



# User Guide

3G/4G Wireless N Router  
TL-MR3420

# Contents

About This Guide .....	1
<b>Chapter 1. Get to Know About Your Router .....</b>	<b>2</b>
1. 1. Product Overview.....	3
1. 2. Panel Layout.....	3
1. 2. 1.Top View .....	3
1. 2. 2.The Side and Back Panel .....	5
<b>Chapter 2. Connect the Hardware .....</b>	<b>6</b>
2. 1. Position Your Router .....	7
2. 2. Connect Your Router.....	7
2. 2. 1.Plug and Play via 3G/4G USB Modem .....	7
2. 2. 2.Connect to DSL/Cable/Satellite Modem .....	8
<b>Chapter 3. Set Up Internet Connection .....</b>	<b>10</b>
3. 1. Log In to the Router .....	11
3. 2. Use Quick Setup Wizard .....	11
3. 3. Set Up IPv6 Tunnel.....	12
3. 3. 1.Use the Public IPv6 Tunnel Service-6to4.....	12
3. 3. 2.Specify the 6rd Tunnel with Parameters Provided by Your ISP .....	13
<b>Chapter 4. Guest Network.....</b>	<b>14</b>
4. 1. Create a Network for Guests .....	15
4. 2. Customize Guest Network Options.....	15
<b>Chapter 5. Parental Controls .....</b>	<b>17</b>
<b>Chapter 6. Bandwidth Control .....</b>	<b>21</b>
6. 1. Set Upstream and Downstream Bandwidth.....	22
6. 2. Controlling Rules .....	22
<b>Chapter 7. USB Settings.....</b>	<b>24</b>
7. 1. Access the USB Storage Device .....	25
7. 1. 1.Access the USB Device Locally.....	25
7. 1. 2.Access the USB Device Remotely .....	26
7. 1. 3.Customize Access Settings .....	28

7.2.	Media Sharing .....	31
7.3.	Printer Sharing.....	32

**Chapter 8. Network Security ..... 36**

8.1.	Protect the Network from Cyber Attacks .....	37
8.2.	Service Filtering .....	38
8.3.	Access Control .....	38
8.4.	IP & MAC Binding .....	40
8.5.	Yandex DNS .....	41

**Chapter 9. NAT Forwarding..... 43**

9.1.	Share Local Resources on the Internet by Virtual Servers.....	44
9.2.	Open Ports Dynamically by Port Triggering.....	45
9.3.	Make Applications Free from Port Restriction by DMZ .....	46
9.4.	Make Xbox Online Games Run Smoothly by UPnP .....	47

**Chapter 10.VPN..... 49**

**Chapter 11.Customize Your Network Settings..... 52**

11.1.	Change the LAN Settings .....	53
11.2.	Specify DHCP Server Settings .....	53
11.3.	Set Up a Dynamic DNS Service Account .....	55
11.4.	Create Static Routes.....	55
11.5.	Specify Wireless Settings.....	57
11.6.	Use WPS for Wireless Connection .....	58
11.6.1.	Use the WPS Wizard for Wi-Fi Connections.....	58
11.6.2.	Use the PIN for Wi-Fi connections.....	59
11.7.	Schedule Your Wireless Function .....	59

**Chapter 12.Manage the Router ..... 61**

12.1.	Set Up System Time .....	62
12.2.	Change Operation Mode.....	63
12.3.	Test the Network Connectivity .....	63
12.4.	Upgrade the Firmware .....	63
12.4.1.	Online Upgrade .....	64
12.4.2.	Manual Upgrade .....	64
12.5.	Backup and Restore Configuration Settings.....	65
12.6.	Auto Reboot.....	66
12.7.	Change the Login Password .....	66
12.8.	Local Management .....	67

12. 9. Remote Management.....	68
12. 10. System Log.....	68
12. 11. Monitor the Internet Traffic Statistics.....	70
<b>FAQ .....</b>	<b>72</b>







# 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, <b>Advanced</b> > <b>Wireless</b> > <b>MAC Filtering</b> means the MAC Filtering function page is under the Wireless menu that is located in the Advanced tab.
 <b>Note:</b>	Ignoring this type of note might result in a malfunction or damage to the device.
 <b>Tips:</b>	Indicates important information that helps you make better use of your device.
symbols on the web page	<ul style="list-style-type: none"><li> click to edit the corresponding entry.</li><li> click to delete the corresponding entry.</li><li> click to enable or disable the corresponding entry.</li><li> click to view more information about items on the page.</li></ul>

## 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.

This chapter 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 the 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.

## 1.2. Panel Layout

### 1.2.1. Top View








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

#### LED Explanation

Name	Status	Indication
⏻ (Power)	On	Power is on.
	Off	Power is off.

## LED Explanation

Name	Status	Indication
 (Wi-Fi)	On	The wireless function is enabled.
	Off	The wireless function is disabled.
 (LAN)	On	At least one powered-on device is connected to a LAN port.
	Off	No powered-on device is connected to a LAN port.
 (Internet)	Green	The internet is available.
	Off	The WAN port is not connected.
	Red	The WAN port is connected, but the internet is not available.
 (USB)	On	The inserted USB device is ready to use.
	Flashing	The USB device is being detected.
	Off	No device is plugged into the USB port.
 (WPS)	On	A device is connected to the router successfully using WPS.
	Quick Flashing	A device fails to connect to the router using WPS.
	Slow Flashing	A device is being connecting to the router using WPS. This process takes up to 2 minutes.
	Off	No WPS connection is established.



## 1.2.2. The Side and Back Panel



The following parts (view from left to right) are located on the rear and side 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/off the router.
WAN Port	For connecting to a DSL/Cable modem, or an Ethernet jerk.
Ethernet Ports (1-4)	For connecting the router to your PC or other Ethernet network devices.
WIFI Button	Press this button to turn on/off the Wi-Fi of the router.
WPS/RESET Button	Press this button, and immediately press the WPS button on your device to establish WPS connection.
	Press this button for about 5 seconds to factory reset the router.
USB Port	For connecting to a 3G/4G modem or a USB disk.
Antennas	Upright the antennas for best Wi-Fi performance.

## Chapter 2

---

# Connect the Hardware

---

This chapter contains the following sections:

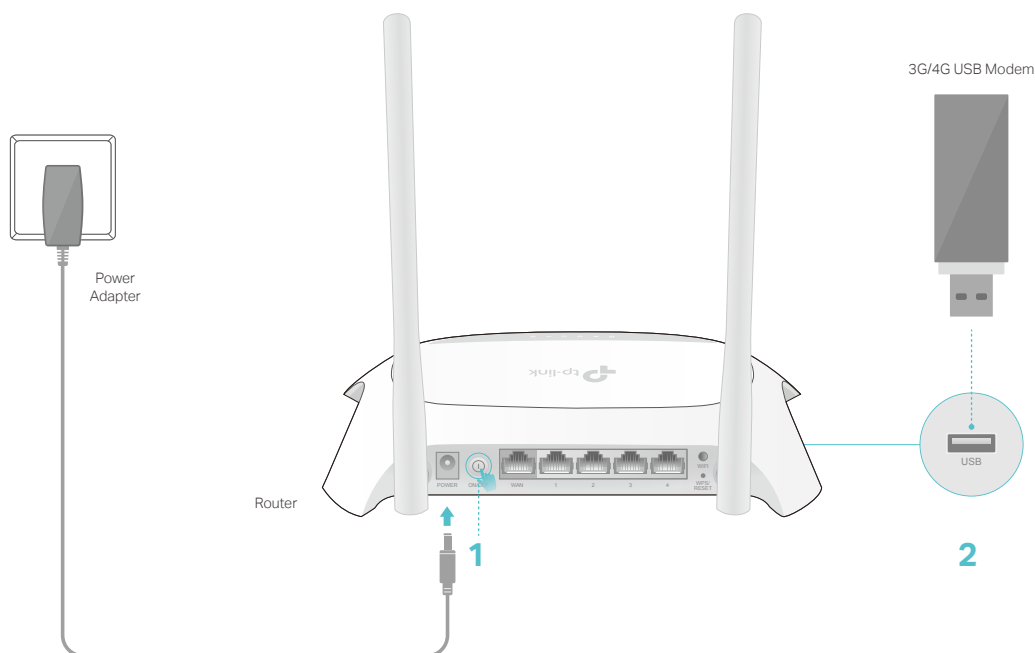
- [Position Your Router](#)
- [Connect Your Router](#)

## 2.1. Position Your Router

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

## 2.2. Connect Your Router

### 2.2.1. Plug and Play via 3G/4G USB Modem

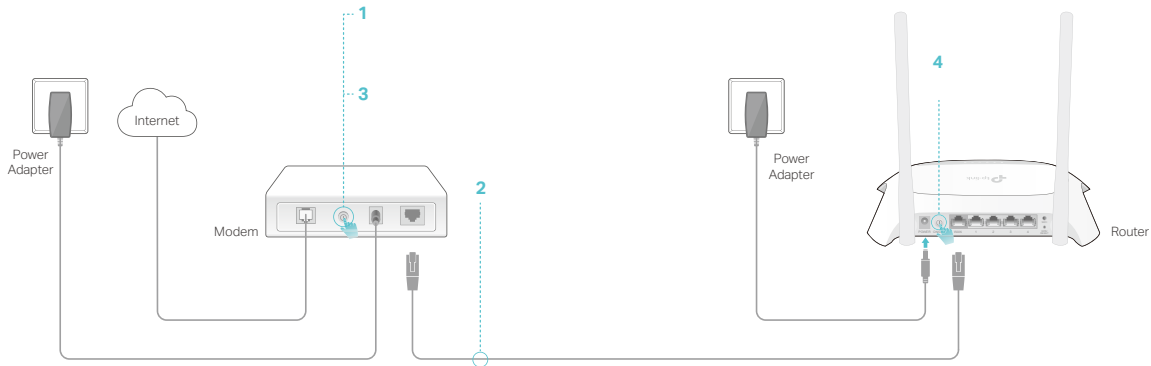


- 1) Press to turn on the router.
- 2) Plug in a 3G/4G USB modem with a SIM/UIM card.
- 3) Wait about 2 minutes and then confirm that the following LEDs are on and solid.



**Note:**

- If the Internet LED (🌐) is off or red, please refer to [FAQ](#).
- If the Wi-Fi LED (📶) is off, press the Wi-Fi button on the rear panel and then check the LED again.
- You can find the latest modem compatibility list in our website: <http://www.tp-link.com/en/comp-list.html>.

**2. 2. 2. Connect to DSL/Cable/Satellite Modem**

- 1) Power off the modem and remove the backup battery if it has one.
- 2) Connect the modem to the router's WAN port via an Ethernet cable.
- 3) Turn on the modem and then wait about 2 minutes for it to restart.
- 4) Press to turn on the router.
- 5) Confirm that the following LEDs are on and solid to verify the hardware connection is correct.

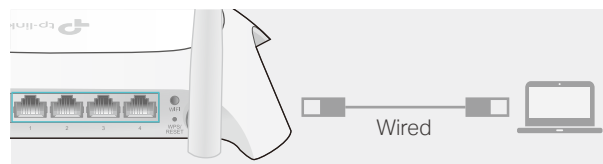


**Note:** If the Wi-Fi LED (📶) is off, press the WIFI button on the rear panel and then check the LED again.

1. Connect your computer to the router.

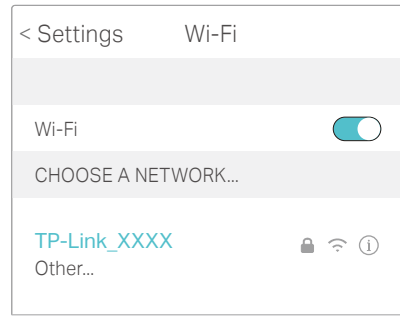
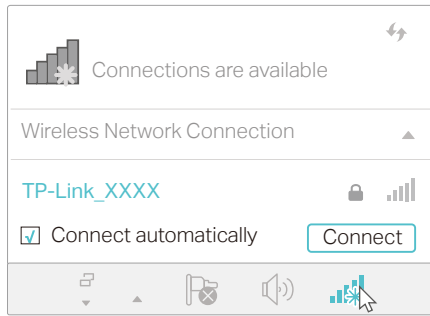
- **Method 1: Wired**

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 the Wi-Fi settings of your smart device, and then select the SSID to join the network.



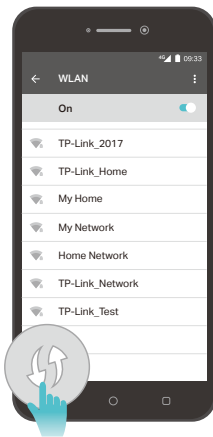
- **Method 3: Use the WPS button**

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

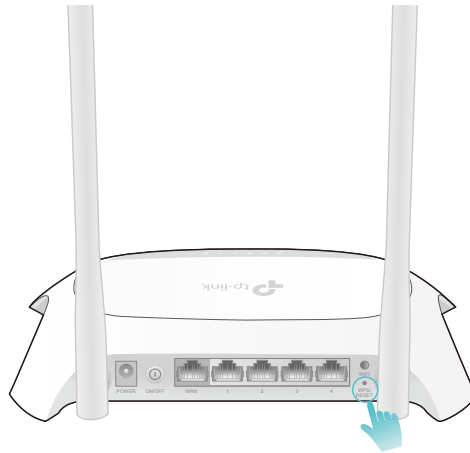
**Note:**

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



Close to



## Chapter 3

---

# 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 many ISP information built in, automates many of the steps and verifies that those steps have been successfully completed.

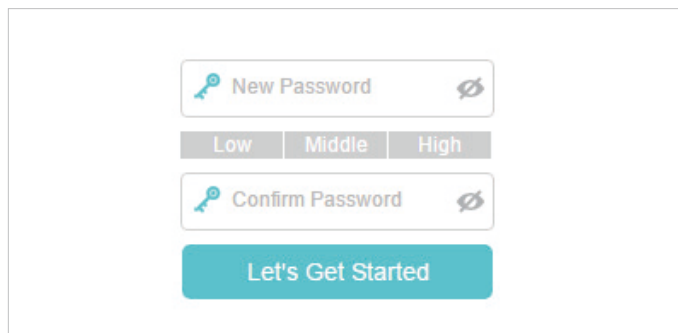
It contains the following sections:

- [Log In to the Router](#)
- [Use Quick Setup Wizard](#)
- [Set Up IPv6 Tunnel](#)

## 3.1. Log In to the Router

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

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



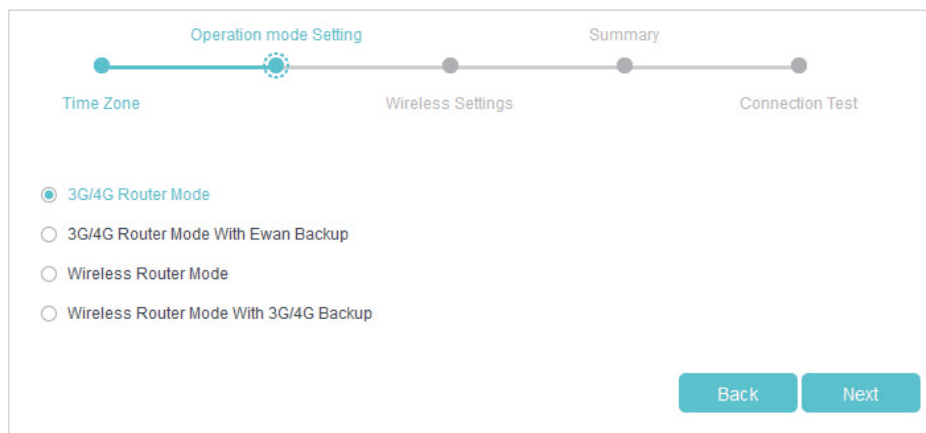
3. Follow the step-by-step instructions to set up your router to access the internet.

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

## 3.2. Use Quick Setup Wizard

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Quick Setup](#), select your [Time zone](#) and click [Next](#) to continue.
3. Select the [Operation Mode](#) as needed and click [Next](#). Then follow the screen instructions to complete the configuration.



■ **Note:** The router can be configured with a primary WAN/3G/4G connection and a 3G/4G USB modem/WAN connection as a backup solution to ensure “always on” internet. In this case, select [3G/4G Router Mode with Ewan Backup](#) or [Wireless Router Mode with 3G/4G Backup](#).

## 3.3. Set Up IPv6 Tunnel

The IPv6 Tunnel feature helps you obtain IPv6 resources based on an IPv4 WAN connection or vice versa.

IPv6 Tunnel is a transition mechanism that allows isolated IPv6 hosts and networks to reach each other over IPv4-only infrastructure before IPv6 completely supplants IPv4. It is a temporary solution for networks that do not support native dual-stack, where both IPv6 and IPv4 run independently.

The router provides three tunneling mechanisms: [6to4](#), [6rd](#) and [DS-Lite](#). The way to set up 6rd and DS-Lite tunnel are similar.

### 3.3.1. Use the Public IPv6 Tunnel Service-6to4

The 6to4 tunnel is a kind of public service. If there are any 6to4 servers on your network, you can use this mechanism to access IPv6 service. If your ISP provides you with an IPv4-only connection but you want to visit IPv6 websites, you can try to set up a 6to4 tunnel.

**I want to:** Set up the IPv6 tunnel though my ISP doesn't provide me with the tunnel service.

**How can I do that?**

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [Network](#) > [IPv6 Tunnel](#).
3. Tick the check box, select [6to4](#) as the tunneling mechanism and select a WAN connection from the drop-down list, then click [Save](#).

**Note:** If there is no available WAN connection to choose, make sure you have connected to the internet.

**Done!** Now you can visit the IPv6 websites with the 6to4 tunnel.

**Note:** Still not being able to access IPv6 resources means that not any 6to4 public server was found in your network. You can contact your ISP to sign up for IPv6 connection service.



### 3.3.2. Specify the 6rd Tunnel with Parameters Provided by Your ISP

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

**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](#) > [Network](#) > [IPv6 Tunnel](#).
3. Tick the check box, select [6rd](#) as the tunneling mechanism and select a WAN connection from the drop-down list.
4. According to the parameters provided by your ISP, choose [Auto](#) or [Manual](#). More parameters are needed if you choose [Manual](#).
5. Click [Save](#).

IPv6 Tunnel

Note: You must reconfigure the IPv6 Tunnel settings every time you reboot the router. Make sure the desired WAN connection is connected before the configuration.

IPv6 Tunnel:  Enable

Tunneling Mechanism:

WAN Connection:

Configuration Type:  Auto  Manual

IPv4 Mask Length:

6rd Prefix:

6rd Prefix Length:

Border Relay IPv4 Address:

[Save](#)

**Note:**

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

**Done!**

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

**Tips:** The way to set up DS-Lite tunnel is similar to that of 6rd tunnel. If you are provided with an IPv6-only WAN connection and have signed up for DS-Lite tunnel service, specify the DS-Lite tunnel by referring to the steps above.

## Chapter 4

---

# Guest Network

---

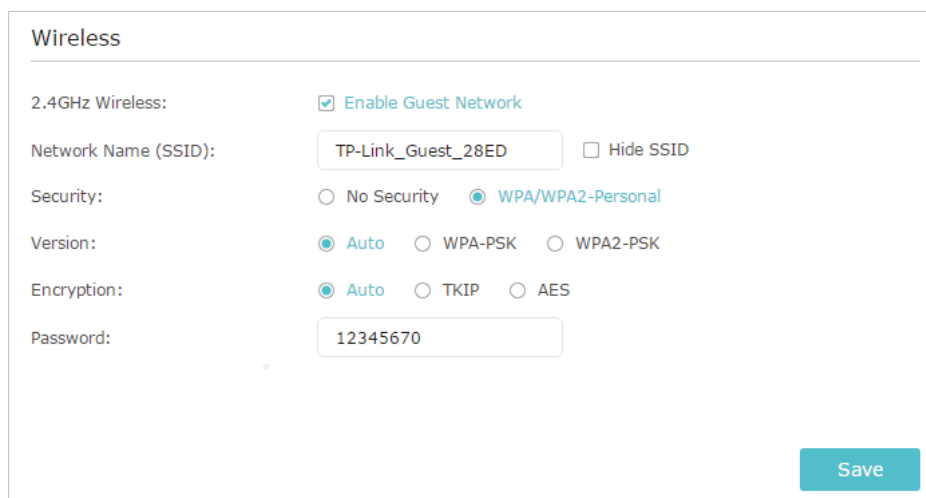
This function allows you to provide Wi-Fi access for guests without disclosing your main network. When you have guests in your house, apartment, or workplace, you can create a guest network for them. In addition, you can customize guest network options to ensure network security and privacy.

It contains the following sections:

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

## 4. 1. Create a Network for Guests

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [Guest Network](#). Locate the [Wireless](#) section.
3. Create a guest network as needed.
  - 1) 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.



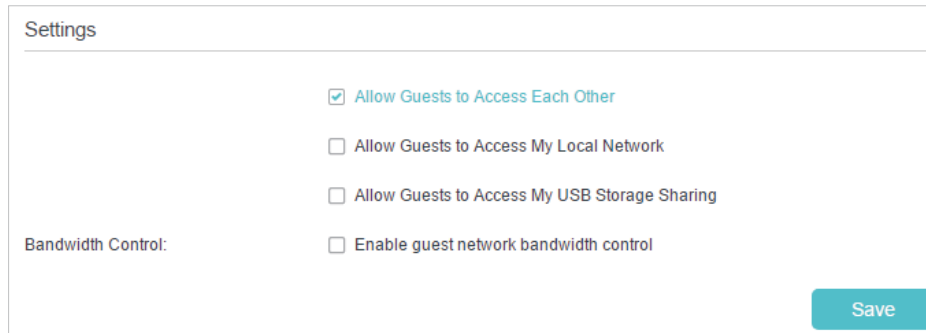
The screenshot shows the 'Wireless' configuration page for a guest network. The '2.4GHz Wireless' section is active, and the 'Enable Guest Network' checkbox is checked. The 'Network Name (SSID)' is set to 'TP-Link\_Guest\_28ED', and the 'Hide SSID' checkbox is unchecked. The 'Security' is set to 'WPA/WPA2-Personal', with 'Auto' selected for both 'Version' and 'Encryption'. The 'Password' field contains '12345670'. 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.

## 4. 2. Customize Guest Network Options

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



Settings

Allow Guests to Access Each Other

Allow Guests to Access My Local Network

Allow Guests to Access My USB Storage Sharing

Bandwidth Control:  Enable guest network bandwidth control

Save

- [Allow Guests to Access 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.

- [Allow Guests to Access My USB Storage Sharing](#)

Tick this checkbox if you want to allow the wireless clients on your guest network to access your files on the USB disk connected to your router.

- [Enable guest network bandwidth control](#)

Tick this checkbox if you want to apply the Bandwidth Control settings to the wireless devices on your guest network .

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

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

## Chapter 5

---

# Parental Controls

---

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

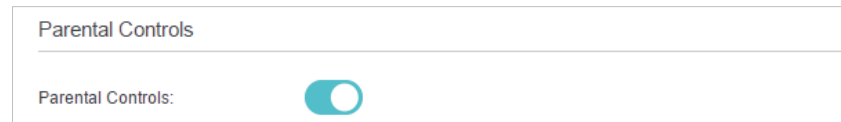
**I want to:**

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](http://www.tp-link.com) and [Wikipedia.org](http://Wikipedia.org) from 18:00 (6PM) to 22:00 (10PM) at the weekend and not other times.

**How can I do that?**

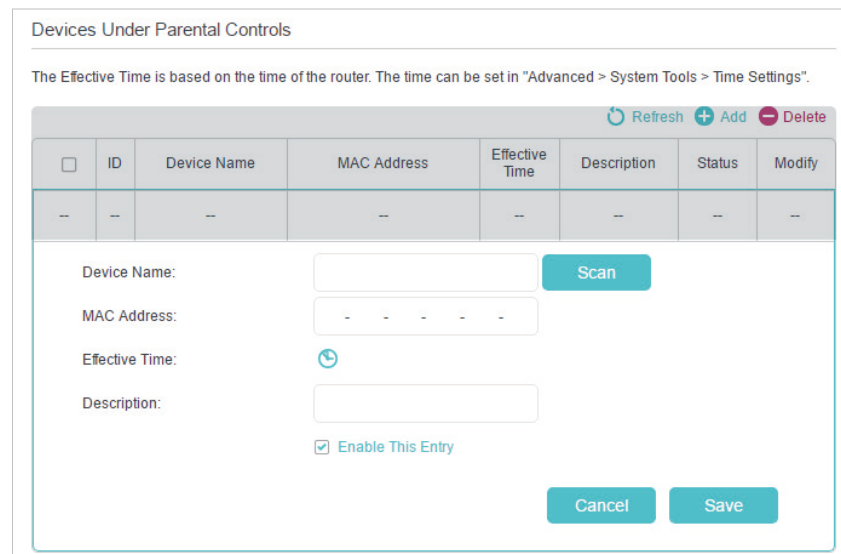
1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to **Advanced > Parental Controls** and enable **Parental Controls**.



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

The Effective Time is based on the time of the router. The time can be set in "Advanced > System Tools > Time Settings".

Refresh + Add - Delete

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

Device Name:  **Scan**


MAC Address:

Effective Time:

Description:

Enable This Entry

**Cancel** **Save**

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

System Time: 05/22/2017 09:47:14

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
0:00							
1:00							
2:00							
3:00							
4:00							
5:00							
6:00							
7:00							
8:00							
9:00							
10:00							
11:00							
12:00							
13:00							
14:00							
15:00							
16:00							
17:00							
18:00							
19:00							
20:00							
21:00							
22:00							
23:00							
24:00							

Effective Time

Reset OK

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

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 Keyword](#) . 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 Keyword

-

Save

**Done!**

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



## Chapter 6

---

# Bandwidth Control

---

This chapter introduces how to set bandwidth limits minimize the impact caused when the connection is under heavy load.

It contains the following sections:

- [Set Upstream and Downstream Bandwidth](#)
- [Controlling Rules](#)

## 6.1. Set Upstream and Downstream Bandwidth

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced > Bandwidth Control](#).
3. Enable [Bandwidth Control](#) and enter the [Total Upstream Bandwidth](#) and [Total Downstream Bandwidth](#).

Bandwidth Control

Bandwidth Control:  Enable

Total Upstream Bandwidth:  Kbps

Total Downstream Bandwidth:  Kbps

[Save](#)

4. Click [Save](#).

## 6.2. Controlling Rules

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced > Bandwidth Control](#).
3. Click [Add](#) and fill in the blanks.

Controlling Rules

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

<input type="checkbox"/>	IP Range/Port Range	Priority	Up (min/max)	Down (min/max)	Status	Modify
<input type="checkbox"/>	--	--	--	--	--	--

IP Range:  -

Port Range:  -  (1-65535)

Protocol:

Priority:  (1 means the highest priority.)

Upstream:  to  Kbps

Downstream:  to  Kbps

Enable This Entry

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

- **IP Range:** Enter the IP range of your devices that you want to apply Bandwidth Control to.
- **Port Range:** Enter the Port range of the protocols.
- **Protocal:** Select the protocols of services that you want to control.
- **Priority:** Select priority from 1 to 5. 1 means the highest priority.
- **Upstream/Downstream:** Enter the minimun and maxmium upstream/downstream bandwidth you want to allocate.

4. Click **Save**.

## Chapter 7

---

# USB Settings

---

This chapter describes how to use the USB ports to share files, media and a printer from the USB storage devices over your home network locally, or remotely through the internet.

The router supports USB external flash drives, hard drives and USB printers.

It contains the following sections:

- [Access the USB Storage Device](#)
- [Media Sharing](#)
- [Printer Sharing](#)

## 7.1. Access the USB Storage Device

Insert your USB storage device into the router's USB port and then access files stored there locally or remotely.

### 🔗 Tips:

- If you use USB hubs, make sure no more than 4 devices are connected to the router.
- If the USB storage device requires using bundled external power, make sure the external power has been connected.
- If you use a USB hard drive, make sure its file system is FAT32, exFat, NTFS or HFS+.
- Before you physically disconnect a USB device from the router, safely remove it to avoid data damage: Go to [Advanced](#) > [USB Settings](#) > [Device Settings](#) and click [🔌 Safely Remove](#).

### 7.1.1. Access the USB Device Locally

Insert your USB storage device into the router's USB port and then refer to the following table to access files stored on your USB storage device.

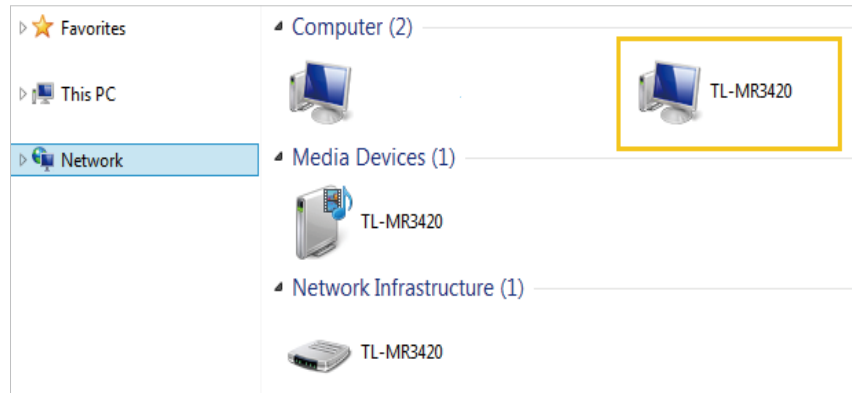
#### Windows computer

#### ➤ Method 1:

Go to [Computer](#) > [Network](#), then click the Network Server Name (TL-MR3420 by default) in the [Computer](#) section.

#### 📌 Note:

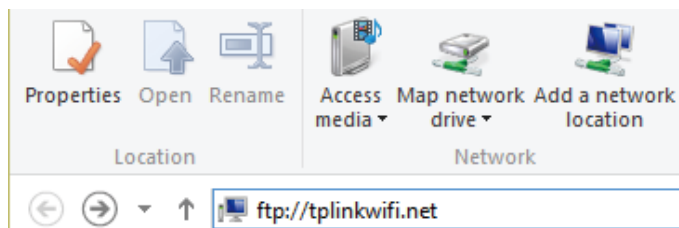
Operations in different systems are similar. Here we take Windows 8 as an example.



Windows  
computer

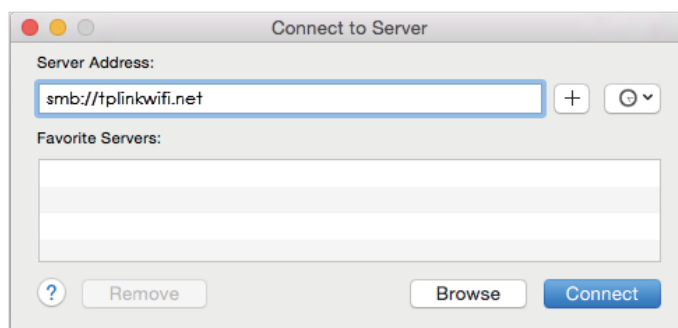
## ➤ Method 2:

Open the [Windows Explorer](#) (or go to [Computer](#)) and type the server address [\\tplinkwifi.net](#) or [ftp://tplinkwifi.net](#) in the address bar, then press [Enter](#).



## Mac

- 1) Select [Go > Connect to Server](#).
- 2) Type the server address [smb://tplinkwifi.net](#).
- 3) Click [Connect](#).



- 4) When prompted, select the [Guest](#) radio box. (If you have set up a username and a password to deny anonymous access to the USB disks, you should select the [Registered User](#) radio box. To learn how to set up an account for the access, refer to [To set up authentication for data security](#).)

## Tablet

Use a third-party app for network files management.

🔗 **Tips:** You can also access your USB disk by using your Network/Media Server Name as the server address. Refer to [To customize the address of the USB disk](#) to learn more.

## 7.1.2. Access the USB Device Remotely

You can access your USB disk outside the local area network. For example, you can:

- Share photos and other large files with your friends without logging in to (and paying for) a photo-sharing site or email system.
- Get a safe backup for the materials for a presentation.
- Remove the files on your camera's memory card from time to time during the journey.

**Note:** If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), you cannot use this feature because private addresses are not routed on the Internet.

Follow the steps below to configure remote access settings.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to **Advanced > USB Sharing > USB Storage Device**.
3. Tick the **FTP(via Internet)** checkbox, and then click **Save**.

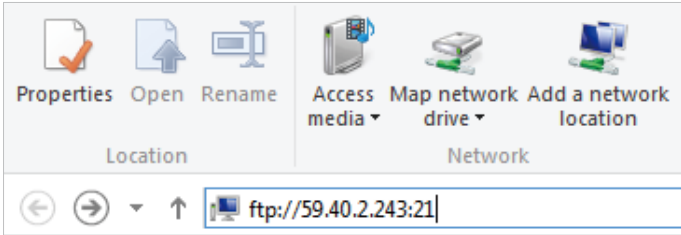
Sharing Settings

---

Network/Media Server Name:

Enable	Access Method	Access Address	Port
<input checked="" type="checkbox"/>	Media Server	--	--
<input checked="" type="checkbox"/>	Network Neighborhood	\\TL-MR3420	--
<input checked="" type="checkbox"/>	FTP	ftp://192.168.1.1:21	<input type="text" value="21"/>
<input checked="" type="checkbox"/>	FTP(via Internet)	ftp://0.0.0.0:21	21

4. Refer to the following table to access your USB disk remotely.

Computer	<ol style="list-style-type: none"> <li>1) Open the <a href="#">Windows Explorer</a> (or go to <a href="#">Computer</a>, only for Windows users) or open a web browser.</li> <li>2) Type the server address in the address bar: Type in <code>ftp://&lt;WAN IP address of the router&gt;:&lt;port number&gt;</code> (such as <code>ftp://59.40.2.243:21</code>). If you have specified the domain name of the router, you can also type in <code>ftp://&lt;domain name&gt;:&lt;port number&gt;</code> (such as <code>ftp://MyDomainName:21</code>)</li> </ol> <div data-bbox="549 525 1230 758" style="text-align: center; border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  <p>The screenshot shows the Windows Explorer interface. At the top, there are two tabs: 'Location' and 'Network'. The 'Location' tab is active, showing icons for 'Properties', 'Open', and 'Rename'. The 'Network' tab shows icons for 'Access media', 'Map network drive', and 'Add a network location'. Below the tabs is a navigation pane with back, forward, and up arrows. The address bar contains the text 'ftp://59.40.2.243:21'.</p> </div> <ol style="list-style-type: none"> <li>3) Press <a href="#">Enter</a> on the keyboard.</li> <li>4) Access with the username and password you set in <a href="#">To set up authentication for data security</a>.</li> </ol> <p><b>Tips:</b> You can also access the USB disk via a third-party app for network files management, which can resume broken file transfers.</p>
	Tablet

**Tips:** Click [Set Up a Dynamic DNS Service Account](#) to learn how to set up a domain name for your router.

### 7.1.3. Customize Access Settings

By default, all the network clients can access all folders on your USB disk. You can customize your sharing settings by setting a sharing account, sharing specific contents and setting a new sharing address on the router's web management page.

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

➤ **To customize the address of the USB disk:**

You can customize the server name and use the name to access your USB disk.

1. On the Sharing Settings part, make sure [Network Neighborhood](#) is ticked, and enter a Network/Media Server Name as you like, such as [MyShare](#), then click [Save](#).



Sharing Settings

Network/Media Server Name:

Enable	Access Method	Access Address	Port
<input checked="" type="checkbox"/>	Media Server	--	--
<input checked="" type="checkbox"/>	Network Neighborhood	\\MyShare	--
<input checked="" type="checkbox"/>	FTP	ftp://192.168.1.1:21	<input type="text" value="21"/>
<input checked="" type="checkbox"/>	FTP(via Internet)	ftp://0.0.0.0:21	21

- Now you can access the USB disk by visiting <\\MyShare> (for Windows) or <smb://MyShare> (for Mac).
- **To only share specific content:**
- Focus on the [Folder Sharing](#) section. Click the button to disable [Share All](#), then click [Add](#) to add a new sharing folder.

Folder Sharing

Share All:

<input type="checkbox"/>	ID	Folder Name	Folder Path	Media Sharing	Volume Name	Status	Modify
--	--	--	--	--	--	--	--

Volume Name:

Folder Path:

Folder Name:

Enable Authentication



Enable Write Access

Enable Media Sharing

- Select the [Volume Name](#) and [Folder Path](#), then enter a [Folder Name](#) as you like.
- Decide the way you share the folder:

- **Enable Authentication:** Tick to enable authentication for this folder sharing, and you will be required to log in to the Sharing Account to access the USB disk. Refer to [To set up authentication for data security](#) to learn more.
- **Enable Write Access:** If you tick this checkbox, network clients can modify this folder.
- **Enable Media Sharing:** Tick to enable media sharing for this folder, and you can view photos, play music and watch movies stored on the USB disk directly from DLNA-supported devices. Click [Media Sharing](#) to learn more.




#### 4. Click **OK**.

 **Tips:** The router can share 32 volumes at most. You can click  on the page to detach the corresponding volume you do not need to share.

Folder Sharing

Share All:

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

<input type="checkbox"/>	ID	Folder Name	Folder Path	Media Sharing	Volume Name	Status	Modify
<input type="checkbox"/>	1	SHARE	G:/media_server	On	sda1		 

#### ➤ **To set up authentication for data security:**

You can set up authentication for your USB device so that network clients will be required to enter username and password when accessing the USB disk.


1. On the Sharing Account part, Choose [Use Default Account](#) or [Use New Account](#). The username and password are both [admin](#) for default account. If your choose [Use New Account](#), you have to customize the username and a password.

Sharing Account

Content sharing requires a sharing account. You can use the login account or create a new one.

Account:  [Use Default Account](#)  
 [Use New Account](#)

Username:

Password:   (Same as Login Password)

[Save](#)

#### **Note:**

For Windows users, do not set the sharing username the same as the Windows username. Otherwise, Windows credential mechanism may cause the following problems:

- If the sharing password is also the same as the Windows password, authentication will not work since the Windows will automatically use its account information for USB access.
- If the sharing password is different from the Windows password, the Windows will be unable to remember your credentials and you will always be required to enter the sharing password for USB access.

2. Enable **Authentication** to apply the account you just set.
  - If you leave **Share All** enabled, click the button to enable **Authentication** for all folders.

Folder Sharing

Share All:

Enable Authentication:

- If **Share All** is disabled, enable **Authentication** for specific folders.

Folder Sharing

Share All:

+ Add - Delete

<input type="checkbox"/>	ID	Folder Name	Folder Path	Media Sharing	Volume Name	Status	Modify
--	--	--	--	--	--	--	--

Volume Name:

Folder Path:

Folder Name:

Enable Authentication

Enable Write Access


Enable Media Sharing

**Note:** Due to Windows credential mechanism, you might be unable to access the USB disk after changing Authentication settings. Please log out from the Windows and try to access again. Or you can change the address of the USB disk by referring to [To customize the address of the USB disk](#).

## 7.2. Media Sharing

The feature of **Media Sharing** allows you to view photos, play music and watch movies stored on the USB disk directly from DLNA-supported devices, such as your computer, tablet and PS2/3/4.

1. When your USB disk is inserted into the router, your DLNA-supported devices (such as your computer and pad) connected to the router can detect and play the media files on the USB disks.
2. Refer to the following table for detailed instructions.

Windows Computer	<ul style="list-style-type: none"> <li>Go to <b>Computer &gt; Network</b>, then click the Media Server Name (TL-MR3420 by default) in the <b>Media Devices</b> section.</li> </ul> <p><b>Note:</b> Here we take Windows 8 as an example.</p>  <p>The screenshot shows the Windows 8 Network view. On the left, the 'Network' link is selected. The main area displays three categories: 'Computer (2)', 'Media Devices (1)', and 'Network Infrastructure (1)'. Under 'Media Devices (1)', a device icon labeled 'TL-MR3420' is highlighted with a yellow box.</p>
Tablet	<ul style="list-style-type: none"> <li>Use a third-party DLNA-supported player.</li> </ul>

## 7.3. Printer Sharing

The feature of Printer Sharing helps you share a printer with different computers connected to the router.

**Note:** Printers unlisted on this page may be incompatible with the router:  
<http://www.tp-link.com/common/compatible/print-server/>.

### 1. Install the Driver of the Printer

Make sure you have installed the driver of the printer on each computer that needs printer service.

If you do not have the driver, contact the printer manufacturer.

### 2. Connect the Printer

Cable a printer to the USB port with the USB cable. Wait several seconds until the USB LED becomes solid on.

### 3. Install the TP-Link USB Printer Controller Utility

TP-Link USB Printer Controller Utility helps you access the shared printer. Download and install the utility on each computer that needs printer service.

1) Visit <http://www.tp-link.com/app/usb/>.


2) Click **PC Utility** (for Windows users) or **Mac Utility** to download the installation file and uncompress it.

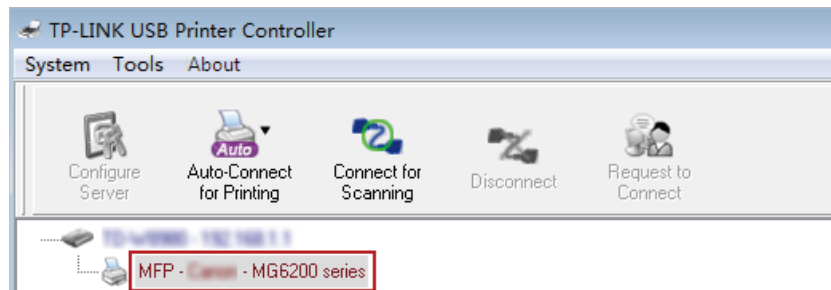


3) Open the uncompressed folder, then click [TP-Link USB Printer Controller Setup](#) (for Windows users) or [TP-Link UDS Printer Controller Installer](#) (for Mac users) to install the utility.

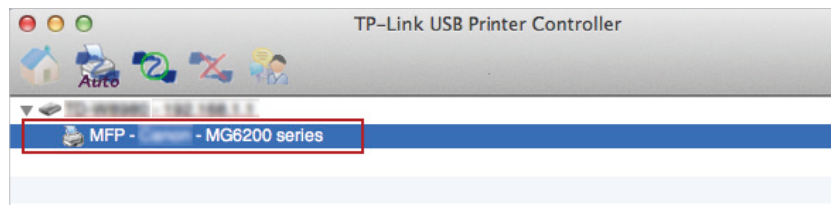
#### 4. Access the Printer

You should set the shared printer as Auto-Connect Printer on every computer that needs printer service.

- 1) Double-click the icon  on your desktop to launch the USB Printer Controller.
- 2) Highlight the printer you share.

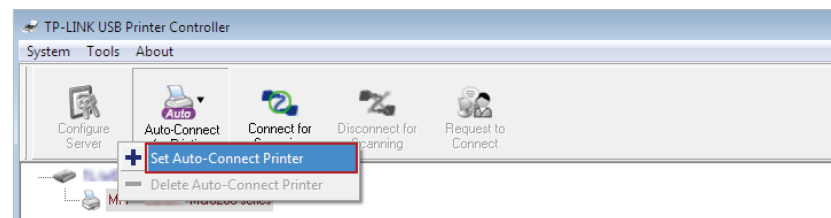


Windows

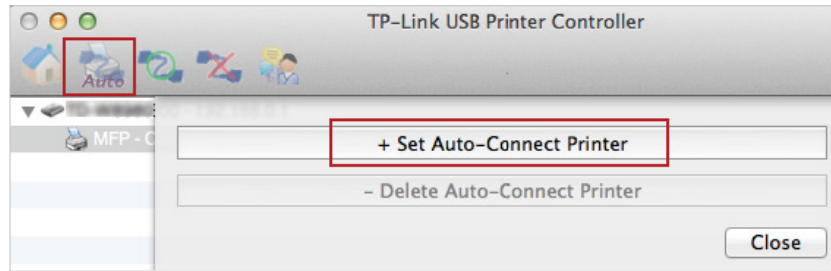


Mac

3) Click the [Auto-Connect for printing](#) tab to pull down a list, then select [Set Auto-Connect Printer](#).

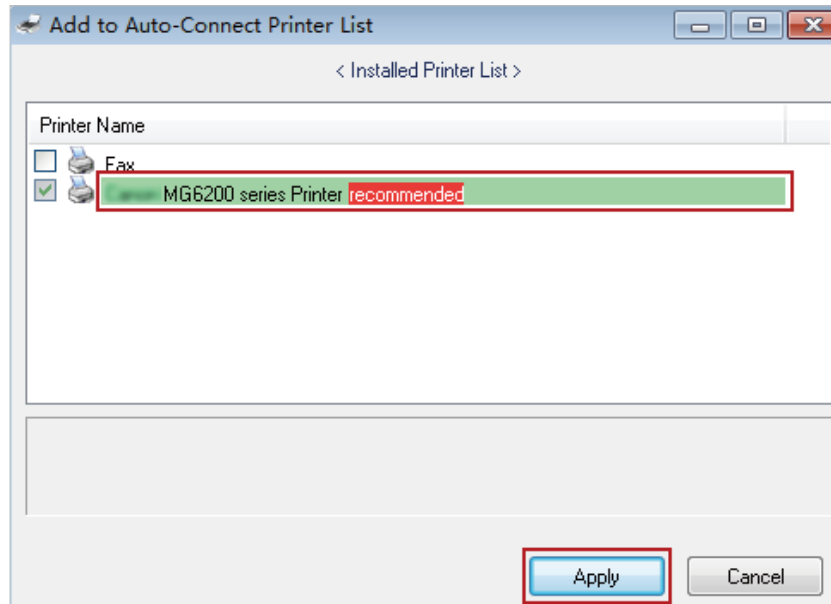


Windows

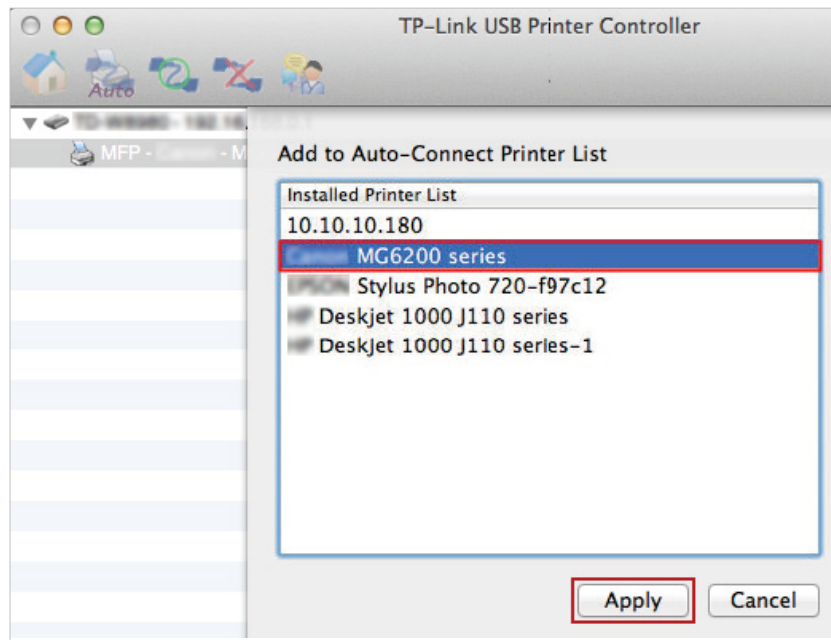


Mac

4) Select the printer you share, then click [Apply](#).

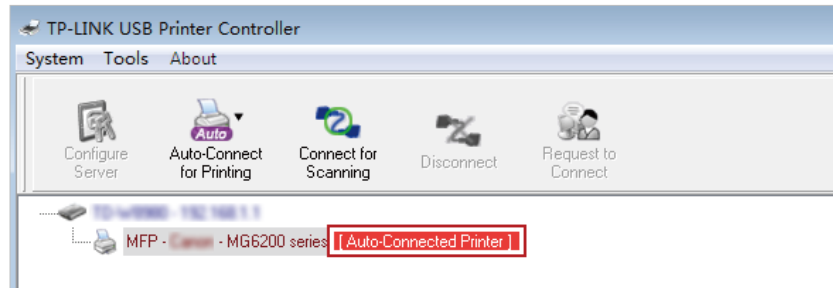


Windows



Mac

- 5) You will see the printer marked as **Auto-Connect Printer**. Now you can print with this printer.



Windows



Mac

 **Tips:**

The Print Server also allows different clients to share the scan feature of MFPs (Multi-Function Printers). To scan with **TP-Link USB Printer Controller**, right-click the printer and select **Network Scanner**. Then, a scanning window will pop up. Finish the scanning process by following on-screen instructions.

## 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](#)
- [Service Filtering](#)
- [Access Control](#)
- [IP & MAC Binding](#)
- [Yandex DNS](#)



## 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 > Firewall & DoS Protection**.
3. Enable **DoS Protection**.

DoS Protection:

DoS Protection

ICMP-Flood Attack Filtering: -Please Select-

UDP-Flood Attack Filtering: -Please Select-

TCP-Flood Attack Filtering: -Please Select-

Save

4. Set the level (**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 **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
--	--	--	--

5. Click **Save**.

## 8.2. Service Filtering

Service Filtering is used to prevent certain users from accessing a specific service. It can even block a user from accessing the internet.

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



4. Click [Add](#).

The screenshot shows the 'Filtering List' dialog box. At the top, there are buttons for 'Refresh', 'Add', and 'Delete'. Below these is a table with the following columns: ID, Service Type, Port, IP Address, Status, and Modify. The table currently contains one row with dashes in all cells. Below the table, there are several input fields: 'Service Type' (dropdown menu set to 'Any(ALL)'), 'Protocol' (dropdown menu set to 'TCP/UDP'), 'Starting Port' (text input '1' with a range '(1-65535)' to its right), 'Ending Port' (text input '65535' with a range '(1-65535)' to its right), and another 'Service Type' dropdown menu set to 'Any(ALL)'. At the bottom, there are radio buttons for 'Filter Service For': 'Single IP Address', 'IP Address Range', and 'All IP Addresses' (which is selected). There are 'Cancel' and 'Save' buttons at the bottom right.

5. Select a service type from the drop-down list and the corresponding parameters will be automatically filled in. Select Custom if your desired service type is not listed and enter the corresponding parameters.
6. Specify the IP address(es) this filtering rule will be applied to.
7. Click [Save](#).

## 8.3. Access Control

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

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

**How can I do that?**

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

Access Control

Access Control:

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

**To block specific device(s):**

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

Access Mode

Default Access Mode:  Blacklist  Whitelist

[Save](#)

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

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

Online Devices

[Refresh](#) [Block](#)

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

**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).

The screenshot shows a window titled "Devices in Whitelist". At the top right, there are "+ Add" and "- Delete" buttons. Below is a table with the following structure:

<input type="checkbox"/>	ID	Device Name	MAC Address	Modify
<input type="checkbox"/>	--	--	--	--

Below the table, there are two input fields: "Device Name:" and "MAC Address:". At the bottom right, there are "Cancel" and "OK" buttons.

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](#).

## 8.4. IP & MAC Binding

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

**I want to:**

Prevent ARP spoofing and ARP attacks.

**How can I do that?**

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

The screenshot shows the "IP & MAC Binding" settings page. The "IP & MAC Binding" toggle switch is turned on (blue).

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

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

MAC Address:

IP Address:

Enable This Entry

- 2) Enter the [MAC address](#) and [IP address](#) that you want to bind.
- 3) Tick the [Enable This Entry](#) checkbox and click [Save](#).

**Done!**

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

## 8.5. Yandex DNS

Yandex DNS filter will secure your devices from malicious websites and will restrict adult websites for your children devices. You can configure a general filtering rule for all devices or a separate one for certain devices.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [Security](#) > [Yandex DNS](#).
3. Enable [Yandex DNS](#). Select [Disable](#), [Basic](#), [Safe](#) or [Child](#) for the [Enable Yandex DNS for all devices](#).

**Note:** If [Disable](#) is selected, set Yandex DNS rules for certain devices.

Yandex DNS

Yandex DNS:

Enable Yandex DNS for all devices:

4. Click [Save](#).

➤ **To set a Yandex DNS rule for a certain device:**

1. Click [Add](#).

Yandex DNS rule for special device

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

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

MAC Address:  [Scan](#)

Control Mode:

Description:  (Optional)

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

2. Click [Scan](#) to find a connected device you want to apply this rule to. You can also manually enter the MAC address of the device if it's currently disconnected from the router.
3. Select a [Control Mode](#) and enter a description for this rule.
4. Click [Save](#).

## 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](#)

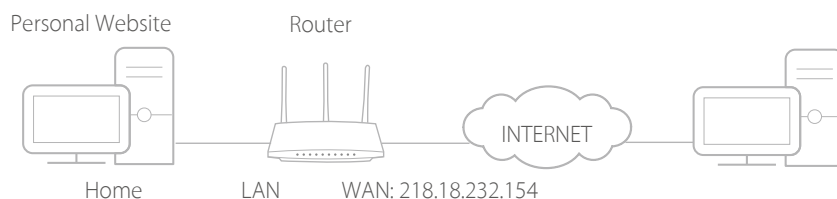
## 9.1. Share Local Resources on the Internet by Virtual Servers

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 192.168.1.100.
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 192.168.1.100 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:  [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.

## 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.

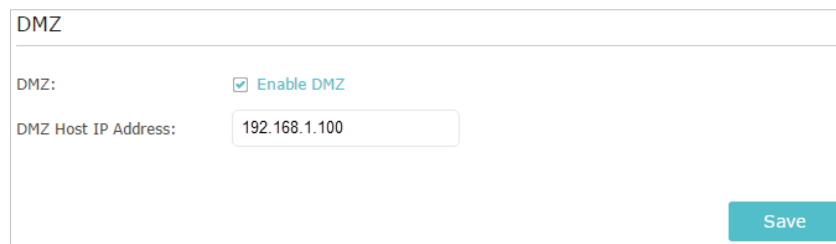
**Note:** When DMZ is enabled, the DMZ host is totally exposed to the internet, which may bring some potential safety hazards. If DMZ is not in use, please disable it in time.

**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 192.168.1.100.
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 192.168.1.100 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.

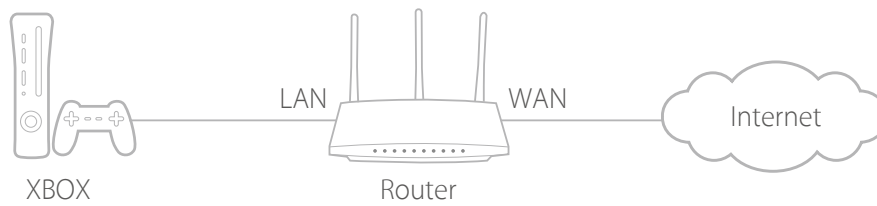
## 9.4. Make Xbox Online Games Run Smoothly by UPnP

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

---

The VPN (Virtual Private Networking) feature allows you to access your home network in a secured way through internet when you are out of home.

With IPsec VPN, you can access the network securely when out of home. To use the VPN Service, you need to configure Dynamic DNS Service or assign a static IP address for the router's WAN port. And the System Time should be synchronized with the internet.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to **Advanced > VPN > IPsec VPN**.
3. Enable **Dead Peer Detection**.

IPsec VPN

---

Dead Peer Detection:

4. Click **Add** and enter correspond parameters.

+ Add - Delete

<input type="checkbox"/>	Connection Name	Remote Gateway	Local Address	Remote Address	Status	Enable	Modify
--	--	--	--	--	--	--	--

IPsec Connection Name:

Remote IPsec Gateway (URL):

Tunnel access from local IP addresses:

IP Address for VPN:

Subnet Mask:

Tunnel access from remote IP addresses:

IP Address for VPN:

Subnet Mask:

Key Exchange Method:

Authentication Method:

Pre-Shared Key:

Perfect Forward Secrecy:

Advanced

- **IPsec Connection Name:** Enter a name for the IPsec VPN connection.
- **Remote IPsec Gateway (URL):** Enter the destination gateway IP address which is the public WAN IP or domain name of the remote VPN server endpoint.

- **Tunnel access from local IP addresses:** Select [Subnet Address](#) if you want the whole LAN to join the VPN network, or select [Single Address](#) if you want a single IP to join the VPN network.
- **IP Address for VPN:** Enter the IP address of your LAN.
- **Subnet Mask:** Enter the subnet mask of your LAN.
- **Tunnel access from remote IP addresses:** Select [Subnet Address](#) if you want the whole remote LAN to join the VPN network, or select [Single Address](#) if you want a single IP to join the VPN network.
- **IP Address for VPN:** Enter the IP address of the remote LAN.
- **IP Subnet Mask:** Enter the subnet mask of the remote LAN.
- **Key Exchange Method:** Select [Auto \(IKE\)](#) or [Manual](#) to be used to authenticate IPSec peers.
- **Authentication Method:** Select [Pre-Shared Key](#) (recommended).
- **Pre-Shared Key:** Create a pre-shared key to be used for authentication.
- **Perfect Forward Secrecy:** Select [Enable](#) or [Disable](#) as an additional security protocol for the pre-shared key.

You can configure the advanced settings as needed. It's recommended to keep the default values. If you want to change these settings, make sure that both VPN server endpoints use the same Encryption Algorithm, Integrity Algorithm, Diffie-Hellman Group and Key Lifetime in both phase1 and phase2.

5. Click [Save](#).

## Chapter 11

---

# Customize Your Network Settings

---

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

It contains the following sections:

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



## 11.1. Change the LAN Settings

The router is preset with a default LAN IP 192.168.1.1, which you can use to log in to its web management page. The LAN IP address together with the Subnet Mask also defines the subnet that the connected devices are on. If the IP address conflicts with another device on your local network or your network requires a specific IP subnet, you can change it.

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

DHCP Server

IP Version:  IPv4  IPv6

MAC Address: 50-C7-BF-44-88-81

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255.255.255.0

IGMP Snooping:  Enable

Second IP:  Enable

DHCP:  Enable

Save

4. Click [Save](#).

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

## 11.2. Specify DHCP Server Settings

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

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

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

DHCP:  Enable

DHCP Server  DHCP Relay

IP Address Pool: 192 . 168 . 1 . 100 - 192 . 168 . 1 . 199

Address Lease Time: 1440 minutes. (1-2880. The default value is 1440.)

Default Gateway: 192 . 168 . 1 . 1 (Optional)

Default Domain: (Optional)

Primary DNS: 0 . 0 . 0 . 0 (Optional)

Secondary DNS: 0 . 0 . 0 . 0 (Optional)

Save

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

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

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

Address Reservation

+ Add - Delete

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

MAC Address: - - - - - Scan

IP Address: . . . .

Group: Default

Enable This Entry

Cancel Save

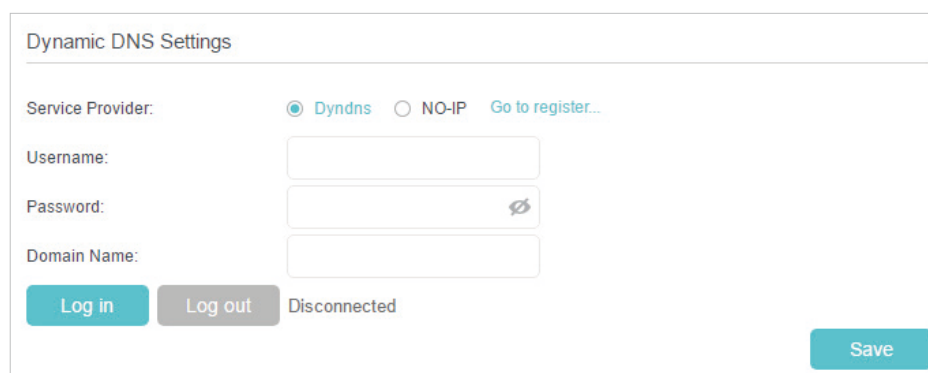
2. Click [Scan](#) to find a connected device you want to apply this rule to. You can also manually enter the MAC address of the device if it's currently disconnected from the router.
3. Enter the [IP address](#) to reserve for the client device..
4. Tick the [Enable This Entry](#) checkbox and click [Save](#).

## 11.3. Set Up a Dynamic DNS Service Account

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

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

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



Dynamic DNS Settings

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

Username:

Password:

Domain Name:

Disconnected

4. Click **Log In** and **Save**.

**Tips:** If you want to use a new DDNS account, please click **Logout** first, and then log in with a new account.

## 11.4. Create Static Routes

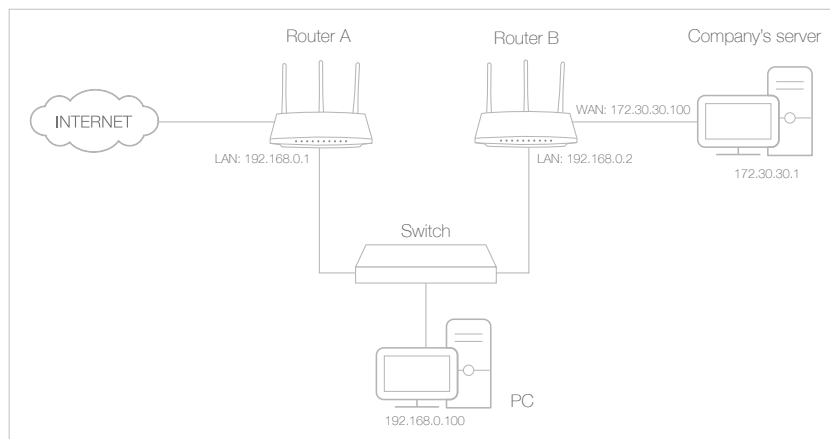
Static routing is a form of routing that is configured manually by a network administrator or a user by adding entries into a routing table. The manually-configured routing information guides the router in forwarding data packets to the specific destination.

### I want to:

Visit multiple networks and servers at the same time.

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

configure the static routing.



## How can I do that?

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

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

Network Destination: 172 . 30 . 30 . 1  
 Subnet Mask: 255 . 255 . 255 . 255  
 Gateway: 192 . 168 . 0 . 2  
 Interface: LAN

Enable This Entry

Cancel Save

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

**Subnet Mask:** Determines the destination network with the destination IP address. If the destination is a single IP address,

enter 255.255.255.255; otherwise, enter the subnet mask of the corresponding network IP. In the example, the destination network is a single IP, so here enter 255.255.255.255.

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

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

5. Click [Save](#).
6. Check the [System Routing Table](#) below. If you can find the entry you've set, the static routing is set successfully.

System Routing Table				
Active Routes Number: 3				<a href="#">Refresh</a>
ID	Network Destination	Subnet Mask	Gateway	Interface
1	172.30.30.1	255.255.255.255	192.168.0.2	lan
2	192.168.0.0	255.255.255.0	0.0.0.0	lan
3	192.168.0.2	255.255.255.255	0.0.0.0	lan

**Done!**

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

## 11.5. Specify Wireless Settings

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

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

### ➤ To enable or disable the wireless function:

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

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

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

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

➤ **To hide SSID:**

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

➤ **To change the security option:**

1. Go to [Advanced > Wireless > Wireless Settings](#).
2. Select an option from the [Security](#) drop-down list. We recommend you don't change the default settings unless necessary. If you select other options, configure the related parameters according to the help page.

**In addition**

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

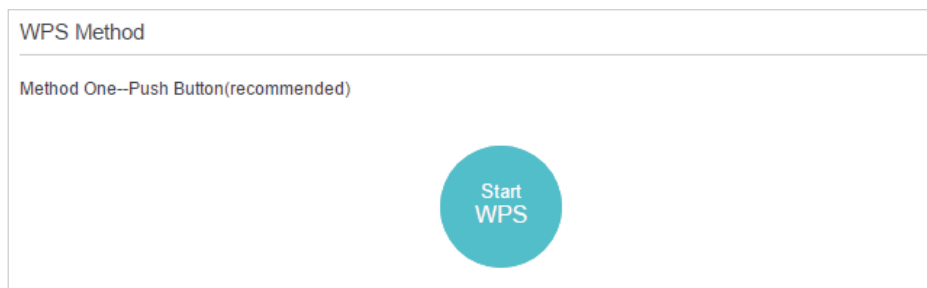
## 11.6. Use WPS for Wireless Connection

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

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

### 11.6.1. Use the WPS Wizard for Wi-Fi Connections

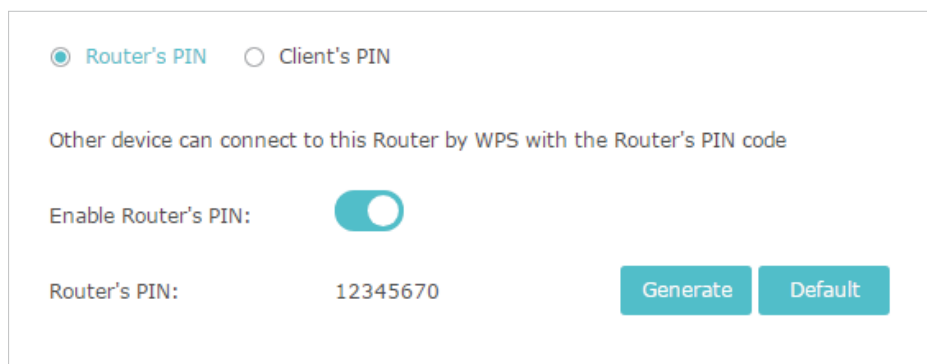
1. Click the [Start WPS](#) button on the screen. Within two minutes, press the WPS button on the client device.



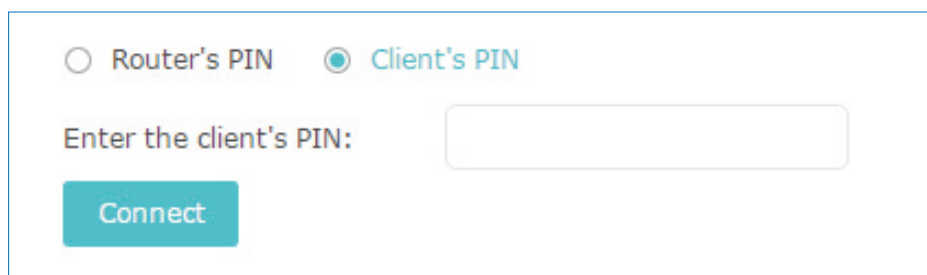
2. **Success** will appear on the above screen and the WPS LED on the router will keep on for five minutes if the client has been successfully added to the network.

### 11.6.2. Use the PIN for Wi-Fi connections

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



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



**Note:**

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

## 11.7. Schedule Your Wireless Function

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

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

Wireless Off Time

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

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

From:

To:

Repeat:  Every Day  Selected Day

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

5. Click [Save](#).



## Chapter 12

---

# Manage the Router

---

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

It contains the following sections:

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

## 12.1. Set Up System Time

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

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

➤ **To get time from the PC :**

1. Click [Get from PC](#).
2. Click [Save](#).

➤ **To get time from the internet :**

1. Select your local [Time Zone](#) from the drop-down list.

System Time

Current Time: 05/24/2017 16:42:52

Time Zone: (GMT+08:00) Beijing, Chongqing, Urumchi, Hong Kong, Taipei, Kuala Lumpur, Perth

Date: 5/24/2017 (MM/DD/YY)

Time: 16 : 42 : 47

NTP Server I: 0.0.0.0 (Optional)

NTP Server II: 0.0.0.0 (Optional)

Get from PC Get from the Internet Save

2. In the [NTP Server I](#) field, enter the IP address or domain name of your desired NTP Server.
3. (Optional) In the [NTP Server II](#) field, enter the IP address or domain name of the second NTP Server.
4. Click [Get from the Internet](#) and click [Save](#).

➤ **To set up Daylight Saving Time:**

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

Daylight Saving Time

Enable Daylight Saving Time

Start: 2017 Mar Last Sun 02:00

End: 2017 Oct Last Sun 03:00

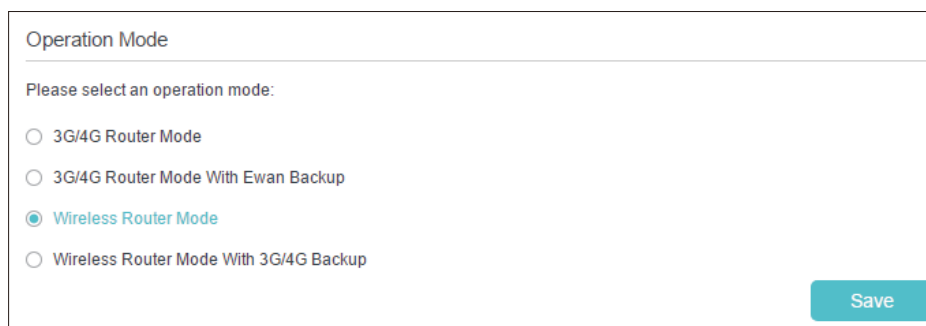
Save

2. Select the correct [Start](#) date and time when daylight saving time starts at your local time zone.
3. Select the correct [End](#) date and time when daylight saving time ends at your local time zone.
4. Click [Save](#).

## 12.2. Change Operation Mode

The router supports four operation works. Select one to best suit your network needs.

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



Operation Mode

Please select an operation mode:

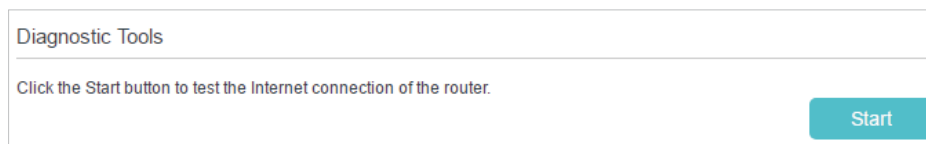
- 3G/4G Router Mode
- 3G/4G Router Mode With Ewan Backup
- Wireless Router Mode
- Wireless Router Mode With 3G/4G Backup

[Save](#)

## 12.3. Test the Network Connectivity

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

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



Diagnostic Tools

Click the Start button to test the Internet connection of the router.

[Start](#)

3. Click [Start](#) to begin the diagnostics.

## 12.4. Upgrade the Firmware


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

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

**Note:**

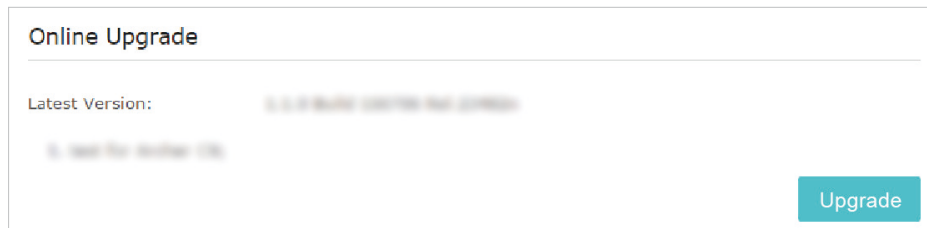
- Make sure you remove all attached USB devices from the router before the firmware upgrade to prevent data loss.
- Backup your router configuration before firmware upgrade.
- Do NOT turn off the router during the firmware upgrade.

### 12.4.1. Online Upgrade


1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. When the latest firmware is available for your router, the update icon  will display in the top-right corner of the page. Click the icon to go to the [Firmware Upgrade](#) page. Alternatively, you can go to [Advanced](#) > [System Tools](#) > [Firmware Upgrade](#), and click [Check for upgrade](#) to see whether the latest firmware is released.

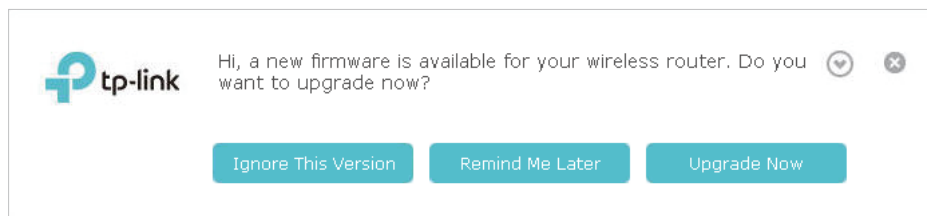


3. Focus on the [Online Upgrade](#) section, and click [Upgrade](#).



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

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



### 12.4.2. Manual Upgrade

1. Download the latest firmware file for the router from [www.tp-link.com](http://www.tp-link.com).
2. Visit <http://tplinkwifi.net>, and log in with or the password you set for the router.

3. Go to [Advanced](#) > [System Tools](#) > [Firmware Upgrade](#).
4. Focus on the Device Information section. Make sure the downloaded firmware file is matched with the [Hardware Version](#).
5. Focus on the [Local Upgrade](#) section. Click [Browse](#) to locate the downloaded new firmware file, and click [Upgrade](#).

Local Upgrade

---

New Firmware File:  [Browse](#)

[Upgrade](#)

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

## 12.5. Backup and Restore Configuration Settings

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

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

### ➤ To backup configuration settings:

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

Backup

---

Save a copy of your current settings.

[Backup](#)

### ➤ To restore configuration settings:

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

Restore

---

Restore previous settings from a saved file.

File:  [Browse](#)


[Restore](#)

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

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

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

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



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

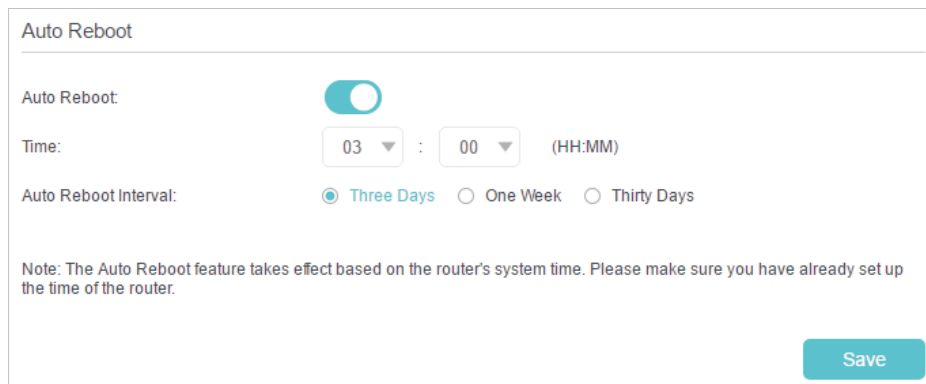
**Note:**

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

## 12.6. Auto Reboot

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [System Tools](#) > [Reboot](#).
3. Enable [Auto Reboot](#).
4. Specify the time at which your router will reboot and the [Auto Reboot Interval](#).
5. Click [Save](#).



## 12.7. Change the Login Password

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

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

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

Account Management

Old Password:

New Password:  Low Middle High

Confirm New Password:

Save

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

## 12.8. Local Management

Local Management allows local devices to access and manage the router. By default, all local devices can access and manage the router via HTTP.

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

Local Management

Port for HTTP:

Local Management via HTTPS:  Enable

Port for HTTPS:

Only Allow the Following IP/MAC:  Enable

IP/MAC Address:

Save

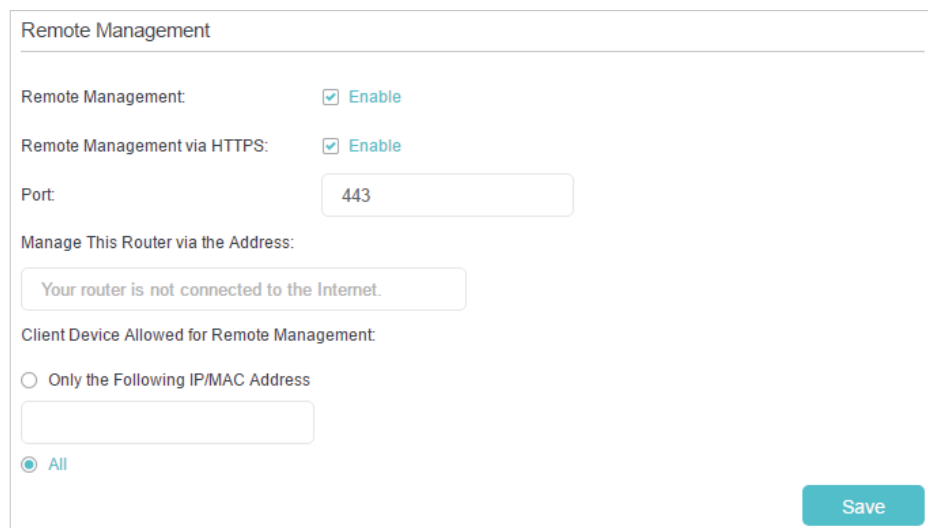
3. Enable [Local Management via HTTPS](#) if you want to access the router via both HTTPS and HTTP, or keep it disabled if you only want to access the router via HTTP.
4. Keep the Port for HTTP and Port for HTTPS as the default settings.
5. If you only want to allow one specific device to manage the router, enter the IP Address or MAC Address of the device in the [IP/MAC Address](#) field.
6. Click [Save](#).

**Note:** If a warning pops up when you visit <https://tplinkwifi.net>, click Trust (or a similar option) to continue.

## 12.9. Remote Management

Remote Management allows remote devices to access and manage the router. By default, all remote devices cannot access and manage the router.

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



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

- Remote Management:**  Enable
- Remote Management via HTTPS:**  Enable
- Port:** 443
- Manage This Router via the Address:** A text box containing the message 'Your router is not connected to the Internet.'
- Client Device Allowed for Remote Management:**
  - Only the Following IP/MAC Address (with an empty text box below it)
  - All
- Save** button

3. Enable **Remote Management** if you want to allow Remote Management via HTTPS, or enable **Remote Management** and then disable **Remote Management via HTTPS** if you want to allow Remote Management via HTTP.
4. Keep the Port as the default setting.
5. Decide which remote device can access the router remotely:
  - **Only the Following IP/MAC Address** - Enter the IP Address or MAC Address of the remote device to access the router.
  - **All** - All remote devices can access the router.
6. Click **Save**.

📌 Note: If a warning pops up when you visit the above address remotely, click Trust (or a similar option) to continue.

## 12.10. System Log

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

➤ **To save the system log locally:**

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



3. Choose the type and level of the system logs as needed.
4. Click [Save Log](#) to save the system logs to a local disk.

### System Log

Type:

Level:

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

ID	Time	Type	Level	Log Content
1	2017-05-24 18:09:12	DHCP	Notice	Send DISCOVER with request ip 0.0.0.0 and unicast flag 1
2	2017-05-24 18:09:09	DHCP	Notice	Send DISCOVER with request ip 0.0.0.0 and unicast flag 1
3	2017-05-24 18:09:04	DHCP	Notice	Send DISCOVER with request ip 0.0.0.0 and unicast flag 0
4	2017-05-24 18:09:01	DHCP	Notice	Send DISCOVER with request ip 0.0.0.0 and unicast flag 0
5	2017-05-24 18:08:58	DHCP	Notice	Send DISCOVER with request ip 0.0.0.0 and unicast flag 0
6	2017-05-24 18:08:58	DHCP	Notice	Send DISCOVER with request ip 0.0.0.0 and unicast flag 1
7	2017-05-24 18:08:55	DHCP	Notice	Send DISCOVER with request ip 0.0.0.0 and unicast flag 1
8	2017-05-24 18:08:44	DHCP	Notice	Recv no OFFER, DHCP Service unavailable

[1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) ... [47](#)

[Log Settings](#) [Save Log](#)

➤ **To send the system log to a remote server:**

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

Log Settings

Save Locally

Minimum Level: Information

Save Remotely

Minimum Level: Information

Server IP: 192.168.1.100

Server Port: 514

Local Facility Name: User

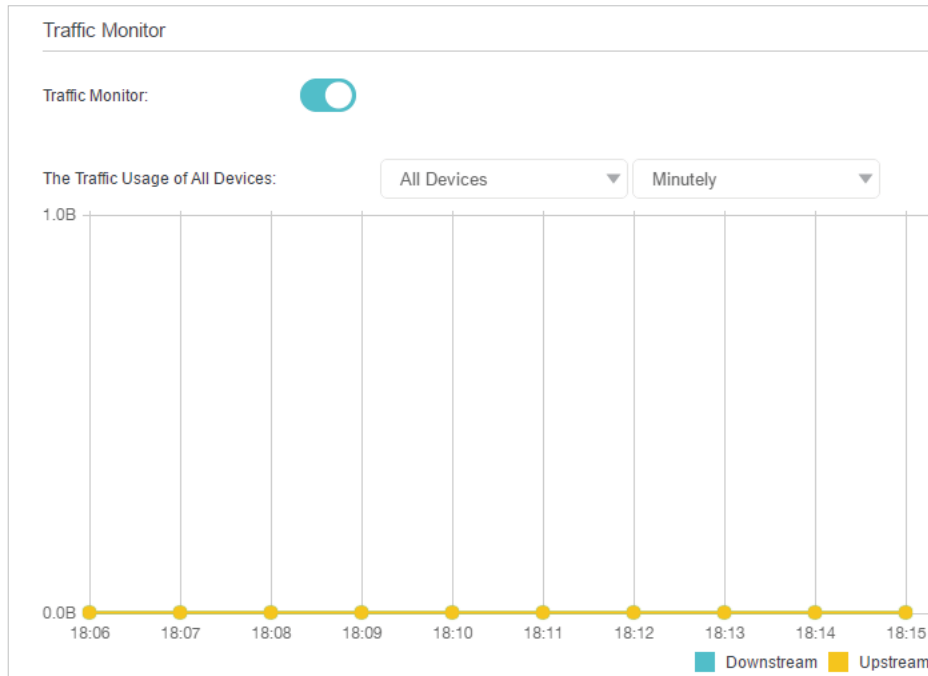
Back Save

4. Select [Save Remotely](#). If the remote server has a log viewer client or a sniffer tool implemented, you can view and analyze the system log remotely in real-time.
5. Select the minimum level of system logs to be saved from the drop-down list. The list is in descending order, with the lowest level listed last.
6. Specify the IP address of the remote system log server in the Server IP field.
7. Specify the port number of the remote system log server in the Server Port field.
8. Select the local facility name of the remote server from the drop-down list.
9. Click [Save](#).

## 12. 11. Monitor the Internet Traffic Statistics

The Traffic Statistics page displays the traffic usage of a device in the past 10 minutes or that of all devices in the past 10 minutes/24 hours/7 days, allowing you to monitor the volume of internet traffic statistics.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [System Tools](#) > [Traffic Monitor](#).
3. Toggle on [Traffic Monitor](#). You can monitor the traffic usage of a device in the past 10 minutes or that of all devices in the past 10 minutes/24 hours/7 days.



# FAQ

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

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

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

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

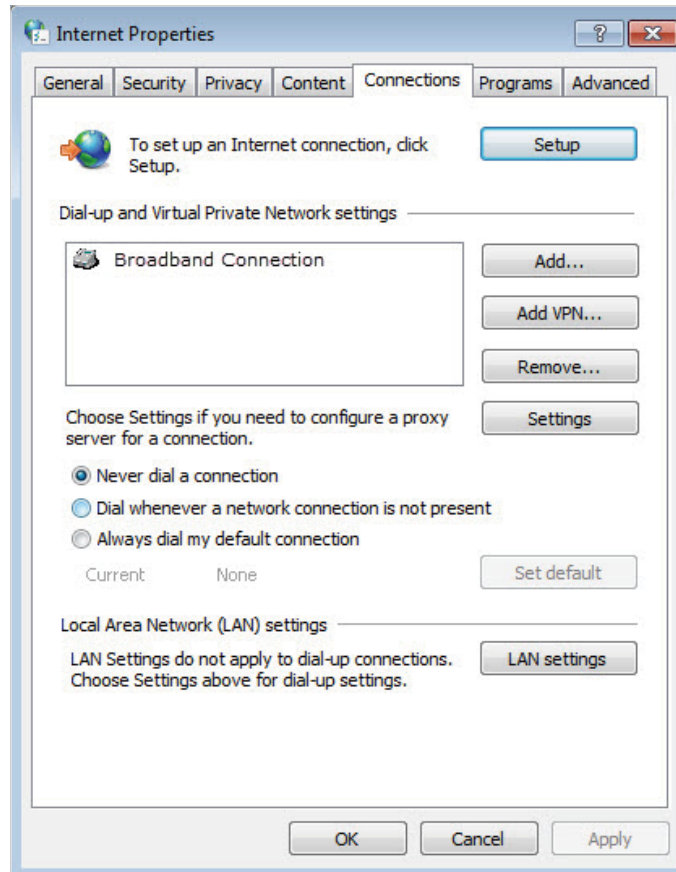
- Press and hold the WPS/Reset button of the router for about 5 seconds, and then visit <http://tplinkwifi.net> to create a new login password.

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

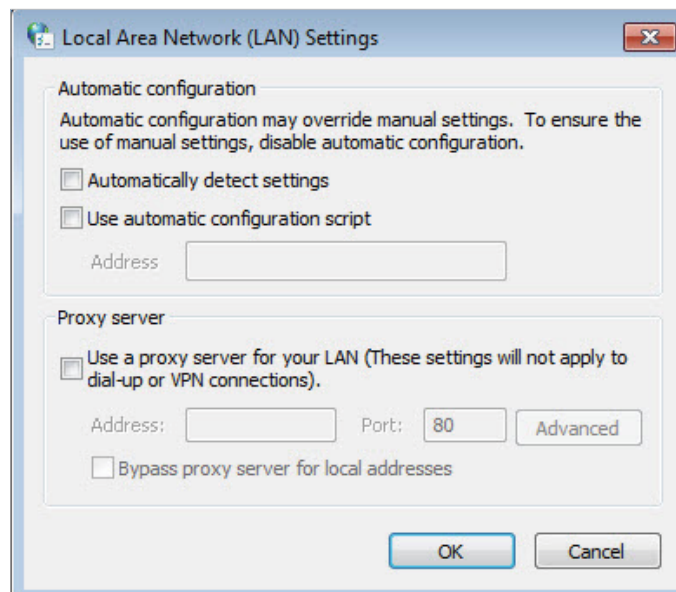
## Q3. What should I do if I can't log in to the router's web management page?

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

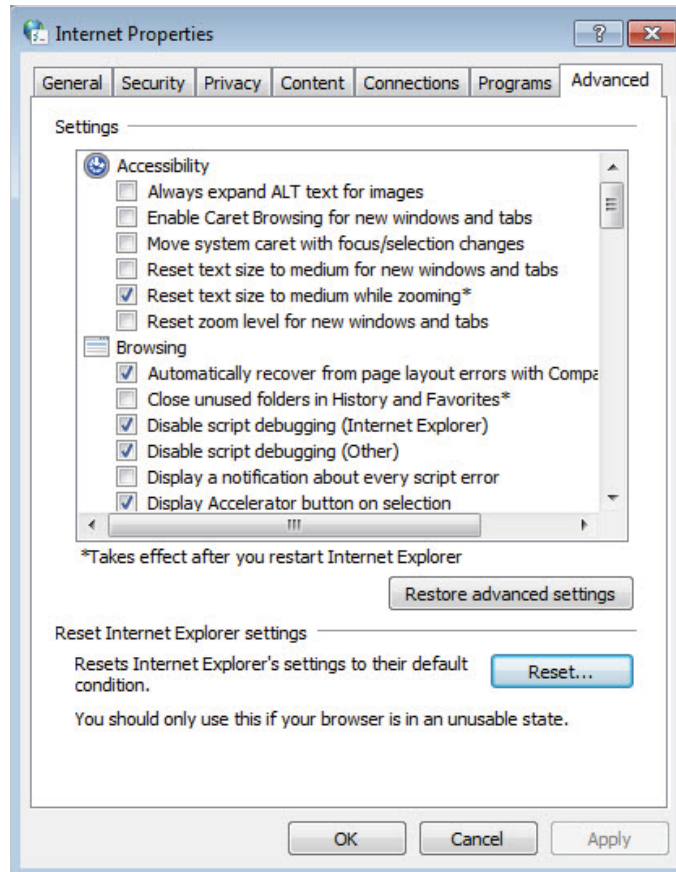
- Make sure your computer is connected to the router correctly and the corresponding LED indicator(s) light up.
- Make sure the IP address of your computer is configured as [Obtain an IP address automatically](#) and [Obtain DNS server address automatically](#).
- Make sure <http://tplinkwifi.net> or <http://192.168.1.1> is correctly entered.
- Check your computer's settings:
  - 1) Go to [Start](#) > [Control Panel](#) > [Network and Internet](#), and click [View network status and tasks](#).
  - 2) Click [Internet Options](#) on the bottom left.
  - 3) Click [Connections](#) and select [Never dial a connection](#).



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



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



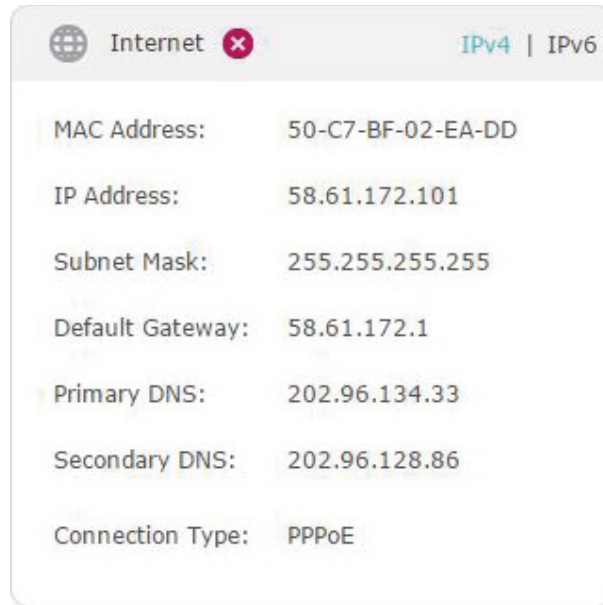
- Use another web browser or computer to log in again.
- Reset the router to factory default settings and try again. If login still fails, please contact the technical support.

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

#### Q4. What should I do if I can't access the internet even though the configuration is finished?

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to **Advanced** > **Status** to check internet status:

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



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

1) Go to [Advanced](#) > [Network](#) > [LAN Settings](#).

2) Enter 8.8.8.8 as Primary DNS, click [Save](#).

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

A screenshot of a DHCP configuration form. At the top, "DHCP:" is followed by a checked "Enable" checkbox. Below that are two radio buttons: "DHCP Server" (selected) and "DHCP Relay". The "IP Address Pool:" is set to "192 . 168 . 1 . 100" - "192 . 168 . 1 . 199". "Address Lease Time:" is set to "120" minutes, with a note "(1-2880. The default value is 1440.)". "Default Gateway:" is set to "192 . 168 . 1 . 1" (Optional). "Default Domain:" is empty (Optional). "Primary DNS:" is set to "0 . 0 . 0 . 0" (Optional). "Secondary DNS:" is set to "0 . 0 . 0 . 0" (Optional). A "Save" button is in the bottom right corner.

- Restart the modem and the router.
  - 1) Power off your modem and router, and leave them off for 1 minute.
  - 2) Power on your modem first, and wait about 2 minutes until it gets a solid cable or internet light.
  - 3) Power on the router.
  - 4) Wait another 1 or 2 minutes and check the internet access.
- Reset the router to factory default settings and reconfigure the router.
- Upgrade the firmware of the router.

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

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

Setting	Value
MAC Address:	50-C7-BF-02-EA-DD
IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Default Gateway:	0.0.0.0
Primary DNS:	0.0.0.0
Secondary DNS:	0.0.0.0
Connection Type:	PPPoE

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

MAC Clone

Use Default MAC Address  
 Use Current Computer MAC Address  
 Use Custom MAC Address

Save

**Tips:**

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

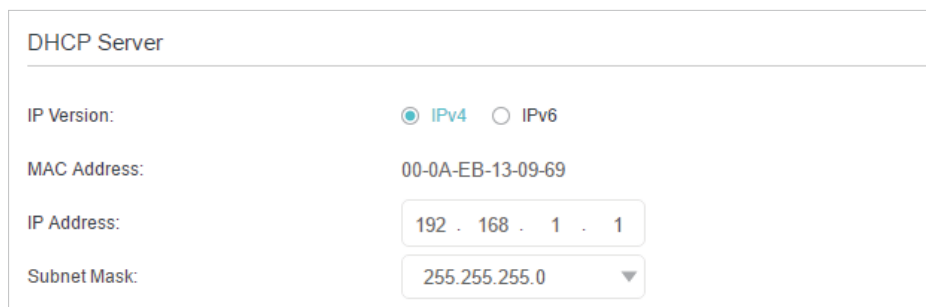
- Modify the LAN IP address of the router.



**Note:**

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

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



The screenshot shows the 'DHCP Server' configuration page. It includes the following fields and values:

- IP Version:** IPv4 (selected), IPv6
- MAC Address:** 00-0A-EB-13-09-69
- IP Address:** 192 . 168 . 1 . 1
- Subnet Mask:** 255.255.255.0

- Restart the modem and the router.
  - 1) Power off your modem and router, and leave them off for 1 minute.
  - 2) Power on your modem first, and wait about 2 minutes until it get a solid cable or internet light.
  - 3) Power on the router.
  - 4) Wait another 1 or 2 minutes and check the internet access.
- Double check the internet connection type.
  - 1) Confirm your internet connection type, which can be learned from the ISP.
  - 2) Visit <http://tplinkwifi.net>, and log in with or the password you set for the router.
  - 3) Go to **Advanced > Network > Internet (or EWAN Settings)**.
  - 4) Select your **Internet Connection Type** and fill in other parameters.
  - 5) Click **Save**.

The screenshot shows the IPv4 configuration page. The 'Internet Connection Type' is set to 'Dynamic IP'. Below it, a dropdown menu is open, showing options: 'Static IP', 'Dynamic IP' (highlighted), 'PPPoE', 'BigPond Cable', 'L2TP', and 'PPTP'. The 'Secondary DNS' field is set to '0.0.0.0'. There are 'Renew' and 'Release' buttons. A red message says 'WAN port is unplugged.'. At the bottom left, there is an 'Advanced' toggle. At the bottom right, there is a 'Save' button.

6) Restart the modem and the router again.

- Please upgrade the firmware of the router.

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

### Q5. What should I do if I can't get internet access from the 3G/4G USB modem?

- Go to our website at [www.tp-link.com](http://www.tp-link.com), click [Support](#) > [Compatibility List](#) > [TL-MR3420](#) and make sure that your 3G/4G USB modem is on the compatibility list.
- Make sure that you have a valid SIM/UIM card inserted into the 3G/4G USB modem.
- Plug the 3G/4G USB modem directly into your computer and disable the PIN verification via the modem utility to check if you have the internet connection on your computer.
- Obtain the latest dial number and APN from your ISP, and update the information through the router's web management page.

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

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

- Make sure the wireless function of your device is enabled if you're using a laptop with built-in wireless adapter. You can refer to the relevant document or contact the laptop manufacturer.
- Make sure the wireless adapter driver is installed successfully and the wireless adapter is enabled.
  - On Windows 7

- 1) If you see the message [No connections are available](#), it is usually because the wireless function is disabled or blocked somehow.
- 2) Click [Troubleshoot](#) and windows might be able to fix the problem by itself.
  - **On Windows XP**
    - 1) If you see the message [Windows cannot configure this wireless connection](#), this is usually because windows configuration utility is disabled or you are running another wireless configuration tool to connect the wireless.
    - 2) Exit the wireless configuration tool (the TP-Link Utility, for example).
    - 3) Select and right click on [My Computer](#) on desktop, select [Manage](#) to open Computer Management window.
    - 4) Expand [Services and Applications](#) > [Services](#), find and locate [Wireless Zero Configuration](#) in the Services list on the right side.
    - 5) Right click [Wireless Zero Configuration](#), and then select [Properties](#).
    - 6) Change [Startup type](#) to [Automatic](#), click on Start button and make sure the Service status is [Started](#). And then click [OK](#).

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

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

Wireless Settings 2.4GHz

Enable Wireless Radio

Network Name (SSID):   Hide SSID

Security:

Version:  Auto  WPA2-PSK

Encryption:  Auto  TKIP  AES

Password:

Mode:

Channel:

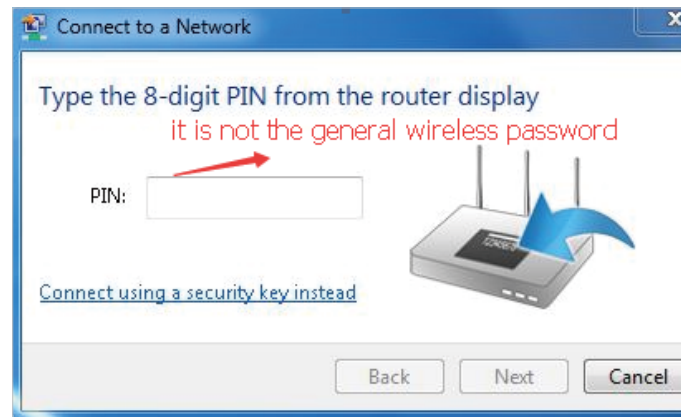
Channel Width:

Transmit Power:  Low  Middle  High

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

- **Authenticating problem/password mismatch:**

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




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

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

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

- Check the wireless signal strength of your network. If it is weak (1~3 bars), please move the router closer and try again.
- Change the wireless Channel of the router to 1, 6 or 11 to reduce interference from other networks.
- Re-install or update the driver for your wireless adapter of the computer.

## **COPYRIGHT & TRADEMARKS**

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

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

## CE Mark Warning



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

### **OPERATING FREQUENCY(the maximum transmitted power)**

2412MHz—2472MHz(20dBm)

### **RF Exposure Information**

This device meets the EU requirements (2014/53/EU Article 3.1a) on the limitation of exposure of the general public to electromagnetic fields by way of health protection.

The device complies with RF specifications when the device used at 20 cm from your body.

TP-Link hereby declares that the device is in compliance with the essential requirements and other relevant provisions of directives 2014/53/EU, 2009/125/EC and 2011/65/EU.

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

### **Canadian Compliance Statement**

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

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

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

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

### **Radiation Exposure Statement:**

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

## Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

## Industry Canada Statement

CAN ICES-3 (B)/NMB-3(B)

## Korea Warning Statements:

당해 무선설비는 운용중 전파혼신 가능성이 있음.

## NCC Notice & BSMI Notice:

注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性或功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機需忍受合法通信或工業、科學以及醫療用電波輻射性電機設備之干擾。

## 安全諮詢及注意事項


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






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



## Safety Information

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

## Explanations of the symbols on the product label

Symbol	Explanation
	DC voltage
	Indoor use only
	<b>RECYCLING</b> This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/EU in order to be recycled or dismantled to minimize its impact on the environment. User has the choice to give his product to a competent recycling organization or to the retailer when he buys a new electrical or electronic equipment.