



Archer C59 User Guide

AC1350 Wireless Dual Band Router

Contents

About This Guide	1
Chapter 1. Get to Know About Your Router	2
1. 1. Product Overview	3
1. 2. Panel Layout	3
1. 2. 1.Top View.....	3
1. 2. 2.The Back Panel.....	4
Chapter 2. Connect the Hardware.....	6
2. 1. Position Your Router.....	7
2. 2. Connect Your Router	7
Chapter 3. Log into Your Router.....	10
Chapter 4. Set Up Internet Connection	12
4. 1. Use Quick Setup Wizard	13
4. 2. Manually Set up Your Internet Connection	13
4. 3. Set Up an IPv6 Internet Connection	17
Chapter 5. Guest Network	21
5. 1. Create a Network for Guests	22
5. 2. Customize Guest Network Options.....	23
Chapter 6. USB Application.....	24
6. 1. Local Storage Sharing	25
6. 1. 1.Access the USB disk	25
6. 1. 2.Customize Your Settings.....	27
6. 2. Remote Access via FTP Server.....	30
6. 2. 1.Access the USB Disk	30
6. 2. 2.Customize Your Settings.....	33
6. 3. Media Sharing.....	34
6. 3. 1.Access the USB Disk	35
6. 3. 2.Customize Your Settings.....	36

6.4. Printer Sharing	37
Chapter 7. Parental Controls.....	41
Chapter 8. QoS.....	45
8.1. Prioritize Internet Traffic with QoS.....	46
Chapter 9. Network Security.....	50
9.1. Protect the Network from Cyber Attacks	51
9.2. Access Control	52
9.3. IP & MAC Binding.....	54
Chapter 10.NAT Forwarding.....	55
10.1. Share Local Resources on the Internet by Virtual Servers.....	56
10.2. Open Ports Dynamically by Port Triggering.....	57
10.3. Make Applications Free from Port Restriction by DMZ	58
10.4. Make Xbox Online Games Run Smoothly by UPnP	59
Chapter 11.VPN Server.....	61
11.1. Use OpenVPN to Access Your Home Network.....	62
11.2. Use PPTP VPN to Access Your Home Network.....	63
Chapter 12.Customize Your Network Settings	69
12.1. Change the LAN Settings	70
12.2. Configure to Support IPTV Service	70
12.3. Specify DHCP Server Settings.....	72
12.4. Set Up a Dynamic DNS Service Account.....	73
12.5. Create Static Routes	74
12.6. Specify Wireless Settings	76
12.7. Use WPS for Wireless Connection	78
12.7.1.Set the Router's PIN	78
12.7.2.Use the WPS Wizard for Wi-Fi Connections	78
Chapter 13.Manage the Router	79
13.1. Set Up System Time	80
13.2. Test the Network Connectivity.....	81
13.3. Upgrade the Firmware.....	82

13. 3. 1.Online Upgrade.....	83
13. 3. 2.Local Upgrade	83
13. 3. 3.Restore Interrupted Upgrade after Power Failure.....	84
13. 4. Backup and Restore Configuration Settings	84
13. 5. Change the Administrator Account	86
13. 6. Password Recovery.....	86
13. 7. Local Management.....	87
13. 8. Remote Management	88
13. 9. System Log	89
13. 10. Monitor the Internet Traffic Statistics.....	91
13. 11. Control LEDs	92
FAQ.....	94

About This Guide

This guide is a complementation 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
<i>Blue Italic</i>	Hyperlinks are in blue italic. You can click to redirect to a website or a specific section.
Blue	Contents to be emphasized and texts on the web page are in blue, including the menus, items, buttons, etc.
>	The menu structures to show the path to load the corresponding page. For example, Advanced > Wireless > MAC Filtering means the MAC Filtering function page is under the Wireless menu that is located in the Advanced tab.
 Note:	Ignoring this type of note might result in a malfunction or damage to the device.
 Tips:	Indicates important information that helps you make better use of your device.
symbols on the web page	 click to edit the corresponding entry.  click to delete the corresponding entry.  click to enable or disable the corresponding entry.  click to view more information about items on the page.

More Info

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

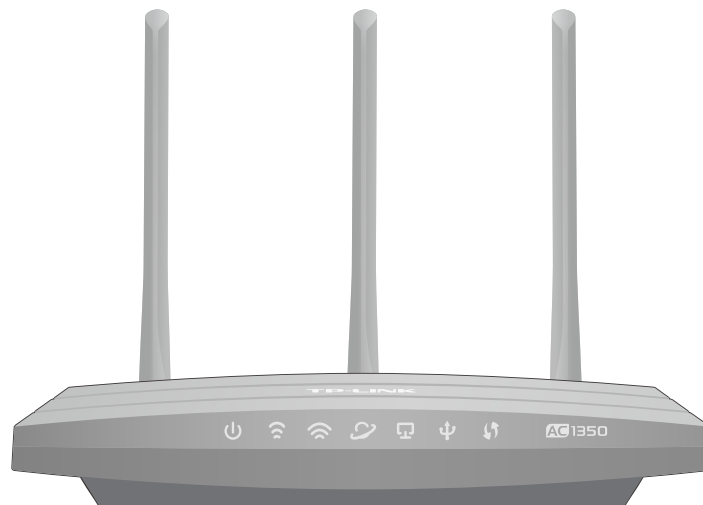
1.1. Product Overview

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 and the powerful Tether app.

1.2. Panel Layout

1.2.1. Top View



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

LED Explanation

Name	Status	Indication
 (Power)	On	System initialization completes.
	Flashing	System initialization or firmware upgrade is in process. Do not disconnect or power off the router.
	Off	Power is off.
 (2.4GHz Wireless)	On	The 2.4GHz wireless band is working properly.
	Off	The 2.4 GHz wireless band is disabled.

LED Explanation

Name	Status	Indication
 (5GHz Wireless)	On	The 5GHz wireless band is working properly.
	Off	The 5GHz wireless band is disabled.
 (Internet)	Green On	Internet is available.
	Orange On	The router’s Internet port is connected, but the Internet is not available.
	Off	The router’s Internet port is not connected.
 (Ethernet)	On	At least one Ethernet port is connected.
	Off	No Ethernet port is connected.
 (USB)	On	The USB device is identified and ready to use.
	Flashing	The USB device is being identified.
	Off	No USB device is plugged into the USB port or the USB device is not identified or USB device has been safely ejected.
 (WPS)	On/Off	Turns on when a WPS connection is established, and goes off about 5 minutes later.
	Flashing	A wireless device is trying to connect to the network via WPS. This process may take up to 2 minutes.

1.2.2. The Back Panel



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

Item	Description
WPS Button	Press this button, and immediately press the WPS button on your client device. The WPS LED of the router should change from flashing to solid on, indicating successful WPS connection.
Reset Button	Press this button for about 5 seconds to reset the router to its factory default settings.
Ethernet Ports (1/2/3/4)	For connecting your PCs or other wired network devices to the router.
Internet Port	For connecting to a DSL/Cable modem, or Ethernet port.
USB Port	For connecting to a USB storage device or a USB printer.
Power On/Off Button	Press this button to power on or off the router.
Power Port	For connecting the router to a power socket via the provided power adapter.
Wi-Fi Button	Press this button for about 2 seconds to turn on or off the wireless function of your router.
Antennas	Used for wireless operation and data transmitting. Upright them for the best Wi-Fi performance.

Chapter 2

Connect the Hardware

This chapter contains the following sections:

- *Position Your Router*
- *Connect Your Router*

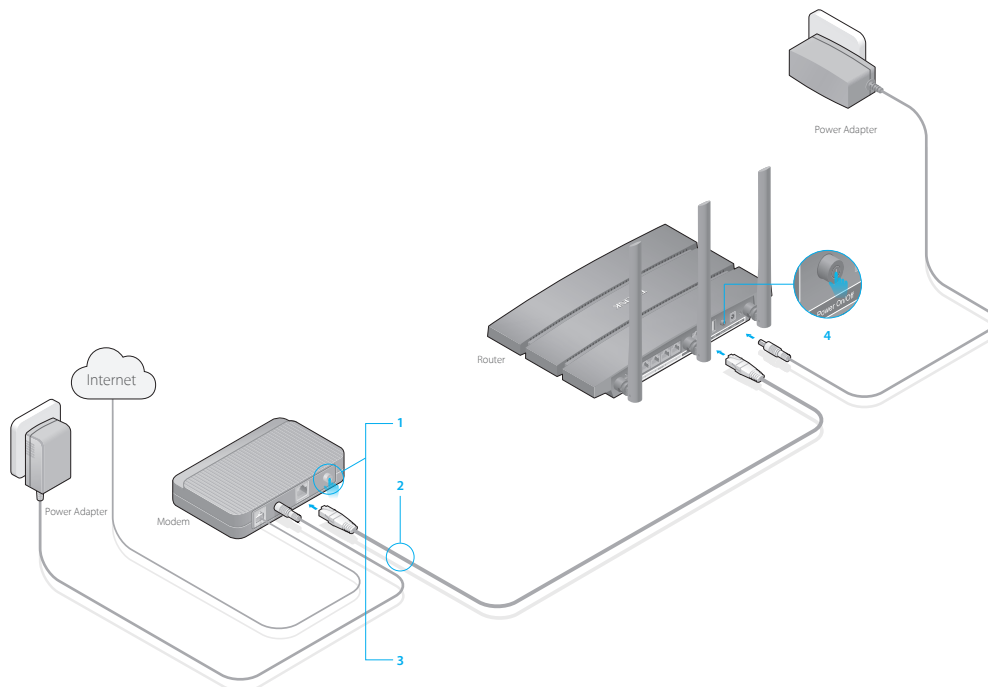
2.1. Position Your Router

- The Product should not be located where it will be exposed to moisture or excessive heat.
- Place the router in a location where it can be connected to the various 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 away from the strong electromagnetic radiation and the device of electromagnetic sensitive.

2.2. Connect Your Router

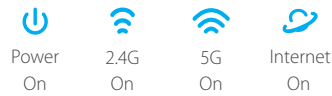
1. Follow the steps below to connect your router.

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



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

5) Verify that the hardware connection is correct by checking these LEDs.

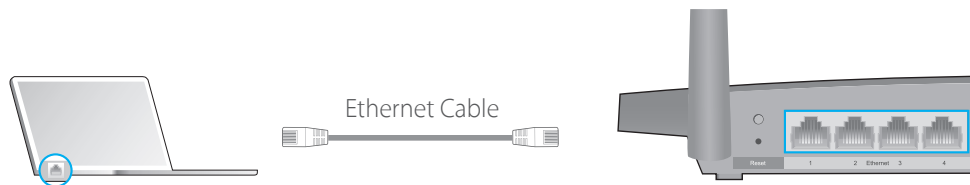


Tips: If 2.4GHz LED and 5GHz LED are off, press the Wi-Fi button for about 2 seconds, and then check the LEDs again in a few seconds.

2. Connect your computer to the router.

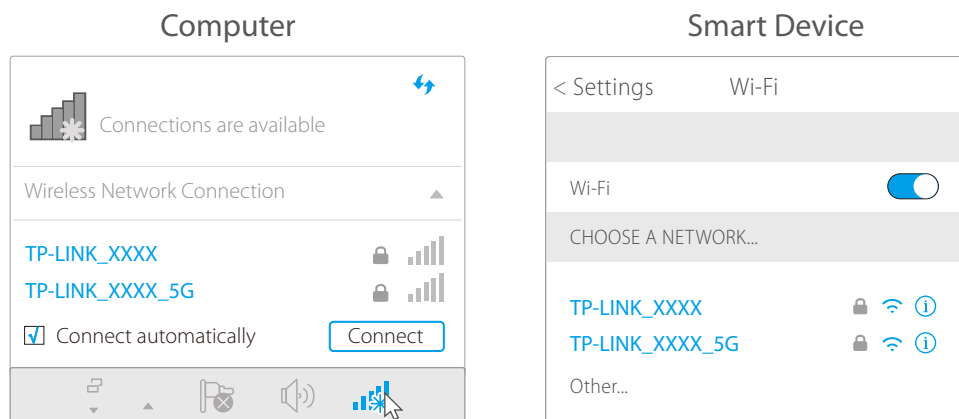
• Method 1: Wired

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



• Method 2: Wirelessly

- 1) Find the SSID (Network Name) and Wireless Password/PIN printed on the label at the bottom of the router.
- 2) Click the network icon of your computer or go to Wi-Fi Setting of your smart device, and then select the SSID to join the network.



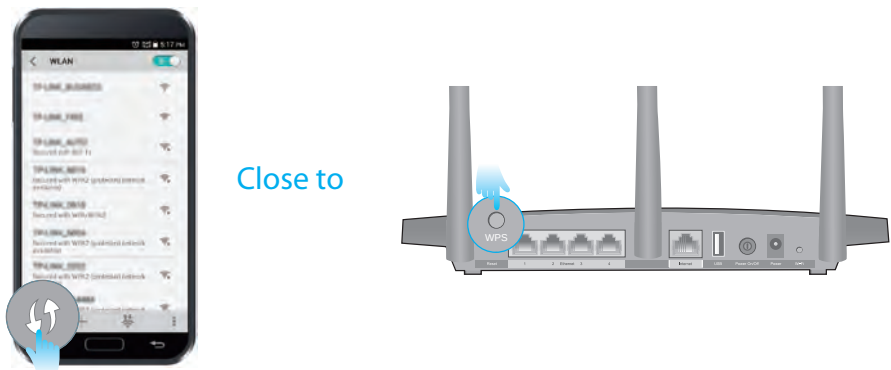
• Method 3: Use the WPS button

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

Note:

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

1. Tap the WPS icon on the device's screen.
2. Immediately press the WPS button on your router.



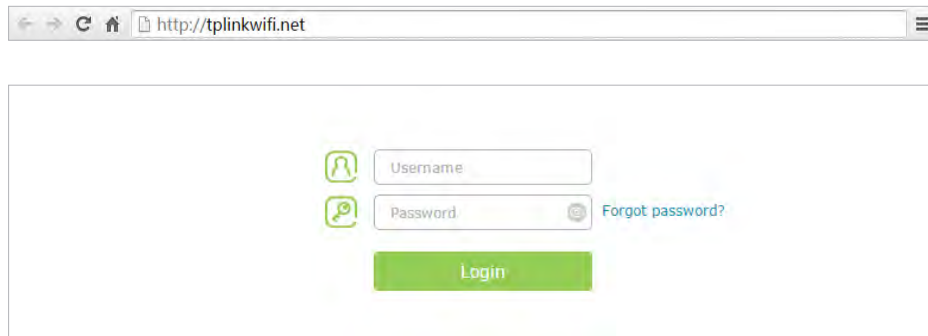
Chapter 3

Log into Your Router

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

Follow the steps below to log into your router.

1. Set up the TCP/IP Protocol in [Obtain an IP address automatically](#) mode on your computer.
2. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router. The default one is [admin](#) for both username and password.



Note:

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

Chapter 4

Set Up Internet Connection

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

This chapter contains the following sections:

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

4.1. Use Quick Setup Wizard

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

🔗 **Tips:**

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

Follow the steps below to set up your router.

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

📌 **Note:**

During the quick setup process:

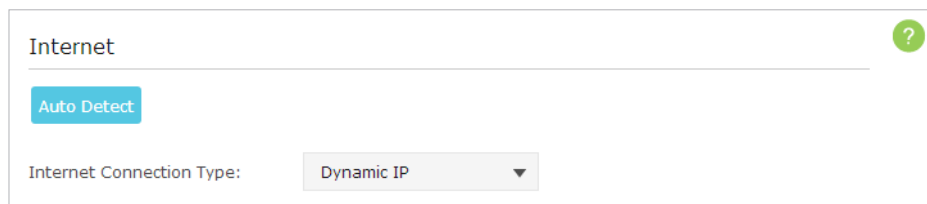
- If you are not sure of the [Internet Connection Type](#), please click **Auto Detect** or contact your ISP for Internet connection information.
- If you have changed the preset wireless network name (SSID) and wireless password, all your wireless devices must use the new SSID and password to connect to the router.

4.2. Manually Set up Your Internet Connection

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

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

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



📌 **Note:**

If you are unsure of what your connection type is, click **Auto Detect**. Since different connection types need different cables and connection information, you can also refer to the demonstrations in Step 4 to determine your connection type.

4. Follow the instructions on the page to continue the configuration. Parameters on the figures are just used for demonstration.
 - 1) If you choose **Dynamic IP**, you need to select whether to clone the MAC address or not. Dynamic IP users are usually equipped with a cable TV or fiber cable.

Internet

Auto Detect

Internet Connection Type: Dynamic IP ▼

☒ Do NOT Clone MAC Address

☐ Clone Current Computer MAC Address

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

Save

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

Internet

Auto Detect

Internet Connection Type: Static IP ▼

IP Address:

Subnet Mask:

Default Gateway:

Primary DNS:

Secondary DNS: (Optional)

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

Save

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

Internet

Auto Detect

Internet Connection Type: PPPoE ▼

Username:

Password:

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

Save

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

Internet

Auto Detect

Internet Connection Type: L2TP ▼

Username:

Password:

Secondary Connection: ☒ Dynamic IP ☐ Static IP

VPN Server IP/Domain Name:

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

Save

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

Internet

Auto Detect

Internet Connection Type: PPTP

Username:

Password:

Secondary Connection: ☒ Dynamic IP ☐ Static IP

VPN Server IP/Domain Name:

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

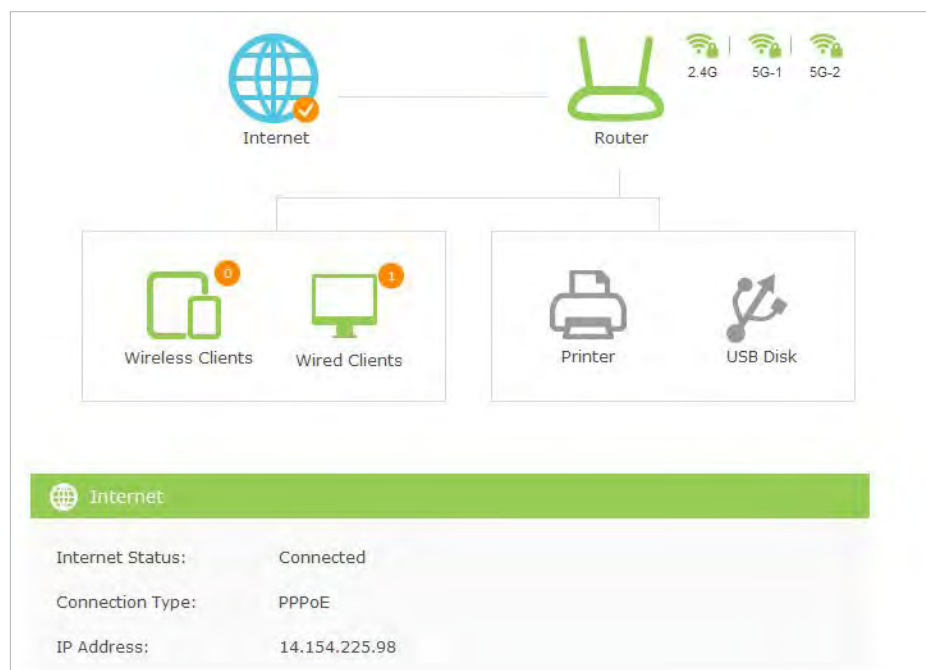
Save

- Click [Save](#). To check your Internet connection, click [Network Map](#) on the left of the page.

Note:

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

- After the connection succeeds, the screen will display as follows. Here we take PPPoE as an example.



Tips:

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

4.3. Set Up an IPv6 Internet Connection

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

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

Internet

IPv6: ☒

Internet Connection Type: Static IP

LAN

Assigned Type: DHCP ☐ SLAAC+RDNSS

Address Prefix: /64

Address: FE80::20A:EBFF:FE16:E4B8/64

Save

Tips:

If you do not know what your Internet connection type is, contact your ISP or judge according to the already known information provided by your ISP.

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

- 1) **Static IP:** Fill in blanks and click [Save](#).

Internet

IPv6: ☒

Internet Connection Type: Static IP

IPv6 Address:

Default Gateway:

Primary DNS:

Secondary DNS:

MTU Size: 1500 bytes. (The default is 1500, do not change unless necessary.)

Save

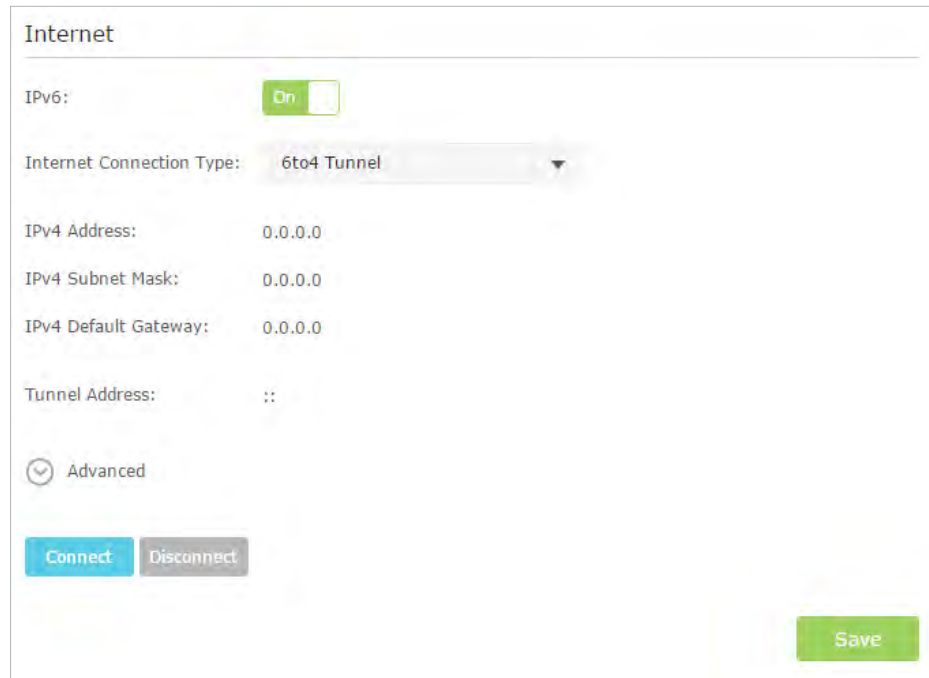
- 2) **Dynamic IP(SLAAC/DHCPv6):** Click [Advanced](#) to do more configuration if your ISP requires. Click [Save](#) and then click [Renew](#) to finish the configuration.

The screenshot shows the 'Internet' configuration window. At the top, 'IPv6:' is set to 'On' with a green toggle switch. Below it, 'Internet Connection Type:' is set to 'Dynamic IP (SLAAC/DHCPv6)' in a dropdown menu. The 'IPv6 Address:', 'Primary DNS:', and 'Secondary DNS:' fields are all empty, showing '::'. There are 'Renew' and 'Release' buttons. An 'Advanced' link with a dropdown arrow is visible. At the bottom right is a green 'Save' button.

- 3) **PPPoE:** Fill in the Username and Password. Click [Advanced](#) to do more configuration if your ISP requires. Click [Save](#) and then click [Connect](#) to finish the configuration.

The screenshot shows the 'Internet' configuration window. 'IPv6:' is set to 'On' with a green toggle switch. 'Internet Connection Type:' is set to 'PPPoE' in a dropdown menu. Below it is a checkbox labeled 'PPPoE same session with IPv4 connection' which is unchecked. There are input fields for 'Username:' and 'Password:'. The 'IPv6 Address:' field is empty, showing '::'. There are 'Connect' and 'Disconnect' buttons. An 'Advanced' link with a dropdown arrow is visible. At the bottom right is a green 'Save' button.

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



Internet

IPv6: ☒ On

Internet Connection Type: 6to4 Tunnel ▼

IPv4 Address: 0.0.0.0

IPv4 Subnet Mask: 0.0.0.0

IPv4 Default Gateway: 0.0.0.0

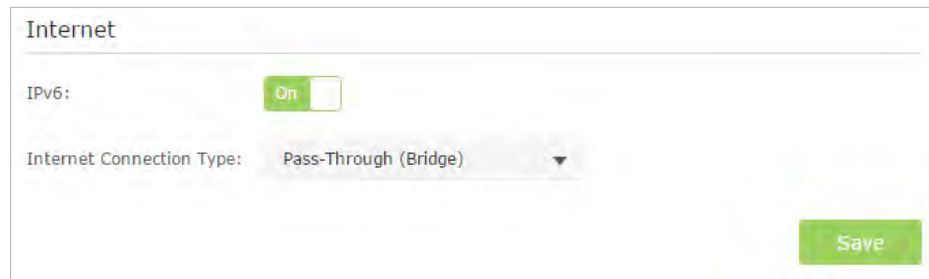
Tunnel Address: ::

☒ Advanced

[Connect](#) [Disconnect](#)

[Save](#)

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



Internet

IPv6: ☒ On

Internet Connection Type: Pass-Through (Bridge) ▼

[Save](#)

4. Configure LAN ports. Windows users are recommended to choose from the first two types. Fill in [Address Prefix](#) provided by your ISP, and click [Save](#).

[Tips:](#)

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



LAN

Assigned Type: ☐ DHCPv6 ☒ SLAAC+ Stateless DHCP ☐ SLAAC+ RDNSS

Address Prefix: /64

Address: FE80::20A:EBFF:FEAC:881B/64

[Save](#)

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

Internet 		IPv4 IPv6
MAC Address:	00-0A-EB-16-E4-B9	
IP Address:	2001:c68:202:2111::120/64	
Subnet Mask:	255.255.255.0	
Default Gateway:	fe80::edd0:80d2:7f5e:6be7	
Primary DNS:	2001:c68:202:2111::1	
Secondary DNS:	2001:c68:202:2111::2	
Connection Type:	PPPoE	

🔗 Tips:

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

Chapter 5

Guest Network

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

This chapter contains the following sections:

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

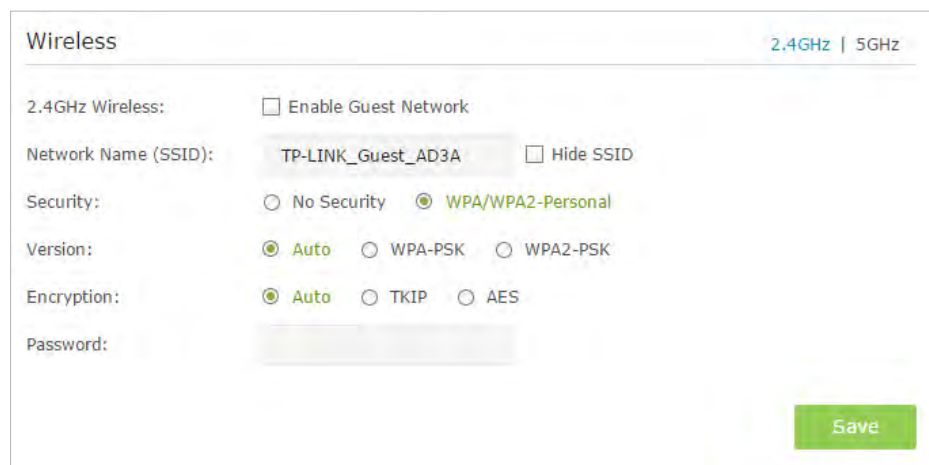
5.1. Create a Network for Guests

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [Advanced](#) > [Guest Network](#). Locate the [Wireless](#) section.
3. Create a guest network according to your needs.
 - 1) Enable [2.4GHz Wireless](#) network or [5GHz Wireless](#) network.

■ **Note:**

Guest network and WDS cannot be enabled at the same time. If WDS was enabled, disable it at [Advanced](#) > [System Tools](#) > [System Parameters](#).

- 2) Customize the SSID. Don't select [Hide SSID](#) unless you want your guests to manually input the SSID for guest network access.
- 3) Set [Security](#) to [WPA/WPA2 Personal](#), keep the default [Version](#) and [Encryption](#) values, and customize your own password.



Wireless 2.4GHz | 5GHz

2.4GHz Wireless: ☐ Enable Guest Network

Network Name (SSID): ☐ Hide SSID

Security: ☐ No Security ☒ WPA/WPA2-Personal

Version: ☒ Auto ☐ WPA-PSK ☐ WPA2-PSK

Encryption: ☒ Auto ☐ TKIP ☐ AES

Password:

[Save](#)

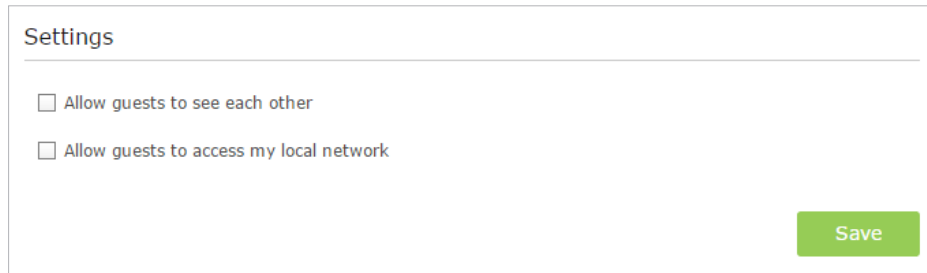
4. Click [Save](#). Now your guests can access your guest network using the SSID and password you set!

💡 **Tips:**

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

5.2. Customize Guest Network Options

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



Settings

☐ Allow guests to see each other

☐ Allow guests to access my local network

Save

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

Select 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, Samba, Ping, and FTP.

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

Select 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, Samba, Ping, and FTP.

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

 Tips:

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

Chapter 6

USB Application

This chapter describes how to share and access USB devices connected to the router among different clients. The router only supports USB external flash drives, hard drives and USB printers.

■ **Note:**

A very few TP-LINK Routers may not equipped with USB ports. Please ignore this chapter if your router doesn't have USB port(s).

This chapter contains the following sections:

- [*Local Storage Sharing*](#)
- [*Remote Access via FTP Server*](#)
- [*Media Sharing*](#)
- [*Printer Sharing*](#)

6.1. Local Storage Sharing

Share your USB storage devices with different users on the network.

6.1.1. Access the USB disk

1. Connect Your USB Disk

Insert your USB storage device into the router's USB port directly or using a USB cable. Wait several seconds until the USB LED becomes solid on.

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](#).

2. Access Your USB Disk

By default, all the network clients can access all folders on your USB disk. Refer to the following table for access instructions. You can also customize your sharing content and set a sharing account by referring to [Customize Your Settings](#).

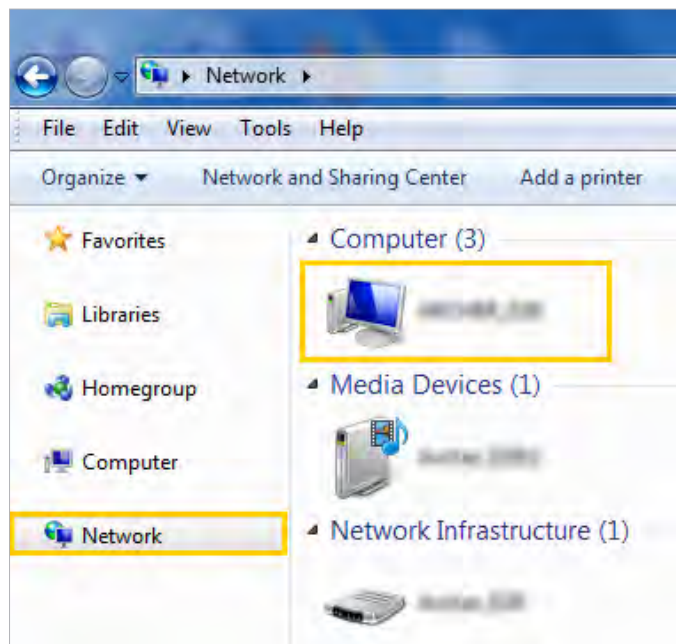
Windows computer

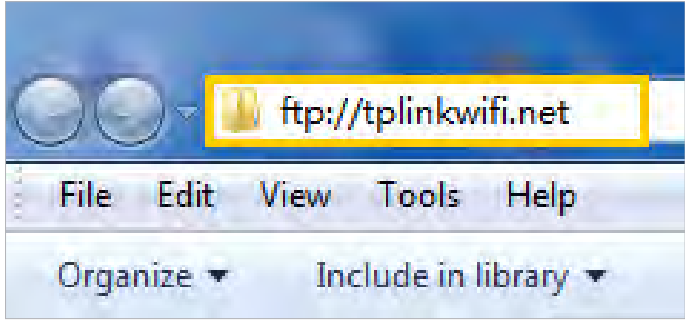
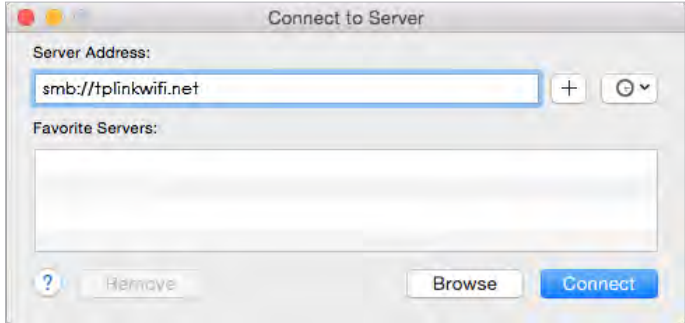
➤ Method 1:

Go to [Computer](#) > [Network](#), then click the Network Server Name (*Model number-share* by default) in the [Computer](#) section.

Note:

Operations in different systems are similar. Here we take Windows 7 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.)
pad	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.

6.1.2. Customize Your Settings

➤ To Only Share Specific Content

By default, [Share All](#) is enabled so all content on the USB disk is shared. If you want to only share specific folders, follow the steps below:

1. Visit <http://tplinkwifi.net>, then log in with the username and password you set for the router.
2. Select [Basic](#) > [USB Settings](#) > [Sharing Access](#). 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: ☐ Off Toggle On to share all files and folders or keep it Off to only share the specified folders.

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

☐	ID	Folder Name	Folder Path	Media Sharing	Volume Name	Active	Modify
☐	—	—	—	—	—	—	—

Volume Name:

Folder Path: [Browse](#)

Folder Name:

☒ Allow Guest Network Access

☐ Enable Authentication

☒ Enable Write Access

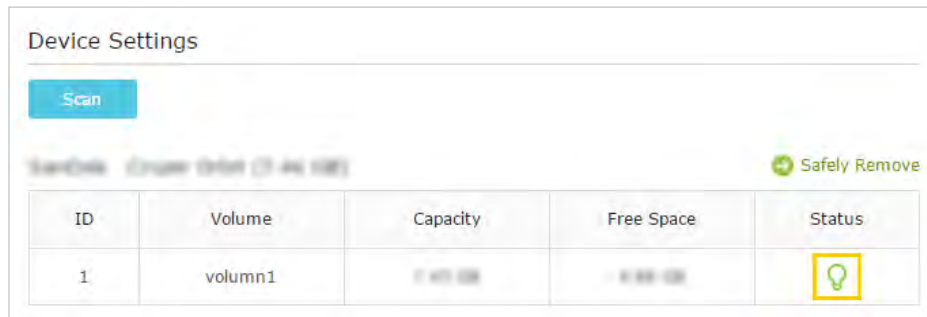
☒ Enable Media Sharing

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

3. Select the [Volume Name](#) and [Folder Path](#), then enter a [Folder Name](#) as you like.
4. Decide the way you share the folder:
 - [Allow Guest Network Access](#): If you tick this check box, guest network users can access the folder.
 - [Enable Authentication](#): If you tick this check box, you will be required to use a username and password to access the folder. Refer to [To Set up Authentication for Data Security](#) to learn more.
 - [Enable Write Access](#): If you tick this check box, network clients can modify the folder.
 - [Enable Media Sharing](#): If you tick this check box, you can view photos, play music and watch movies in the folder directly from DLNA-supported devices. Click [Media Sharing](#) to learn more.
5. Click [OK](#).

 Tips:

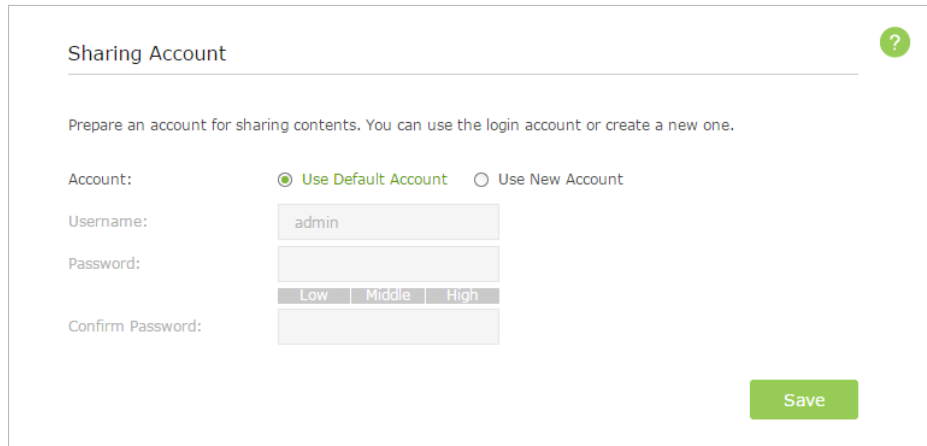
The router can share 32 volumes at most. You can click  on the page to detach the corresponding volume you do not need to share.



➤ **To Set up Authentication for Data Security**

If you enable **Authentication**, network clients will be required to enter the username and password you set when accessing the USB disk.

1. Visit <http://tplinkwifi.net>, then log in with the username and password you set for the router.
2. Select **Advanced** > **USB Settings** > **Sharing Access**. Focus on the **Sharing Account** section.



Sharing Account 

Prepare an account for sharing contents. You can use the login account or create a new one.

Account: ☒ Use Default Account ☐ Use New Account

Username:

Password: Low Middle High

Confirm Password:

Save

3. Choose **Use Default Account** (admin) or **Use New Account** and click **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.

4. 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:

On

Toggle On to share all files and folders or keep it Off to only share the specified folders.

Enable Authentication:

On

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

Folder Sharing

Share All:

Off

Toggle On to share all files and folders or keep it Off to only share the specified folders.

+ Add

- Delete

☐	ID	Folder Name	Folder Path	Media Sharing	Volume Name	Status	Modify
☐							

Volume Name:

Folder Path:

Folder Name:

Browse

☒ Allow Guest Network Access

☒ Enable Authentication

☒ Enable Write Access

☒ Enable Media Sharing

Cancel

OK

Note:

Due to Windows credential mechanism, you might be unable to access the USB disk after changing Authentication settings. Please log out from 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](#).

➤ **To Customize the Address of the USB Disk**

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

1. Visit <http://tplinkwifi.net>, then log in with the username and password you set for the router.
2. Select **Advanced** > **USB Settings** > **Sharing Access**. Focus on the **Sharing Settings** section.
3. Make sure **Network Neighborhood** is ticked, and enter a Network/Media Server Name as you like, such as **My-Share**, then click **Save**.

Sharing Settings

Network/Media Server Name:

Enable	Access Method	Link	Port
☒	Network Neighborhood	\\My-Share	---
☒	FTP	ftp://192.168.0.74:21	21
☐	FTP (Via Internet)	ftp://0.0.0.0:21 Edit	21

[Save](#)

4. Now you can access the USB disk by visiting [\\My-Share](#) (for Windows) or [smb://My-Share](#) (for Mac).

6.2. Remote Access via FTP Server

You can access your USB disk outside the local area network.

For example:

- 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.

6.2.1. Access the USB Disk

1. Connect Your USB Disk

Insert your USB storage device into the router's USB port directly or using a USB cable. Wait several seconds until the USB LED becomes solid on.

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: Select [Advanced](#) > [USB Settings](#) > [Device Settings](#) and click [Safely Remove](#).

2. Enable Authentication for Data Security

It is strongly recommended that you set and apply a sharing account for data security.

- 1) Visit <http://tplinkwifi.net>, then log in with the username and password you set for the router.
- 2) Select [Advanced](#) > [USB Settings](#) > [Sharing Access](#).
- 3) Choose [Use default Account](#) (admin) or [Use New Account](#) and click [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.

4) Enable [Authentication](#) to apply the sharing account.

- If you leave [Share All](#) enabled, click the button to enable [Authentication](#) for all folders.

- If [Share All](#) is disabled, enable [Authentication](#) for specific folders.

Folder Sharing

Share All: ☐ Off Toggle On to share all files and folders or keep it Off to only share the specified folders.

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

☐	ID	Folder Name	Folder Path	Media Sharing	Volume Name	Status	Modify
☐							

Volume Name:

Folder Path: [Browse](#)

Folder Name:

☒ Allow Guest Network Access

☒ **Enable Authentication**

☒ Enable Write Access

☒ Enable Media Sharing

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

Note:

Due to Windows credential mechanism, you might be unable to access the USB disk after changing Authentication settings. Please log out from Windows and try to access again.

3. Enable the FTP (via Internet)

Select the check box to enable [FTP\(via Internet\)](#), then click [Save](#).

Sharing Settings

Network/Media Server Name:

Enable	Access Method	Link	Port
☐	Network Neighborhood	\\C2600-Share	---
☐	FTP	ftp://192.168.0.74:21	21
☒	FTP (Via Internet)	ftp://0.0.0.0:21 Edit	21

[Save](#)

4. Access Your USB Disk via Internet

Now different clients with Internet connection can access the USB disk:

Computer	1) Open the Windows Explorer (or go to Computer, only for Windows users) or open a web browser. 2) Type the server address in the address bar: Type in ftp://<WAN IP address of the router>:<port number> (such as ftp://59.40.2.243:21). If you have specified the domain name of the router, you can also type in ftp://<domain name>:<port number> (such as ftp://MyDomainName:21) The Address Bar the Windows Explorer (Windows 7) 3) Press [Enter] on the keyboard. 4) Access with the username and password you set in Step 2 Enable Authentication for Data Security. Tips: You can also access the USB disk via a third-party app for network files management, which can resume broken file transfers.
	Pad Use a third-party app for network files management.

Tips:

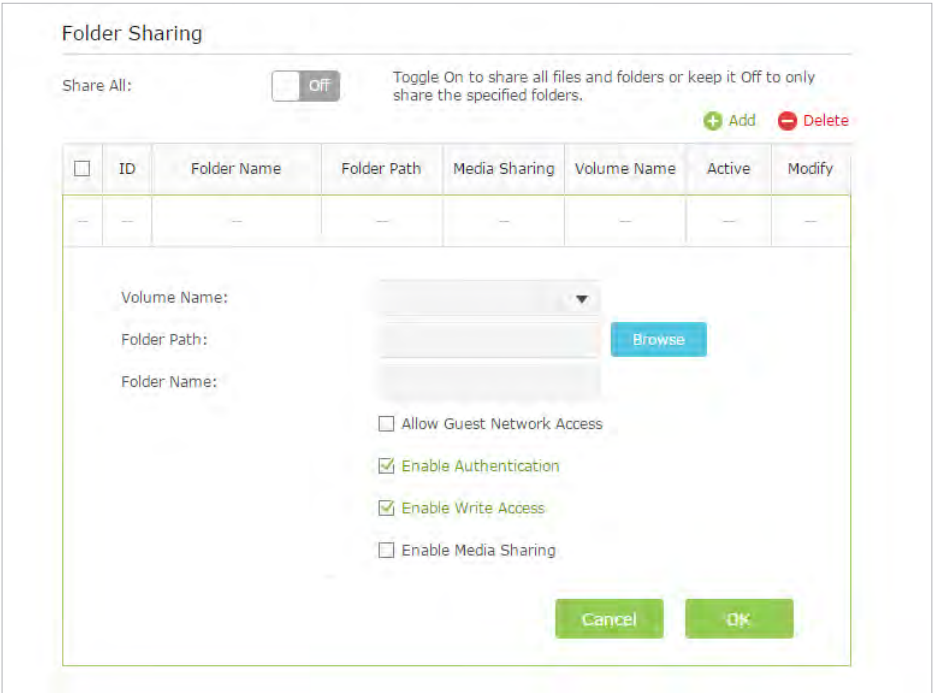
Click [Set Up a Dynamic DNS Service Account](#) to learn how to set up a domain name for you router.

6.2.2. Customize Your Settings

➤ To Only Share Specific Content

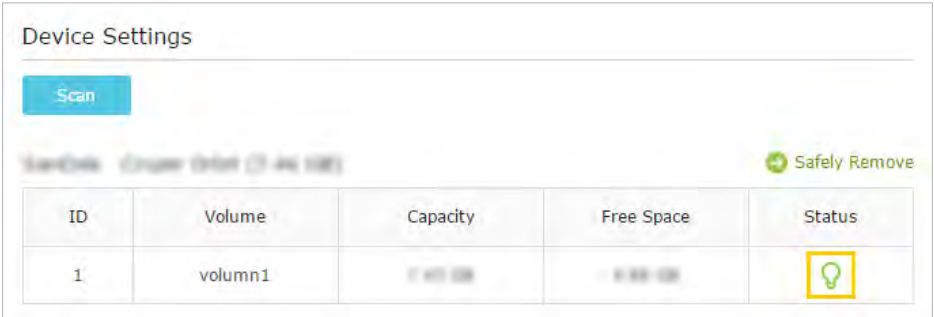
By default, [Share All](#) is enabled so all content on the USB disk is shared. If you want to only share specific folders, follow the steps below:

1. Visit <http://tplinkwifi.net>, then log in with the username and password you set for the router.
2. Select [Basic](#) > [USB Settings](#) > [Sharing Access](#). Focus on the [Folder Sharing](#) section. Click the button to disable [Share All](#), then click [Add](#) to add a new sharing folder.



- 3. Select the **Volume Name** and **Folder Path**, then specify the **Folder Name** as you like.
- 4. Tick **Enable Authentication**. If you allow network clients to modify this folder, tick **Enable Write Access**.
- 5. 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.



6.3. Media Sharing

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

6.3.1. Access the USB Disk

1. Connect Your USB Disk

Insert your USB storage device into the router's USB port directly or using a USB cable. Wait several seconds until the USB LED becomes solid on.

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](#).

2. Access the Media Files on Your USB Disk

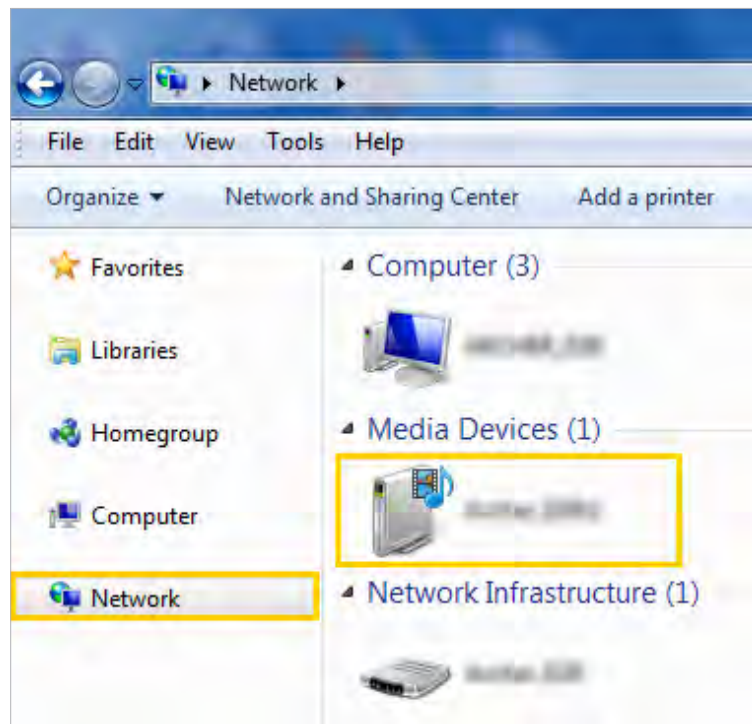
Now the DLNA-supported devices (such as your computer and pad) connected to the router can detect and play the media files on the USB disks.

Windows computer

- Go to [Computer](#) > [Network](#), then click the Media Server Name (*Model number-share* by default) in the [Media Devices](#) section.

Note:

Here we take Windows 7 as an example.



Pad

- Use a third-party DLNA-supported player.

6.3.2. Customize Your Settings

➤ To Only Share Specific Content

By default, **Share All** is enabled so all content on the USB disk is shared. If you want to only share specific folders, follow the steps below:

1. Visit <http://tplinkwifi.net>, then log in with the username and password you set for the router.
2. Select **Basic** > **USB Settings** > **Sharing Access**.
3. Focus on the section of **Folder Sharing**. Click the button to disable **Share All**, then click **Add** to add a new sharing folder.

Folder Sharing

Share All: ☐ Off Toggle On to share all files and folders or keep it Off to only share the specified folders.

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

☐	ID	Folder Name	Folder Path	Media Sharing	Volume Name	Active	Modify
☐	—	—	—	—	—	—	—

Volume Name:

Folder Path: [Browse](#)

Folder Name:

☐ Allow Guest Network Access

☐ Enable Authentication

☐ Enable Write Access

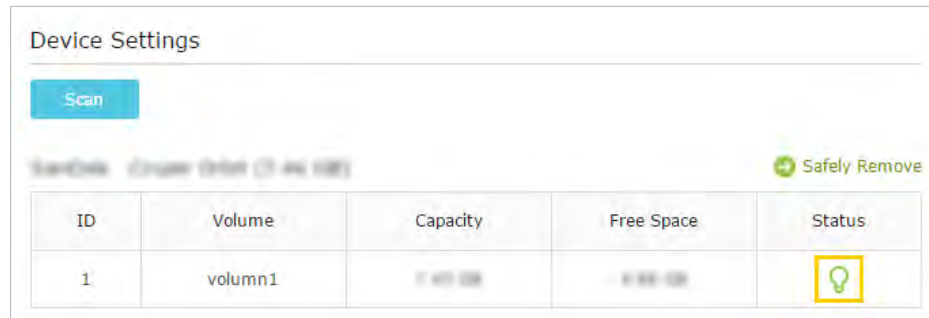
☒ Enable Media Sharing

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

4. Select the **Volume Name** and **Folder Path**, then enter a **Folder Name** as you like.
5. Tick **Enable Media Sharing** and 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.



6.4. Printer Sharing

The **Printer Sharing** feature 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.

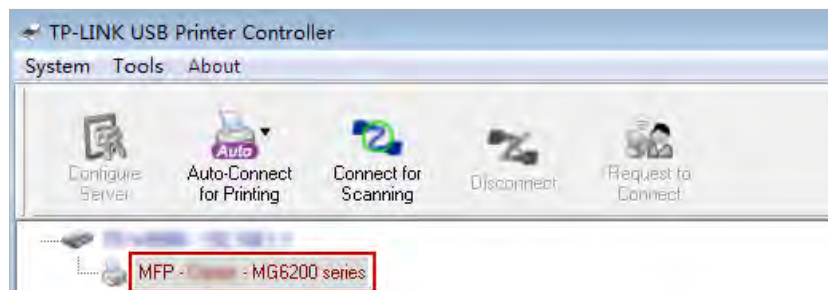


- 3) Open the uncompressed folder, then click [TP-LINK USB Printer Controller Setup](#) (for Windows users) or [TP-Link UDS Printer Controller Installer](#) (for Mac users) to install the utility.

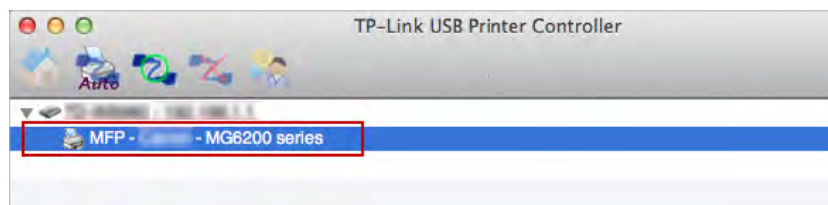
4. Access the Printer

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.

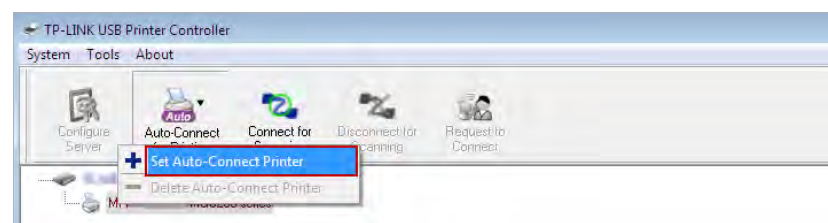


Windows

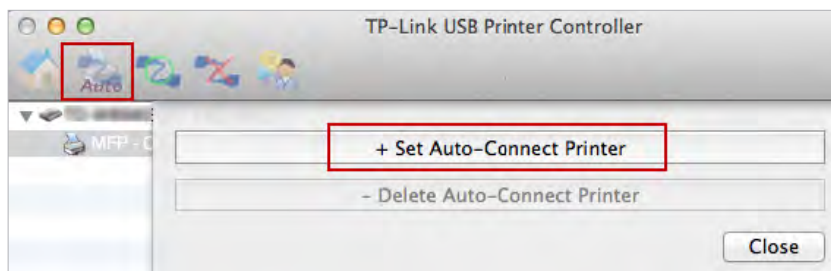


Mac

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

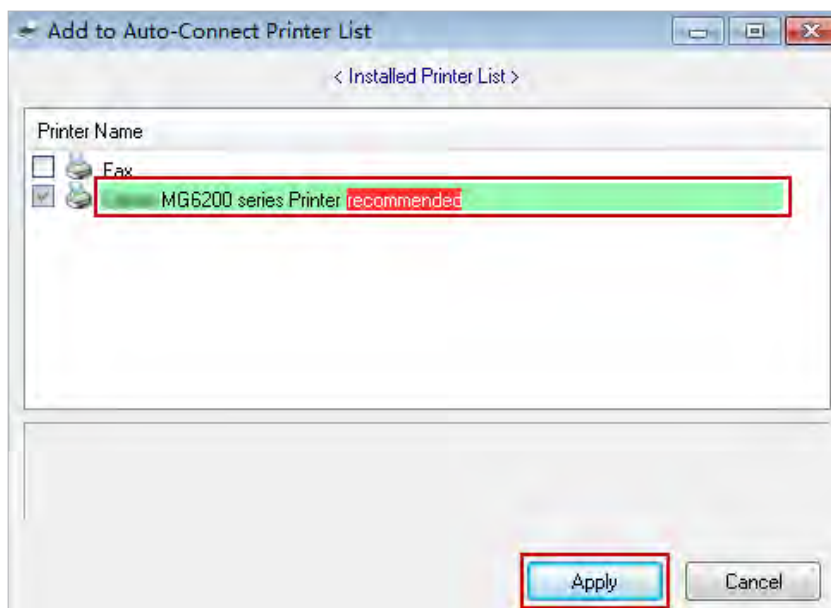


Windows

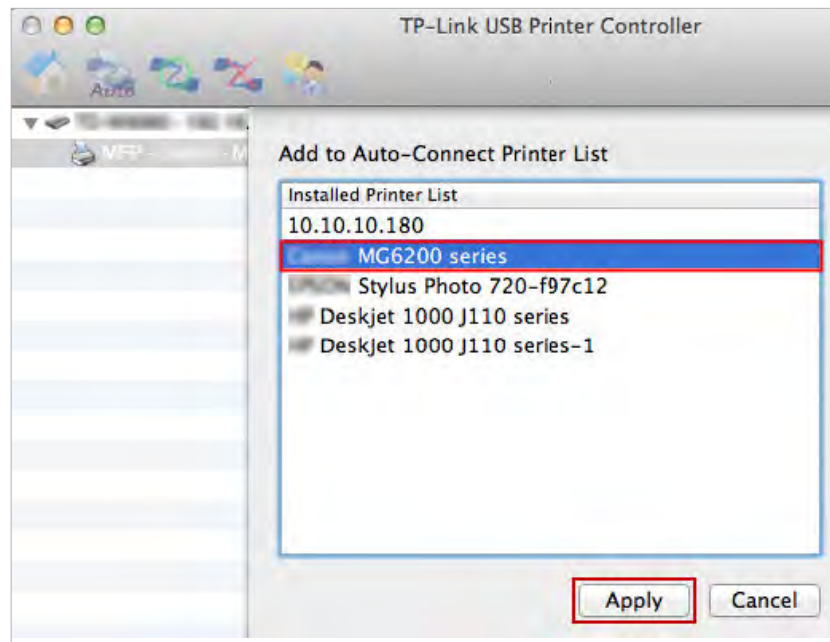


Mac

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

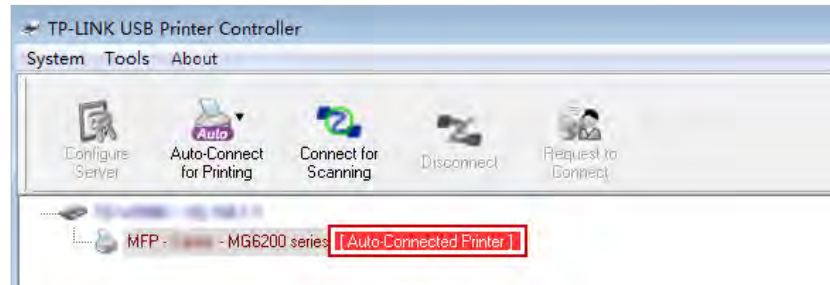


Windows



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 7

Parental Controls

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

I want to:

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

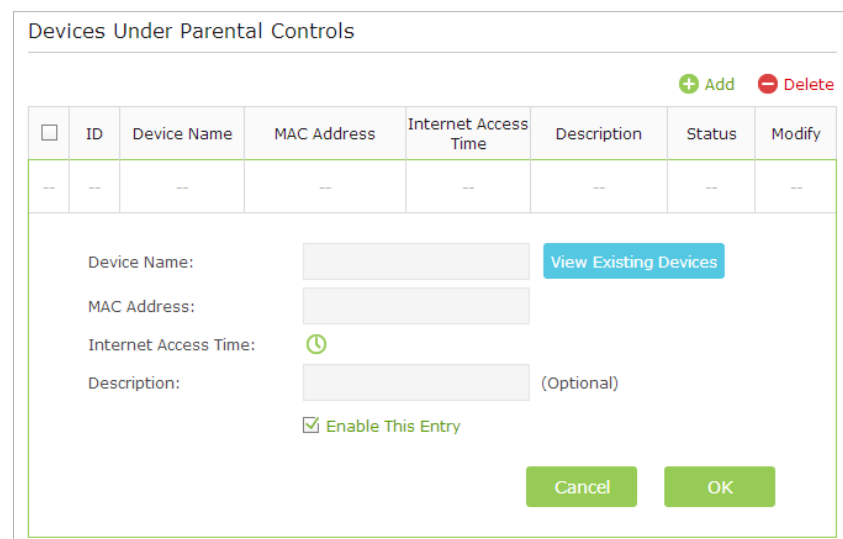
For example, I want to allow my children's devices (e.g. a computer or a tablet) to access only www.tp-link.com and Wikipedia.org from 18:00 (6PM) to 22:00 (10PM) at the weekend and not other times.

How can I do that?

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



3. Click [Add](#). And then Click [View Existing Devices](#), and select the access device. Or, input the [Device Name](#) and [MAC Address](#) manually.



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

System Time: Tue, 6th Jan, 2015 03:07:56 GMT-08:00

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

Internet Access Time

Cancel Reset OK

5. Enter a [Description](#) for the entry. Keep the [Enable This Entry](#) checkbox selected. Click [OK](#).
6. Select [Whitelist](#) as the restriction policy.

Content Restriction

Restriction Policy: ☐ Blacklist ☒ [Whitelist](#)

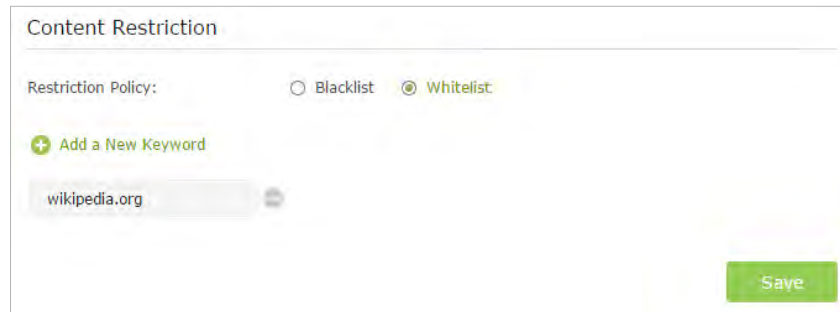
Tips:

1. With [Blacklist](#) selected, the controlled devices cannot access any websites containing the specified keywords during the Internet Access Time period.
2. 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 keyword or 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.

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



The screenshot shows a web-based interface for 'Content Restriction'. At the top, the title 'Content Restriction' is displayed. Below it, the 'Restriction Policy:' section has two radio buttons: 'Blacklist' and 'Whitelist', with 'Whitelist' being the selected option. Underneath, there is a green plus icon followed by the text 'Add a New Keyword'. A text input field contains the value 'wikipedia.org'. To the right of the input field is a small circular icon with a minus sign. In the bottom right corner, there is a green button labeled 'Save'.

Done!

Now you can control your children's Internet access according to your needs.

Chapter 8

QoS

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

This chapter contains the following sections:

- *Prioritize Internet Traffic with QoS*
- *Update the Database*

8. 1. Prioritize Internet Traffic with QoS

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

I want to:

Specify priority levels for some devices or applications.

[For example](#), I have several devices that are connected to my wireless network. I would like to :

- Set my ftp server with faster surfing speed;
- Set my phone an intermediate speed on the Internet;
- Set the WIFI-GUEST with slower surfing speed.

How can I do that?

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

QoS

QoS: ☒ Enable QoS

Upload Bandwidth: 100 Mbps

Download Bandwidth: 100 Mbps

☒ Advanced

High Priority: 60%

Middle Priority: 30%

Low Priority: 10%

Save

2. Add a high priority QoS rule for the ftp server.
 - 1) Click [Add](#) in the [High Priority](#) section.

QoS Rule List

High Priority:60%	Middle Priority:30%	Low Priority:10%
Add	Add	Add

2) Select **By Application** and select **ftp** in the list. Then click **OK**.

QoS Rule

Type: ☐ By Device ☒ By Application ☐ By Physical Port

Application

☐ SSH	☐ BT	☐ HTTPS
☐ Telnet	☐ Emule	☐ SMTP
☐ VPN	☐ Facebook	☐ POP3
☐ DNS	☐ Vonage	☒ FTP
☐ ICMP	☐ netTalk	☐ PPTP
☐ NNTP	☐ iTalkBB	☐ L2TP
☐ MSN	☐ GTalk	☐ IPSec
☐ Skype	☐ HTTP	☐ Whatsapp

Custom Application [>](#)

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

Tips:

If your application isn't listed on the screen, click **Custom Application** to add application manually.

Custom Application

Name:

Protocol:

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

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

- **Name:** Enter a name for your applicaiton.
- **Protocol:** Select the protocol for your application, if your are not sure, select **ALL**.

- **Port:** Enter the destination port for your application, usually each application has a fixed port, please ensure you enter the correct the port. In this case, the destination port for ftp is 21.

3. Add a middle priority QoS rule for the phone.

1) Select **By Device** and then click **View Existing Devices**.

QoS Rule

Type: ☒ By Device ☐ By Application ☐ By Physical Port

Device Name: [View Existing Devices](#)

MAC Address:

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

2) Choose the respective device from the list.

Access Devices List

ID	Device Name	IP Address	MAC Address	Operation
1	192.168.0.64	192.168.0.64	00-0A-EB-00-13-01	Choose
2	192.168.0.200	192.168.0.200	50-E5-49-1E-06-80	Choose
3	192.168.0.4	192.168.0.4	00-0A-EB-13-01-02	Choose
4	192.168.0.20	192.168.0.20	40-16-9F-BF-51-0C	Choose

3) Click **OK**.

QoS Rule

Type: ☒ By Device ☐ By Application ☐ By Physical Port

Device Name: [View Existing Devices](#)

MAC Address:

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

4. Add a low priority rule for the WIFI-GUEST: Select **By Physical Port** and then select **WIFI-HOST**. Click **OK**.

QoS Rule

Type:

☐ By Device

☐ By Application

☒ By Physical Port

Port:

☐ LAN1

☐ LAN2

☐ LAN3

☐ LAN4

☐ WIFI-HOST

☒ WIFI-GUEST

Cancel

OK

5. The QoS rules list will display in the table.

QoS Rule List

High Priority:60%	Middle Priority:30%	Low Priority:10%
Add	Add	Add

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

Done!

Now QoS is implemented to Prioritize Internet Traffic.

Chapter 9

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.

This chapter contains the following sections:

- *Protect the Network from Cyber Attacks*
- *Access Control*
- *IP & MAC Binding*

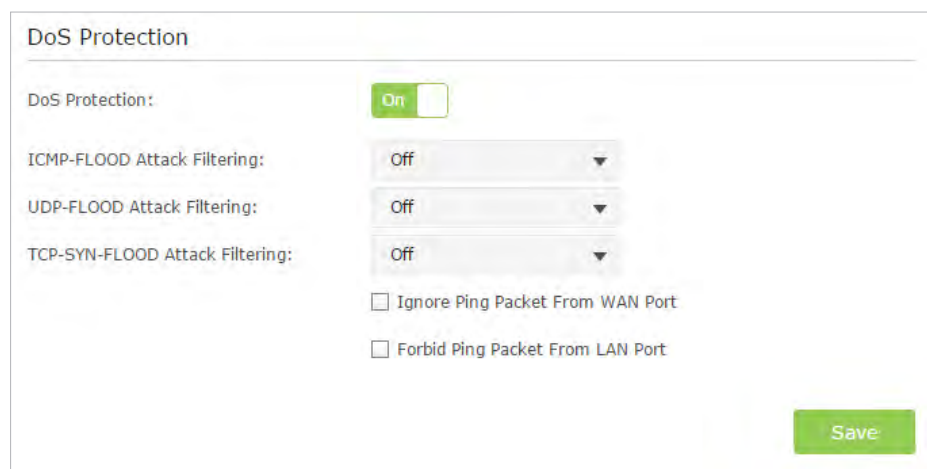
9.1. Protect the Network from Cyber Attacks

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 username and password you set for the router.
2. Go to [Advanced](#) > [Security](#) > [Settings](#).



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

Tips:

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

Blocked DoS Host List

Host Number: 0 Refresh Delete

☐	ID	IP Address	MAC Address
--	--	--	--

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

9.2. Access Control

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

I want to:

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

How can I do that?

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

Access Control

Access Control: On

- 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 [Devices Online](#) table by ticking the box.

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

Online Devices						
						Refresh Block
☐	ID	Device Name	IP Address	MAC Address	Connection Type	Modify
☒	1	XXXXXXXXXX	192.168.0.88	00-0A-EB-13-7B-00	Wired	✖
☒	2	XXXXXXXXXX	192.168.0.170	00-0A-EB-13-23-9E	Wired	✖
☒	3	XXXXXXXXXX	192.168.0.133	00-0A-EB-C2-02-38	Wired	✖
☐	4	XXXXXXXXXX	192.168.0.190	E8-DE-27-B5-E2-A3	Wired	✖
☐	5	XXXXXXXXXX	192.168.0.226	00-0A-EB-13-23-97	Wired	✖

To allow specific device(s)

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

Access Mode	
Default Access Mode:	
☐ Blacklist	☒ Whitelist
Save	

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

Devices in Whitelist				
				+ Add - Delete
☐	ID	Device Name	MAC Address	Modify
☐	1	XXXXXXXXXX	00-0A-EB-14-7B-00	✎ ✖
☐	2	XXXXXXXXXX	00-0A-EB-13-20-91	✎ ✖
☐	3	XXXXXXXXXX	00-0A-EB-AD-72-1C	✎ ✖

Device Name:
 MAC Address:
[Cancel](#) [OK](#)

- 3) Click [OK](#).

Done!

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

9.3. IP & MAC Binding

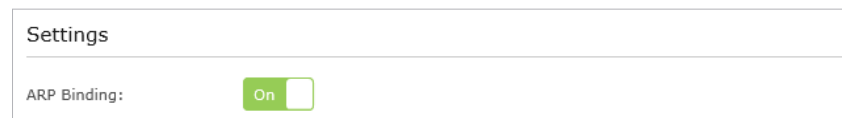
IP & MAC Binding, namely, ARP (Address Resolution Protocol) Binding, is used to bind network device's IP address to its MAC address. This will prevent ARP Spoofing and other ARP attacks by denying network access to an device with matching IP address in the Binding list, but unrecognized MAC address.

I want to:

Prevent ARP spoofing and ARP attacks.

How can I do that?

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



Settings

ARP Binding: ☒ On

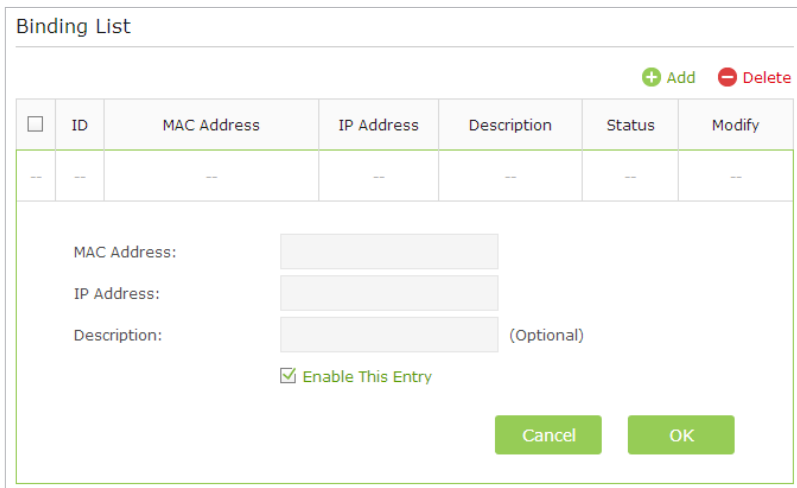
4. Bind your device(s) according to your need.

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 [Binding List](#) section.



Binding List

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

☐	ID	MAC Address	IP Address	Description	Status	Modify
☐	---	---	---	---	---	---

MAC Address:

IP Address:

Description: (Optional)

☒ Enable This Entry

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

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

Done!

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

Chapter 10

NAT Forwarding

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

With forwarding feature the router can penetrate the isolation of NAT and allows the external hosts on the Internet to initiatively communicate with the devices in the local network, thus to realize some special functions.

TP-LINK router includes 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.

This chapter 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*

10.1. Share Local Resources on the Internet by Virtual Servers

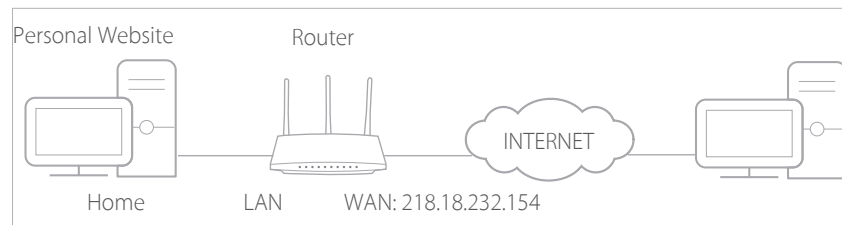
When you build up a server in the local network and want to share it on the Internet, Virtual Servers can realize the service and provide it to the Internet users. At the same time Virtual Servers can keep the local network safe as other services are still invisible from the Internet.

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

I want to:

Share my personal website I've built in local network with my friends through the Internet.

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



How can I do that?

1. Assign a static IP address to your PC, for example 192.168.0.100.
2. Visit <http://tplinkwifi.net>, and log in with the username and 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 with contents. Enter the PC's IP address 192.168.0.100 into the **Internal IP** field.
5. Click **OK**.

Virtual Servers

+ 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

Tips:

1. 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.
2. 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.
3. 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:

1. WAN IP should be a public IP address. For the WAN IP is assigned dynamically by 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.
2. 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.

10.2. Open Ports Dynamically by Port Triggering

Port Triggering can specify a triggering port and its corresponding external ports. When a host in 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 and video players, common applications include 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 username and 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 **External Port**, **Internal Port** and **Protocol** will be automatically filled with contents. 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

Cancel
OK

Tips:

1. You can add multiple port triggering rules according to your network need.
2. The triggering ports can not be overlapped.
3. 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.

10.3. Make Applications Free from Port Restriction by DMZ

When a PC is set to be a DMZ (Demilitarized Zone) host in 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 hazard. If DMZ is not in use, please disable it in time.

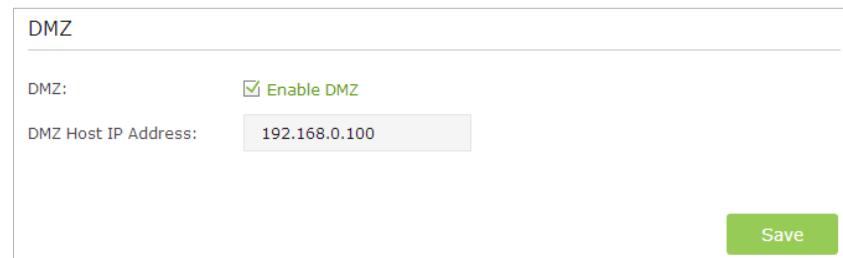
I want to:

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 with all ports opened.

How can I do that?

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



DMZ

DMZ: ☒ Enable DMZ

DMZ Host IP Address:

Save

5. Click [Save](#).

Done!

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

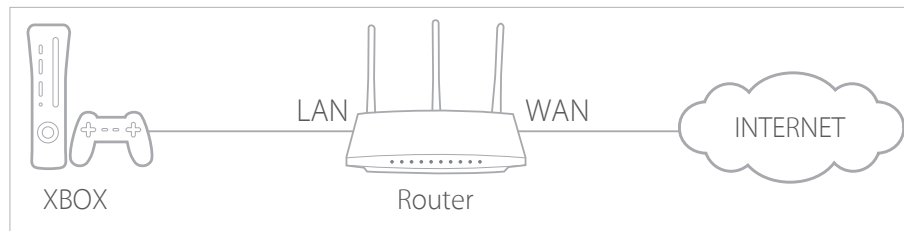
10.4. Make Xbox Online Games Run Smoothly by UPnP

UPnP (Universal Plug and Play) protocol allows the 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 both sides of NAT device can freely communicate with each other 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:**

1. UPnP is enabled by default in this router.
2. Only the application supporting UPnP protocol can use this feature.
3. 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 username and password you set for the router.
2. Go to **Advanced** > **NAT Forwarding** > **UPnP** and toggle on or off according to your needs.

UPnP

UPnP: ☒ On

UPnP Service List

Total Clients: 0 [Refresh](#)

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

Chapter 11

VPN Server

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

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

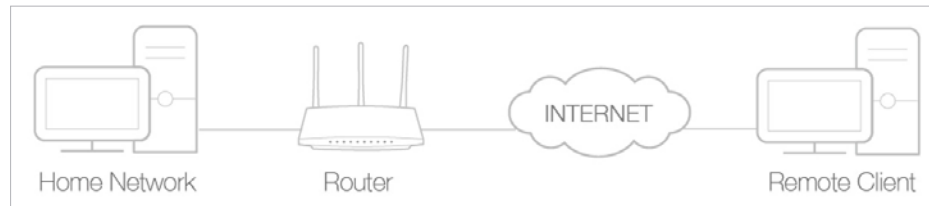
PPTP VPN is more easily used and its speed is faster, it's compatible with most operating systems and also supports mobile devices. Its security is poor and your packets may be cracked easily, and PPTP VPN connection may be prevented by some ISP.

This chapter contains the following sections, please choose the appropriate VPN server connection type according to your needs.

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

11.1. Use OpenVPN to Access Your Home Network

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



Step1. Set up OpenVPN Server on Your Router

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

OpenVPN

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

☒ Enable VPN Server

Service Type: ☒ UDP ☐ TCP

Service Port: 1194

VPN Subnet/Netmask: 10.8.0.0 255.255.255.0

Client Access: ☒ Home Network Only ☐ Internet and Home Network

Save

Note:

1. Before you enable VPN Server, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router's WAN port and synchronize your System Time with Internet.
2. The first time you configure the OpenVPN Server, you may need to **Generate** a certificate before you enable the VPN Server.
3. Select the **Service Type** (communication protocol) for OpenVPN Server: UDP, TCP.
4. Enter a VPN **Service Port** to which a VPN client connects, and the port number should be between 1024 and 65535.
5. In **VPN Subnet/Netmask** field, enter the range of IP addresses that can be leased to the client by the OpenVPN server.
6. Select your **Client Access** type., select **Home Network Only** if you only want the remote client to access your home network, select **Internet and Home Network** if the remote client also want to access Internet through VPN Server.

7. Click [Save](#).
8. Click [Generate](#) to generate a new certificate.

Certificate

Generate the certificate.

Generate

Note:

If you have already generated one, please skip this step, or click [Generate](#) to update the certificate.

9. Click [Export](#) to save the OpenVPN configuration file. Remote client will use this configuration file to access your router.

Configuration File

Export the configuration.

Export

Step 2. Configure OpenVPN Connection on Your Remote Client

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

Note:

You need to install the [OpenVPN](#) client utility on each client that you plan to use for VPN connections to your router. Mobile devices should download third-party app from Google Play or Apple App Store.

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

11.2. Use PPTP VPN to Access Your Home Network

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

Step 1. Set up PPTP VPN Server on Your Router

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

PPTP VPN

☒ Enable VPN Server

Client IP Address: - (up to 10 clients)

☒ Advanced

Allow Samba (Network Place) access: ☒

Allow NetBIOS passthrough: ☒

Allow Unencrypted connections: ☒

Save

Note:

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

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

Account List (up to 16 users)

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

☐	ID	Username	Password	Modify
☐	—	—	—	—

Username:

Password:

Cancel **OK**

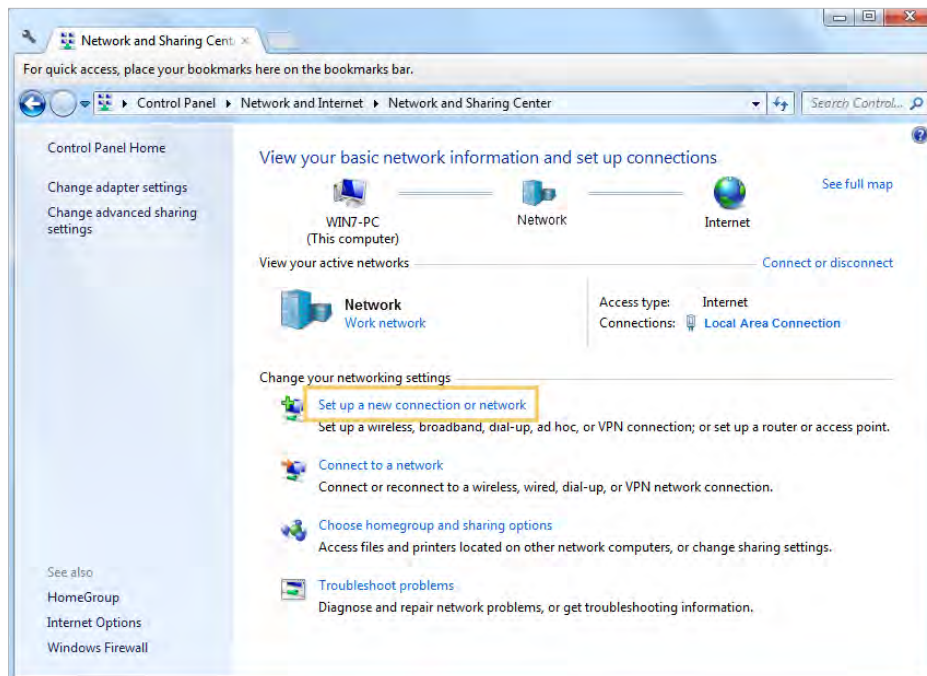
- 1) Click [Add](#).

- 2) Enter the [Username](#) and [Password](#) to authenticate clients to the PPTP VPN Server.
- 3) Click [OK](#).

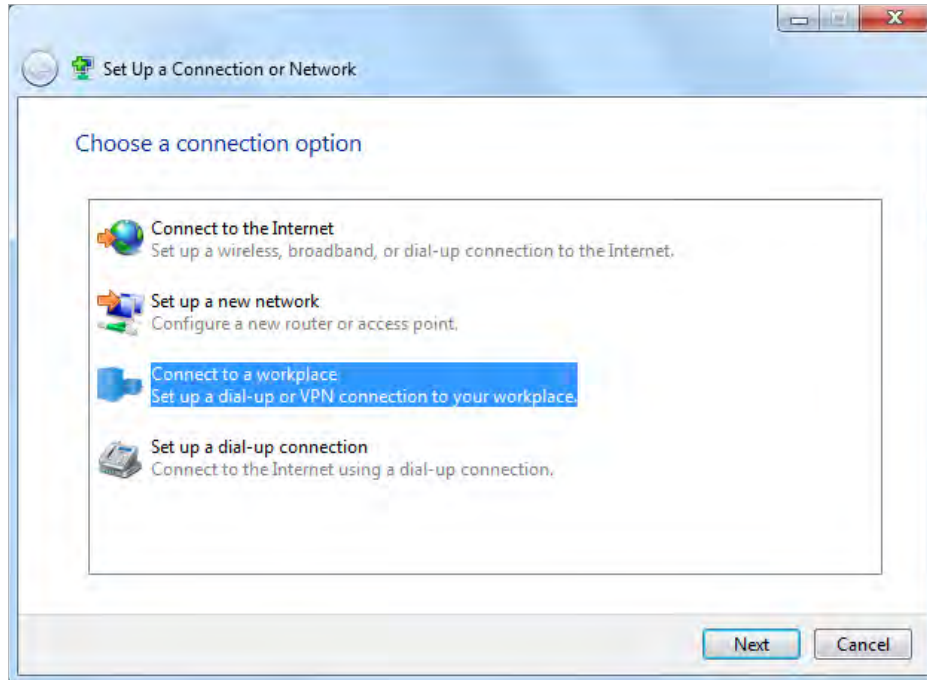
Step 2. Configure PPTP VPN Connection on Your Remote Client

Remote client can use Windows built-in PPTP software or third-party PPTP software to connect to PPTP Server. Here we use [Windows built-in PPTP software](#) as an example.

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



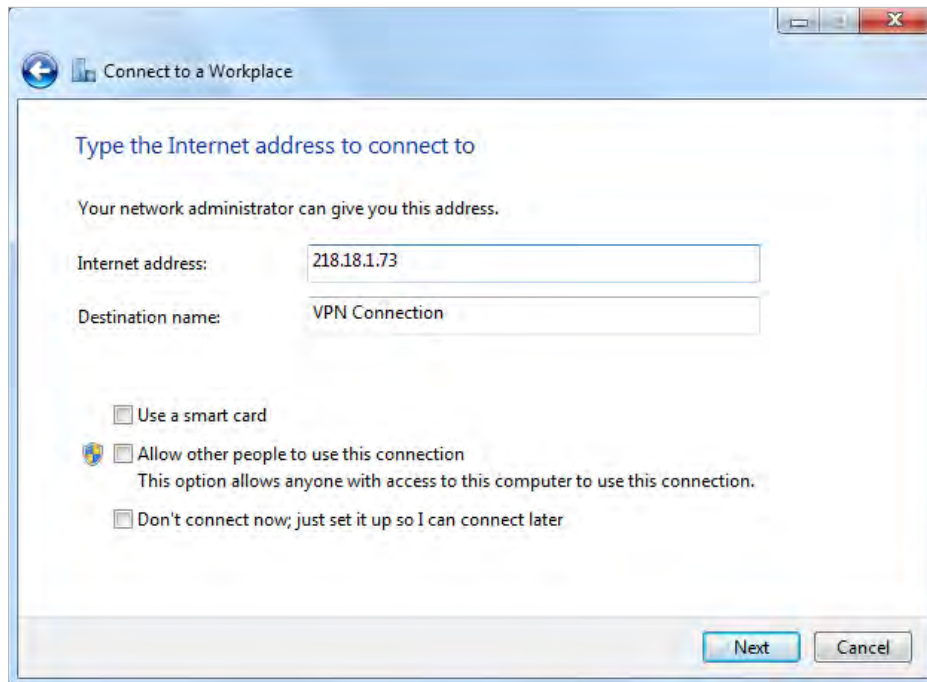
3. Select **Connect to a workplace** and click **Next**.



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

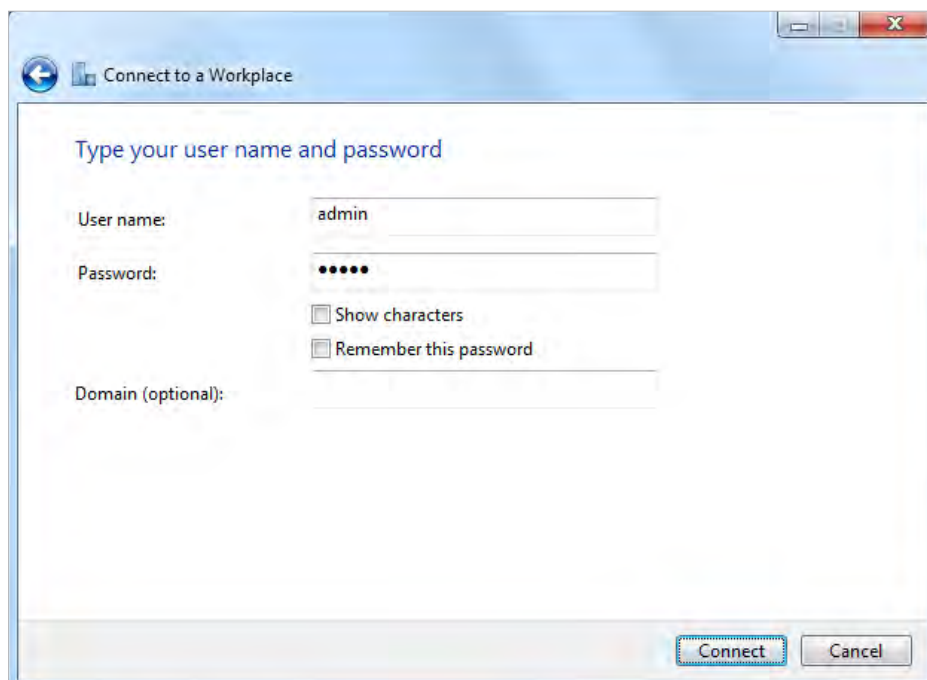


5. Enter the WAN IP address of the router (for example: 218.18.1.73) in the **Internet address** field. Click **Next**.



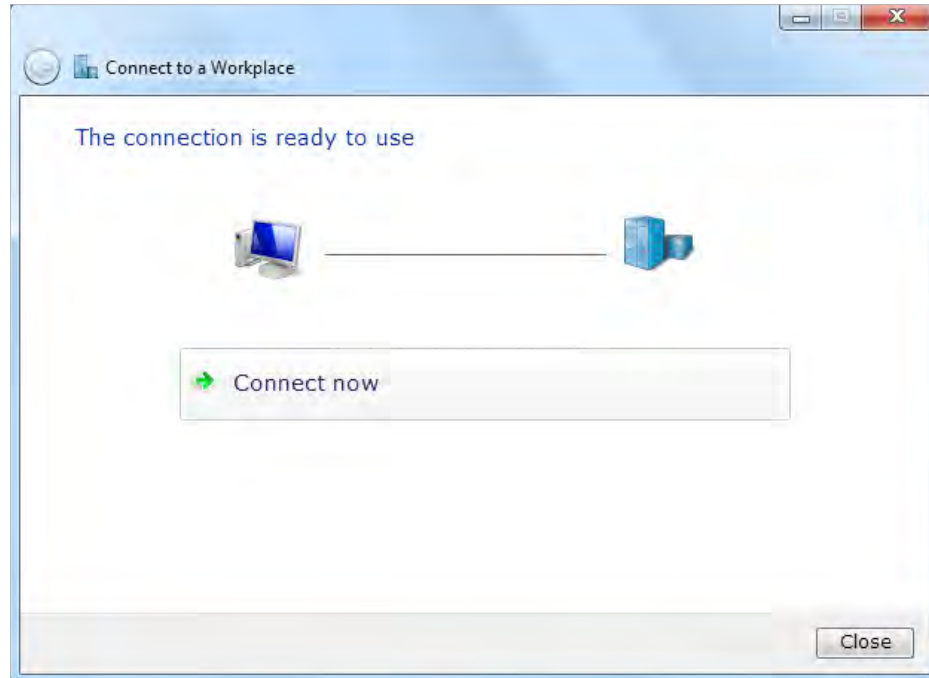
The screenshot shows the 'Connect to a Workplace' dialog box. The title bar says 'Connect to a Workplace'. The main text says 'Type the Internet address to connect to'. Below this, it says 'Your network administrator can give you this address.' There are two input fields: 'Internet address:' with the value '218.18.1.73' and 'Destination name:' with the value 'VPN Connection'. Below these fields are three checkboxes: 'Use a smart card' (unchecked), 'Allow other people to use this connection' (unchecked) with a subtext 'This option allows anyone with access to this computer to use this connection.', and 'Don't connect now; just set it up so I can connect later' (unchecked). At the bottom right are 'Next' and 'Cancel' buttons.

6. Enter the **User name** and **Password**, it's the username and password you have set on your router, and click **Connect**.



The screenshot shows the 'Connect to a Workplace' dialog box. The title bar says 'Connect to a Workplace'. The main text says 'Type your user name and password'. There are two input fields: 'User name:' with the value 'admin' and 'Password:' with masked characters '•••••'. Below the password field are two checkboxes: 'Show characters' (unchecked) and 'Remember this password' (unchecked). Below these fields is a 'Domain (optional):' input field. At the bottom right are 'Connect' and 'Cancel' buttons.

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



Chapter 12

Customize Your Network Settings

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

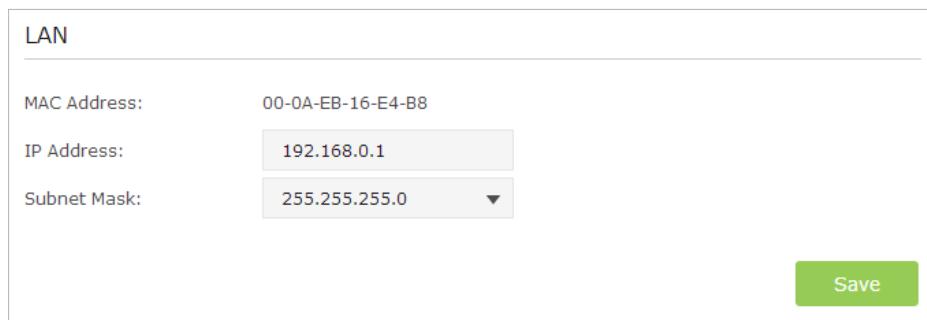
This chapter contains the following sections:

- *Change the LAN Settings*
- *Configure to Support IPTV Service*
- *Specify DHCP Server Settings*
- *Set Up a Dynamic DNS Service Account*
- *Create Static Routes*
- *Specify Wireless Settings*
- *Use WPS for Wireless Connection*

12.1. Change the LAN Settings

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

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



LAN

MAC Address: 00-0A-EB-16-E4-B8

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0 ▼

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.

12.2. Configure to Support IPTV Service

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

How can I do that?

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

IGMP Proxy:	☒ Enable
IGMP Version:	V2 ▼

2) Click [Save](#).

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

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

1) Tick [Enable IPTV](#).

2) Select the appropriate [Mode](#) according to your ISP.

- Select [Bridge](#) if your ISP is not listed and no other parameters are required, and then skip to Step 4.
- Select [Custom](#) if your ISP is not listed but provides necessary parameters.

IPTV:	☒ Enable IPTV
Mode:	Bridge ▼ Bridge Russia Singapore-ExStream Malaysia-Unifi Malaysia-Maxis Custom
LAN1:	
LAN2:	
LAN3:	
LAN4:	
Save	

3) After you have selected a mode, the necessary parameters are predetermined. You can perform other configuration, e.g. enter the [IPTV Multicast VLAN ID](#) and select the [IPTV Multicast VLAN Priority](#) in [Russia](#) mode according to your ISP.

4) For [Russia](#), [Singapore-ExStream](#), [Malaysia-Unifi](#) and [Malaysia-Maxis](#) mode, connect the set-top box to the predetermined LAN port. For [Bridge](#) and [Custom](#) mode, select the [LAN](#) type and connect the set-top box to the corresponding port.

5) Click [Save](#).

Done!

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

[Tips](#)

Qos and IPTV cannot be enabled at the same time.

12.3. Specify DHCP Server Settings

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

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

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



The screenshot shows the 'Settings' page for the DHCP Server. It includes a checkbox for 'Enable DHCP Server' which is checked. Below this are input fields for 'IP Address Pool' (192.168.0.100 - 192.168.0.199), 'Address Lease Time' (120 minutes), 'Default Gateway' (192.168.0.1), 'Primary DNS', and 'Secondary DNS'. A green 'Save' button is located at the bottom right.

Settings	
DHCP Server:	☒ Enable DHCP Server
IP Address Pool:	192.168.0.100 - 192.168.0.199
Address Lease Time:	120 minutes. (1-2880. The default value is 120.)
Default Gateway:	192.168.0.1 (Optional)
Primary DNS:	(Optional)
Secondary DNS:	(Optional)
Save	

1. Make sure that the [Enable DHCP Server](#) checkbox is selected.
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 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

☐	ID	MAC Address	Reserved IP Address	Description	Status	Modify
☐	---	---	---	---	---	---

MAC Address:

View Existing Devices

IP Address:

Description:

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

☐ Enable This Entry

Cancel

OK

2. Click [View Existing Devices](#) or enter the [MAC address](#) of the client device.
3. Enter the [IP address](#) to reserve for the client device.
4. Enter the [Description](#) for this entry.
5. Tick the [Enable This Entry](#) checkbox and click [OK](#).

12.4. Set Up a Dynamic DNS Service Account

Most ISPs assign a dynamic IP address to the router and you can use this IP address to access your router remotely. However, the IP address can change any 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 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.

To set up DDNS, please follow the instructions below:

1. Visit <http://tplinkwifi.net>, and log in with the username and 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, select a service provider and click [Go to register](#).

Dynamic DNS

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

Username:

Password:

Domain Name:

Update Interval:

4. Enter the username, password and domain name of the account (such as lisadns.ddns.net).

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

Tips:

If you want to use a new DDNS account, please [logout](#) first, and then login with the new account.

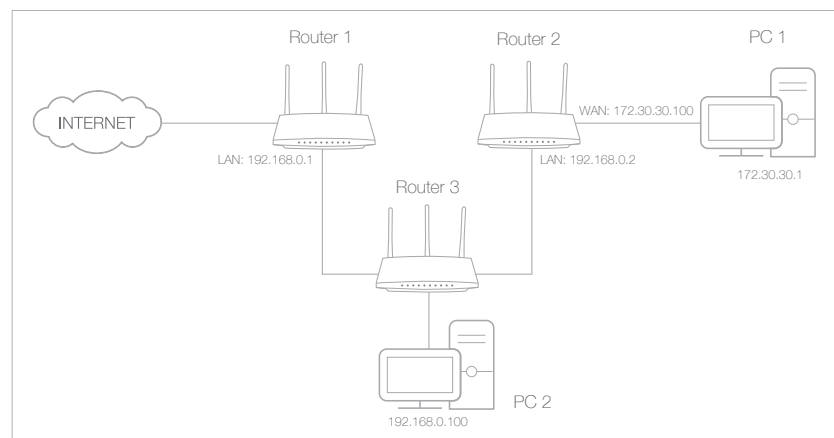
12.5. Create Static Routes

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

I want to:

Visit multiple networks and servers at the same time.

[For example](#), in a small office, my PC can surf the Internet, but I also want to visit my company's network. Now I have a switch and another router. 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 router's LAN IP addresses to two different IP addresses on the same subnet. Disable Router 2's DHCP function.
2. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
3. Go to [Network](#) > [Advanced Routing](#).
4. Click [Add](#) and finish the settings according to the following explanations:

Static Routing

+ Add - Delete

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

Network Destination:

Subnet Mask:

Default Gateway:

Interface:

Description:

☒ Enable This Entry

Network Destination: The destination IP address that you want to assign to a static route. This IP address cannot be on the same subnet with the WAN IP or LAN IP of the router. 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 2 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, so **LAN** should be selected.

Description: Enter a description for this static routing entry.

5. Click **OK**.

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

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

Done!

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

12.6. Specify Wireless Settings

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

Visit <http://tplinkwifi.net>, and log in with the username and 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 clear the **Enable Wireless Radio** checkbox. In this case, all the wireless settings will be invalid.

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

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

■ Note:

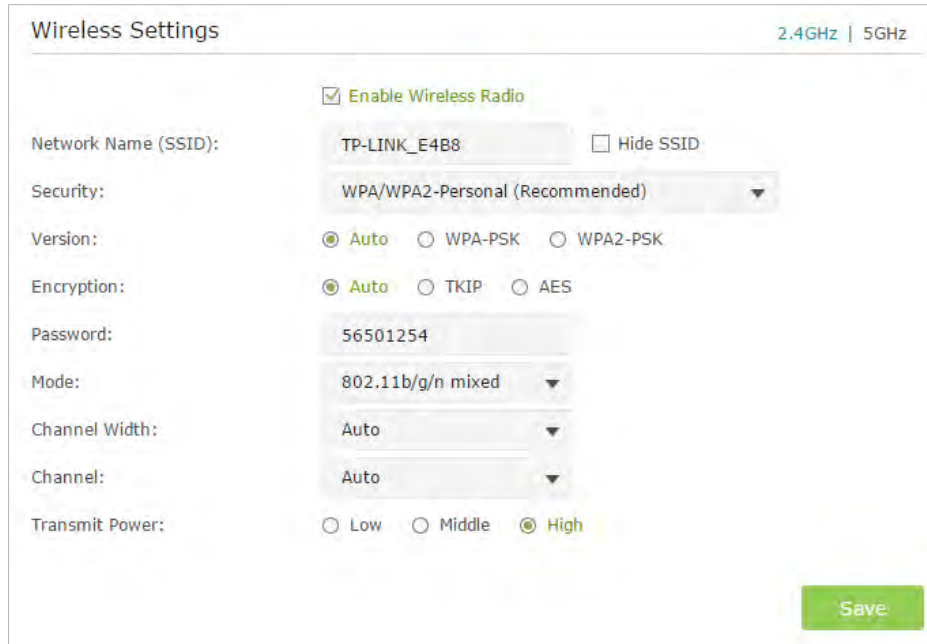
If you change the wireless settings with a wireless device, you will be disconnected when the settings are effective. Please write down the new SSID and password for future use.

➤ **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](#).

The image shows a 'Wireless Settings' configuration page. At the top right, there are tabs for '2.4GHz' and '5GHz'. The main settings include: 'Enable Wireless Radio' (checked), 'Network Name (SSID):' (TP-LINK_E4B8) with a 'Hide SSID' checkbox, 'Security:' (WPA/WPA2-Personal (Recommended)), 'Version:' (Auto, WPA-PSK, WPA2-PSK), 'Encryption:' (Auto, TKIP, AES), 'Password:' (56501254), 'Mode:' (802.11b/g/n mixed), 'Channel Width:' (Auto), 'Channel:' (Auto), and 'Transmit Power:' (Low, Middle, High). A green 'Save' button is at the bottom right.

2. Select the wireless network [2.4GHz](#) or [5GHz](#).
3. Select an option from the [Security](#) drop-down list. We recommend you don't change the default settings unless necessary. If you select other options, configure the related parameters according to the help page.

In addition

- [Mode](#) - Select a transmission mode according to your wireless client devices. It is recommended to just leave it as default.
- [Channel Width](#) - Select a channel width (bandwidth) for the wireless network.
- [Channel](#) - Select an operating channel for the wireless network. It is recommended to leave the channel to [Auto](#), if you are not experiencing the intermittent wireless connection issue.
- [Transmit Power](#) - Select either [High](#), [Middle](#) or [Low](#) to specify the data transmit power. The default and recommended setting is [High](#).

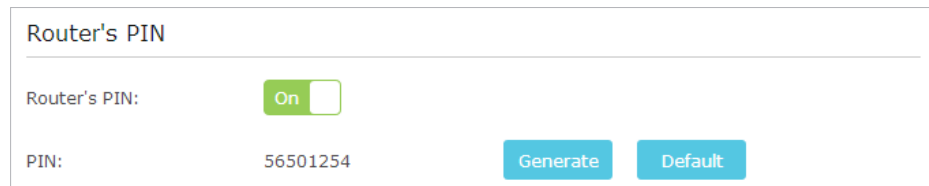
12.7. Use WPS for Wireless Connection

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 username and password you set for the router.
2. Go to [Advanced](#) > [Wireless](#) > [WPS](#).

12.7.1. Set the Router's PIN

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



Router's PIN

Router's PIN: ☒ On

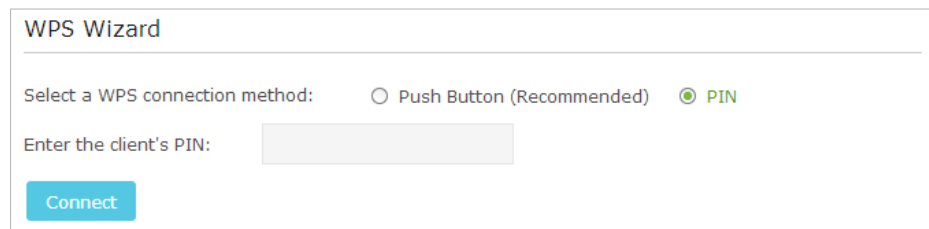
PIN: 56501254 [Generate](#) [Default](#)

Note:

1. If you want to enable/disable the WPS feature, go to [System Tools](#) > [System Parameters](#) > [WPS](#), select or clear the [Enable WPS](#) check box.
2. 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.

12.7.2. Use the WPS Wizard for Wi-Fi Connections

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



WPS Wizard

Select a WPS connection method: ☐ Push Button (Recommended) ☒ PIN

Enter the client's PIN:

[Connect](#)

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.

Chapter 13

Manage the Router

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

This chapter includes the following sections:

- *Set Up System Time*
- *Test the Network Connectivity*
- *Upgrade the Firmware*
- *Backup and Restore Configuration Settings*
- *Change the Administrator Account*
- *Password Recovery*
- *Local Management*
- *Remote Management*
- *System Log*
- *Monitor the Internet Traffic Statistics*
- *Control LEDs*

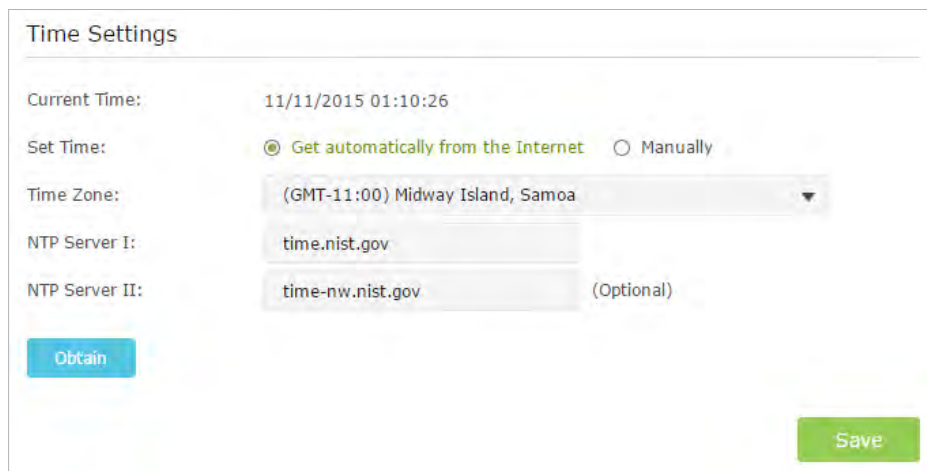
13.1. Set Up System Time

System time is the time displayed while the router is running. The system time you configure here will be used for other time-based functions like Parental Controls. You can choose the way you prefer to obtain the system time.

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

➤ **To get time from the Internet:**

1. In the [Set Time](#) field, select [Get automatically from the Internet](#).

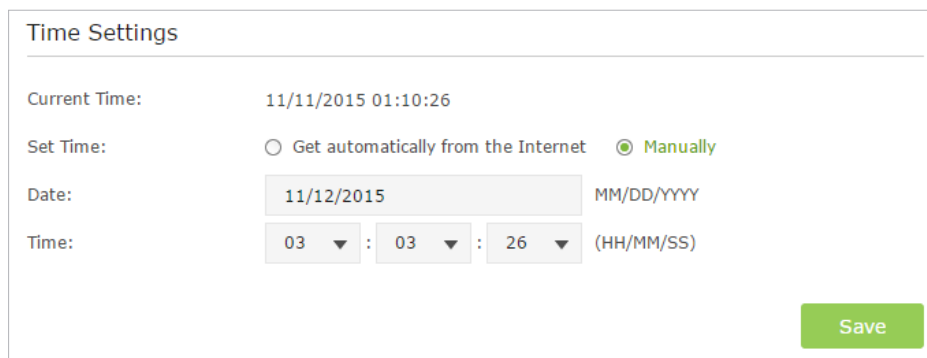


The screenshot shows the 'Time Settings' page. At the top, 'Current Time' is 11/11/2015 01:10:26. Under 'Set Time', the radio button for 'Get automatically from the Internet' is selected, while 'Manually' is unselected. The 'Time Zone' dropdown is set to '(GMT-11:00) Midway Island, Samoa'. 'NTP Server I' is 'time.nist.gov' and 'NTP Server II' is 'time-nw.nist.gov' (Optional). There is an 'Obtain' button and a 'Save' button.

2. Select your local [Time Zone](#) from the drop-down list.
3. In the [NTP Server I](#) field, enter the IP address or domain name of your desired NTP Server.
4. In the [NTP Server II](#) field, enter the IP address or domain name of the second NTP Server. (Optional)
5. Click [Obtain](#) to get the current Internet time and click [Save](#).

➤ **To manually set the date and time:**

1. In the [Set Time](#) field, select [Manually](#).



The screenshot shows the 'Time Settings' page with the 'Manually' radio button selected. The 'Date' field is set to '11/12/2015' with a format hint 'MM/DD/YYYY'. The 'Time' field is set to '03 : 03 : 26' with a format hint '(HH/MM/SS)'. There is a 'Save' button.

2. Set the current **Date** (In **MM/DD/YYYY** format).
3. Set the current **Time** (In **HH/MM/SS** format).
4. Click **Save**.

➤ **To set up Daylight Saving Time:**

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

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**.

13.2. Test the Network Connectivity

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

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

3. Enter the information with the help of page tips:
 - 1) Choose **Ping** or **Traceroute** as the diagnostic tool to test the connectivity;
 - **Ping** is used to test the connectivity between the router and the tested host, and measure the round-trip time.

- **Traceroute** is used to display the route (path) your router has passed to reach the tested host, and measure transit delays of packets across an Internet Protocol network.

2) Enter the **IP Address** or **Domain Name** of the tested host.

4. Click **Start** to begin the diagnostics.

Tips:

Click **Advanced**, you can modify the ping count, ping packet size or the Traceroute Max TTL. It's recommended to keep the default value.

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

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

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

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

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

13.3. Upgrade the Firmware

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

We will inform you through the web management page if there's any update firmware available for your router. Also, the latest firmware will be released at TP-LINK official website, you can download it from the **Support** page of our website www.tp-link.com for free.

Note:

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

13.3.1. Online Upgrade

1. Visit <http://tplinkwifi.net>, and log in with the username and password you've 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.



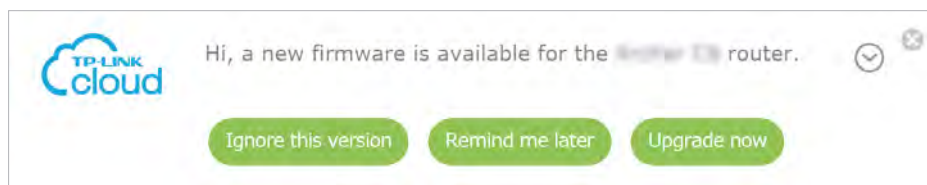
3. Focus on the [Online Upgrade](#) section, and click [Upgrade](#).



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

 Tips:

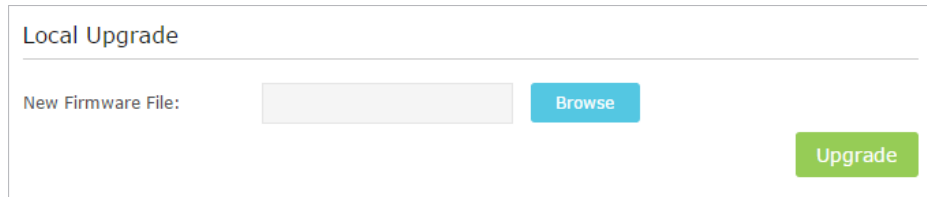
If there's a new and important firmware update for your router, you will see the notification (similar as shown below) on your computer as long as a web browser is opened. Click [Upgrade now](#), and log into the web management page with the username and password you set for the router. You will see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



13.3.2. Local Upgrade

1. Download the latest firmware file for the router from www.tp-link.com.
2. Visit <http://tplinkwifi.net>, and log in with the username and 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**.



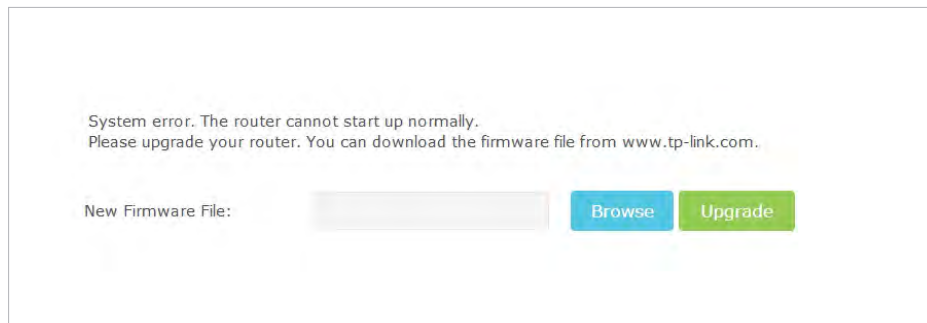
The screenshot shows the 'Local Upgrade' section of a router's web interface. It features a label 'New Firmware File:' followed by a text input field and a blue 'Browse' button. To the right of these elements is a green 'Upgrade' button.

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

13.3.3. Restore Interrupted Upgrade after Power Failure

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

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



The screenshot shows a system error message on the router's web interface. The message reads: 'System error. The router cannot start up normally. Please upgrade your router. You can download the firmware file from www.tp-link.com.' Below the message is the 'New Firmware File:' label, a text input field, a blue 'Browse' button, and a green 'Upgrade' button.

4. Click **Browse** and select the downloaded firmware file.
5. Click **Upgrade** and wait for a few minutes until the router completes the upgrading and restarts.

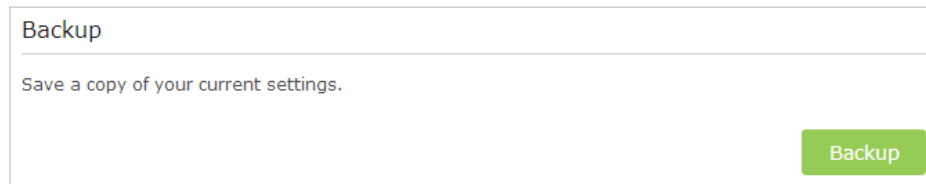
13.4. Backup and Restore Configuration Settings

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

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

➤ **To backup configuration settings:**

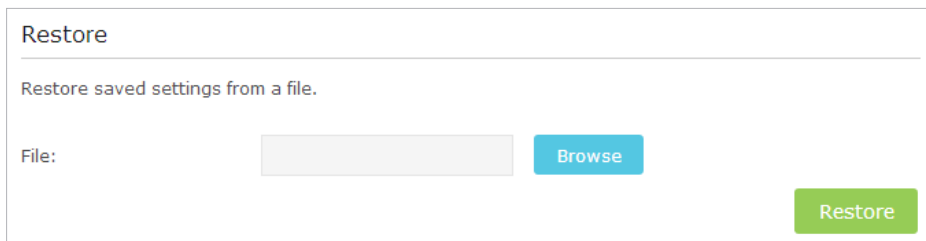
Click [Backup](#) to save a copy of the current settings to your local computer. A '.bin' file of the current settings will be stored to your computer.



The screenshot shows a web interface titled "Backup". Below the title is a horizontal line, followed by the text "Save a copy of your current settings.". In the bottom right corner, there is a green button labeled "Backup".

➤ **To restore configuration settings:**

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



The screenshot shows a web interface titled "Restore". Below the title is a horizontal line, followed by the text "Restore saved settings from a file.". Underneath, there is a label "File:" followed by a text input field and a blue button labeled "Browse". In the bottom right corner, there is a green button labeled "Restore".

2. Wait a few moments 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.



The screenshot shows a web interface titled "Factory Default Restore". Below the title is a horizontal line, followed by the text "Revert all the configuration settings to their default values.". In the bottom right corner, there is a green button labeled "Factory Restore".

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

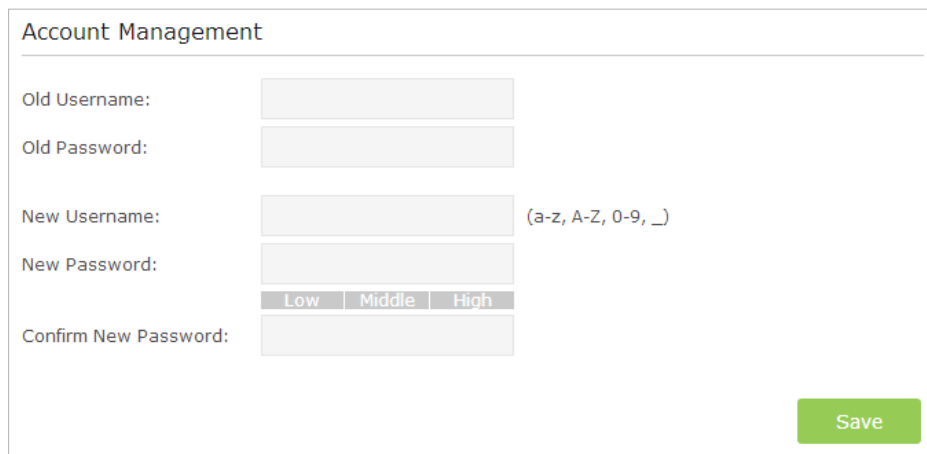
■ **Note:**

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

13.5. Change the Administrator Account

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

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



The screenshot shows the 'Account Management' section of a web interface. It contains several input fields: 'Old Username:', 'Old Password:', 'New Username:', 'New Password:', and 'Confirm New Password:'. The 'New Password:' field has a strength indicator below it with three tabs: 'Low', 'Middle', and 'High'. To the right of the 'New Username:' field, there is a hint '(a-z, A-Z, 0-9, _)'. A green 'Save' button is located at the bottom right of the form.

3. Enter the old username and old password. Enter the new username and enter the new password twice (both case-sensitive). Click [Save](#).
4. Use the new username and password for the following logins.

13.6. Password Recovery

This feature allows you to recover your default login username and password in case you forget them.

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

 Tips:

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

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

Password Recovery

☒ Enable Password Recovery

From:

To:

SMTP Server:

☒ Enable Authentication

Username:

Password:

Test Email Save

5. Click [Save](#).

You can click [Test Email](#) to test whether the configuration is successful. To recover the default login username and password, please refer to [FAQ](#).

13.7. Local Management

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

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

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

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

Local Management

Access for All LAN Connected Devices: ☒ On

Toggle On to enable the management for all devices on LAN or keep it Off to enable the management for a specific device.

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

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

Local Management

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

+ Add - Delete

☐	ID	MAC Address	Description	Status	Modify
☐	--	--	--	--	--

MAC Address: View Existing Devices

Description:

☐ Enable This Entry

Cancel
OK

☐	1	50-E5-49-1E-06-80	Your PC!		
--------------------------	---	-------------------	----------	--	--

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

13.8. Remote Management

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

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

Remote Management

☒ Disable Remote Management
☐ Enable Remote Management for All Devices
☐ Enable Remote Management for Specified Devices

Web Management Port:

Remote Management IP Address:

Save

- **Forbid all devices to manage the router remotely:** Select [Disable Remote Management](#) and click [Save](#).
- **Allow all devices to manage the router remotely:**
 - 1) Select [Enable Remote Management for All Devices](#).
 - 2) Enter [Web Management Port](#) (1024-65535 or 80).
 - 3) Click [Save](#).

Devices on the Internet can log in to [http://Router's WAN IP address:port number](#) (such as [http://113.116.60.229:1024](#)) to manage the router.

 Tips:

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

- **Allow specific devices to manage the router remotely:**
 - 1) Select [Enable Remote Management for Specified Devices](#).
 - 2) Enter [Web Management Port](#) (1024-65535 or 80).
 - 3) In [Remote Management IP address](#), enter the IP address of the remote device to manage the router.
 - 4) Click [Save](#).

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

 Tips:

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

13.9. System Log

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

➤ **To Save the System Log in Local:**

1. Visit [http://tplinkwifi.net](#), and log in with the username and password you set for the router.
2. Go to [Advanced > System Tools > System Log](#).
3. Choose the type and level of the system logs according to your need.
4. Click [Save Log](#) to save the system logs to local.

System Log

Log Filter: Type= ALL and Level= ALL

Refresh Delete All

ID	Time	Type	Level	Log Content
1	2015-11-02 15:42:37	Local Management	NOTICE	[14777] Accessable mode change: Devices in the list.
2	2015-11-02 15:40:45	Local Management	NOTICE	[9995] Accessable mode change: All devices.
3	2015-11-02 15:40:42	Local Management	NOTICE	[9879] Accessable mode change: Devices in the list.
4	1970-01-03 18:20:01	IP & MAC Binding	INFO	[25481] Daemon connection succeeded
5	1970-01-03 18:20:01	IP & MAC Binding	INFO	[25481] Config interface initialization succeeded

1

Mail Settings

Mail Log Save Log

➤ To Send the System Log to a Mailbox at a Fixed Time:

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

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

Mail Settings

From: zhangsan@hotmail.com

To: homezhang@hotmail.com

SMTP Server: smtp-mail.outlook.com

☒ Enable Authentication

Username: zhangsan

Password:

☒ Enable Auto Mail

☒ Log at 08 : 00 (HH:MM) everyday

☐ Log every 24 hours

Save

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

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

- 4) Select **Enable Authentication**.

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

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

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

- 8) Set a fixed time. The recipient will receive the system log sent at this time every day.

5. Click **Save**.

13. 10. Monitor the Internet Traffic Statistics

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

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

3. Toggle on [Traffic Statistics](#), and then you can monitor the traffic statistics in [Traffic Statistics List](#) section.

Traffic Statistics					
Traffic Statistics: ☒					
Traffic Statistics List					
Refresh Reset All Delete All					
IP Address/MAC Address	Total Packets	Total Bytes	Current Packets	Current Bytes	Modify
192.168.0.200/ 50-E5-49-1E-06-80	0	0	0	0	Refresh Delete
192.168.0.20/ 40-16-9F-BF-51-0C	1	594	0	0	Refresh Delete
192.168.0.155/ 00-14-78-43-45-45	1	346	0	0	Refresh Delete
192.168.0.1/ 00-0A-EB-13-09-19	1	594	0	0	Refresh Delete
192.168.0.123/ C4-E9-84-23-06-C6	1	594	0	0	Refresh Delete
192.168.0.4/ 00-0A-EB-13-01-02	2	412	0	0	Refresh Delete
192.168.0.100/ C8-85-50-5D-02-40	0	0	0	0	Refresh Delete
192.168.0.184/ C8-85-50-5D-02-40	0	0	0	0	Refresh Delete
< 1 2 >					

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

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

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

Click [Refresh](#) to reset the statistic information of the specific device.

Click [Delete](#) to delete the specific device item in the list.

13. 11. Control LEDs

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

➤ To turn on or off the LEDs:

- Press the LED button on the router (if available) about 2 seconds to turn on or off the LEDs.
- Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router. Click the [LED](#) icon on the top right of the page.

➤ **To turn off LEDs during Night Mode Period:**

- 1) Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
- 2) Go to [Advanced](#) > [System Tools](#) > [System Parameters](#).
- 3) In the [LED Control](#) section, select the [Enable Night Mode](#) checkbox.
- 4) Specify a time period in the [Night Mode Period](#) according to your need, and the LEDs will be off during this period.
- 5) Click [Save](#) to make the settings effective.

LED Control

Night mode:

☒ Enable Night Mode

Night Mode Period:

22

▼

:

00

▼

to

06

▼

:

00

▼

(HH:MM)

Save

FAQ

Q1. What can I do if I forgot my wireless password?

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

1. Visit <http://tplinkwifi.net>.
2. Go to [Advanced](#) > [Wireless](#) > [Wireless Settings](#) to retrieve or reset your wireless password.

Q2. What can I do if I forgot my login password of the web management page?

The default username and password of the web management page are [admin](#) (in lowercase). **If your router supports Password Recovery and you have enabled it**, please follow the steps below to reset the password without resetting the router:

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

1. Visit <http://tplinkwifi.net>.
2. Click [Forgot password](#) > [Send Code](#), the verification code will be sent to the mailbox you set.
3. Log into your mailbox to copy the verification code.
4. Paste the verification code on the window which pops up in Step 2.
5. Click [Confirm](#) (the default login username and password will be reset as [admin](#) after the click).
6. Use [admin](#) (in lowercase) as both username and password to login.

 **Tips:** Please refer to [Password Recovery](#) to learn how to configure Password Recovery.

If you have altered the username and password but Password Recovery is disabled:

1. Reset the router to factory default settings: press and hold the Reset button for about 7 seconds and then release;
2. Visit <http://tplinkwifi.net>, enter [admin](#) (in lowercase) as both username and password to login.

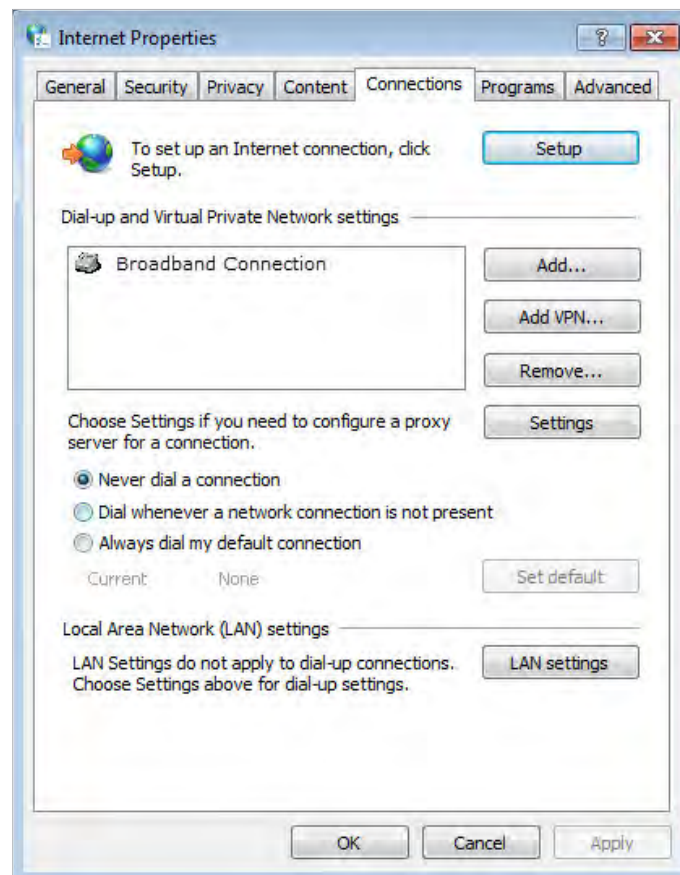
 **Note:** You'll need to reconfigure the router to surf the Internet once the router is reset, and please mark down your new password for future use.

Q3. I cannot log into the router's web management page, what can I do?

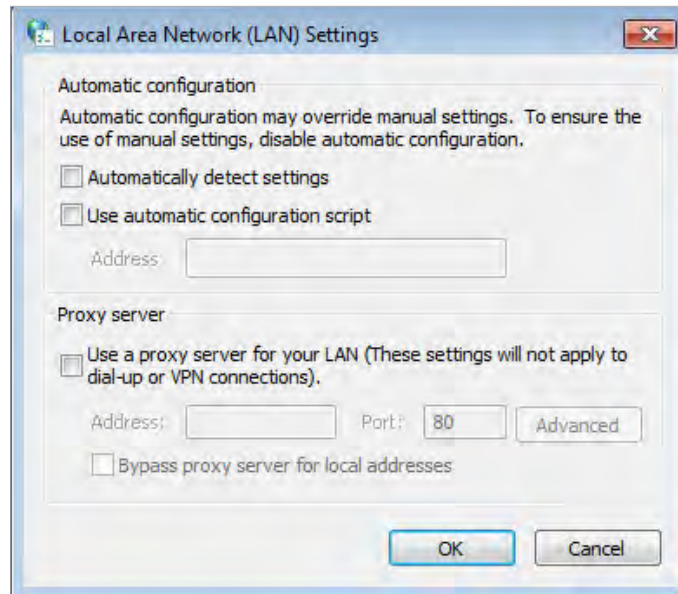
This can happen for a variety of reasons. Please try the methods below to login again.

- Make sure the router connect to the computer correctly and the corresponding LED indicator(s) light up.

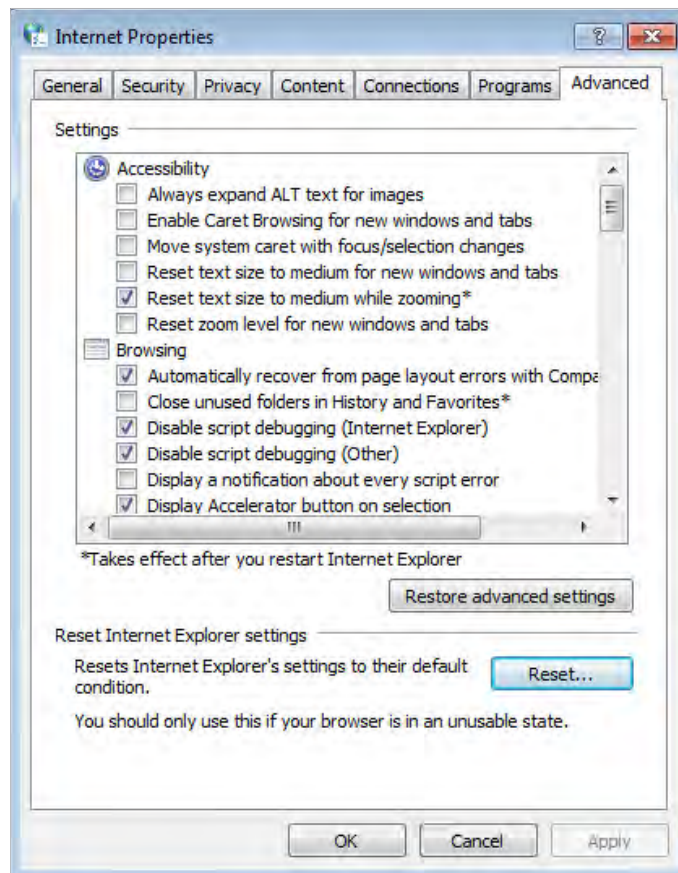
- Make sure the IP address of your computer is configured as [Obtain an IP address automatically](#) and [Obtain DNS server address automatically](#).
- Make sure you enter the correct IP address to login: <http://tplinkwifi.net>.
- Check your computer's settings:
 - 1) Go to [Start](#) > [Control Panel](#) > [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 login again.
- Reset the router to factory default settings and try again. If login still fails, please contact the technical support.

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

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

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

Note:

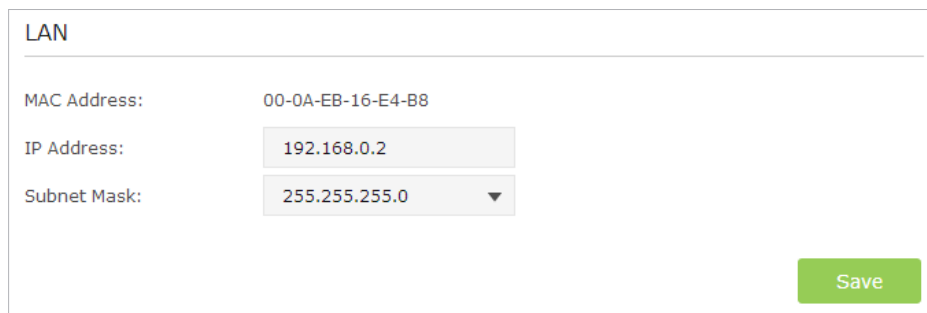
- WDS bridging only requires configuration on the extended router.
- WDS bridging function can be enabled either in 2.4GHz frequency or 5GHz frequency for a dual-band router. We use the WDS bridging function in 2.4GHz frequency as example.

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

2. Configure the IP address of the router:

- 1) Go to [Advanced](#) > [Network](#) > [LAN](#), configure the IP address of the extended router to be in the same subnet with the root router; (For example, the IP address of the root router is 192.168.0.1, the IP address of the extended router can be 192.168.0.2~192.168.0.254. We take 192.168.0.2 as example.)
- 2) Click [Save](#).

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



LAN	
MAC Address:	00-0A-EB-16-E4-B8
IP Address:	192.168.0.2
Subnet Mask:	255.255.255.0
Save	

3. Survey the SSID to be bridged:

- 1) Go to [Advanced](#) > [System Tools](#) > [System Parameters](#) and focus on the [2.4GHz WDS](#) section, click [Enable WDS Bridging](#).
- 2) Click [Survey](#), locate the root router's SSID and click [Choose](#) (Here we take TP-LINK_2512 as example).
- 3) If the root router has wireless password, you should enter the wireless password of the root router.
- 4) Click [Save](#).

2.4GHz WDS

WDS Bridging:

☒ Enable WDS Bridging

SSID(to be bridged):

TP-LINK_2512

Survey

MAC Address(to be bridged):

00-00-00-84-25-12

Example: 00-1D-0F-11-22-33

WDS Mode:

Auto

Security:

☐ None
☒ WPA-PSK/WPA2-PSK
☐ WEP

Password:

123456789

Save

4. Disable DHCP:

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

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

Q5.I cannot access the Internet even though the configuration is finished, what can I do?

1. Visit <http://tplinkwifi.net>.
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:

Internet

IPv4 | IPv6

MAC Address:

00-0A-EB-AC-88-16

IP Address:

59.40.0.91

Subnet Mask:

255.255.255.0

Default Gateway:

59.40.0.1

Primary DNS:

202.96.128.166

Secondary DNS:

202.96.134.133

Connection Type:

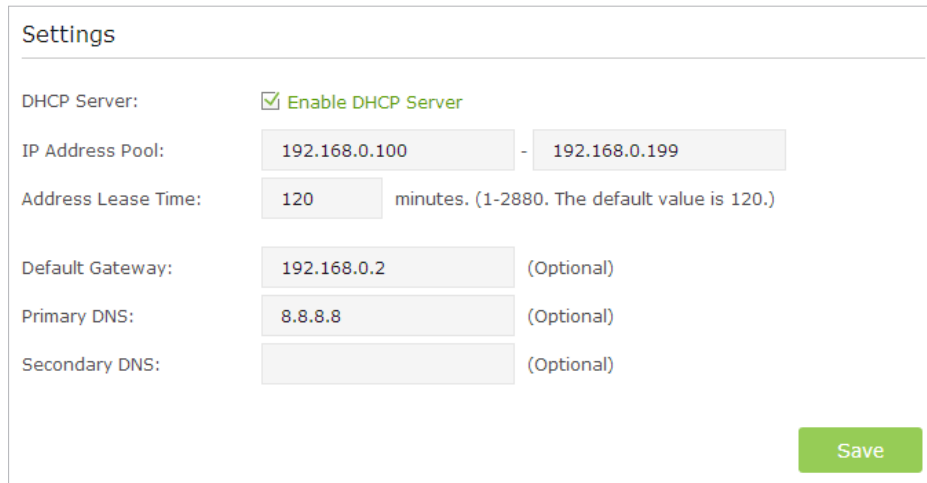
Dynamic IP

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

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

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

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



Settings

DHCP Server: ☒ Enable DHCP Server

IP Address Pool: 192.168.0.100 - 192.168.0.199

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

Default Gateway: 192.168.0.2 (Optional)

Primary DNS: 8.8.8.8 (Optional)

Secondary DNS: (Optional)

Save

- Power cycle the modem and the TP-LINK router.
 - 1) Power off your modem and TP-LINK router, leave them off for 1 minute.
 - 2) Power on your modem first, wait about 2 minutes until it gets a solid cable or Internet light.
 - 3) Power back TP-LINK 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:

Internet	
MAC Address:	00-0A-EB-AC-88-16
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:	None

- 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 username and password you set for the router.
 - 2) Go to **Advanced** > **Network** > **Internet** and focus on the **MAC Clone** section.
 - 3) Choose an option to your need (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:

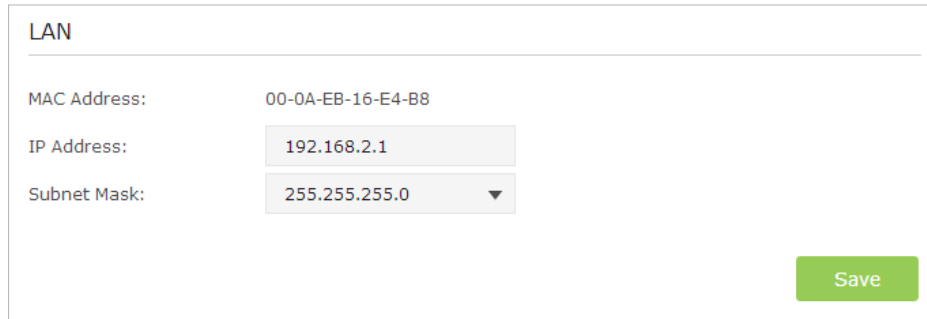
- Some ISP will register the MAC address of your computer when you access the Internet for the first time through their Cable modem, if you add a router into your network to share your Internet connection, the ISP will not accept it as the MAC address is changed, so we need to clone your computer's MAC 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, it may conflict with the IP range of your existent ADSL modem/router. If so, the router is not able to communicate with your modem and cause you can't access the Internet. To resolve this problem, we need to change the LAN IP address of the router to avoid such conflict, for example, 192.168.2.1.

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



LAN

MAC Address: 00-0A-EB-16-E4-B8

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0 ▼

Save

- Power cycle the modem and the TP-LINK router.
 - 1) Power off your modem and TP-LINK router, leave them off for 1 minute.
 - 2) Power on your modem first, wait about 2 minutes until it get a solid cable or Internet light.
 - 3) Power back TP-LINK 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 the username and password you set for the router.
 - 3) Go to [Advanced](#) > [Network](#) > [Internet](#).
 - 4) Select your [Internet Connection Type](#) and fill in other parameters with the help of page tips.
 - 5) Click [Save](#).

IPv4

Internet Connection Type: PPPoE ▼

Static IP

Dynamic IP

PPPoE

BigPond Cable

L2TP

PPTP

Username:

Password:

IP Address:

Primary DNS:

Secondary DNS: 0.0.0.0

⌵ Advanced

Connect Disconnect

Save

6) Power cycle the modem and the TP-LINK router again.

- Please upgrade the firmware of the router.

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

Q6. I cannot find my wireless network or I cannot connect the wireless network, what can I do?

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) Clicking on [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 closer if it is currently too far away.
- Go to [Advanced](#) > [Wireless](#) > [Wireless Settings](#), and check the wireless settings, double check your Wireless Network Name and SSID is not hided.

Wireless Settings 2.4GHz | 5GHz

☒ Enable Wireless Radio

Network Name (SSID): ☐ Hide SSID

Security:

Version: ☒ Auto ☐ WPA-PSK ☐ WPA2-PSK

Encryption: ☐ Auto ☐ TKIP ☒ AES

Password:

Mode:

Channel Width:

Channel:

Transmit Power: ☐ Low ☐ Middle ☒ High

[Save](#)

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 © 2016 TP-LINK TECHNOLOGIES CO., LTD. All rights reserved.

FCC STATEMENT



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

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

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

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

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

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

FCC RF Radiation Exposure Statement

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

"To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 22 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

The device is restricted in indoor environment only.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

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.

RF Exposure Information

This device meets the EU requirements (1999/519/EC) 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.

Restricted to indoor use.

Canadian Compliance Statement

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

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

Cet appareil est conforme aux norms CNR exemptes de licence d'Industrie Canada. Le fonctionnement est soumis aux deux conditions suivantes:

1. cet appareil ne doit pas provoquer d'interférences et
2. cet appareil doit accepter toute interférence, y compris celles susceptibles de provoquer un fonctionnement non souhaité de l'appareil.

Caution:

The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

Avertissement:

Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

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 23cm 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 23 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行；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機需忍受合法通信或工業、科學以及醫療用電波輻射性電機設備之干擾。

減少電磁波影響，請妥適使用。

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.

For EU/EFTA, this product can be used in the following countries:

AT	BE	BG	CH	CY	CZ	DE	DK
EE	ES	FI	FR	GB	GR	HR	HU
IE	IS	IT	LI	LT	LU	LV	MT
NL	NO	PL	PT	RO	SE	SI	SK

Explanations of the symbols on the product label

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