



User Guide

AC2300 Wireless MU-MIMO Gigabit 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	4
1. 2. 3.The Back Panel.....	5
Chapter 2. Connect the Hardware	6
2. 1. Position Your Router	7
2. 2. Connect Your Router.....	7
Chapter 3. Log In to Your Router.....	10
Chapter 4. Set Up Internet Connection	12
4. 1. Use Quick Setup Wizard	13
4. 2. Manually Set up Your Internet Connection	13
4. 3. Set Up an IPv6 Internet Connection	16
Chapter 5. Set Up the Router as an Access Point	20
Chapter 6. TP-Link Cloud Service	23
6. 1. Register a TP-Link ID.....	24
6. 2. Change Your TP-Link ID Information.....	24
6. 3. Manage the User TP-Link IDs	25
6. 3. 1.Add TP-Link ID to Manage the Router.....	26
6. 3. 2.Remove TP-Link ID(s) from Managing the Router.....	26
6. 4. Manage the Router via the TP-Link Tether App	27
Chapter 7. Guest Network.....	28
7. 1. Create a Network for Guests	29
7. 2. Customize Guest Network Options.....	30
Chapter 8. Parental Controls	31

Chapter 9. QoS	35
9.1. Prioritize Internet Traffic with QoS	36
9.2. Update the Database	37
Chapter 10. Network Security	39
10.1. Protect the Network from Cyber Attacks	40
10.2. Access Control	41
10.3. IP & MAC Binding	43
Chapter 11. NAT Forwarding	44
11.1. Share Local Resources on the Internet by Virtual Servers	45
11.2. Open Ports Dynamically by Port Triggering	46
11.3. Make Applications Free from Port Restriction by DMZ	47
11.4. Make Xbox Online Games Run Smoothly by UPnP	48
Chapter 12. VPN Server	50
12.1. Use OpenVPN to Access Your Home Network	51
12.2. Use PPTP VPN to Access Your Home Network	52
Chapter 13. Customize Your Network Settings	57
13.1. Change the LAN Settings	58
13.2. Set Up Link Aggregation	58
13.3. Configure to Support IPTV Service	59
13.4. Specify DHCP Server Settings	60
13.5. Set Up a Dynamic DNS Service Account	62
13.6. Create Static Routes	63
13.7. Specify Wireless Settings	65
13.8. Use WPS for Wireless Connection	67
13.8.1. Method 1: Use the WPS Button	67
13.8.2. Method 2: Use the WPS Button on the Web Management Page	68
13.8.3. Method 3: Enter the Router's PIN on Your Client Device	68
13.8.4. Method 4: Enter the Client Device's PIN on the Router	69
13.9. Schedule Your Wireless Function	69
Chapter 14. Manage the Router	71
14.1. Set Up System Time	72
14.2. Control LEDs	74
14.3. Test the Network Connectivity	74
14.4. Set Up Port Mirroring	76

14. 5. Upgrade the Firmware	76
14. 5. 1. Online Upgrade	77
14. 5. 2. Local Upgrade	77
14. 5. 3. Restore Interrupted Upgrade after Power Failure	78
14. 6. Backup and Restore Configuration Settings	78
14. 7. Set the Router to Reboot Regularly	80
14. 8. Change the Administrator Account	80
14. 9. Default Password Recovery	81
14. 10. Local Management	82
14. 11. Remote Management	83
14. 12. System Log	84
FAQ	87

About This Guide

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

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

Conventions

In this guide the following conventions are used:

Convention	Description
<u>Underlined</u>	Underlined words or phrases are hyperlinks. You can click to redirect to a website or a specific section.
Teal	Contents to be emphasized and texts on the web page are in teal, including the menus, items, buttons, etc.
>	The menu structures to show the path to load the corresponding page. For example, Advanced > Wireless > MAC Filtering means the MAC Filtering function page is under the Wireless menu that is located in the Advanced tab.
Note:	Ignoring this type of note might result in a malfunction or damage to the device.
Tips:	Indicates important information that helps you make better use of your device.
symbols on the web page	<ul style="list-style-type: none">✎ click to edit the corresponding entry.🗑 click to delete the corresponding entry.🔍 click to enable or disable the corresponding entry.📄 click to view more information about items on the page.

More Info

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

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

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

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

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

Chapter 1

Get to Know About Your Router

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

It contains the following sections:

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

1.1. Product Overview

The TP-Link router is designed to fully meet the need of Small Office/Home Office (SOHO) networks and users demanding higher networking performance. The powerful antennas ensure continuous Wi-Fi signal to all your devices while boosting widespread coverage throughout your home, 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. You can check the router's working status by following the LED Explanation table.

LED 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.

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](#)

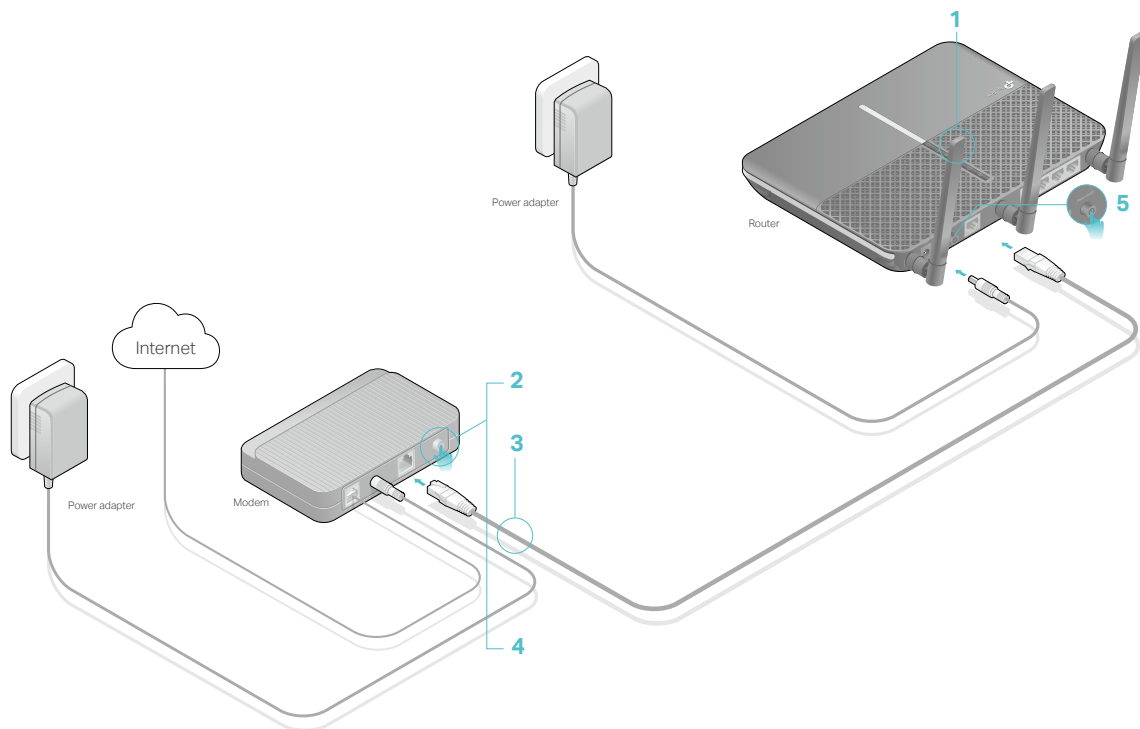
2.1. Position Your Router

- 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.



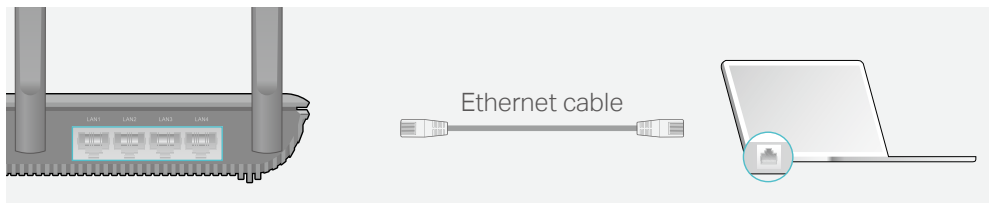
Note:

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.

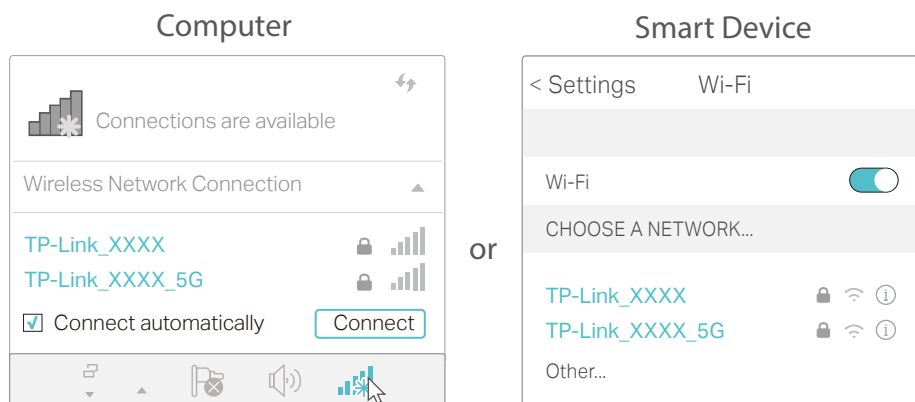
• **Method 1: Wired**

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**

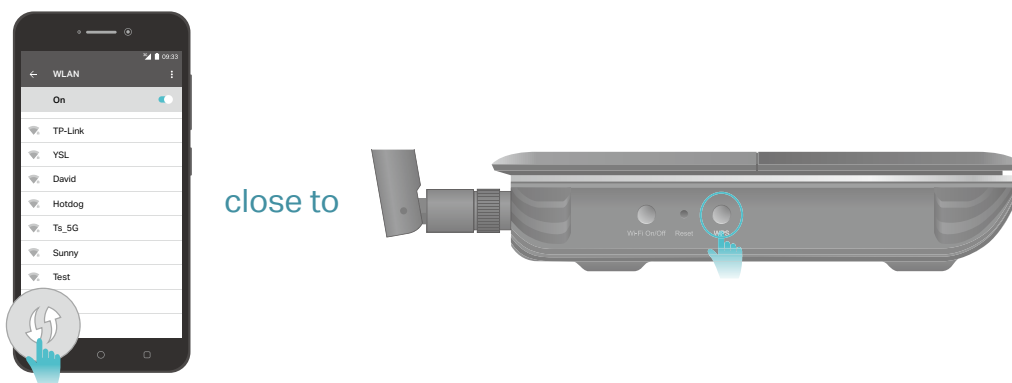
Wireless devices that support WPS, including Android phones, tablets, and most USB network adapters, can be connected to your router through this method.

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.



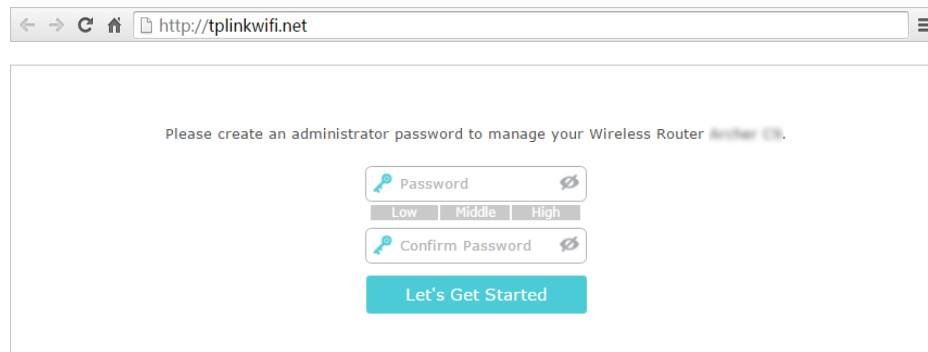
Chapter 3

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

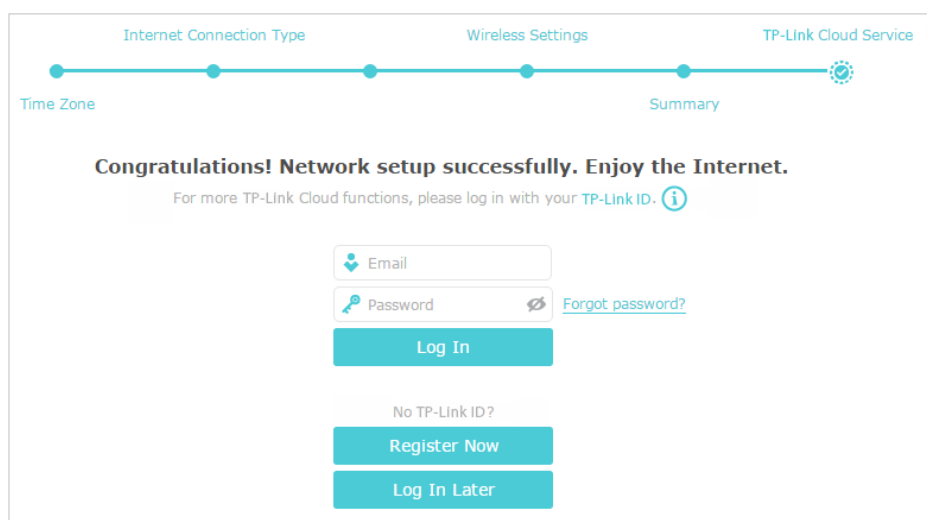
The Quick Setup Wizard will guide you through the process to set up your router.

☞ **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:

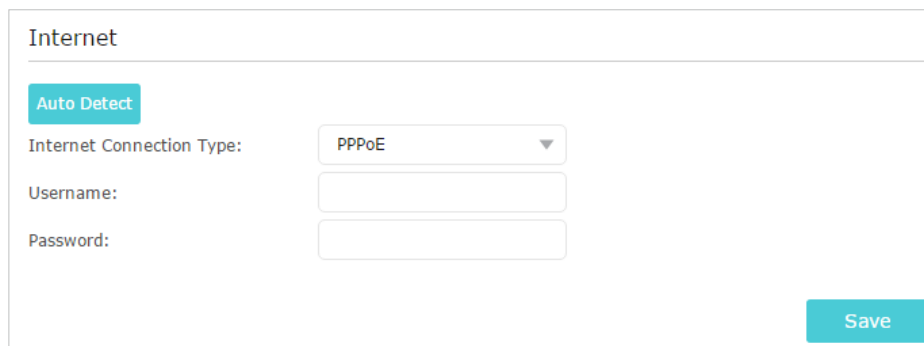
Default Gateway:

Primary DNS:

Secondary DNS: (Optional)

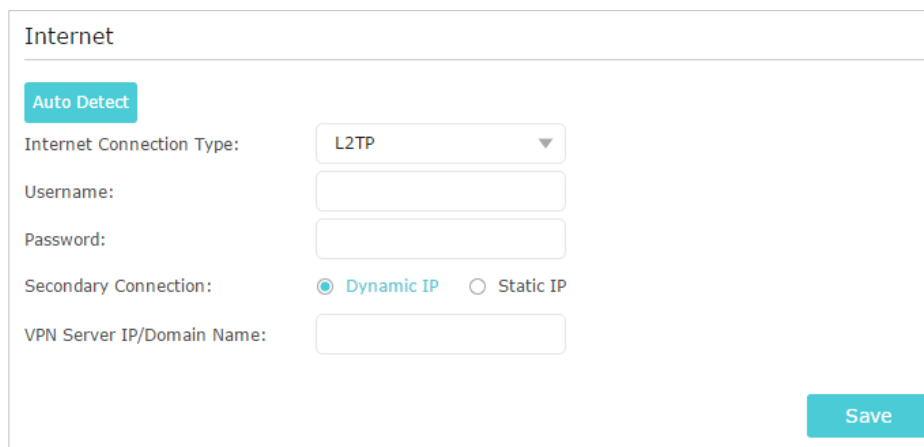
Save

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



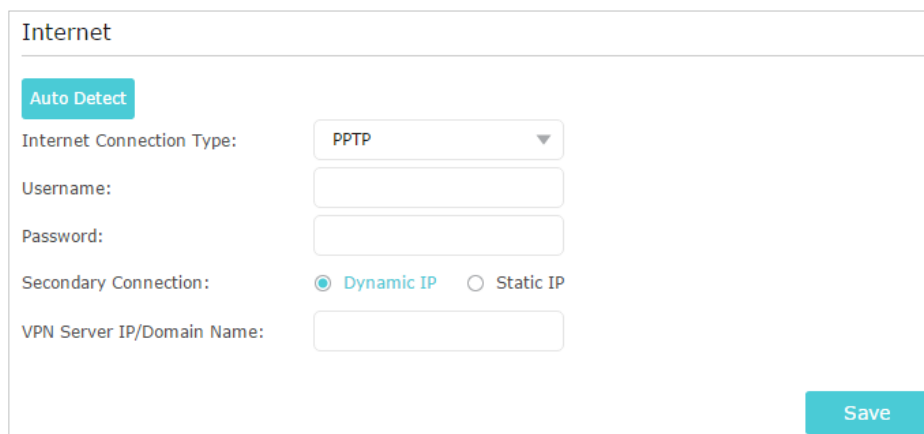
The screenshot shows the 'Internet' configuration page. At the top left is a teal 'Auto Detect' button. Below it, the 'Internet Connection Type' dropdown menu is set to 'PPPoE'. There are two empty text input fields for 'Username:' and 'Password:'. A teal 'Save' button is located at the bottom right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



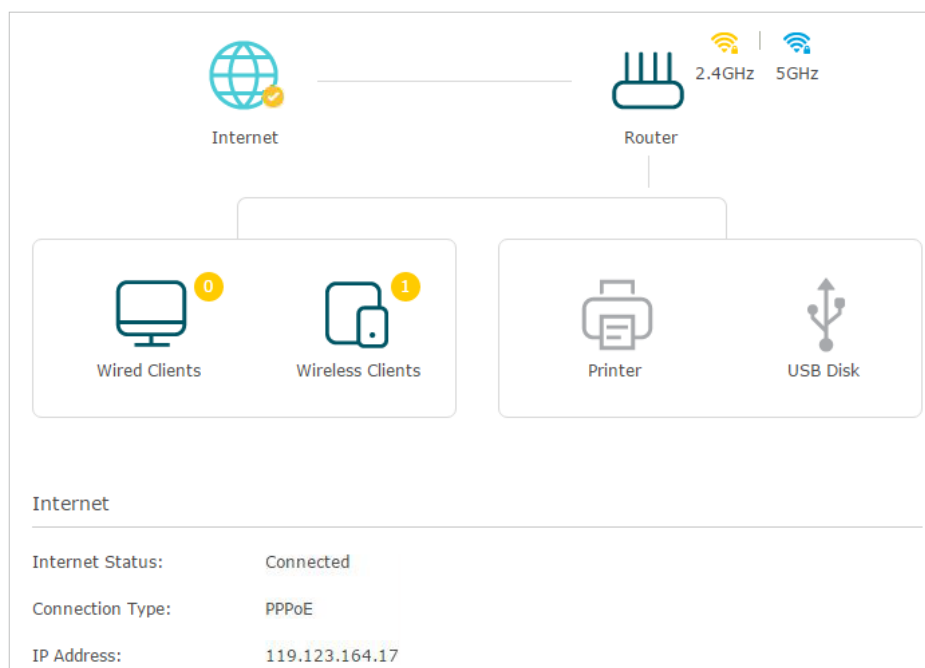
The screenshot shows the 'Internet' configuration page. The 'Internet Connection Type' dropdown menu is set to 'PPTP'. Below the 'Password:' field, there are two radio buttons for 'Secondary Connection': 'Dynamic IP' (which is selected) and 'Static IP'. There is an empty text input field for 'VPN Server 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.

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

- 1) **Static IP:** Fill in blanks and click **Save**.

The screenshot shows the 'Internet' configuration page. At the top, the title is 'Internet'. Below it, there is a toggle switch for 'IPv6' which is turned on. Underneath, the 'Internet Connection Type' is set to 'Static IP' in a dropdown menu. There are four empty text input fields for 'IPv6 Address:', 'Default Gateway:', 'Primary DNS:', and 'Secondary DNS:'. Below these is an 'MTU Size' field with the value '1500' and a note: 'bytes. (The default is 1500, do not change unless necessary.)'. A 'Save' button is located at the bottom right of the form.

- 2) **Dynamic IP(SLAAC/DHCPv6):** Click **Advanced** to input further information if your ISP requires. Click **Save** and then click **Renew**.

The screenshot shows the 'Internet' configuration page. At the top, the title is 'Internet'. Below it, there is a toggle switch for 'IPv6' which is turned on. Underneath, the 'Internet Connection Type' is set to 'Dynamic IP (SLAAC/DHCPv6)' in a dropdown menu. The 'IPv6 Address:', 'Primary DNS:', and 'Secondary DNS:' fields are all filled with '::'. Below these fields are two buttons: 'Renew' (highlighted in teal) and 'Release' (grey). There is a checkbox labeled 'Advanced' which is checked. A 'Save' button is located at the bottom right of the form.

- 3) **PPPoE:** 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** and then click **Connect**.

Note:

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

The screenshot shows the 'Internet' configuration window. At the top, the title is 'Internet'. Below it, there is a section for 'IPv6' with a toggle switch that is turned on. Underneath, the 'Internet Connection Type' is set to 'PPPoE' in a dropdown menu. A checkbox labeled 'PPPoE same session with IPv4 connection' is checked. The 'IPv6 Address' field contains '::'. There is an 'Advanced' section with a heart icon and a downward arrow. At the bottom, there are three buttons: 'Connect' (teal), 'Disconnect' (grey), and 'Save' (teal).

- 4) **6to4 Tunnel:** An IPv4 internet connection type is a prerequisite for this connection type ([Manually Set up Your Internet Connection](#)). Click **Advanced** to input further information if your ISP requires. Click **Save** and then click **Connect**.

The screenshot shows the 'Internet' configuration window. At the top, the title is 'Internet'. Below it, there is a section for 'IPv6' with a toggle switch that is turned on. Underneath, the 'Internet Connection Type' is set to '6to4 Tunnel' in a dropdown menu. The 'IPv4 Address', 'IPv4 Subnet Mask', and 'IPv4 Default Gateway' fields all contain '0.0.0.0'. The 'Tunnel Address' field contains '::'. There is an 'Advanced' section with a heart icon and a downward arrow. At the bottom, there are three buttons: 'Connect' (teal), 'Disconnect' (grey), and 'Save' (teal).

- 5) **Pass-Through (Bridge):** Click **Save** and skip to step 6.

The screenshot shows the 'Internet' configuration window. At the top, the title is 'Internet'. Below it, there is a section for 'IPv6' with a toggle switch that is turned on. Underneath, the 'Internet Connection Type' is set to 'Pass-Through (Bridge)' in a dropdown menu. At the bottom, there is a 'Save' button (teal).

5. Configure LAN ports. Windows users are recommended to choose from the first two types. Fill in **Address Prefix** provided by your ISP, and click **Save**.

🔗 Tips:

Find [Help](#) on the management interface to know more about items.

LAN


Assigned Type: DHCPv6 SLAAC+Stateless DHCP SLAAC+RDNSS

Address Prefix: /64

Address: FE80::E4A:8FF:FE13:5053/64

[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:

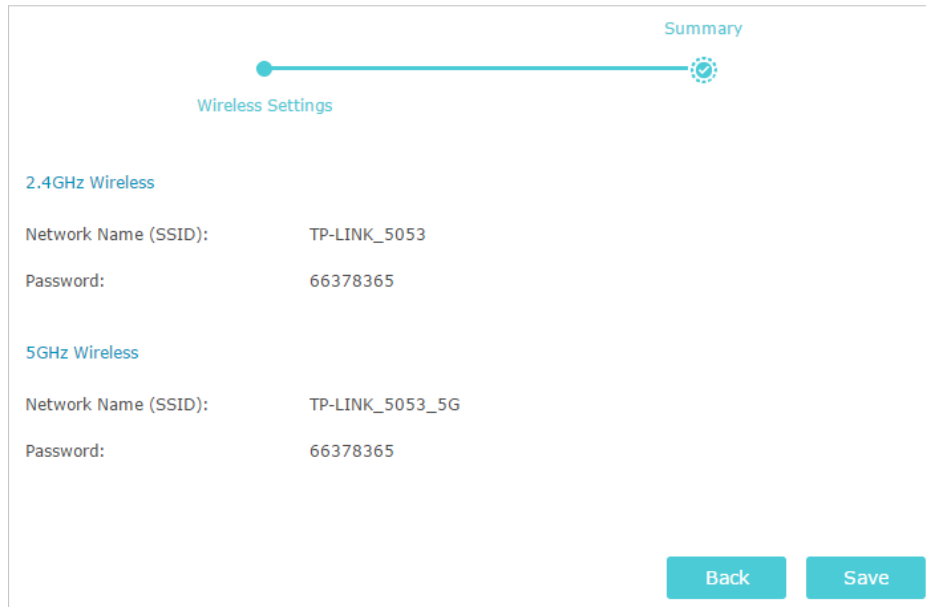
5GHz Wireless: Enable Wireless Radio

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 and USB Sharing, are 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.

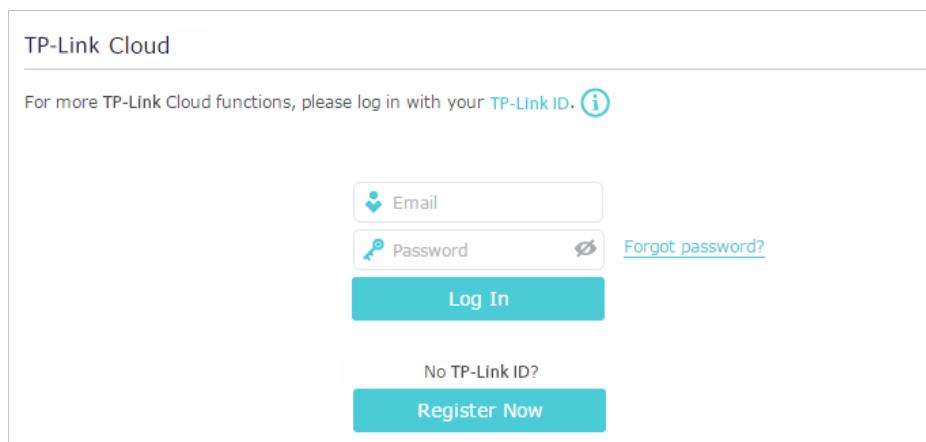
It contains the following sections:

- [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.

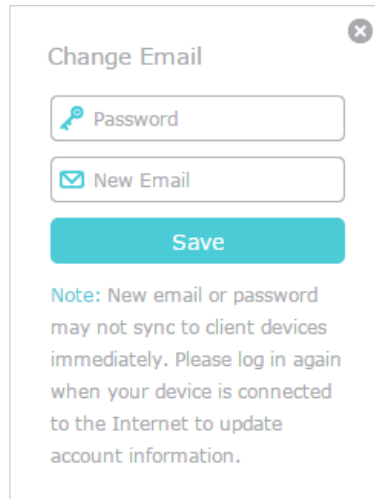
6.2. Change Your TP-Link ID Information

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

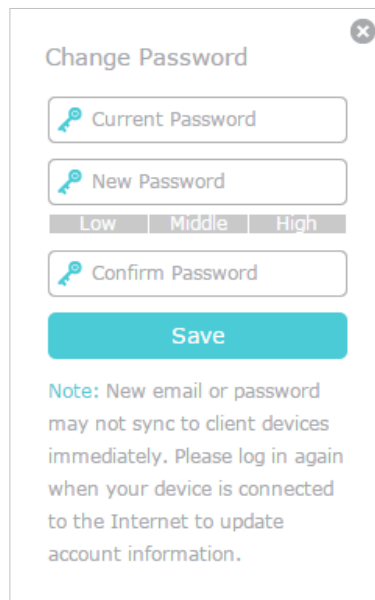
New Email

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 [2.4 GHz Wireless](#) guest network 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. It is divided into two sections: '2.4GHz Wireless' and '5GHz Wireless'. In both sections, the 'Enable Guest Network' checkbox is checked. The 'Network Name (SSID)' field is filled with 'TP-LINK_Guest_5053' for 2.4GHz and 'TP-LINK_Guest_5053_5G' for 5GHz. The 'Hide SSID' checkbox is unchecked. Under the 'Security' section, 'WPA/WPA2-Personal' is selected. The 'Version' is set to 'Auto' and 'Encryption' is also set to 'Auto'. The 'Password' field contains '66378365'. A 'Save' button is located at the bottom right of the form.

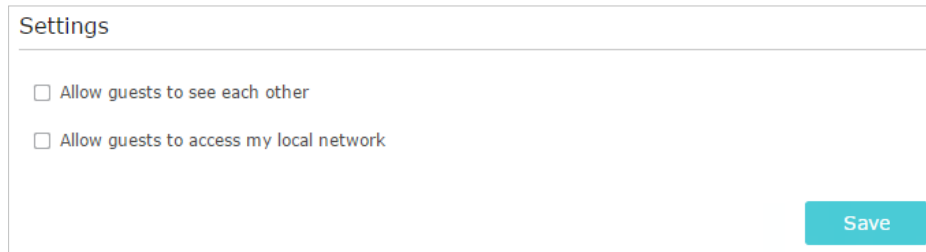
4. Click [Save](#). Now your guests can access your guest network using the SSID and password you set!

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.


I want to:

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

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

How can I do that?

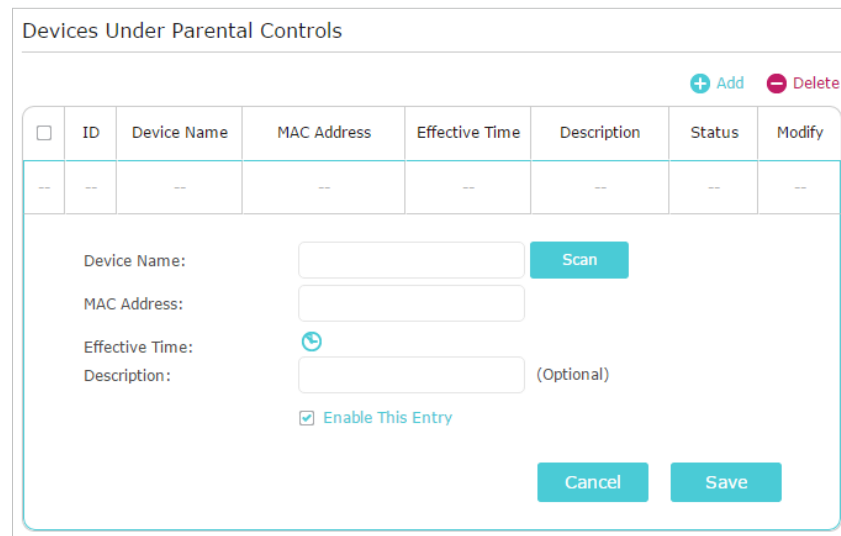
1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > Parental Controls** and enable **Parental Controls**.



Parental Controls

Parental Controls:

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




Devices Under Parental Controls

+ Add - Delete

<input type="checkbox"/>	ID	Device Name	MAC Address	Effective Time	Description	Status	Modify
--	--	--	--	--	--	--	--

Device Name: **Scan**


MAC Address:

Effective Time: 

Description: (Optional)

Enable This Entry

Cancel **Save**

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

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

Tips:

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

7. Click [+ Add a New Domain Name](#) . Enter a website and click [Save](#).

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

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

Content Restriction

Content Restriction:

Restriction Policy: Blacklist Whitelist

[+ Add a New Domain Name](#)

Done!

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

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.

It contains the following sections:

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

9. 1. Prioritize Internet Traffic with QoS

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

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

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

How can I do that?

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

The screenshot shows the QoS configuration interface. At the top, there's a title 'QoS'. Below it, the 'QoS' section has a checkbox for 'Enable QoS' which is checked. Underneath, there are two input fields: 'Upload Bandwidth' set to '1000' with a 'Mbps' dropdown, and 'Download Bandwidth' also set to '1000' with a 'Mbps' dropdown. A section titled 'Advanced' is expanded, showing three sliders for priority levels: 'High Priority' at 60%, 'Middle Priority' at 30%, and 'Low Priority' at 10%. A 'Save' button is located at the bottom right of the form.

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

QoS Rule

Type: By Device By Application

Device Name: [View Existing Devices](#)

MAC Address:

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

2) Choose the respective device from the list.

Access Devices List

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

3) Click **OK**.

QoS Rule

Type: By Device By Application

Device Name: [View Existing Devices](#)

MAC Address:

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

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

Note:

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

Done!

Now QoS is implemented to prioritize Internet traffic.

9.2. Update the Database

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

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

Database Upgrade

New Database File: [Browse](#)

Database Version: Qos database 1.5.0

[Upgrade](#)

Chapter 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](#)

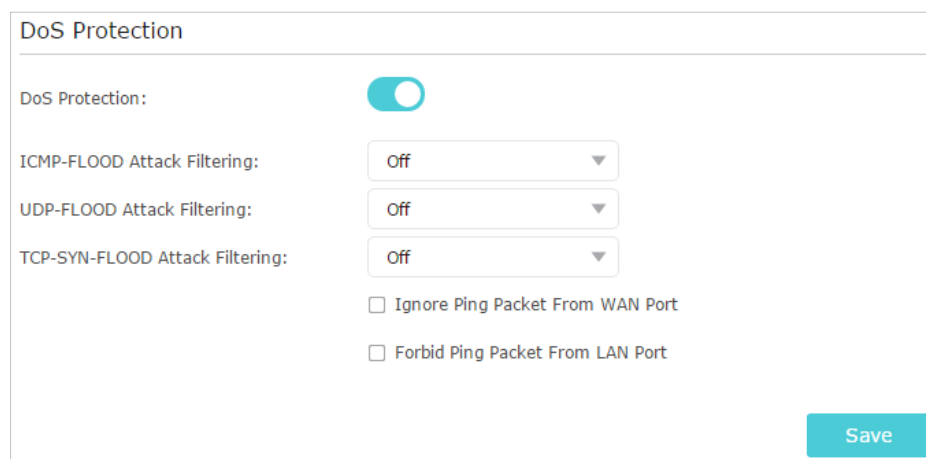
10.1. Protect the Network from Cyber Attacks

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](#) > [Firewall & Dos Protection](#).



DoS Protection

DoS Protection:

ICMP-FLOOD Attack Filtering:

UDP-FLOOD Attack Filtering:

TCP-SYN-FLOOD Attack Filtering:

Ignore Ping Packet From WAN Port

Forbid Ping Packet From LAN Port

Save

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

 **Tips:**

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

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

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

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?

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

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

- If you also want to control access of the devices connected to the guest network, toggle on Guest Devices Control.

Guest Devices Control	
Guest Devices Control:	<input checked="" type="checkbox"/>

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

To block specific device(s)

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

Access Mode

Default Access Mode: Blacklist Whitelist

Save

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

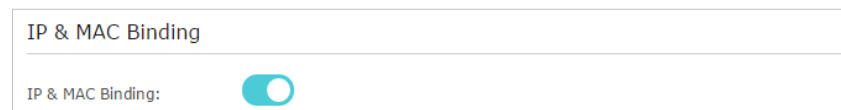
10.3. IP & MAC Binding

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 an 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 **IP & MAC Binding**.



IP & MAC Binding

IP & MAC Binding:

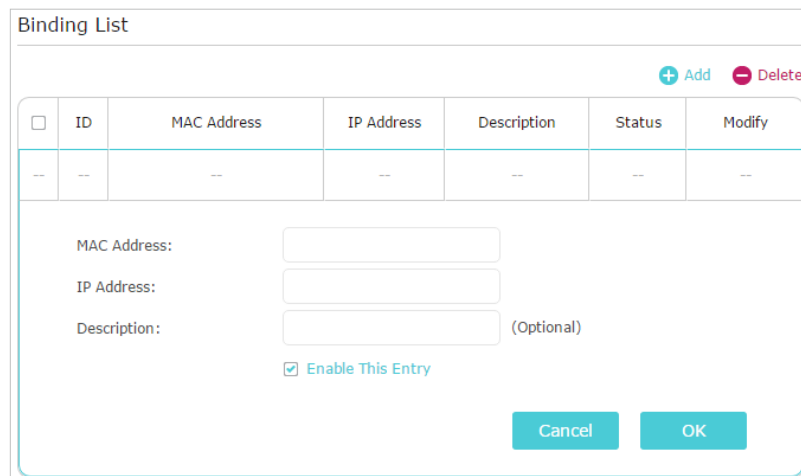
4. Bind your device(s) according to your need.

To bind the connected device(s):

Click  to add the corresponding device to the **Binding List**.

To bind the unconnected device

- 1) Click **Add** in the **Binding List** section.



Binding List

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

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

MAC Address:

IP Address:

Description: (Optional)

Enable This Entry

- 2) Enter the **MAC address** and **IP address** that you want to bind. Enter a **Description** for this binding entry.
- 3) Check the box for **Enable This Entry** 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](#)

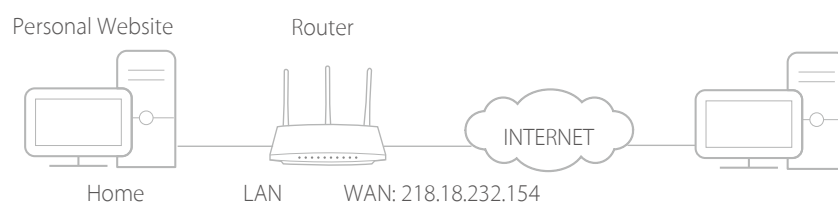
11.1. Share Local Resources on the Internet by Virtual Servers

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

☐	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](#).

- 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.
- Click [OK](#).

Port Triggering

+ Add - Delete

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

Application: [View Existing Applications](#)

Triggering Port: (XX,1-65535)

Triggering Protocol: ▼

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

External Protocol: ▼

[Enable This Entry](#)

💡 **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:

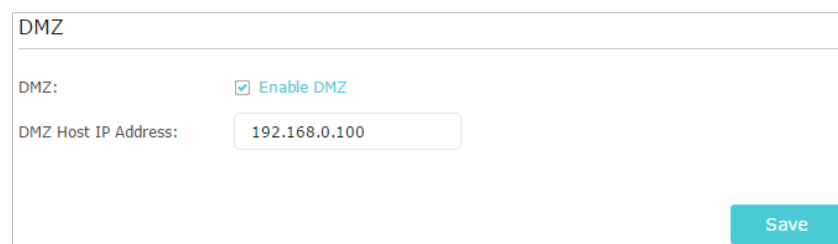
When DMZ is enabled, the DMZ host is totally exposed to the internet, which may bring some potential safety hazards. If DMZ is not in use, please disable it in time.

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](#) filed.



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.

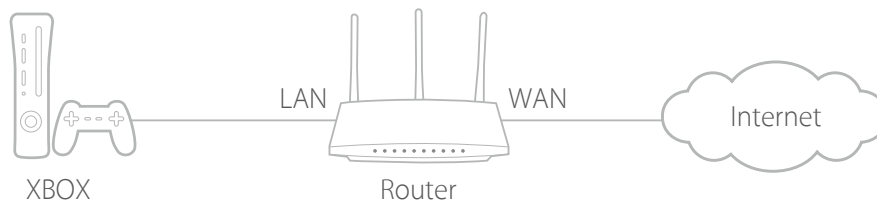
11.4. Make Xbox Online Games Run Smoothly by UPnP

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.

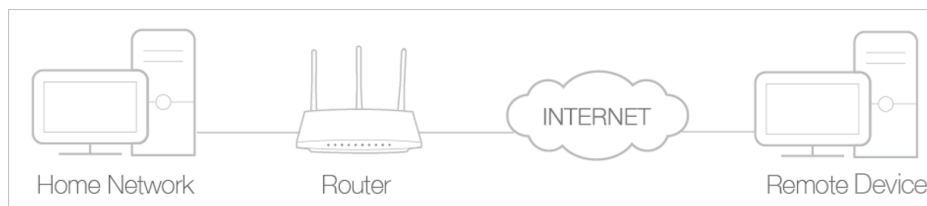
PPTP VPN is more easily used and its speed is faster, it's compatible with most operating systems and also supports mobile devices. Its security is poor and your packets may be cracked easily, and PPTP VPN connection may be prevented by some ISP.

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

[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.
- 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.