



User Guide

AC1200 Wireless MU-MIMO Gigabit Router
Archer A6

Contents

About This Guide	1
Chapter 1. Get to Know About Your Router	2
1. 1. Product Overview.....	3
1. 2. Appearance	3
1. 2. 1.The Front Panel	3
1. 2. 2.The Back Panel.....	4
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	17
4. 4. Configure the Router in Access Point Mode	20
Chapter 5. Guest Network.....	21
5. 1. Create a Network for Guests	22
5. 2. Customize Guest Network Options.....	23
Chapter 6. Parental Controls	24
Chapter 7. QoS.....	28
7. 1. Prioritize Internet Traffic with QoS.....	29
Chapter 8. Network Security	31
8. 1. Protect the Network from Cyber Attacks	32
8. 2. Access Control	33
8. 3. IP & MAC Binding	34
Chapter 9. NAT Forwarding.....	36

9. 1.	Share Local Resources on the Internet by Virtual Servers.....	37
9. 2.	Open Ports Dynamically by Port Triggering.....	38
9. 3.	Make Applications Free from Port Restriction by DMZ.....	39
9. 4.	Make Xbox Online Games Run Smoothly by UPnP.....	40

Chapter 10.VPN Server 42

10. 1.	Use OpenVPN to Access Your Home Network.....	43
10. 1. 1.	Step1. Set up OpenVPN Server on Your Router.....	43
10. 1. 2.	Step 2. Configure OpenVPN Connection on Your Remote Device	44
10. 2.	Use PPTP VPN to Access Your Home Network.....	44
10. 2. 1.	Step 1. Set up PPTP VPN Server on Your Router.....	44
10. 2. 2.	Step 2. Configure PPTP VPN Connection on Your Remote Device....	46

Chapter 11.Customize Your Network Settings..... 50

11. 1.	Change the LAN Settings.....	51
11. 2.	Configure to Support IPTV Service.....	51
11. 3.	Specify DHCP Server Settings.....	53
11. 4.	Set Up a Dynamic DNS Service Account.....	54
11. 5.	Create Static Routes.....	55
11. 6.	Specify Wireless Settings.....	57
11. 7.	Use WPS for Wireless Connection.....	58
11. 7. 1.	Set the Router's PIN.....	58
11. 7. 2.	Use the WPS Wizard for Wi-Fi Connections.....	59
11. 8.	Schedule Your Wireless Function.....	59
11. 9.	TxBF, MU-MIMO.....	60

Chapter 12.Manage the Router 61

12. 1.	Set Up System Time.....	62
12. 2.	Control LEDs.....	63
12. 3.	Test the Network Connectivity.....	64
12. 4.	Upgrade the Firmware.....	65
12. 5.	Backup and Restore Configuration Settings.....	66
12. 6.	Set the Router to Reboot Regularly.....	67
12. 7.	Change the Login Password.....	67
12. 8.	Password Recovery.....	68
12. 9.	Local Management.....	69
12. 10.	Remote Management.....	70
12. 11.	System Log.....	71
12. 12.	Monitor the Internet Traffic Statistics.....	73
12. 13.	Configure the System Parameters.....	74

12. 13. 1. Wireless Advanced	74
12. 13. 2. WDS	75
12. 13. 3. WPS.....	76
12. 13. 4. NAT	77
12. 13. 5. DoS Protection	77
12. 13. 6. Duplex.....	78

FAQ	79
------------------	-----------







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](#)
- [Appearance](#)

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. Appearance

1.2.1. The Front Panel



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

LED Explanation

Name	Status	Indication
⏻ (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.

Name	Status	Indication
📶 (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.
🌐 (Ethernet)	On	At least one Ethernet port is connected to a powered-on device.
	Off	No powered-on device is connected to the router's corresponding Ethernet port.
🌐 (Internet)	Green 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.
🔒 (WPS)	On/Off	This light remains on for 5 minutes when a WPS connection is established, then turns off.
	Flashing	WPS connection is in progress. This may take up to 2 minutes.

1.2.2. The Back Panel



The router's ports (view from left to right) are located on the rear panel.

Item	Description
Power Port	For connecting the router to a power socket via the provided power adapter.

Item	Description
Power On/Off Button	Press this button to power on or off the router.
Reset Button	Press and hold this button for more than 2 seconds to reset the router to its factory default settings.
WPS/Wi-Fi On/Off	Press this button, and immediately press the WPS button on your device. The WPS LED of the router should change from flashing to solid on, indicating successful WPS connection.
	Press and hold the Wi-Fi button for about 3 seconds to turn on or off the wireless function of your router.
Internet Port	For connecting to a DSL/Cable modem, or an Ethernet jack.
Ethernet 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](#)

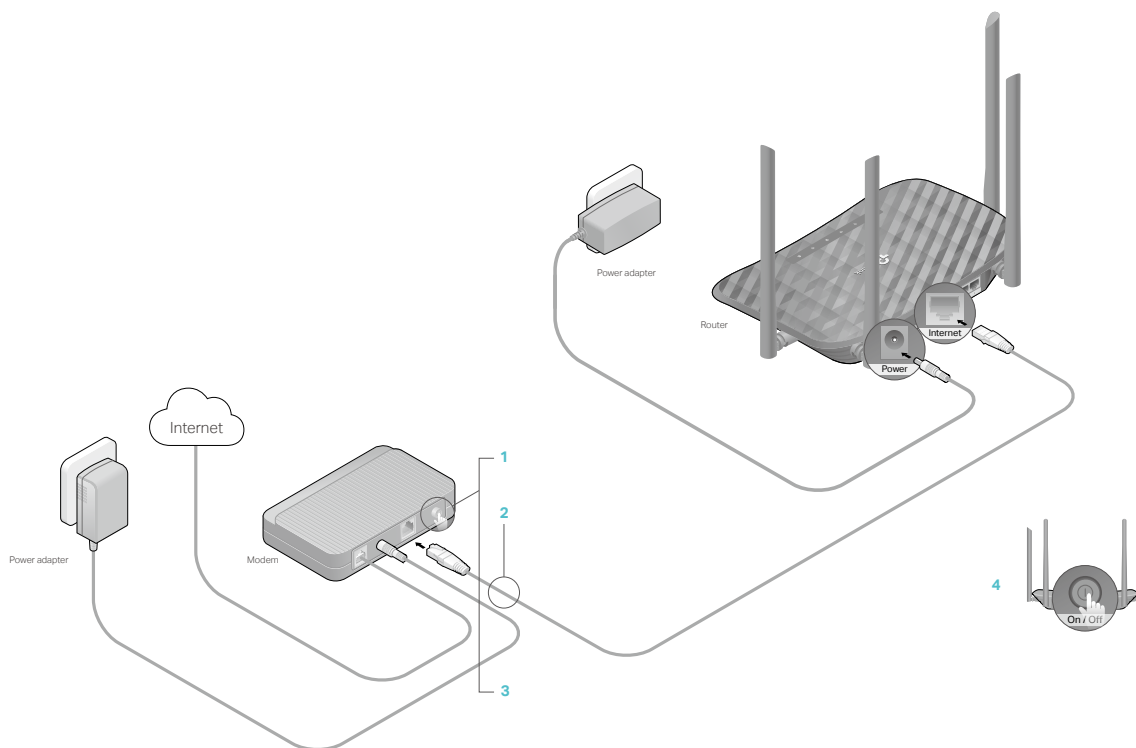
2.1. Position Your Router

- 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 4 and 5 to complete the hardware connection.



1. Turn off the modem, and remove the backup battery if it has one.
2. Connect the modem to your router's Internet port with an Ethernet cable.
3. Turn on the modem, and then wait about **2 minutes** for it to restart.

4. Connect the power adapter to the router and turn on the router.
5. Verify that the following LEDs are on and solid to confirm the hardware is connected correctly.



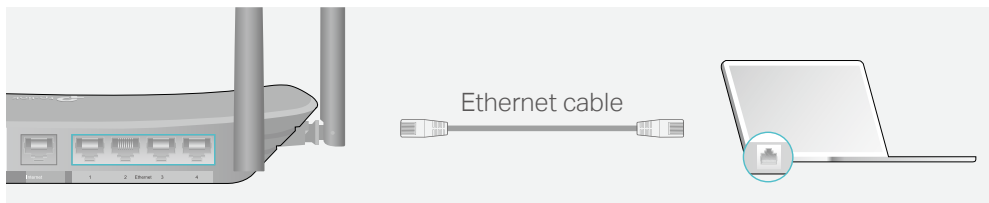
Note:

If the 2.4G LED and 5G LED are off, press and hold the WPS/Wi-Fi On/Off button on the back for about 3 seconds and then release the button. Both LEDs should turn solid on.

6. Connect your computer to the router.

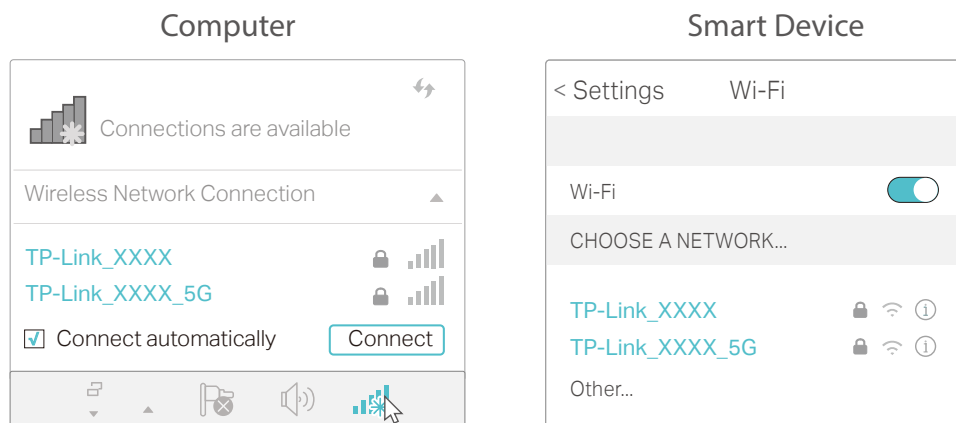
• **Method 1: Wired**

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 cards, can be connected to your router through this method.

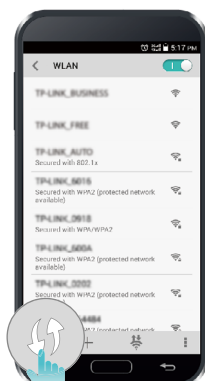
Note:

- WPS is not supported by iOS devices.

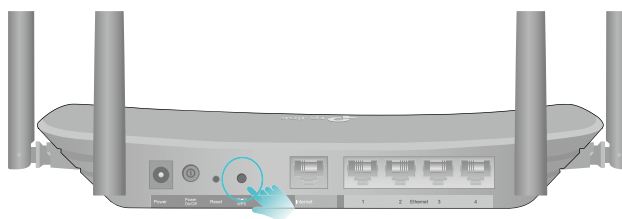
- The WPS function cannot be configured if the wireless function of the router is disabled. Also, the WPS function will be disabled if your wireless encryption is WEP. Please make sure the wireless function is enabled and is configured with the appropriate encryption before configuring the WPS.

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.



close to



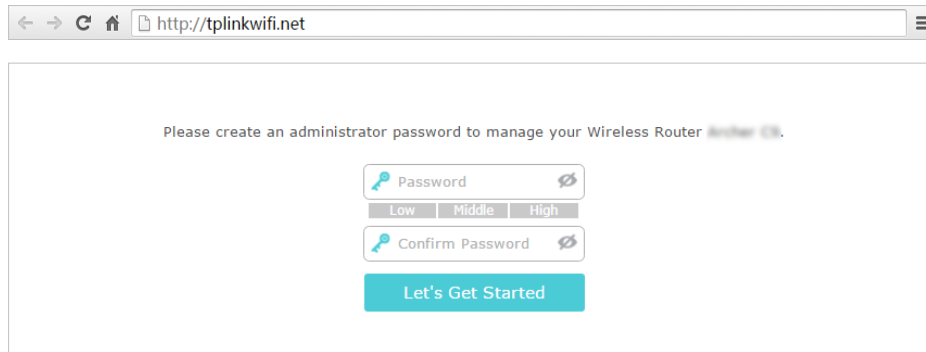
Chapter 3

Log In to Your Router

With a web-based utility, it is easy to configure and manage the router. The web-based utility can be used on any Windows, Mac OS 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 following text: "Please create an administrator password to manage your Wireless Router Router OS." Below this text is a form with 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.

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](#)
- [Configure the Router in Access Point Mode](#)

4.1. Use Quick Setup Wizard

The Quick Setup Wizard will guide you 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.

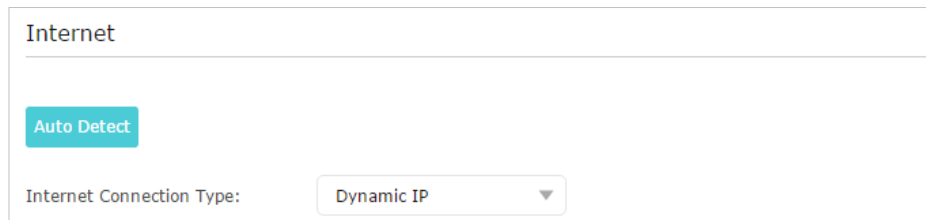
1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Click **Quick Setup** on the top of the page. Then follow the step-by-step instructions to connect your router to the internet.

4.2. Manually Set up Your Internet Connection

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

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

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

Do NOT Clone MAC Address

Clone Current Computer MAC Address

Note: If you are not sure about which Internet Connection Type you have, use Auto Detect or contact your Internet Service Provider (ISP) for assistance.

[Save](#)

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

Internet

[Auto Detect](#)

Internet Connection Type:

IP Address:

Subnet Mask:

Default Gateway:

Primary DNS:

Secondary DNS: (Optional)

Note: If you are not sure about which Internet Connection Type you have, use Auto Detect or contact your Internet Service Provider (ISP) for assistance.

[Save](#)

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

Internet

Auto Detect

Internet Connection Type:

Username:

Password:

Note: If you are not sure about which Internet Connection Type you have, use Auto Detect or contact your Internet Service Provider (ISP) for assistance.

Save

- 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.

Internet

Auto Detect

Internet Connection Type:

Username:

Password:

Secondary Connection: **Dynamic IP** **Static IP**

VPN Server IP/Domain Name:

Note: If you are not sure about which Internet Connection Type you have, use Auto Detect or contact your Internet Service Provider (ISP) for assistance.

Save

- 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.

Internet

Auto Detect

Internet Connection Type: PPTP

Username:

Password:

Secondary Connection: Dynamic IP Static IP

VPN Server IP/Domain Name:

Note: If you are not sure about which Internet Connection Type you have, use Auto Detect or contact your Internet Service Provider (ISP) for assistance.

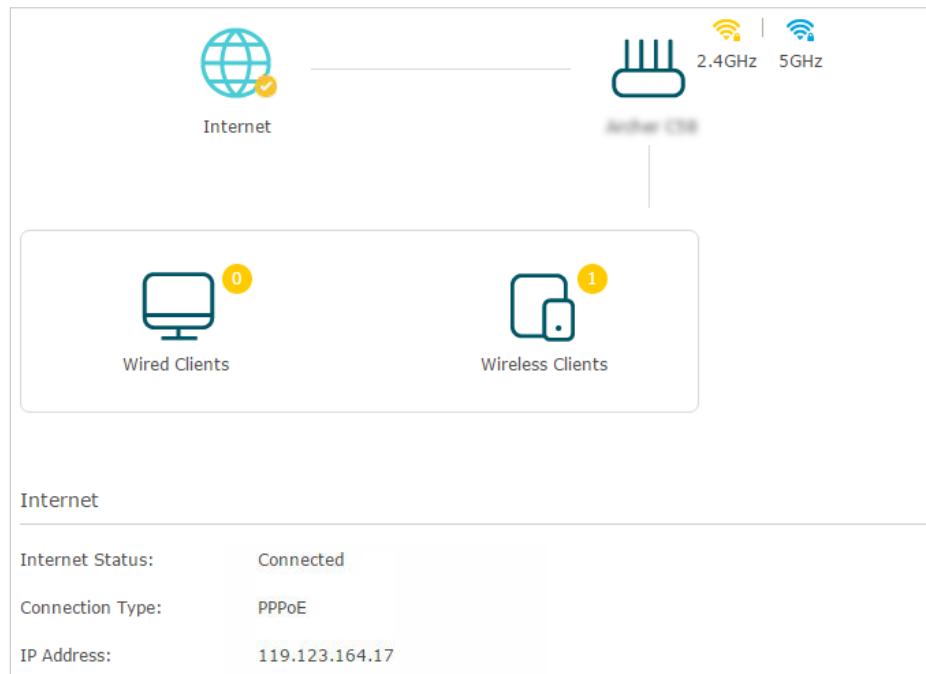
Save

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, Pass-Through (Bridge).

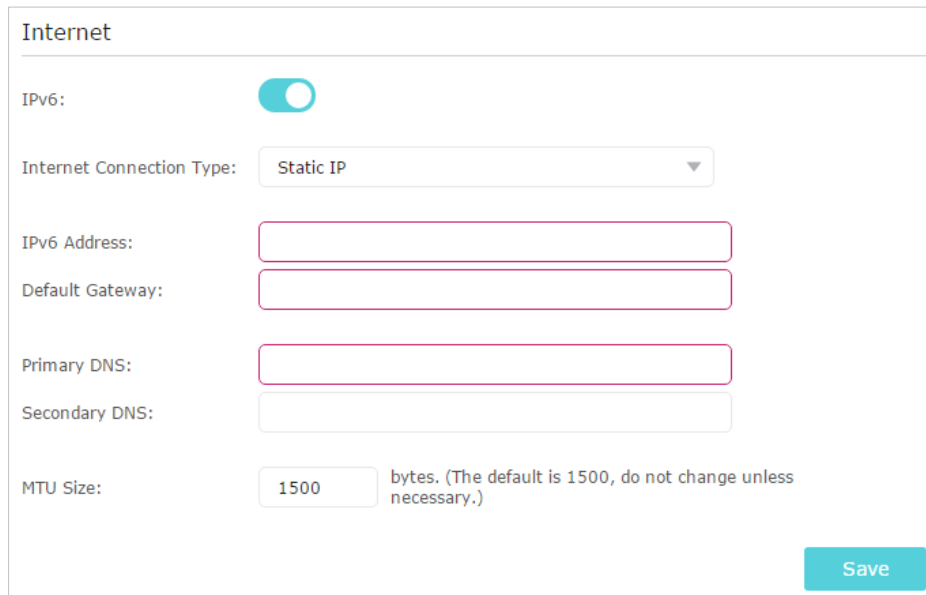
1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced > IPv6](#).
3. Enable IPv6 and select the internet connection type provided by your ISP.

☞ **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 'Internet' is displayed. Below it, the 'IPv6' toggle switch is turned on. The 'Internet Connection Type' is set to 'Static IP'. There are five input fields: 'IPv6 Address', 'Default Gateway', 'Primary DNS', and 'Secondary DNS', all of which are currently empty and have a red border. The 'MTU Size' is set to '1500' bytes, with a note that says '(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 panel. At the top, the title 'Internet' is displayed. Below it, the 'IPv6' toggle switch is turned on. The 'Internet Connection Type' dropdown menu is set to 'Dynamic IP (SLAAC/DHCPv6)'. Below this, the 'IPv6 Address', 'Primary DNS', and 'Secondary DNS' fields are all set to '::'. There are two buttons: 'Renew' (highlighted in teal) and 'Release' (greyed out). At the bottom left, there is a 'Advanced' section with a downward arrow icon. At the bottom right, there is a 'Save' button (highlighted in teal).

- 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 untick the [Use the same session with IPv4 connection](#) checkbox and manually enter the username and password for the IPv6 connection.

The screenshot shows the 'Internet' configuration panel. At the top, the title 'Internet' is displayed. Below it, the 'IPv6' toggle switch is turned on. The 'Internet Connection Type' dropdown menu is set to 'PPPoE'. Below this, there is a checked checkbox labeled 'PPPoE same session with IPv4 connection'. Below that, the 'IPv6 Address' field is set to '::'. There is an 'Advanced' section with a downward arrow icon. At the bottom left, there are two buttons: 'Connect' (highlighted in teal) and 'Disconnect' (greyed out). At the bottom right, there is a 'Save' button (highlighted in 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](#).

Internet

IPv6:

Internet Connection Type: 6to4 Tunnel

IPv4 Address: 0.0.0.0

IPv4 Subnet Mask: 0.0.0.0

IPv4 Default Gateway: 0.0.0.0

TUNNEL ADDRESS: ::

Advanced

Connect Disconnect

Save

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

Internet

IPv6:

Internet Connection Type: Pass-Through (Bridge)

Save

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

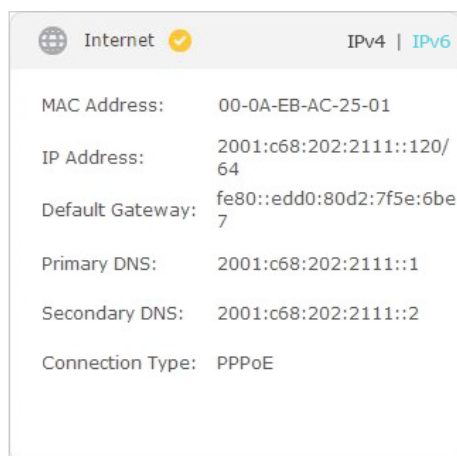
Assigned Type: DHCPv6 **SLAAC+Stateless DHCP** SLAAC+RDNSS

Address Prefix: /64

Address: ::/0

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.



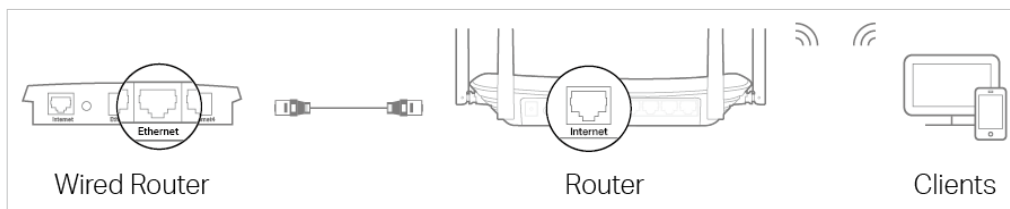
📌 **Tips:**

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

4.4. Configure the Router in Access Point Mode

In Access Point mode, the device can be connected to a wired network and transform the wired access into wireless one to extend the wireless coverage of your existing network. Advanced functions like NAT, Parental Controls and QoS are not supported in this mode.

If you already have a wired router, you can use this mode. To switch to Access Point mode:



1. Connect the router's Internet port to your wired router's Ethernet port via an Ethernet cable as shown above. And power on the router.
2. Connect a computer to the router via an Ethernet cable or wirelessly by using the SSID (network name) and Wireless Password printed on the label at the bottom of the router.
3. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
4. Go to **Advanced > Operation Mode**, select **Access Point** and click **Save**. Log in to the router via <http://tplinkwifi.net> after the router reboots.
5. Go to **Quick Setup** or **Settings > Wireless > Wireless Settings** and set the SSIDs and passwords for the wireless network.

Now, you can connect to the SSIDs and enjoy your existing network.

Chapter 5

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](#)

5. 1. Create a Network for Guests

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

Wireless 2.4GHz | 5GHz

2.4GHz Wireless: Enable Guest Network

Network Name (SSID): Hide SSID

Security: No Security WPA/WPA2-Personal

Version: Auto WPA-PSK WPA2-PSK

Encryption: Auto TKIP AES

Password:

[Save](#)

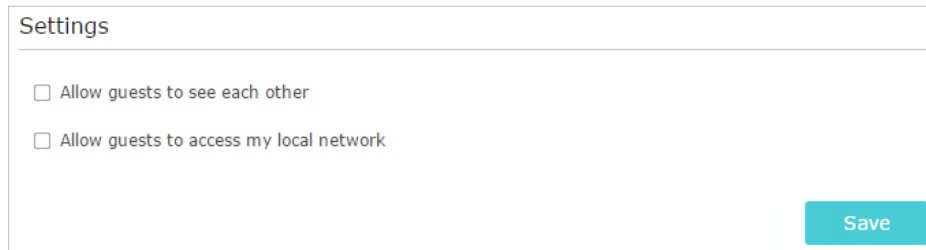
4. Click [Save](#). Now your guests can access your guest network using the SSID and password you set!

Tips:

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

5.2. Customize Guest Network Options

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [Guest Network](#). Locate the [Settings](#) section.
3. Customize guest network options according to your needs.



The screenshot shows a web interface titled "Settings" for the Guest Network. It contains two checkboxes, both of which are unchecked. The first checkbox is labeled "Allow guests to see each other" and the second is labeled "Allow guests to access my local network". A teal "Save" button is located in the bottom right corner of the settings area.

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

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

- [Allow guests to access my local network](#)

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

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

 **Tips:**

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

Chapter 6

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 the password you set for the router.
2. Go to **Advanced > Parental Controls** and enable **Parental Controls**.

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

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

Device Name: **View Existing Devices**

MAC Address:

Internet Access Time: (Optional)

Enable This Entry

Cancel **OK**

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

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

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

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

Time

Cancel Reset Save

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

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

Content Restriction

Restriction Policy: Blacklist **Whitelist**

Tips:

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

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

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

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

Content Restriction

Restriction Policy: Blacklist Whitelist

[+ Add a New Domain Name](#)

[-](#)

[Save](#)

Done!

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

Chapter 7

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 section:

- [Prioritize Internet Traffic with QoS](#)

7. 1. Prioritize Internet Traffic with QoS

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

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

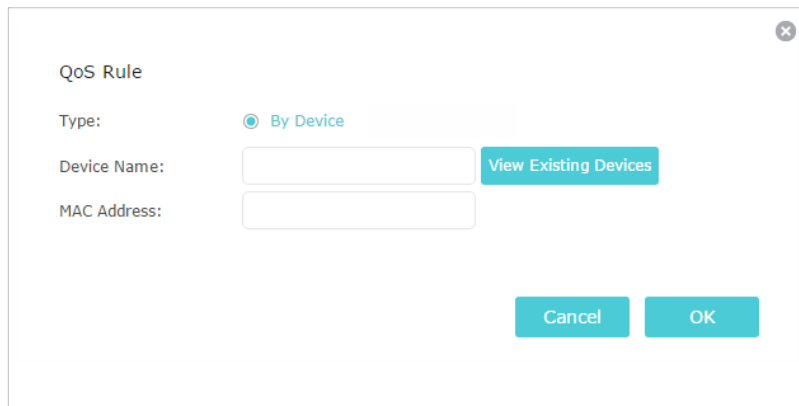
For example, I have several devices that are connected to my wireless network. I would like to set an intermediate speed on the internet for my phone.

How can I do that?

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

The screenshot shows the QoS configuration page. At the top, there is a section for 'QoS' with a checkbox for 'Enable QoS' which is checked. Below this, there are two input fields for 'Upload Bandwidth' and 'Download Bandwidth', both set to '1000' with a unit dropdown menu set to 'Mbps'. There is a toggle for 'Advanced' which is currently turned off. Below the advanced toggle, there are three sliders for priority levels: 'High Priority' is set to 60%, 'Middle Priority' is set to 30%, and 'Low Priority' is set to 10%. A 'Save' button is located at the bottom right of the configuration area.

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



QoS Rule

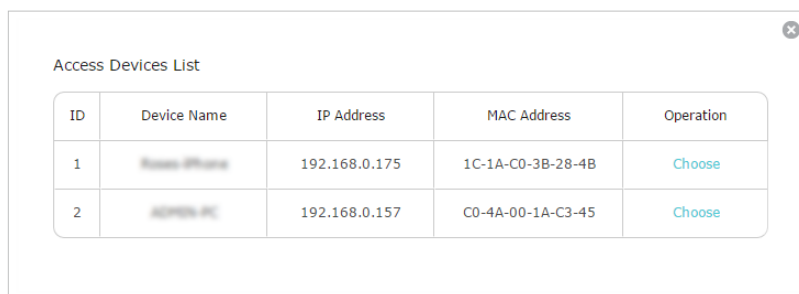
Type: By Device

Device Name: [View Existing Devices](#)

MAC Address:

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

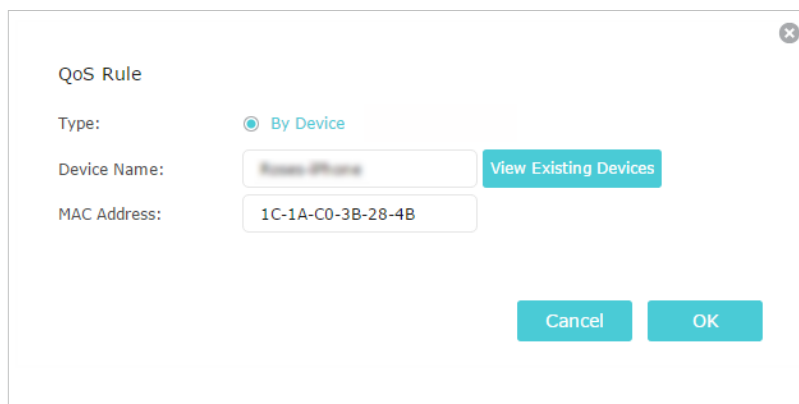
2) Choose the respective device from the list.



Access Devices List

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

3) Click **OK**.



QoS Rule


Type: By Device

Device Name: [View Existing Devices](#)

MAC Address:

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

 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.

Chapter 8

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](#)

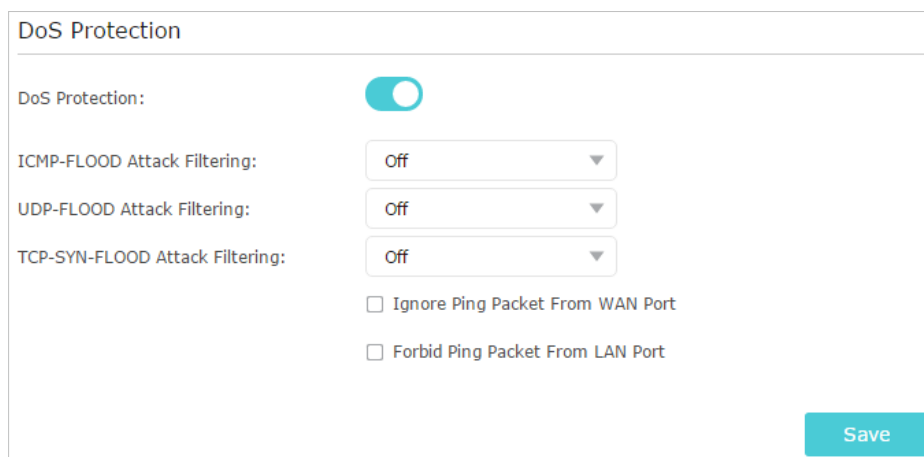
8.1. Protect the Network from Cyber Attacks

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

The SPI Firewall can prevent cyber attacks and validate the traffic that is passing through the router based on the protocol. This function is enabled by default, and it's recommended to keep the default settings.

DoS Protection can protect your home network against DoS attacks from flooding your network with server requests. Follow the steps below to configure DoS Protection.

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



DoS Protection

DoS Protection:

ICMP-FLOOD Attack Filtering:

UDP-FLOOD Attack Filtering:

TCP-SYN-FLOOD Attack Filtering:

Ignore Ping Packet From WAN Port

Forbid Ping Packet From LAN Port

Save

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

 **Tips:**

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

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

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

8.2. Access Control

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

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

How can I do that?

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

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

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

To block specific device(s)

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

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

- Select the device(s) to be blocked in the [Online Devices](#) table by ticking the 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		
<input type="checkbox"/>	2	ADMIN-PC	192.168.0.157	C0-4A-00-1A-C3-45	Wireless		

To allow specific device(s)

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

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

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

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

- 3) Click **OK**.

Done!

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

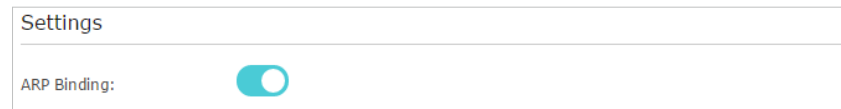
8.3. IP & MAC Binding

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 the password you set for the router.
2. Go to [Advanced](#) > [Security](#) > [IP & MAC Binding](#).
3. Enable [ARP Binding](#).



Settings

ARP Binding:

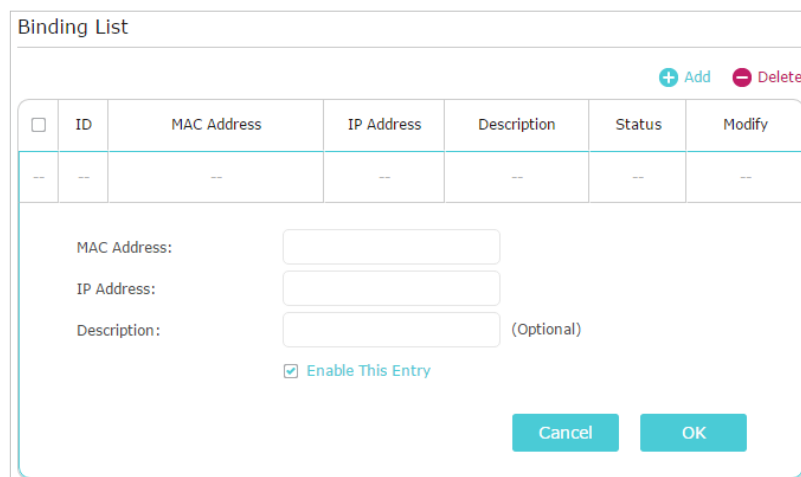
4. Bind your device(s) according to your need.

To bind the connected device(s):

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

To bind the unconnected device

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



Binding List

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

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

MAC Address:

IP Address:

Description: (Optional)

[Enable This Entry](#)

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

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

Done!

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

Chapter 9

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](#)

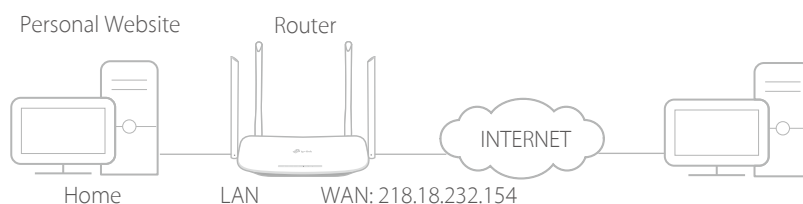
9.1. Share Local Resources on the Internet by Virtual Servers

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 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.

9.2. Open Ports Dynamically by Port Triggering

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

Follow the steps below to configure the Port Triggering rules:

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

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

4. Click [OK](#).

Port Triggering

+ Add - Delete

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

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

Triggering Port: 47624 (XX,1-65535)

Triggering Protocol: ALL

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

External Protocol: ALL

Enable This Entry

Cancel OK

Tips:

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

9.3. Make Applications Free from Port Restriction by DMZ

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

Note:

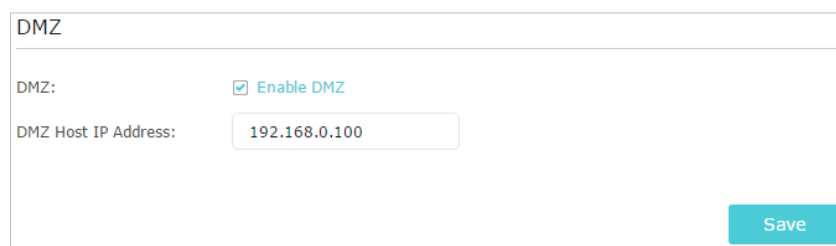
When DMZ is enabled, the DMZ host is totally exposed to the internet, which may bring some potential safety hazards. If DMZ is not in use, please disable it in time.

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

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

How can I do that?

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



DMZ

DMZ: Enable DMZ

DMZ Host IP Address:

Save

5. Click **Save**.

Done!

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

9.4. Make Xbox Online Games Run Smoothly by UPnP

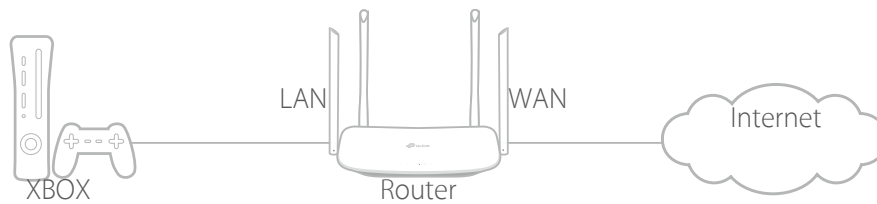
The UPnP (Universal Plug and Play) protocol allows applications or host devices to automatically find the front-end NAT device and send request to it to open the corresponding ports. With UPnP enabled, the applications or host devices on the local network and the internet can freely communicate with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

☞ Tips:

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

For example, when you connect your Xbox to the router which has connected to the internet to play online games, UPnP will send request to the router to open the

corresponding ports allowing the following data penetrating the NAT to transmit. Therefore, you can play Xbox online games without a hitch.



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

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

UPnP

UPnP:

UPnP Service List

Total Clients: 0 [Refresh](#)

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

Chapter 10

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.

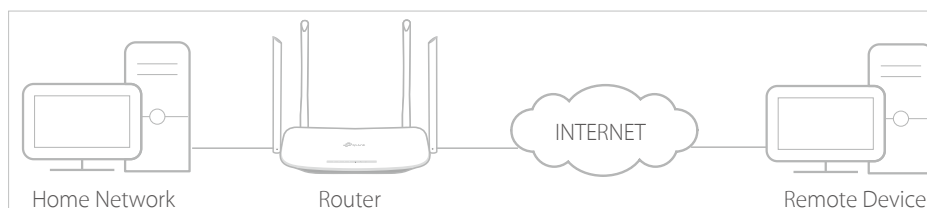
PPTP VPN is more easily used and its speed is faster, it's compatible with most operating systems and also supports mobile devices. Its security is poor and your packets may be cracked easily, and PPTP VPN connection may be prevented by some ISP.

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](#)

10.1. 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.



10.1.1. Step1. Set up OpenVPN Server on Your Router

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

OpenVPN

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

Enable VPN Server

Service Type: **UDP** TCP

Service Port:

VPN Subnet/Netmask:

Client Access: **Home Network Only** Internet and Home Network

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.
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

10. 1. 2. 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.

10. 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.

10. 2. 1. Step 1. Set up PPTP VPN Server on Your Router

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

PPTP VPN

Enable VPN Server

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

⬆️ **Advanced**

Allow Samba (Network Place) access:

Allow NetBIOS passthrough:

Allow Unencrypted connections:

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. Click [Advanced](#) to set the PPTP connection permission according to your needs.
 - Select [Allow Samba \(Network Place\) access](#) to allow your VPN device to access your local Samba server.
 - Select [Allow NetBIOS passthrough](#) to allow your VPN device to access your Samba server using NetBIOS name.
 - Select [Allow Unencrypted connections](#) to allow unencrypted connections to your VPN server.
5. Click [Save](#).
6. Configure the PPTP VPN connection account for the remote device, you can create up to 16 accounts.

Account List (up to 16 users)

+ Add - Delete

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

Username:

Password:

Cancel **OK**

<input type="checkbox"/>	1	admin	admin	✎ 🗑️
--------------------------	---	-------	-------	--