP-Link ID as needed.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID.
2. Go to [Basic > TP-Link Cloud](#), and focus on the [Account Information](#) section.

- **To change your email address:**

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



Change Email


Password

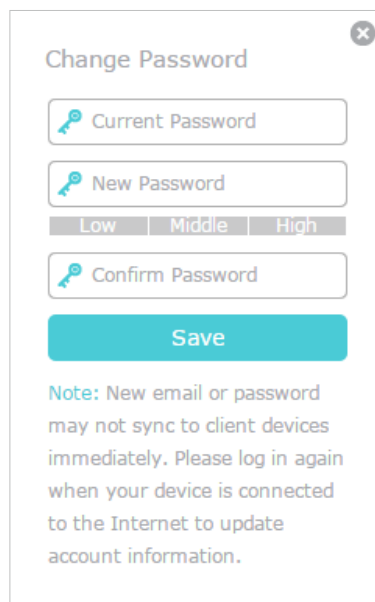
New Email

Save

Note: New email or password may not sync to client devices immediately. Please log in again when your device is connected to the Internet to update account information.

- **To change your password:**

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



Change Password

Current Password

New Password

Low Middle High

Confirm Password

Save

Note: New email or password may not sync to client devices immediately. Please log in again when your device is connected to the Internet to update account information.

6.3. Manage the User TP-Link IDs

The TP-Link ID used to log in to the router for the first time will be automatically bound as the [Admin](#) account. An admin account can add or remove other TP-Link IDs to or from the same router as [Users](#). All accounts can monitor and manage the router locally or remotely, but user accounts cannot:

- Reset the router to its factory default settings either on the web management page or in the Tether app.

- Add/remove other TP-Link IDs to/from the router.

6.3.1. Add TP-Link ID to Manage the Router

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID.
2. Go to **Basic** > **TP-Link Cloud**, and focus on the **Bound Accounts** section.
3. Click **+ Bind**, enter another TP-Link ID as needed and click **Save**.

Note:

If you need another TP-Link ID, please refer to [Manage the Router via TP-Link Tether App](#) to install the app and register a new one.

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

Bound Accounts				
+ Bind - Unbind				
<input type="checkbox"/>	ID	Email	Binding Date	Role
<input type="checkbox"/>	1	*****@****.com	16/11/2016	Admin
<input type="checkbox"/>	2	*****@****.com	16/11/2016	User

6.3.2. Remove TP-Link ID(s) from Managing the Router

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID.
2. Go to **Basic** > **TP-Link Cloud**, and focus on the **Bound Accounts** section.
3. Tick the checkbox(es) of the TP-Link ID(s) you want to remove and click **Unbind**.

Bound Accounts				
+ Bind - Unbind				
<input type="checkbox"/>	ID	Email	Binding Date	Role
<input type="checkbox"/>	1	*****@****.com	16/11/2016	Admin
<input checked="" type="checkbox"/>	2	*****@****.com	16/11/2016	User

6.4. Manage the Router via the TP-Link Tether App

The Tether app runs on iOS and Android devices like smartphones and tablets.

1. Open the Apple App Store or Google Play and search the key word "TP-Link Tether" or simply scan the QR code to download and install the app.



2. Connect your device to the router's wireless network.
3. Launch the Tether app, select the model of your router and log in with your TP-Link ID or the password your set for the router.
4. Manage your router as needed.

Chapter 7

Guest Network

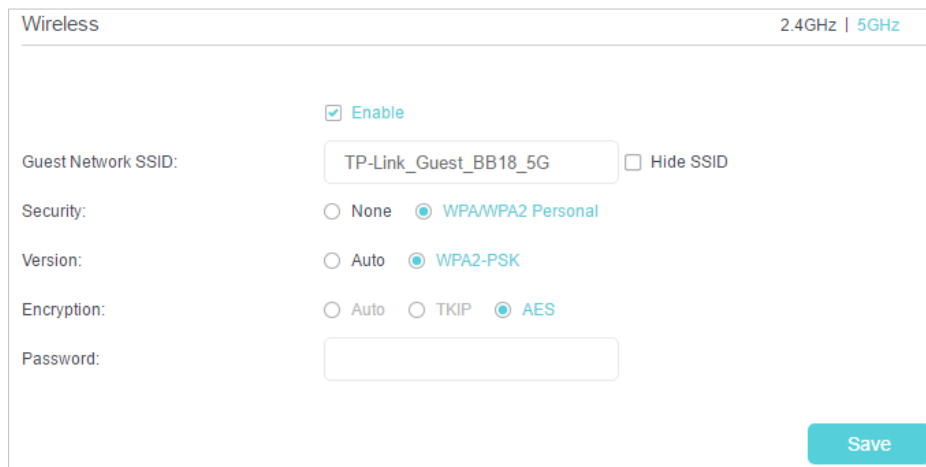
This function allows you to provide Wi-Fi access for guests without disclosing your main network. When you have guests in your house, apartment, or workplace, you can create a guest network for them. In addition, you can customize guest network options to ensure network security and privacy.

It contains the following sections:

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

7.1. Create a Network for Guests

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced** > **Guest Network**. Locate the **Wireless** section.
3. Create a guest network as needed.
 - 1) Tick the checkbox(es) to enable **2.4GHz** or **5GHz** wireless guest 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.



The screenshot shows the 'Wireless' configuration page for a guest network. At the top right, there are tabs for '2.4GHz' and '5GHz'. The 'Enable' checkbox is checked. The 'Guest Network SSID' field contains 'TP-Link_Guest_BB18_5G' and the 'Hide SSID' checkbox is unchecked. Under 'Security', 'WPA/WPA2 Personal' is selected. Under 'Version', 'WPA2-PSK' is selected. Under 'Encryption', 'AES' is selected. A 'Password' field is empty. A 'Save' button is located at the bottom right.

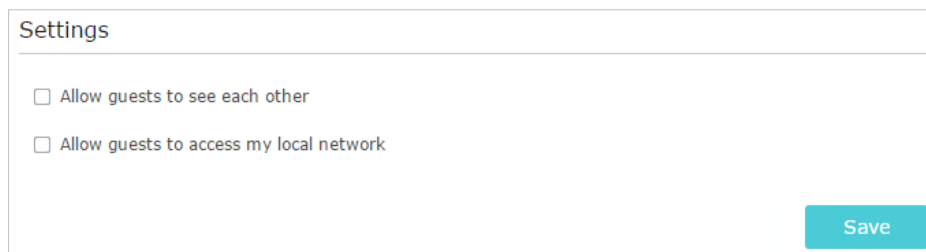
4. Click **Save**. Now your guests can access your guest network using the SSID and password you set!

Tips:

To view guest network information, go to **Advanced** > **Status** and locate the **Guest Network** section.

7.2. Customize Guest Network Options

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced** > **Guest Network**. Locate the **Settings** section.
3. Customize guest network options according to your needs.



Settings

Allow guests to see each other

Allow guests to access my local network

Save

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

Check this box 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](#)

Check this box 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 8

Parental Controls

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

It contains the following sections:

- [Setting Up Access Restrictions](#)
- [Monitoring Internet Usage](#)

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

8.1. Setting Up Access Restrictions

I want to:

Block access to inappropriate online content for my child's devices, restrict internet access to 2 hours every day and block internet access during bed time (10 PM to 7 AM) on weekdays.

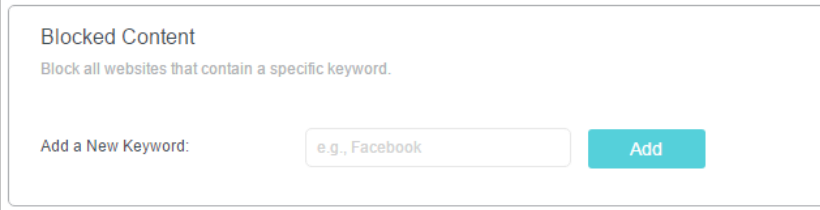
How can I do that?

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

- 1) Enter a **Name** for the profile to make it easier to identify.
- 2) Under **Devices**, click [+](#).
- 3) Select the devices that belong to this family member. Access restrictions will be applied to these devices. Click **Add** when finished.

Note: Only devices that have previously been connected to your router's network are listed here. If you are unable to find the device you want to add, connect it to your network and then try again.

- 4) Click [Next](#).
5. Customize the [Blocked Content](#) according to your needs for this profile.



- 1) Enter a keyword (for example, "Facebook") or a URL (for example, "www.facebook.com"), then click [Add](#). All websites containing the keywords will be blocked.
- 2) Click [Next](#).
6. Set time restrictions on internet access.



- 1) Enable [Time Limits](#) on Monday to Friday and Saturday & Sunday then set the allowed online time to 2 hours each day.
- 2) Enable [Bed Time](#) and use the up/down arrows or enter times in the fields. Devices under this profile will be unable to access the internet during this time period.
- 3) Click [Save](#).

Done!

The amount of time your child spends online is controlled and inappropriate content is blocked on their devices.

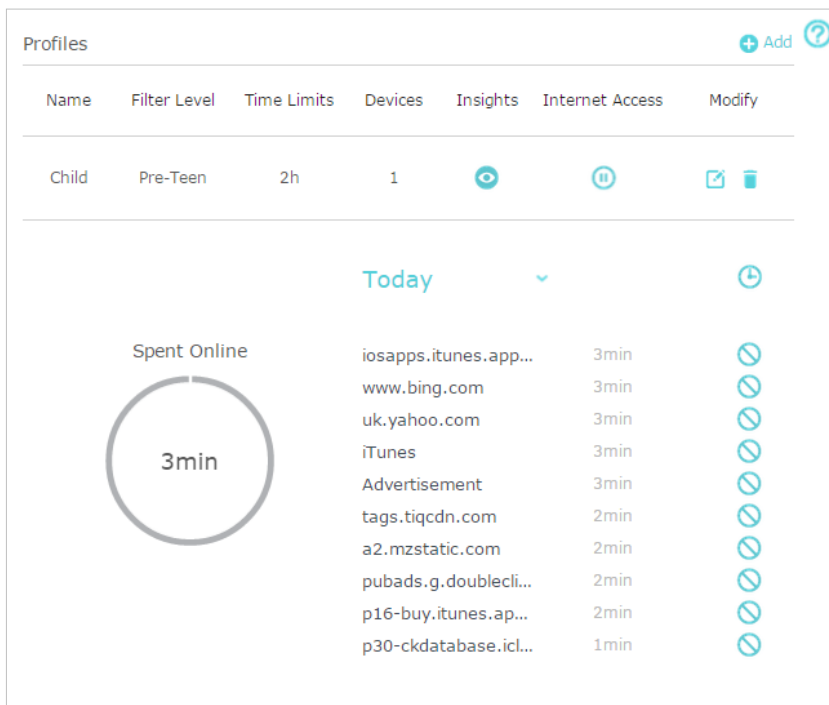
8.2. Monitoring Internet Usage

I want to:

Check which websites my child has visited and how much time they have spent online recently.

How can I do that?

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



3. Find the correct profile and click in the Insights column.

Note: If you have not set up a profile for your child yet, you should do that first by clicking **Add**, then follow the steps to create a profile. Refer to [Scenario 1: Setting Up Access Restrictions](#) for detailed instructions.

4. Use the drop-down menu to view the websites visited and time spent online for any of the last 7 days. Click to view a complete history.

Tip: Click to block the corresponding content for this profile.

Done! You can now check up on your child's online activities.

Chapter 9

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 (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 computer for the next 2 hours.

How can I do that?

1. Enable QoS and set bandwidth allocation.
 - 1) Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
 - 2) Go to [Advanced](#) > [QoS](#) > [Global 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 [Save](#).

Global Settings

QoS Enable QoS

Upload Bandwidth Mbps ▾

Download Bandwidth Mbps ▾

[Save](#)

2. In the [Device Priority](#) section, find your computer and toggle on [Priority](#). Click the entry in the [Timing](#) column and select 2 hours as the duration you want the device to be prioritized for.

Type	Information	Real-time Rate	Traffic Usage	Priority	Timing
	NicoLuo-PC <small>(LAN) 8C:DC:D4:3E:69:CC</small>	↑ 0.06KB/s ↓ 0KB/s	322.8KB	<input checked="" type="checkbox"/>	2 hours ▾ 2 h 0 min Remaining
	Yan <small>(2.4G) 38:CA:DA:3A:D8:B1</small>	↑ 0KB/s ↓ 0KB/s	294.9KB	<input type="checkbox"/>	-

Done! You can now enjoy using your computer for the next 2 hours.

Chapter 10

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.

It contains the following sections:

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

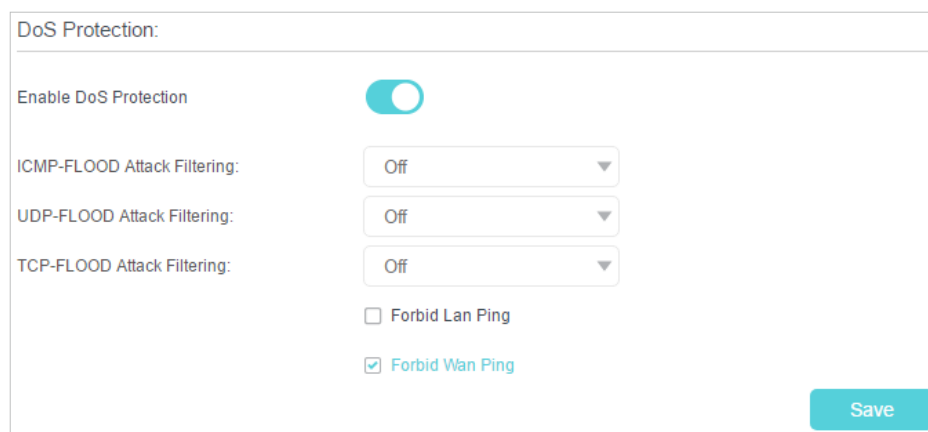
10.1. Protect the Network from Cyber Attacks

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 your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [Security](#) > [Settings](#).



DoS Protection:

Enable DoS Protection

ICMP-FLOOD Attack Filtering:

UDP-FLOOD Attack Filtering:

TCP-FLOOD Attack Filtering:

Forbid Lan Ping

Forbid Wan Ping

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 Settings](#)), and the vicious host will be displayed in the [Blocked DoS Host List](#).

5. If you want to ignore the ping packets from the WAN port, select [Forbid Wan Ping](#); if you want to ignore the ping packets from the LAN port, select [Forbid Lan Ping](#).
6. Click [Save](#).

10.2. Access Control

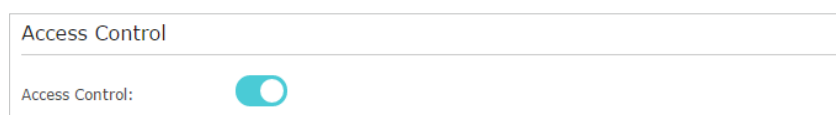
Access Control is used to block or allow specific client devices to access your network (via wired or wireless) based on a list of blocked devices (Blacklist) or a list of allowed devices (Whitelist).

I want to:

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

How can I do that?

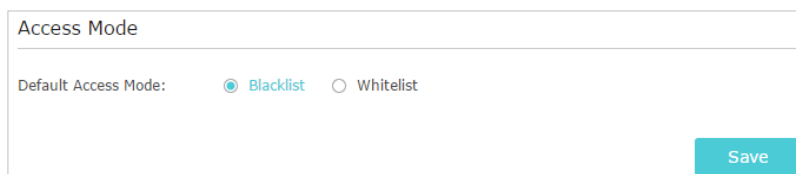
1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [Security](#) > [Access Control](#).
3. Enable [Access Control](#).



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

To block specific device(s):

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



- 2) 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	
--	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: Blacklist [Whitelist](#)

[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
--	--	--	--	--

Device Name:

MAC Address:

[Cancel](#) [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](#).

10.3. IP & MAC Binding

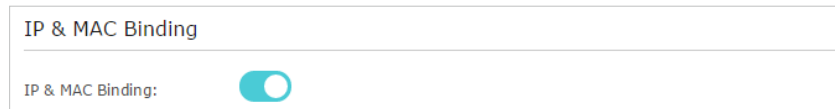
IP & MAC Binding, namely, ARP (Address Resolution Protocol) Binding, is used to bind network device's IP address to its MAC address. This will prevent ARP Spoofing and other ARP attacks by denying network access to a device with matching IP address in the Binding list, but unrecognized MAC address.

I want to:

Prevent ARP spoofing and ARP attacks.

How can I do that?

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



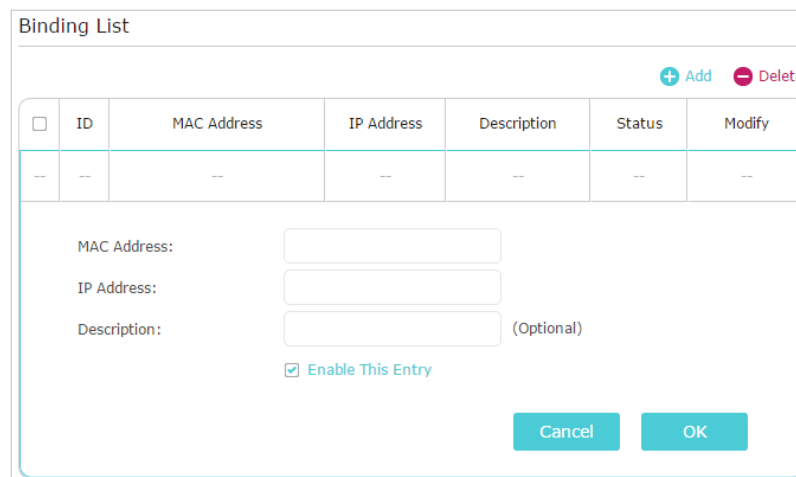
4. Bind your device(s) according to your need.

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.



- 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 11

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.

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](#)

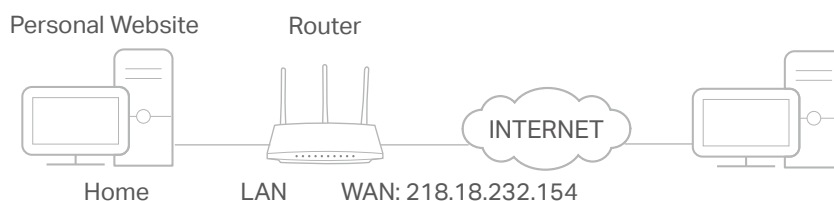
11. 1. Share Local Resources on the Internet by Virtual Servers

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



How can I do that?

1. Assign a static IP address to your PC, for example 192.168.0.100.
2. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
3. Go to [Advanced > NAT Forwarding > 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

<input type="checkbox"/>	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.

11.2. Open Ports Dynamically by Port Triggering

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

Follow the steps below to configure the Port Triggering rules:

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [NAT Forwarding](#) > [Port Triggering](#) and click [Add](#).

3. Click [View 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

<input type="checkbox"/>	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.

11.3. 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.

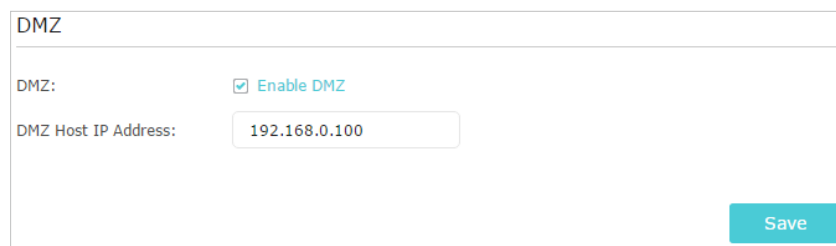
I want to:

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 your TP-Link ID or 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.

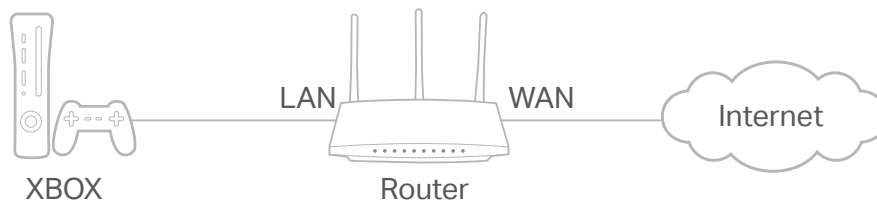
11.4. Make Xbox Online Games Run Smoothly by UPnP

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

☞ **Tips:**

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

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



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

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

UPnP

UPnP:

UPnP Service List

Total Clients: 0 [Refresh](#)

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

Chapter 12

VPN Server

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

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

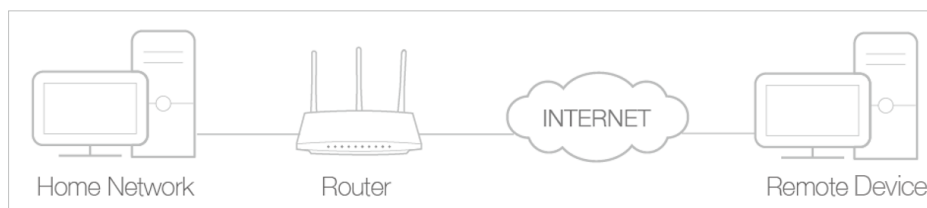
PPTP VPN is more easily used and its speed is faster, it's compatible with most operating systems and also supports mobile devices. Its security is poor and your packets may be cracked easily, and PPTP VPN connection may be prevented by some ISP.

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](#)

12.1. Use OpenVPN to Access Your Home Network

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



- **Step1. Set up OpenVPN Server on Your Router**

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

12.2. Use PPTP VPN to Access Your Home Network

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

- **Step 1. Set up PPTP VPN Server on Your Router**

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

PPTP VPN

Enable VPN Server

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

Username:

Password:

[Save](#)

Note:

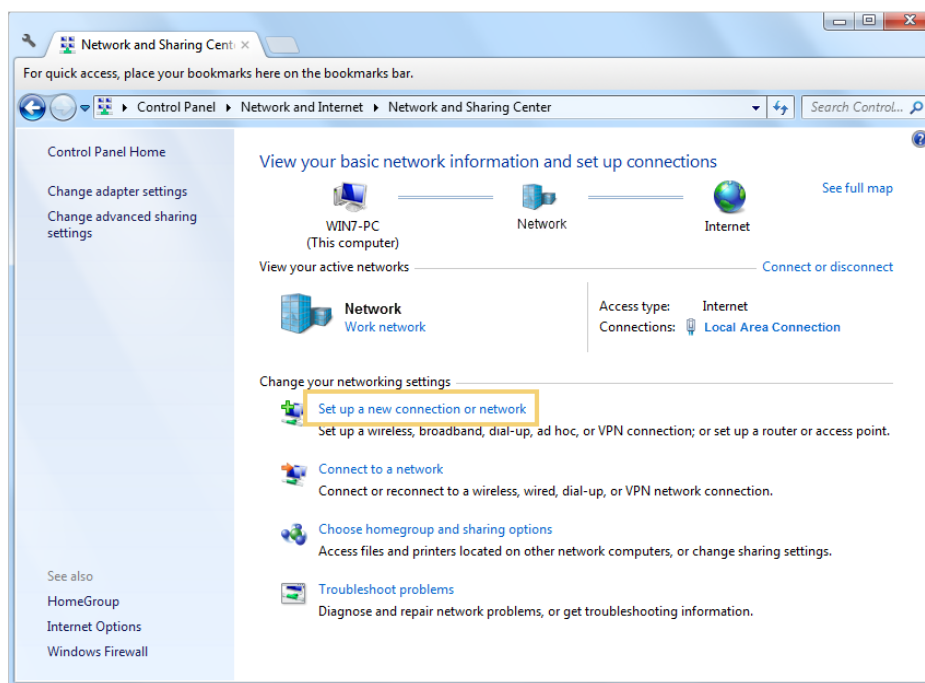
Before you enable [VPN Server](#), we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router's WAN port and synchronize your [System Time](#) with internet.

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. Enter the [Username](#) and [Password](#) to authenticate clients to the PPTP VPN server.
5. Click [Save](#).

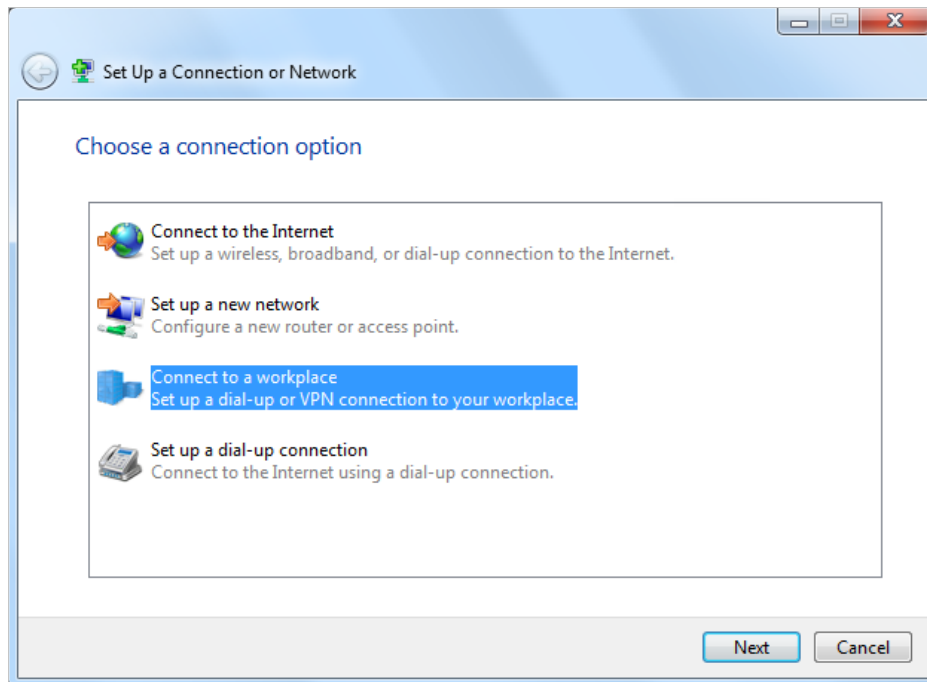
• **Step 2. Configure PPTP VPN Connection on Your Remote Device**

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

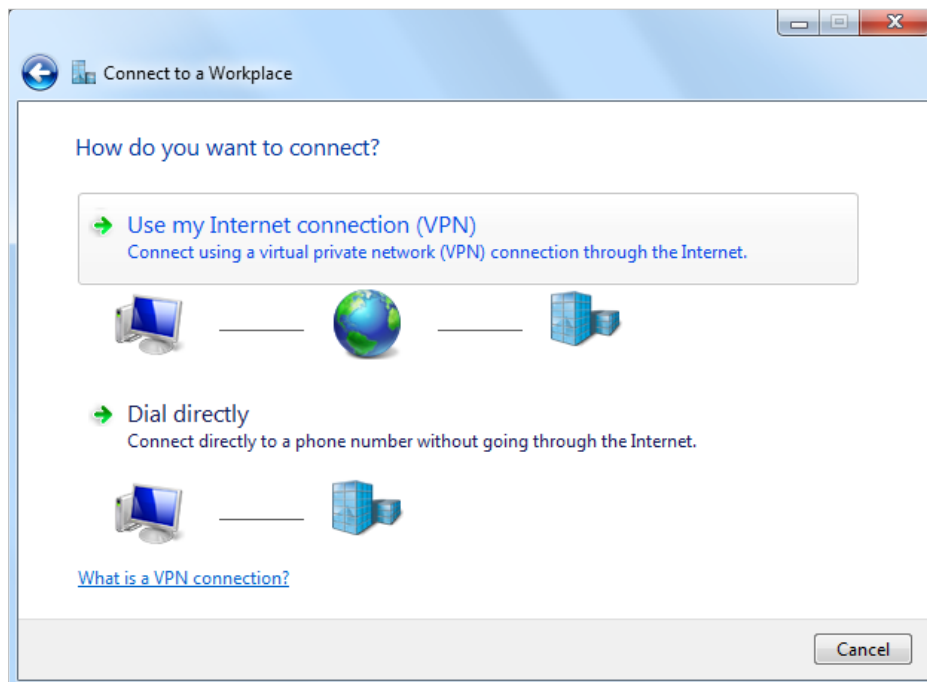
1. Go to [Start](#) > [Control Panel](#) > [Network and Internet](#) > [Network and Sharing Center](#).
2. Select [Set up a new connection or network](#).



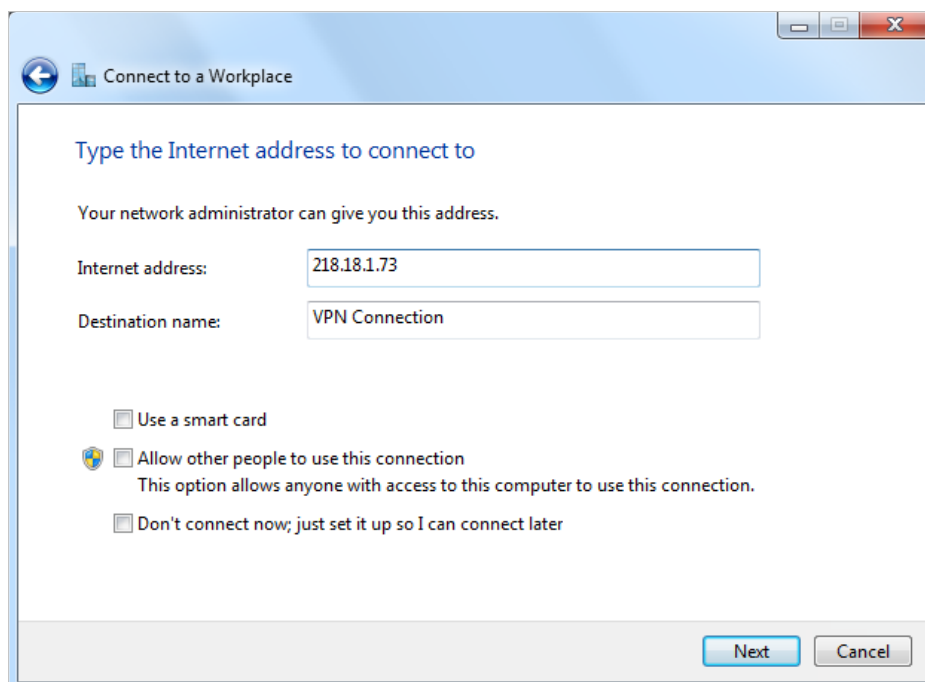
3. Select [Connect to a workplace](#) and click [Next](#).



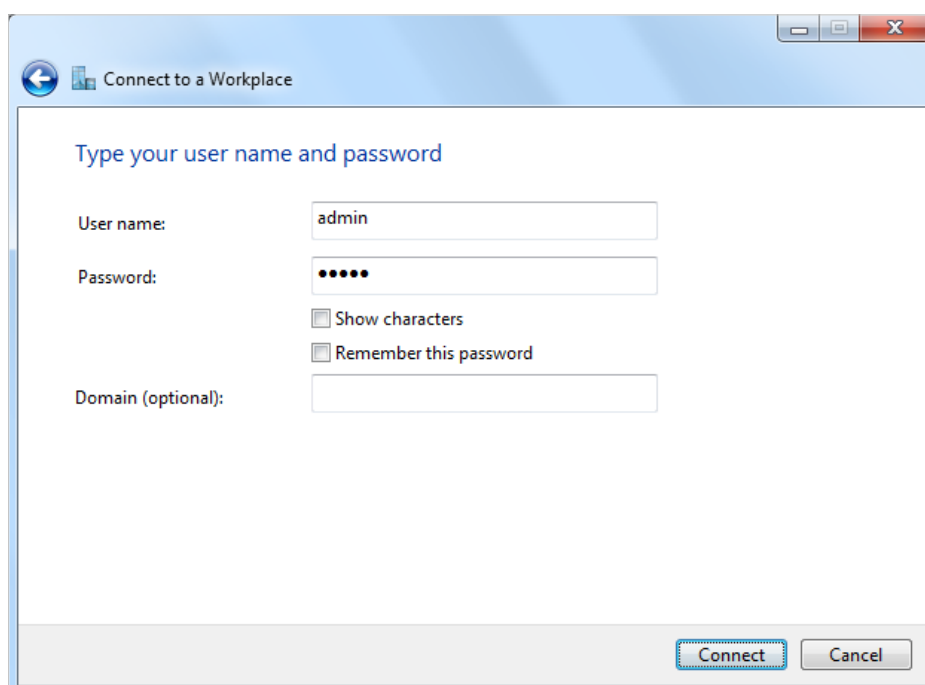
4. Select **Use my Internet connection (VPN)**.



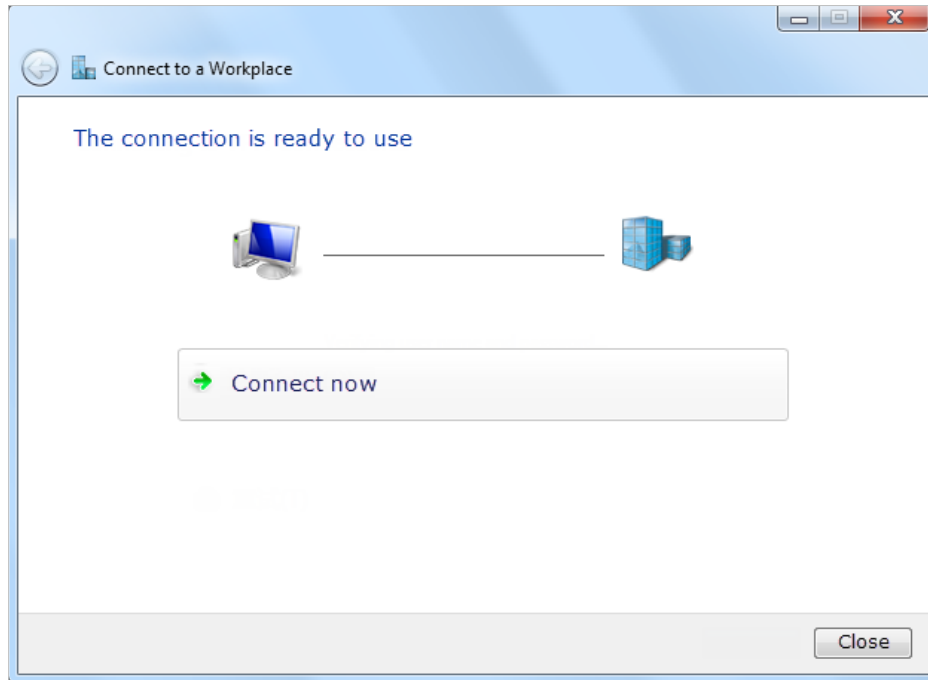
5. Enter the internet IP address of the router (for example: 218.18.1.73) in the **Internet address** field. Click **Next**.



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



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



Chapter 13

Customize Your Network Settings

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

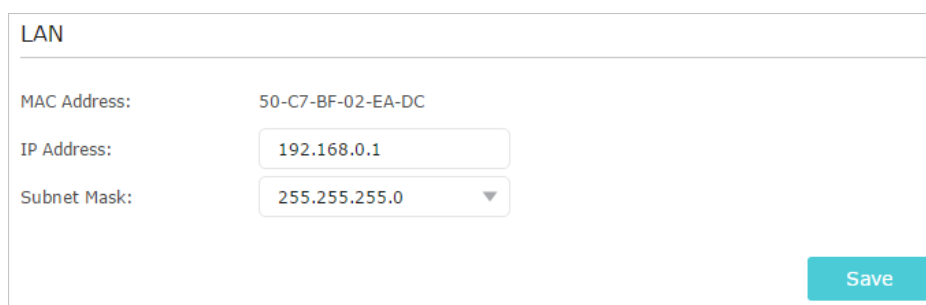
It contains the following sections:

- [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](#)
- [Set Wireless MAC Filtering](#)
- [Schedule Your Wireless Function](#)

13.1. 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 your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [Network](#) > [LAN](#).
3. Type in a new IP Address appropriate to your needs. And leave the [Subnet Mask](#) as the default settings.



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.

13.2. 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 with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [Network](#) > [IPTV/VLAN](#).
3. **If your ISP provides the networking service based on IGMP technology**, e.g., British Telecom(BT) and Talk Talk in UK:
 - 1) IGMP is used to manage multicasting on TCP/IP networks, which is enabled by default. Select the [IGMP Version](#), either V2 or V3, as required by your ISP.

IPTV Settings

IGMP Snooping: Enable

IGMP Proxy: Enable

IGMP Version: V3

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) 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.

IPTV: Enable

Mode: Bridge

LAN1: Singapore-ExStream

LAN2: Malaysia-Unifi

LAN3: Malaysia-Maxis

LAN4: Vietnam-Viettel

LAN4: New Zealand-UFB

Australia-NBN

Portugal-MEO

Save

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.

13.3. Specify DHCP Server Settings

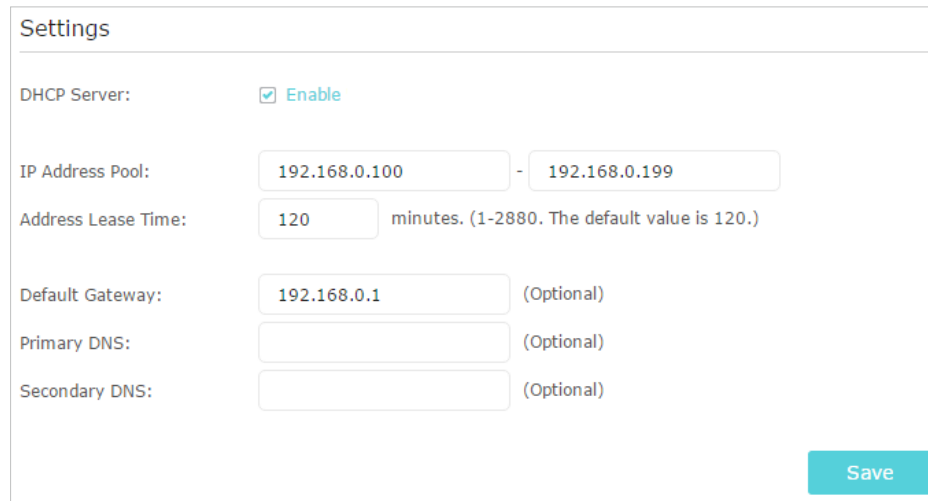
By default, the DHCP (Dynamic Host Configuration Protocol) Server is enabled and the router acts as a DHCP server; it dynamically assigns TCP/IP parameters to client

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 your TP-Link ID or the password you set for the router.

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

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



The screenshot shows the 'Settings' page for the DHCP Server. The 'DHCP Server' checkbox is checked and labeled 'Enable'. The 'IP Address Pool' is set to '192.168.0.100 - 192.168.0.199'. The 'Address Lease Time' is set to '120 minutes. (1-2880. The default value is 120.)'. The 'Default Gateway' is set to '192.168.0.1 (Optional)'. The 'Primary DNS' and 'Secondary DNS' fields are empty and labeled '(Optional)'. A 'Save' button is located at the bottom right.

1. Enable DHCP Server.

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: (a-z, A-Z, 0-9, -, _)

Enable This Entry

2. Click [Scan](#) 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](#).

13.4. 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 your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [Network](#) > [Dynamic DNS](#).
3. Select the DDNS [Service Provider](#) (TP-Link, NO-IP or DynDNS). It is recommended to select TP-Link so that you can enjoy TP-Link's superior DDNS service. Otherwise, please select NO-IP or DynDNS. If you don't have a DDNS account, you have to register first by clicking [Go to register](#).

Dynamic DNS

Service Provider: TP-Link NO-IP DynDNS

Current Domain Name: ---

Domain Name List

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

<input type="checkbox"/>	Domain Name	Registered Date	Status	Operation	Modify
--	--	--	--	--	--

Note:

To enjoy TP-Link's DDNS service, you have to log in with a TP-Link ID. If you have not logged in with one, click [Log in](#).

Dynamic DNS

Service Provider: TP-Link NO-IP DynDNS

DDNS Unavailable

To use our superior TP-LINK DDNS service, please [Log in](#) with your TP-LINK Cloud account, or choose another service provider.

4. Click [Register](#) in the [Domain Name List](#) if you have chosen TP-Link, and enter the [Domain Name](#) as needed.

Dynamic DNS

Service Provider: TP-Link NO-IP DynDNS

Current Domain Name: ---

Domain Name List

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

<input type="checkbox"/>	Domain Name	Registered Date	Status	Operation	Modify
--	--	--	--	--	--

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

Dynamic DNS

Service Provider: TP-Link NO-IP DynDNS [Go to register...](#)

Username:

Password:

Domain Name:

Update Interval:

WAN IP binding: Disable Enable

✘ Not launching

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

Tips:

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

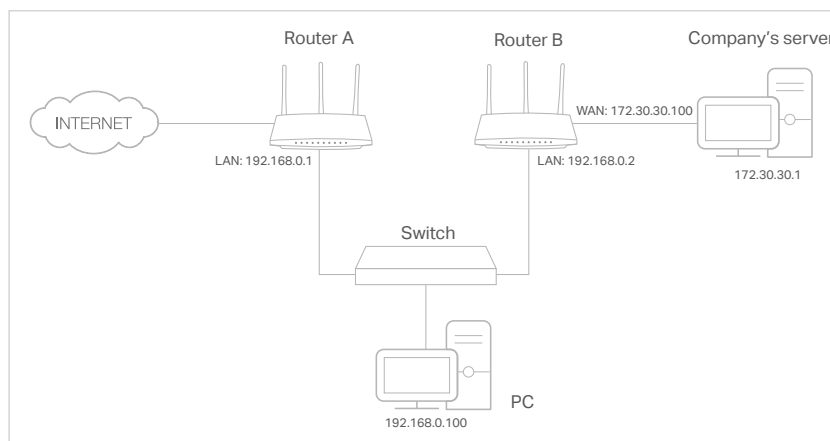
13.5. Create Static Routes

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 your TP-Link ID or the password you set for Router A.
3. Go to [Network](#) > [Advanced Routing](#).
4. Click [Add](#) and finish the settings according to the following explanations:

Static Routing

+ Add - Delete

<input type="checkbox"/>	ID	Network Destination	Subnet Mask	Default Gateway	Interface	Description	Status	Modify
<input type="checkbox"/>	--	--	--	--	--	--	--	--

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: 1				Refresh
ID	Network Destination	Subnet Mask	Gateway	Interface
1	192.168.0.0	255.255.255.0	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.

13.6. 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 your TP-Link ID or the password you set for the router.

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

1. Go to [Advanced](#) > [Wireless](#) > [Wireless Settings](#).
2. The wireless radio is enabled by default. If you want to disable the wireless function of the router, just uncheck the box for [Enable Wireless Radio](#). In this case, all the wireless settings will be invalid.

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

1. Go to [Basic](#) > [Wireless](#).
2. Create a new SSID in [Wireless Network Name \(SSID\)](#) and customize the password for the network in [Password](#). The value is case-sensitive.

Note:

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

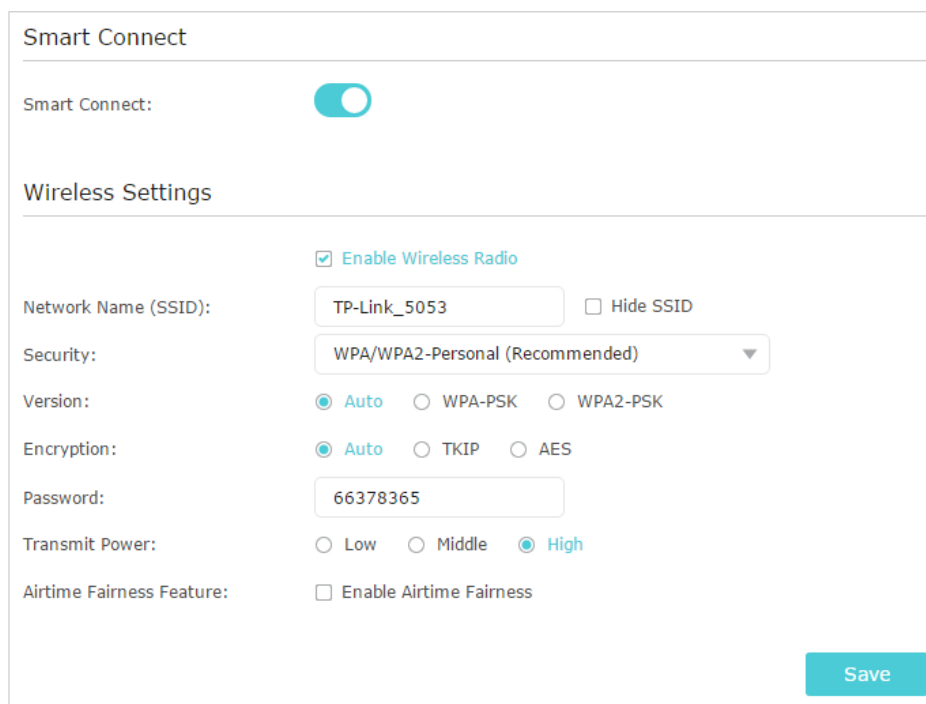
- **To hide SSID:**

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

- **To use the smart connect function**

The smart connect function helps devices run faster by assigning them to best wireless bands based on actual conditions to balance network demands.

1. Go to [Advanced](#) > [Wireless](#) > [Wireless Settings](#).
2. Enable [Smart Connect](#) and click [Save](#).
3. Keep the default or set a new SSID and password, and click [Save](#). This SSID and password will be applied both for 2.4GHz and 5GHz wireless networks.



The screenshot shows a web interface for configuring network settings. At the top, there is a section titled "Smart Connect" with a toggle switch that is turned on. Below this is the "Wireless Settings" section. It includes a checkbox for "Enable Wireless Radio" which is checked. The "Network Name (SSID)" field contains "TP-Link_5053" and there is a "Hide SSID" checkbox. The "Security" dropdown menu is set to "WPA/WPA2-Personal (Recommended)". The "Version" section has three radio buttons: "Auto" (selected), "WPA-PSK", and "WPA2-PSK". The "Encryption" section has three radio buttons: "Auto" (selected), "TKIP", and "AES". The "Password" field contains "66378365". The "Transmit Power" section has three radio buttons: "Low", "Middle", and "High" (selected). The "Airtime Fairness Feature" section has a checkbox for "Enable Airtime Fairness" which is unchecked. A "Save" button is located at the bottom right of the form.

- **To change the security option:**

1. Go to [Advanced](#) > [Wireless](#) > [Wireless Settings](#).
2. Select the wireless network [2.4GHz](#) or [5GHz](#).
3. Select an option from the [Security](#) drop-down list. 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.
- [Transmit Power](#) - Select either [High](#), [Middle](#) or [Low](#) to specify the data transmit power. The default and recommended setting is [High](#).

- **To enable the Airtime Fairness feature**

The Airtime Fairness feature can improve the overall network performance by sacrificing a little bit of network time on your slow devices. Enable Airtime Fairness when you wish to sacrifice some of the networking time from the slow devices, so that your faster devices can achieve better quality of service.

For example, you have a gaming computer next to the router in the living room, and a slower family computer upstairs. Enable the airtime fairness feature so that your gaming computer can perform as optimally as possible.

1. Go to [System Tools > System Parameters > Wireless Advanced](#).
2. Tick the [Enable Airtime Fairness](#) checkbox.
3. Click [Save](#).

13.7. Use WPS for Wireless Connection

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

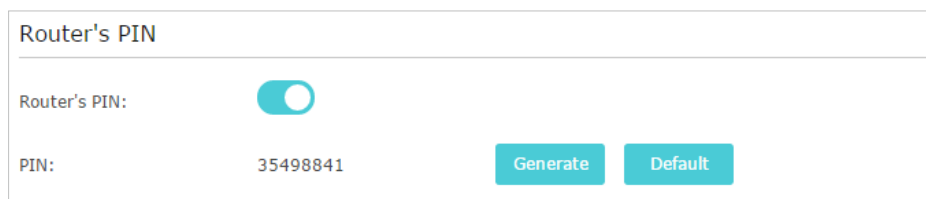
13.7.1. Method 1: Use the WPS Button

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

1. Press the WPS button of the router for 1 second.
2. Press the WPS button of the client device directly.
3. The WPS LED flashes for about 2 minutes during the WPS process.
4. When the WPS LED is on, the client device has successfully connected to the router.

13.7.2. Set the Router's PIN

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.



Router's PIN

Router's PIN:

PIN: 35498841 [Generate](#) [Default](#)

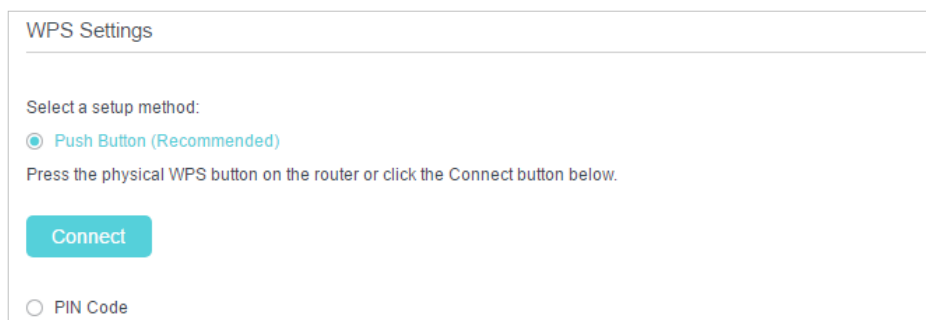
Note:

- 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.

13. 7. 3. Use the WPS Wizard for Wi-Fi Connections

1. Select a setup method:

- **Push Button(Recommended):** Click [Connect](#) on the screen. Within two minutes, press the WPS button on the client device.
- **PIN:** Enter the client's PIN, and click [Connect](#).



WPS Settings

Select a setup method:

Push Button (Recommended)

Press the physical WPS button on the router or click the Connect button below.

[Connect](#)

PIN Code

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.

13. 8. Set Wireless MAC Filtering

Wireless MAC Filtering is used to deny or allow specific wireless client devices to access your network by their MAC addresses.

I want to:

Deny or allow specific wireless client devices to access my network by their MAC addresses.

[For example](#), you want the wireless client A with the MAC address 00-0A-EB-B0-00-0B and the wireless client B with the MAC address 00-0A-EB-00-07-5F to access the router, but other wireless clients cannot access the router.

How can I do that?

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Wireless > Wireless MAC Filtering](#).
3. Click [Enable](#) to enable the Wireless MAC Filtering function.
4. Select [Allow wireless access only from the devices in the list below](#). as the filtering rule.
5. Delete all or disable all entries if there are any entries already.
6. Click [Add](#) in [Devices in Whitelist](#) section and fill in the blank.

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

MAC Address:

Description:

Enable this Entry

- 1) Enter the MAC address 00:0A:EB:B0:00:0B or 00:0A:EB:00:07-5F in the MAC Address field.
 - 2) Enter wireless client A/B in the Description field.
 - 3) Keep **Enable this Entry** selected.
 - 4) Click **OK**.
7. The configured filtering rules should be listed as the picture shows below.

<input type="checkbox"/>	ID	MAC Address	Description	Enable	Modify
<input type="checkbox"/>	1	00:0A:EB:B0:00:0B	Client A		
<input type="checkbox"/>	2	00:0A:EB:00:07:5F	Client B		

Done! Now only client A and client B can access your network.

13.9. Schedule Your Wireless Function

This feature allows you to turn off the wireless networks at a specific time automatically when you do not need the wireless connection.

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

Task Schedule
2.4GHz | 5GHz

Drag the mouse over the schedule table to select the period during which you need your wireless off automatically.
The Wireless Time Schedule is based on the time of the router. The time can be set in "System Tools > Time Settings" page.

Wireless Schedule:

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
0:00							
1:00							
2:00							
3:00							
4:00							
5:00							
6:00							
7:00							
8:00							
9:00							
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							

Effective Time

Restore
Save

4. Drag the mouse over the schedule table to select the period during which you need your wireless off automatically.

5. Click **Save**.

Note:

- The Effective Time Schedule is based on the time of the Router. Make sure that the time of the router is correct before applying this function. For details, refer to [Set Up System Time](#).
- The wireless LEDs (2.4GHz and 5GHz) will be off if the wireless schedule takes effect.
- The wireless network(s) will be automatically turned on after the time period you have set.

Chapter 14

Manage the Router

This chapter will show you the configuration for managing and maintaining your router.

It contains the following sections:

- [Set Up System Time](#)
- [Test the Network Connectivity](#)
- [Upgrade the Firmware](#)
- [Backup and Restore Configuration Settings](#)
- [Set the Router to Reboot Regularly](#)
- [Change the Administrator Account](#)
- [Local Management](#)
- [Remote Management](#)
- [System Log](#)
- [Monitor the Internet Traffic Statistics](#)
- [System Parameters](#)

14. 1. 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. You can choose the way to obtain the system time as needed.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [System Tools](#) > [Time Settings](#).

- **To get time from the Internet:**

1. Click [Get from GMT](#).

The screenshot shows the 'Time Settings' page. It features a 'Time Zone' dropdown menu currently set to '(GMT-08:00) Pacific Time'. Below it is a 'Date' field showing '10/26/2018' with '(MM/DD/YY)' as a placeholder. The 'Time' field is split into three dropdown menus for hours (19), minutes (51), and seconds (18). There are two 'NTP Server' fields: 'NTP Server I' with 'us.pool.ntp.org' and 'NTP Server II' with 'north-america.pool.ntp.org', both marked as '(optional)'. At the bottom, there are three buttons: 'Get from PC', 'Get GMT', and 'Save'.

2. Select your local [Time Zone](#) from the drop-down list.
3. (Optional) Enter the IP address of the NTP Server I or NTP Server II, and the router will get the time from the NTP Server automatically. In addition, the router has some common built-in NTP Servers that will synchronize automatically once it connects to the internet.
4. Click [Save](#).

- **To get time from PC**

1. Click [Get from PC](#).
2. The current system time and date of your PC will display on the interface.
3. Click [Save](#).

🔗 Tips: Make sure the time on your PC is correct if you want to get the PC's system time.

- **To manually set the time:**

1. Set the current [Date](#) (In [MM/DD/YYYY](#) format).
2. Set the current [Time](#) (In [HH/MM/SS](#) format).
3. Click [Save](#).

- **To set up Daylight Saving Time:**

1. Select [Enable Daylight Saving Time](#).

Daylight Saving Time

Daylight Saving Time: [Enable Daylight Saving Time](#)

Start: 2019 [Mar](#) [M](#) [2nd](#) [W](#) [Sun](#) [T](#) [02:00](#)

End: 2019 [Nov](#) [M](#) [1st](#) [W](#) [Sun](#) [T](#) [02:00](#)

[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](#).

14.2. Test the Network Connectivity

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

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [System 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
```

14. 3. 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.

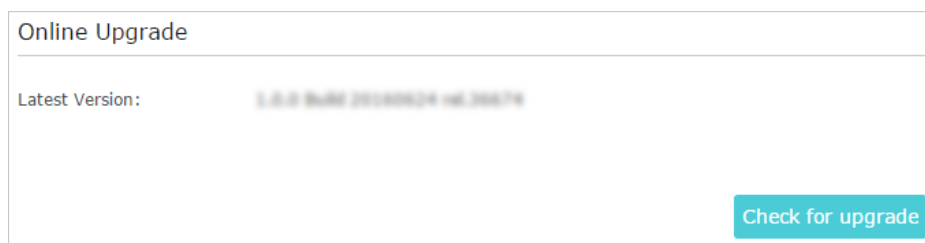
Note:

- Backup your router configuration before firmware upgrade.
- Do NOT turn off the router during the firmware upgrade.

14. 3. 1. Online Upgrade

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. When the latest firmware is available for your router, the update icon  will display in the top-right corner of the page. Click the icon to go to the [Firmware Upgrade](#) page.

Alternatively, you can go to [Advanced](#) > [System Tools](#) > [Firmware Upgrade](#), and click [Check for upgrade](#) to see whether the latest firmware is released.



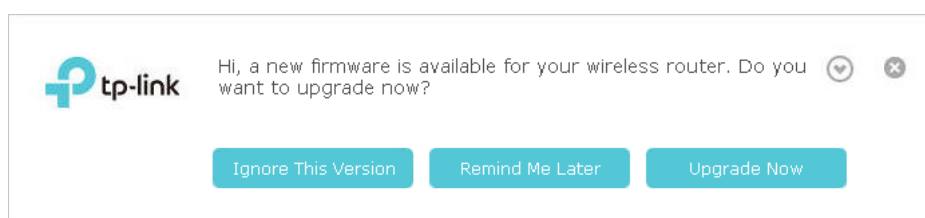
3. Focus on the [Online Upgrade](#) section, and click [Upgrade](#).



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

 **Tips:**

If there's a new and important firmware update for your router, you will see the notification (similar as shown below) on your computer as long as a web browser is opened. Click [Upgrade now](#), and log into the web management page with the username and password you set for the router. You will see the [Firmware Upgrade](#) page.



14.3.2. Local Upgrade

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

Local Upgrade

New Firmware File:

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

14. 3. 3. Restore Interrupted Upgrade after Power Failure

If your router cannot start up after an upgrade interruption due to power failure, follow the steps below to restore the interrupted upgrade. Otherwise, your router cannot work again.

1. Make sure you have the latest firmware file in your computer. If not, try another way to connect your computer to the Internet and download the latest firmware file from www.tp-link.com.
2. Connect your computer to the router with an Ethernet cable.
3. Visit 192.168.0.1 and you will see the following upgrade page.

System error. The router cannot start up normally.
Please upgrade your router. You can download the firmware file from www.tp-link.com.

New Firmware File:

4. Click [Browse](#) and select the downloaded firmware file.
5. Click [Upgrade](#) and wait for a few minutes until the router completes the upgrading and restarts.

14. 4. Backup and Restore Configuration Settings

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

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

- **To backup configuration settings:**

Click [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.

Backup

Save a copy of your current settings.

Backup

- **To restore configuration settings:**

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

Restore

Restore saved settings from a file.

File: Browse

Restore

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

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

- **To reset the router except your login password and bound TP-Link ID:**

1. Click [Restore](#) under the [Factory Default Restore](#) session.

Factory Default Restore

Restore all configuration settings to default values, except your login and cloud account information.

Restore

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

Note:

- During the resetting process, do not turn off the router.
- After reset, you can still use the current login password or the TP-Link ID to log in to the web management page.

- **To reset the router to factory default settings:**

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

Factory Default Restore

Revert all the configuration settings to their default values.

Factory Restore

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.

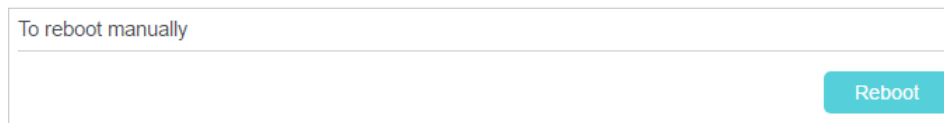
14.5. Set the Router to Reboot Regularly

The Scheduled Reboot feature cleans the cache to enhance the running performance of the router. You can reboot the router manually or set it to reboot regularly.

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

- **To reboot manually**

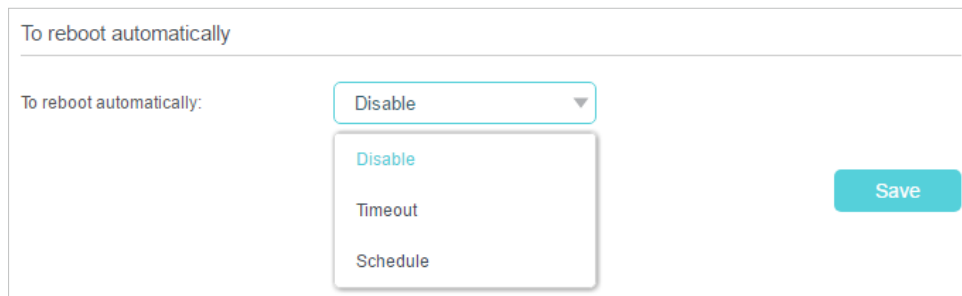
Click [Reboot](#) and wait a few minutes for the router to restart.



The screenshot shows a web interface titled "To reboot manually". It features a large, empty rectangular area for a message or confirmation. On the right side of this area, there is a teal button labeled "Reboot".

- **To reboot regularly**

1. Select [Timeout](#) to reboot the router when time is out or select [Schedule](#) to set when and how often the router reboots regularly.



The screenshot shows a web interface titled "To reboot automatically". Below the title, there is a label "To reboot automatically:" followed by a dropdown menu. The dropdown menu is currently set to "Disable" and is open, showing three options: "Disable", "Timeout", and "Schedule". To the right of the dropdown menu, there is a teal button labeled "Save".

2. Click [Save](#).

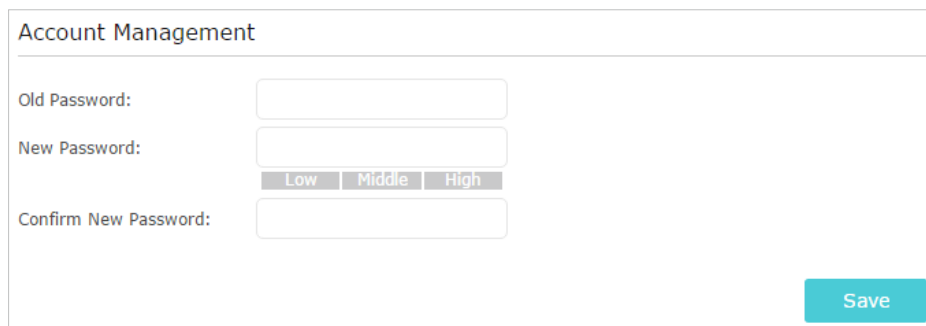
14.6. Change the Administrator Account

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

Note:

If you are using a TP-Link ID to log in to the web management page, the account management feature will be disabled. To manage the TP-Link ID, go to [Basic](#) > [TP-Link Cloud](#).

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



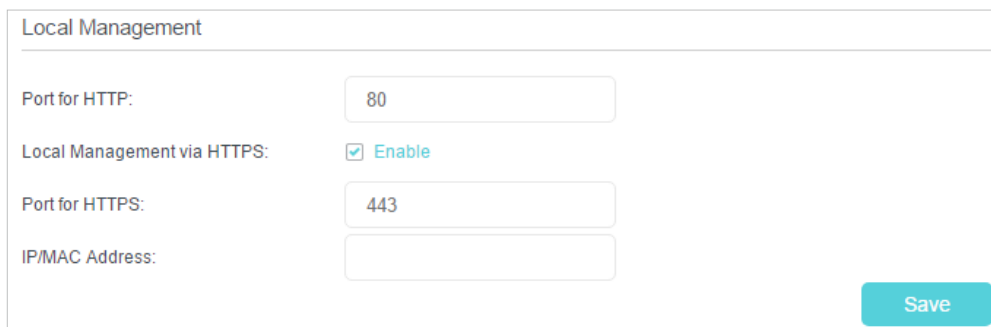
The screenshot shows the 'Account Management' section of a router's web interface. It contains three input fields: 'Old Password', 'New Password', and 'Confirm New Password'. The 'New Password' field has a strength indicator below it with three segments labeled 'Low', 'Middle', and 'High'. A 'Save' button 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.

14.7. Local Management

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

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



The screenshot shows the 'Local Management' section of a router's web interface. It contains four input fields: 'Port for HTTP' (set to 80), 'Local Management via HTTPS' (checked 'Enable'), 'Port for HTTPS' (set to 443), and 'IP/MAC Address'. A 'Save' button is located at the bottom right of the form.

3. Enable [Local Management via HTTPS](#) as needed.
4. Keep the [Port](#) as the default setting. Enter a valid local IP address or MAC address of the device to be allowed to access the router.
5. Click [Save](#) to make the settings effective. Now only the device using the IP address or MAC address you set can manage the router.

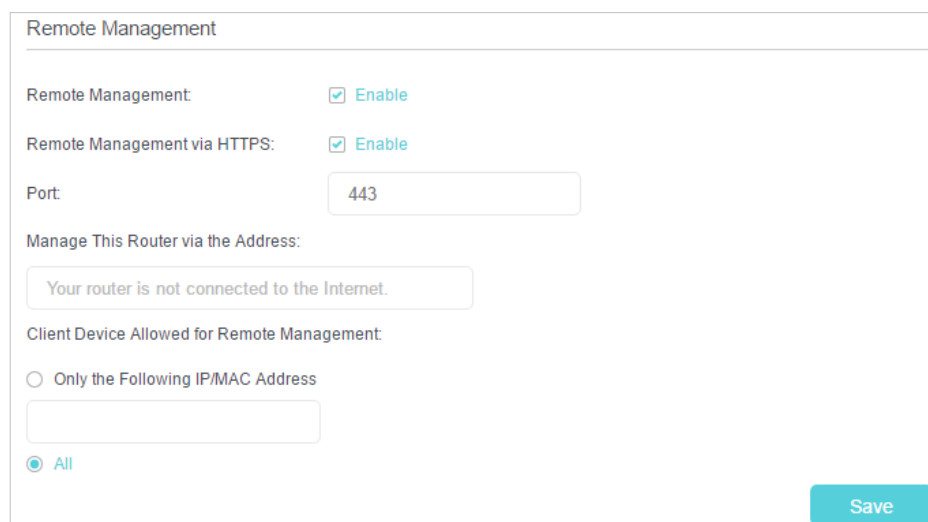
Note:

1. The IP address of the local device must be in the same subnet as the router's LAN IP address.
2. If you want that all local devices can manage the router, just leave the [IP/MAC Address](#) field blank.

14.8. Remote Management

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

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [System Tools](#) > [Administration](#) and enable [Remote Management](#).



The screenshot shows the 'Remote Management' configuration page. It includes the following elements:

- Remote Management:** A checkbox labeled 'Enable' which is checked.
- Remote Management via HTTPS:** A checkbox labeled 'Enable' which is checked.
- Port:** A text input field containing the number '443'.
- Manage This Router via the Address:** A text input field containing the message 'Your router is not connected to the Internet.'
- Client Device Allowed for Remote Management:** Two radio button options: 'Only the Following IP/MAC Address' (unchecked) and 'All' (checked).
- Save:** A teal button labeled 'Save' located at the bottom right of the form.

3. Enable [Remote Management via HTTPS](#) as needed.
4. Enter the port number to be used to access the router with greater security between 1024 and 65535. The default port number for HTTP is 80 and 443 for HTTPS.
5. If you want a specific device to be allowed to access the router remotely, select [Only the Following IP/MAC Address](#) and enter a valid local IP address or MAC address of the device. If you want all devices to be allowed to access the router remotely, select [All](#).
6. Click [Save](#) and now you can remotely access and manage the router via the displayed address.

14.9. 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 in local:**

1. Visit <http://tplinkwifi.net>, and log in your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [System Tools](#) > [System Log](#).
3. Choose the type and level of the system logs as needed.

System Log

Type: ALL ▼

Level: Debug ▼

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

ID	Time	Type	Level	Log Content
1	2019-01-05 19:53:12	IGMP	Warning	V2 igmp router occured! Not matching ours V3.
2	2019-01-05 19:51:07	IGMP	Warning	V2 igmp router occured! Not matching ours V3.
3	2019-01-05 19:51:00	DHCPD	Notice	Recv INFORM from 8C:DC:D4:3E:69:CC
4	2019-01-05 19:49:02	IGMP	Warning	V2 igmp router occured! Not matching ours V3.
5	2019-01-05 19:46:57	IGMP	Warning	V2 igmp router occured! Not matching ours V3.
6	2019-01-05 19:44:52	IGMP	Warning	V2 igmp router occured! Not matching ours V3.
7	2019-01-05 19:43:37	DHCPD	Notice	Recv INFORM from 8C:DC:D4:3E:69:CC
8	2019-01-05 19:42:47	IGMP	Warning	V2 igmp router occured! Not matching ours V3.

◀ 1 2 3 4 5 6 7 8 ... 61 ▶

Log Settings
Save Log

- **To view the system logs:**

1. Select the log Type. Select [ALL](#) to view all kinds of logs, or select a specific type to view the specific logs.
2. Select the log Level and you will see the logs with the specific or higher levels.
3. Click [Refresh](#) to refresh the log list.

- **To save the system logs:**

You can choose to save the system logs to your local computer or a remote server.

Click [Save Log](#) to save the logs in a txt file to your computer.

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

Log Settings

Save Locally

Minimum Level: Information

Save Remotely

Minimum Level: Warning

Server IP: 192.168.0.100

Server Port: 514

Local Facility Name: User

Back
Save

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

14. 10. Monitor the Internet Traffic Statistics

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

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > System Tools > Statistics**.
3. Enable traffic statistics, and then you can monitor the traffic statistics in **Traffic Statistics List** section.

Traffic Statistics

Enable Traffic Statistics:

Traffic Statistics List

↻ Refresh
↻ Reset All
🗑️ Delete All

IP Address/MAC Address	Total Packets	Total Bytes	Current Packets	Current Bytes	Current ICMP Tx	Current UDP Tx	Current SYN Tx	Modify
192.168.0.154 BC:6C:21:9E:2B:35	12	976	0	0	0	0	0	↻ 🗑️

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.

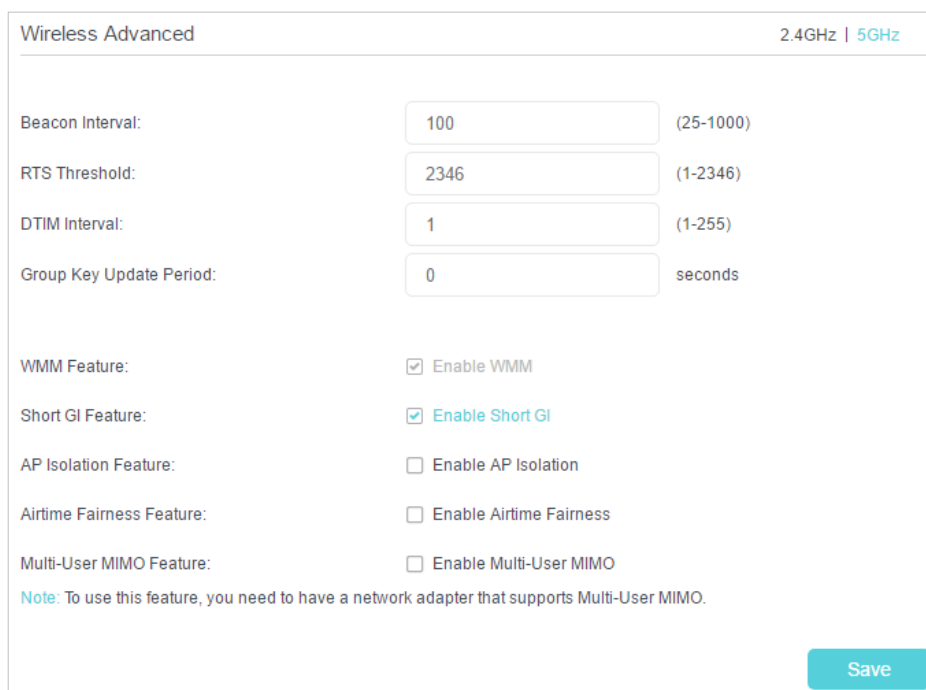
Click  to delete the specific device item in the list.

14. 11. System Parameters

14. 11. 1. Wireless Advanced

You can configure the parameters of traffic transmission rules in wireless networks. It's recommended to keep the default settings if you are not sure of the proper ones in the case. Click  on the management interface to know more about items.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [System Tools](#) > [System Parameters](#). Focus on [Wireless Advanced](#) section.



Wireless Advanced 2.4GHz | 5GHz

Beacon Interval: (25-1000)

RTS Threshold: (1-2346)

DTIM Interval: (1-255)

Group Key Update Period: seconds

WMM Feature: Enable WMM

Short GI Feature: Enable Short GI

AP Isolation Feature: Enable AP Isolation

Airtime Fairness Feature: Enable Airtime Fairness

Multi-User MIMO Feature: Enable Multi-User MIMO

Note: To use this feature, you need to have a network adapter that supports Multi-User MIMO.

[Save](#)

- **WMM Feature** - It is enabled by default and highly recommended, for the WMM function guarantees the packets with high-priority messages being transmitted preferentially.
- **Short GI Feature** - It is enabled by default and highly recommended, for it will increase the packet capacity by reducing the GI (Guard Interval) time.

- **AP Isolation Feature** - If you want to confine and restrict all wireless devices connected to the network from interacting with each other, but still able to access the internet, enable AP Isolation feature.
- **Airtime Fairness Feature** - This feature allows you to optimize the throughput of each flow. The ATF traffic scheduler uses the per-destination airtime targets to balance airtime usage across flow destinations.
- **Multi-User MIMO Feature** - Enable to use Multi-User MIMO Feature. Only available for 5GHz.

■ **Note:** To use this feature, you need to have a network adapter that supports Multi-User MIMO.

14. 11. 2. WDS

WDS (Wireless Distribution System) Bridging feature allows you to bridge a router with an access point to extend the wireless network coverage. The access point should also support WDS Bridging feature.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > System Tools > System Parameters**. Focus on **WDS** section.
3. Enable the WDS Bridging feature.

WDS 2.4GHz | 5GHz

WDS Bridging: Enable WDS Bridging

Wireless Network Name (SSID): Survey

MAC Address (to be bridged):

Security: None WPAWPA2 Personal WEP

Version: WPA-PSK WPA2-PSK

Encryption: TKIP AES

Password: Save

4. Click **Survey** to scan all available networks and select the network you want to bridge. The SSID (network name) and MAC Address will be automatically populated. You can also manually fill in these parameters.
5. Select a **Security** type and enter related parameters, which should be the same as the network to be bridged.
6. Click **Save**.

■ **Note:** You need to enable and configure the WDS Bridging feature for the access point as well.

7. Disable DHCP:

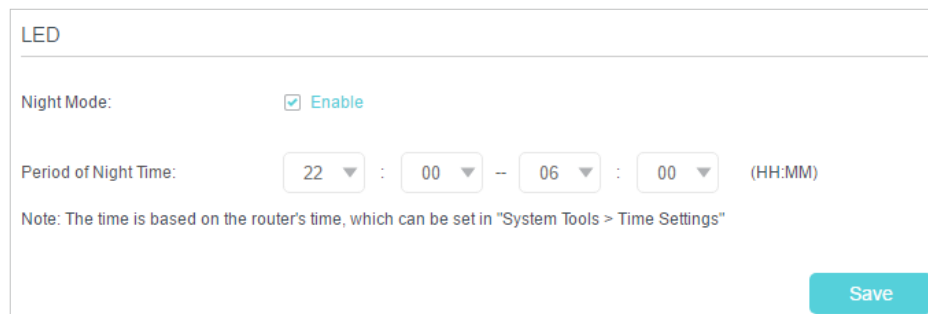
- 1) Go to [Network > DHCP Server](#).
- 2) Deselect [Enable DHCP Server](#) and click [Save](#).

Now you can go to [Advanced > Status > Wireless](#) to check the WDS status. When the [WDS status](#) is [Run](#), it means WDS bridging is successfully built.

14. 11. 3. LEDs Control

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

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced > System Tools > System Parameters](#). Focus on [LED](#) section.
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.



The screenshot shows the 'LED' settings page. At the top, the title 'LED' is displayed. Below it, there is a 'Night Mode' section with a checked checkbox and the text 'Enable'. Underneath, the 'Period of Night Time' is set to '22 : 00 -- 06 : 00 (HH:MM)'. A note below the time selection states: 'Note: The time is based on the router's time, which can be set in "System Tools > Time Settings"'. A blue 'Save' button is located at the bottom right of the form.

5. Click [Save](#).

14. 11. 4. DoS Protection Settings

DoS Protection can protect your home network against DoS attacks from flooding your network with server requests.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced > Security > Settings](#) to enable Dos Protection.
3. Go to [Advanced > System Tools > System Parameters](#).
4. Enter a value between 5 and 7200 to trigger the protection immediately when the number of packets exceeds the preset threshold value.

DoS Protection Settings

ICMP-FLOOD Protection Level:	Low Thresholds:	<input type="text" value="50"/>	(5-7200) Packets/Secs
	Middle Thresholds:	<input type="text" value="20"/>	(5-7200) Packets/Secs
	High Thresholds:	<input type="text" value="10"/>	(5-7200) Packets/Secs
UDP-FLOOD Protection Level:	Low Thresholds:	<input type="text" value="7200"/>	(5-7200) Packets/Secs
	Middle Thresholds:	<input type="text" value="2000"/>	(5-7200) Packets/Secs
	High Thresholds:	<input type="text" value="400"/>	(5-7200) Packets/Secs
TCP-SYN-FLOOD Protection Level:	Low Thresholds:	<input type="text" value="200"/>	(5-7200) Packets/Secs
	Middle Thresholds:	<input type="text" value="100"/>	(5-7200) Packets/Secs
	High Thresholds:	<input type="text" value="50"/>	(5-7200) Packets/Secs

FAQ

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

The default wireless password is printed on the label of the router. If the password has been altered:

1. Connect your computer to the router using an Ethernet cable.
2. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
3. Go to [Basic](#) > [Wireless](#) to retrieve or reset your wireless password.

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

- If you are using a TP-Link ID to log in, click [Forgot password](#) on the login page and then follow the instructions to reset it.
- Alternatively, press and hold the Reset button of the router until the Power LED binks to reset it, and then visit <http://tplinkwifi.net> to create a new login password.

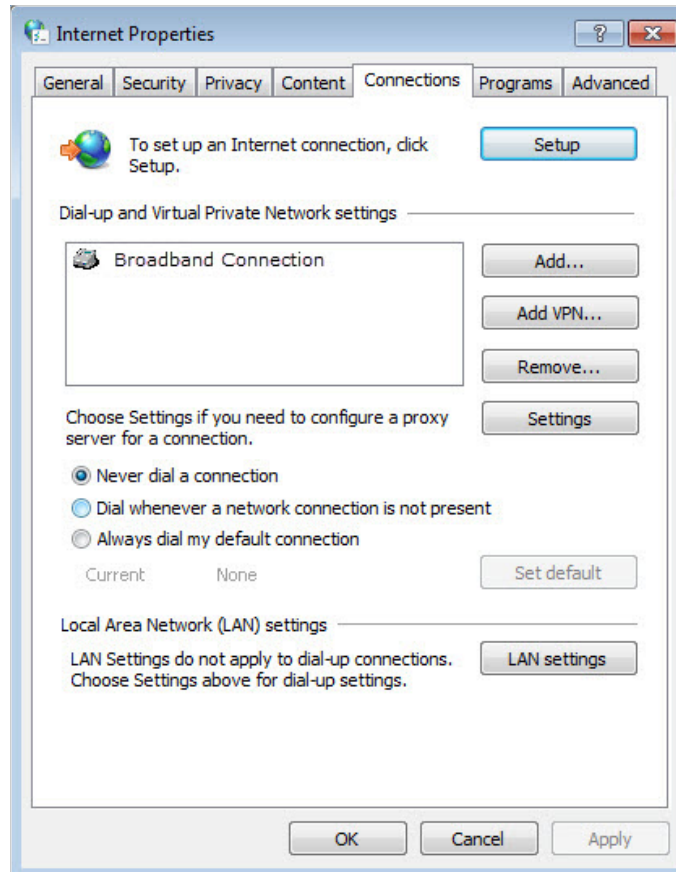
Note:

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.

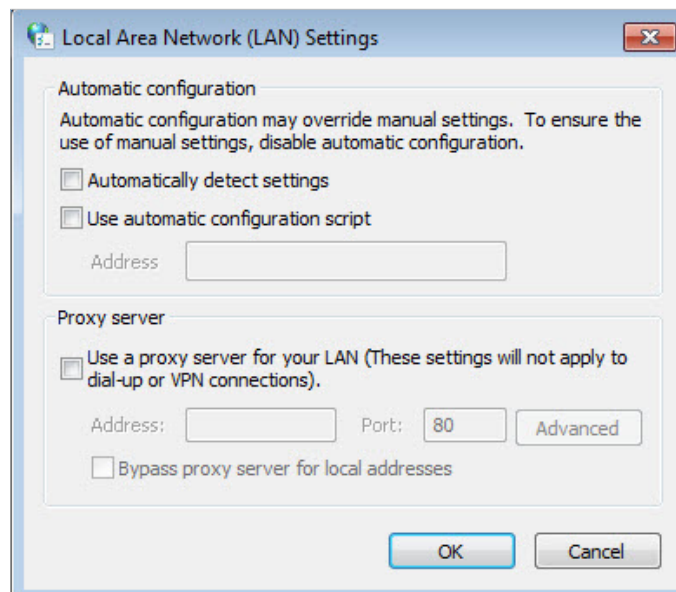
Q3. What should I do if I cannot log in to the router's web management page?

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

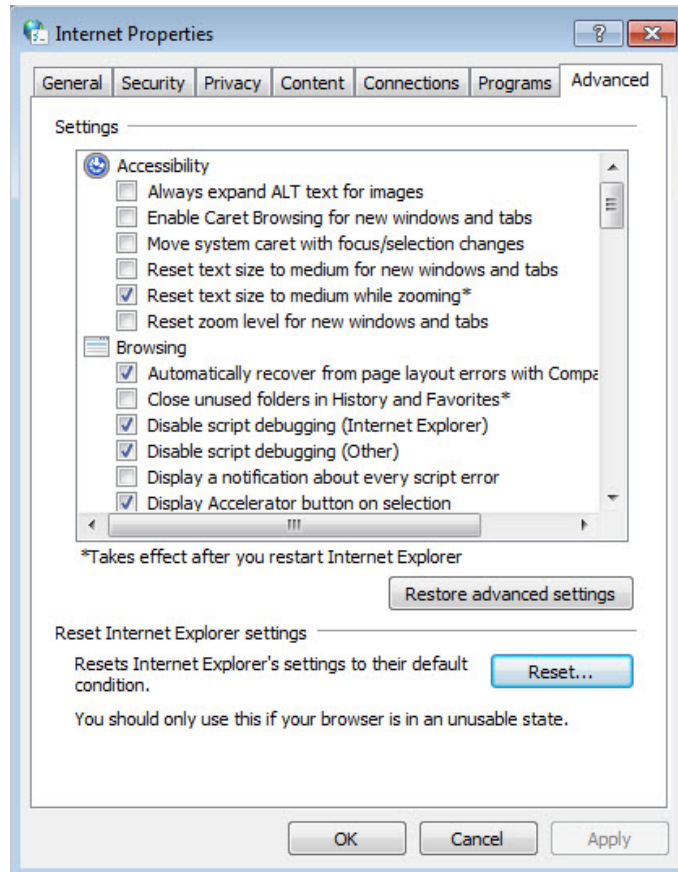
- Make sure your computer is connected to the router correctly and the corresponding LED indicator(s) light up.
- Make sure the IP address of your computer is configured as [Obtain an IP address automatically](#) and [Obtain DNS server address automatically](#).
- Make sure <http://tplinkwifi.net> or <http://192.168.0.1> is correctly entered.
- Check your computer's settings:
 - 1) Go to [Start](#) > [Control Panel](#) > [Network and Internet](#), and click [View network status and tasks](#).
 - 2) Click [Internet Options](#) on the bottom left.
 - 3) Click [Connections](#) and select [Never dial a connection](#).



4) Click [LAN settings](#) and deselect the following three options and click [OK](#).



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



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

■ Note: You'll need to reconfigure the router to surf the internet once the router is reset.

Q4. How do I use the WDS Bridging function to extend my wireless network?

For example, my house covers a large area. The wireless coverage of the router I'm using (the root router) is limited. I want to use an extended router to boost the wireless network of the root router.

■ Note:

- WDS bridging only requires configuration on the extended router.
- WDS bridging function can be enabled either in 2.4GHz frequency or 5GHz frequency for a dual-band router. We use the WDS bridging function in 2.4GHz frequency as example.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.

2. Configure the IP address of the router:

- 1) Go to **Advanced > Network > LAN**, configure the IP address of the extended router to be in the same subnet with the root router; (For example, the IP address

of the root router is 192.168.0.1, the IP address of the extended router can be 192.168.0.2~192.168.0.254. We take 192.168.0.2 as example.)

2) Click [Save](#).

Note: Log in to the web management page again if the IP address of the router is altered.

LAN

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

IP Address: 192.168.0.2

Subnet Mask: 255.255.255.0

Save

3. Survey the SSID to be bridged:

- 1) Go to [Advanced](#) > [System Tools](#) > [System Parameters](#) and focus on the [WDS](#) section. Enable the WDS Bridging feature.
- 2) Click [Survey](#) to scan all available networks and select the network you want to bridge. The SSID (network name) and MAC Address will be automatically populated. You can also manually fill in these parameters.
- 3) Select a [Security](#) type and enter related parameters, which should be the same as the network to be bridged.

2.4GHz WDS

WDS Bridging: Enable WDS Bridging

DHCP Server: Auto On Off

SSID (to be bridged): TP-Link_4F98 [Scan](#)

MAC Address (to be bridged): 0C-4A-08-13-4F-98 Example: 00-1D-0F-11-22-33

Security: No Security WPA-PSK/WPA2-PSK WEP

Password: 12345678

Save

4. Disable DHCP:

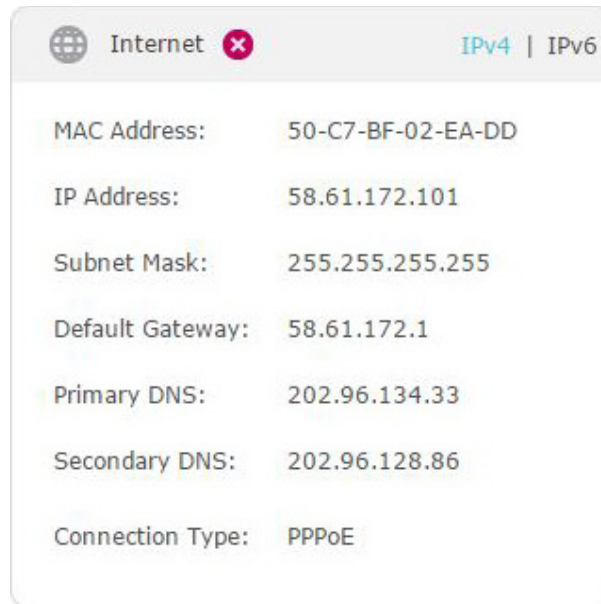
- 1) Go to [Network](#) > [DHCP Server](#).
- 2) Deselect [Enable DHCP Server](#) and click [Save](#).

Now you can go to [Advanced](#) > [Status](#) > [Wireless](#) to check the WDS status. When the [WDS status](#) is [Run](#), it means WDS bridging is successfully built.

Q5. What should I do if I cannot access the internet even though the configuration is finished?

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [Status](#) to check internet status:

As the follow picture shows, if IP Address is a valid one, please try the methods below and try again:



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

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

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

Settings

DHCP Server: Enable DHCP Server

IP Address Pool: -

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

Default Gateway: (Optional)

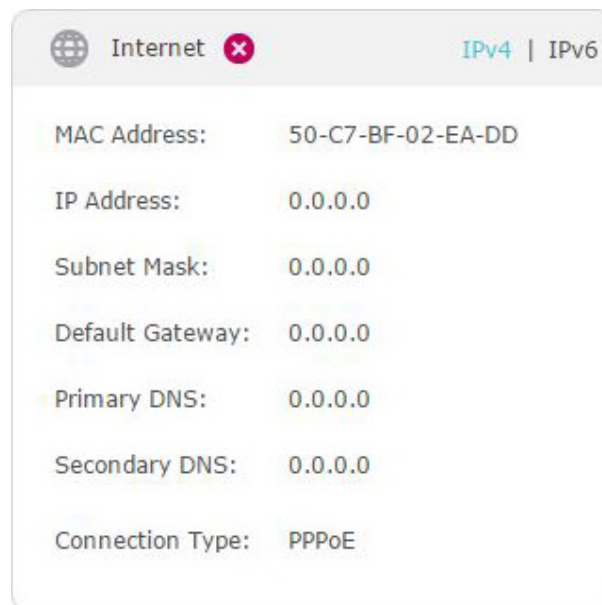
Primary DNS: (Optional)

Secondary DNS: (Optional)

[Save](#)

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

As the picture below shows, if the IP Address is 0.0.0.0, please try the methods below and try again:



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

Tips:

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

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

Note:

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

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

- **Restart the modem and the router.**
 - 1) Power off your modem and router, and leave them off for 1 minute.
 - 2) Power on your modem first, and wait about 2 minutes until it get a solid cable or Internet light.
 - 3) Power on the router.
 - 4) Wait another 1 or 2 minutes and check the internet access.
- **Double check the internet connection type.**

- 1) Confirm your internet connection type, which can be learned from the ISP.
- 2) Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
- 3) Go to [Advanced](#) > [Network](#) > [Internet](#).
- 4) Select your [Internet Connection Type](#) and fill in other parameters.
- 5) Click [Save](#).

The screenshot shows the IPv4 configuration page. The 'Internet Connection Type' dropdown is set to 'Dynamic IP'. Below it, there are input fields for 'IP Address', 'Subnet Mask', 'Default Gateway', 'Primary DNS', and 'Secondary DNS' (with the value 0.0.0.0). There are two buttons: 'Renew' (in teal) and 'Release' (in grey). A red message says 'WAN port is unplugged.' At the bottom left, there is a toggle for 'Advanced' (currently turned off). At the bottom right, there is a 'Save' button in teal.

6) Restart the modem and the router again.

- Please upgrade the firmware of the router.

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

Q6. What should I do if I cannot find my wireless network or I cannot connect the wireless network?

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

- Make sure the wireless function of your device is enabled if you're using a laptop with built-in wireless adapter. You can refer to the relevant document or contact the laptop manufacturer.
- Make sure the wireless adapter driver is installed successfully and the wireless adapter is enabled.

- **On Windows 7**

- 1) If you see the message [No connections are available](#), it is usually because the wireless function is disabled or blocked somehow.

- 2) Click [Troubleshoot](#) and windows might be able to fix the problem by itself.
- **On Windows XP**
 - 1) If you see the message [Windows cannot configure this wireless connection](#), this is usually because windows configuration utility is disabled or you are running another wireless configuration tool to connect the wireless.
 - 2) Exit the wireless configuration tool (the TP-Link Utility, for example).
 - 3) Select and right click on [My Computer](#) on desktop, select [Manage](#) to open Computer Management window.
 - 4) Expand [Services and Applications](#) > [Services](#), find and locate [Wireless Zero Configuration](#) in the Services list on the right side.
 - 5) Right click [Wireless Zero Configuration](#), and then select [Properties](#).
 - 6) Change [Startup type](#) to [Automatic](#), click on Start button and make sure the Service status is [Started](#). And then click [OK](#).

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

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

Wireless Settings 2.4GHz | 5GHz

Enable Wireless Radio

Network Name (SSID): Hide SSID

Security:

Version: Auto WPA-PSK WPA2-PSK

Encryption: Auto TKIP AES

Password:

Mode:

Channel Width:

Channel:

Transmit Power: Low Middle High

If you can find your wireless network but fail to connect, please follow the steps below:

- **Authenticating problem/password mismatch:**

- 1) Sometimes you will be asked to type in a PIN number when you connect to the wireless network for the first time. This PIN number is different from the Wireless Password/Network Security Key, usually you can only find it on the label of your router.




- 2) If you cannot find the PIN or PIN failed, you may choose [Connecting using a security key instead](#), and then type in the [Wireless Password/Network Security Key](#).
- 3) If it continues to show note of [Network Security Key Mismatch](#), it is suggested to confirm the wireless password of your wireless router.

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

- **Windows unable to connect to XXXX / Can not join this network / Taking longer than usual to connect to this network:**
 - Check the wireless signal strength of your network. If it is weak (1~3 bars), please move the router closer and try again.
 - Change the wireless Channel of the router to 1, 6 or 11 to reduce interference from other networks.
 - Re-install or update the driver for your wireless adapter of the computer.

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice.  tp-link 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 © 2019 TP-Link Technologies Co., Ltd. All rights reserved.

FCC STATEMENT



Product Name: AC2600 MU-MIMO Wi-Fi Router

Model Number: Archer A10

Component Name	Model
I.T.E POWER SUPPLY	T090085-2B1

Responsible party:

TP-Link USA Corporation, d/b/a TP-Link North America, Inc.

Address: 145 South State College Blvd. Suite 400, Brea, CA 92821

Website: <http://www.tp-link.com/us/>

Tel: +1 626 333 0234

Fax: +1 909 527 6803

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

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

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

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

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

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

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

FCC RF Radiation Exposure Statement

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

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

The device is restricted in indoor environment only.

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

Issue Date: 2019.01.15

FCC compliance information statement



Product Name: I.T.E POWER SUPPLY

Model Number: T090085-2B1

Responsible party:

TP-Link USA Corporation, d/b/a TP-Link North America, Inc.

Address: 145 South State College Blvd. Suite 400, Brea, CA 92821

Website: <http://www.tp-link.com/us/>

Tel: +1 626 333 0234

Fax: +1 909 527 6803

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

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency

energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

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

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

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

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

Issue Date: 2019.01.15

Canadian Compliance Statement

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

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

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

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

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

Caution:

1. The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;
2. For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5745-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-topoint operation as appropriate; and

The high-power radars are allocated as primary users (i.e. priority users) of the bands 5745-5850 MHz and that these radars could cause interference and/or damage to LELAN devices.

Avvertissement:

1. Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
2. Le gain maximal d'antenne permis pour les dispositifs avec antenne(s) amovible(s) utilisant la bande 5745-5850 MHz doit se conformer à la limitation P.I.R.E spécifiée pour l'exploitation point à point et non point à point, selon le cas.

En outre, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5745-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

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)

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行；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。

4.7.9.1應避免影響附近雷達系統之操作。

4.7.9.2高增益指向性天線只得應用於固定式點對點系統。


安全諮詢及注意事項

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

限用物質含有情況標示聲明書



產品元件名稱	限用物質及其化學符號					
	鉛 Pb	鎘 Cd	汞 Hg	六價鉻 CrVI	多溴聯苯 PBB	多溴二苯醚 PBDE
PCB	○	○	○	○	○	○
外殼	○	○	○	○	○	○
電源適配器	-	○	○	○	○	○
備考1. 超出0.1 wt %” 及 “超出0.01 wt %” 系指限用物質之百分比含量超出百分比含量基準值。						
備考2. “○” 系指該項限用物質之百分比含量未超出百分比含量基準值。						
備考3. “-” 系指該項限用物質為排除項目。						

Safety Information

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

Explanations of the symbols on the product label

Symbol	Explanation
	DC voltage

Symbol	Explanation
	Indoor use only
	<p>RECYCLING</p> <p>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.</p> <p>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.</p>