TP-LINK®

Archer C3150

User Guide

AC3150 Wireless MU-MIMO Gigabit Router

REV1.0.2 1910011860

Contents

About This Guide 1

Chapter 1. Get to Know About Your Router 2

1. 1. Product Overview 3
1. 2. Main Features 4
1. 3. Panel Layout 5
1. 3. 1.Front Panel 5
1. 3. 2.Back Panel 7
1. 3. 3.Side Panel 7

Chapter 2. Connect the Hardware 9

2. 1. Position Your Router 10
2. 2. Connect Your Router 10

Chapter 3. Log Into Your Router 13

Chapter 4. Set Up Internet Connection 15

4. 1. Quick Setup 16
4. 2. Manually Configure Your Internet Connection Settings 18
4. 3. Setting Up an IPv6 Internet Connection 22

Chapter 5. Guest Network 27

5. 1. Create a Network for Guests 28
5. 2. Customize Guest Network Options 29

Chapter 6. USB Settings 30

6. 1. Local Storage Sharing 31
6. 1. 1.Access the USB disk 31
6. 1. 2.Customize Your Settings 33
6. 2. Remote Access via FTP Server 36
6. 2. 1.Access the USB disk 36
6. 2. 2.Customize Your Settings 39
6. 3. Media Sharing 40

6. 3. 1.Access the USB disk 41
6. 3. 2.Customize Your Settings 42
6. 4. Printer Sharing 43

Chapter 7. Parental Controls 47

Chapter 8. Bandwidth Control 51

Chapter 9. Network Security 55

9. 1. Protect the Network from Cyber Attacks 56
9. 2. Access Control 57
9. 3. IP & MAC Binding 59

Chapter 10. NAT Forwarding 61

10. 1. Share Local Resources on the Internet by Virtual Servers 62
10. 2. Open Ports Dynamically by Port Triggering 63
10. 3. Make Applications Free from Port Restriction by DMZ 64
10. 4. Make Xbox Online Games Run Smoothly by UPnP 65

Chapter 11. VPN Server 67

11. 1. Use OpenVPN to Access Your Home Network 68
11. 2. Use PPTP VPN to Access Your Home Network 69

Chapter 12. Customize Your Network Settings 74

12. 1. Change the LAN Settings 75
12. 2. Configure to Support IPTV Service 75
12. 3. Specify DHCP Server Settings 77
12. 4. Set Up a Dynamic DNS Service Account 78
12. 5. Create Static Routes 79
12. 6. Specify Wireless Settings 81
12. 7. Use WPS for Wireless Connection 83
12. 7. 1.Set the Router's PIN 84
12. 7. 2.Use the WPS Wizard for Wi-Fi Connections 84
12. 8. Schedule Your Wireless Function 85
12. 9. Set up a VPN Connection 86

Chapter 13. Manage the Router 91

13. 1. Set Up System Time 92
13. 2. Test the Network Connectivity 93
13. 3. Upgrade the Firmware 94
13. 4. Backup and Restore Configuration Settings 95
13. 5. Change the Administrator Account 96
13. 6. Local Management 96
13. 7. Remote Management 97
13. 8. System Log 98
13. 9. SNMP Settings 99
13. 10. Monitor the Internet Traffic Statistics 100
13. 11. Control LEDs 101

FAQ 103

Specifications 113

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
Blue Italic	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 firmware and management app can be found at Download Center at *http://www.tp-link.com/support*.
- The Quick Installation Guide (QIG) 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 page at *http://www.tp-link.com/support*.

Chapter *1*

Get to Know About Your Router

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

This chapter contains the following sections:

- *Product Overview*
- *Main Features*
- *Panel Layout*

1. 1. Product Overview

What This Product Does

TP-LINK's AC3150 Wireless MU-MIMO Gigabit Router integrates 4-port Switch, Firewall, NAT-router and Wireless AP. Powered by 4x4 MIMO technology, this router delivers exceptional range and speed, which can fully meet the need of office/home networks and the users demanding higher networking performance. Your wireless connections are radio band selectable to avoid interference in your area, and the four built-in Gigabit ports supply high-speed connection to your wired devices.

Making Incredible Speed a Reality

With combined speeds of up to 3150Mbps, the Archer C3150 easily handles demanding activities at the same time. The router uses the latest innovations in Wi-Fi technology to create a faster, stronger, more reliable wireless network for your home. With the Archer C3150, lag, dropped connections, and dead zones will become a thing of the past.

NitroQAM and 4-Stream for Maximum Wi-Fi Speed

The Archer C3150 boasts a powerful combination of advanced Broadcom® NitroQAM™ technology and 4-Stream technology, which boosts wireless speeds up by 25%. This provides the speed and elite performance that you need to support your most demanding online applications, including simultaneous 4K streaming and online gaming.

More Connections and More Speed for Everyone

The Archer C3150 does more than just create faster Wi-Fi, it helps your devices achieve optimal performance by making communication more efficient. With MU-MIMO technology, the Archer C3150 can provide four simultaneous data streams, allowing all connected devices to achieve speeds up to 4X faster than standard AC routers.

Moreover, dynamic Smart Connect technology automatically selects the best available band for each device.

Extraordinary Home Entertainment

Archer C3150 can support many devices when you invite friends to your large house to entertain. It can maintain multiple simultaneous HD streaming, online gaming and other content consumption without lag. The Archer C3150 can provide a maximized coverage and enable your devices to stay covered, near or far as it. Don't let your mobile lifestyle stop the streaming and enjoy your home party.

The Power at the Heart of Your Router

Unlike normal routers, which usually have single core processors, the Archer C3150 features a powerful 1.4GHz dual core processor.

This unlocks the full potential of MU-MIMO and 4-Stream technologies, helping your dual band router maximize its performance potential.

Coverage for Your Entire Home

Four high-performance dual band antennas and high-powered amplifiers help create a strong, far-reaching network for your home. Beamforming technology focuses the Wi-Fi transmission in the direction of your connected devices, concentrating the signal where you need it the most. This allows you to enjoy fast, stable Wi-Fi in every part of your home, as well as on the patio, by the pool, and even in the yard.

A Router You Can Show Off

An elegant, minimalist design allows the Archer C3150 to be integrated seamlessly into the decor of any room. The LED indicators can be switched off to prevent distraction at night when placed in bedrooms or common spaces.

Plug Into Sharing, Plug Into Stability

You can quickly and easily share photos, music, and other files with family and friends. Just connect an external hard drive to the Archer C3150's USB 3.0 port or USB 2.0 port and immediately start enjoying lightning-fast transfers. To help your wired devices reach peak performance for smooth gaming and streaming, you can also create fast, stable wired connections using the four Gigabit Ethernet ports, which transfer data at speeds up to 10x higher than standard Ethernet ports.

Easy Setup and Use

Whether you prefer the powerful Tether App or the intuitive web interface, you can set up your Archer C3150 in minutes. The Tether App allows you to manage network settings, including parental controls and media sharing preferences, from any Android or iOS device.

1. 2. Main Features

Wireless and Wired Performance

- Complies with IEEE 802.11ac.
- One 10/100/1000M Auto-Negotiation RJ45 Internet port, four 10/100/1000M Auto-Negotiation RJ45 Ethernet ports, supporting Auto MDI/MDIX.
- Provides a USB 3.0 port and a USB 2.0 port supporting file sharing and print server.
- Provides WPA/WPA2, WPA-PSK/WPA2-PSK authentication, TKIP/AES encryption security.
- Shares data and Internet access for users, supporting Dynamic IP/Static IP/PPPoE/ PPTP/ L2TP Internet access.

- Supports simultaneous 2.4GHz and 5GHz connections for 3165Mbps of total available bandwidth.
- Supports Virtual Server, Special Application and DMZ host.
- Supports UPnP, Dynamic DNS, Static Routing.
- Provides Automatic-connection and Scheduled Connection on certain time to the Internet.
- Built-in NAT and DHCP server supporting static IP address distributing.
- Supports Parental Controls and Access Control.
- Connects Internet on demand and disconnects from the Internet when idle for PPPoE.
- Provides WEP encryption security and wireless LAN ACL (Access Control List).
- Supports Flow Statistics.
- Supports IPv6.
- Supports firmware upgrade and Web management.
- Supports OpenVPN server, PPTP VPN server.
- Supports beamforming technology.
- Supports Airtime Fairness technology.
- Supports MU-MIMO technology.

Note:
Future firmware upgrade is required to enable MU-MIMO technology.

1. 3. Panel Layout

1. 3. 1. Front Panel



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

LED Explanation

Name	Status	Indication
(LED)	On	All LEDs work normally.
	Off	All LEDs are off without affecting the router's performance.
(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. Please ensure that the power adapter is connected correctly.
(Wireless 2.4GHz)	On	The wireless 2.4GHz band is working properly.
	Off	The wireless 2.4 GHz band is disabled.
(Wireless 5GHz)	On	The wireless 5GHz band is working properly.
	Off	The wireless 5GHz band is disabled.
(Internet)	White	The router is connected to the Internet.
	Orange	The WAN port is connected, but there is no Internet connection.
	Off	The WAN port is not connected.
(LAN)	On	At least one LAN port is connected.
	Off	No LAN port is connected.
(WPS)	On	A wireless device has been successfully added to the network by WPS function.
	Flashing	WPS handshaking is in process and will continue for about 2 minutes. Please press the WPS button on other wireless devices that you want to add to the network while the LED is flashing.
	Off	The router is not in the WPS process.
(USB1)	On	The USB 3.0 device is identified and ready to use.
	Flashing	The USB 3.0 device is being identified.
	Off	No USB 3.0 device is plugged into the USB port or the USB device is not identified or USB device has been safely ejected.
(USB2)	On	The USB 2.0 device is identified and ready to use.
	Flashing	The USB 2.0 device is being identified.
	Off	No USB 2.0 device is plugged into the USB port or the USB device is not identified or USB device has been safely ejected.

Note:

After a device is successfully added to the network by WPS function, the WPS LED will keep on for about 5 minutes and then turn off.

1. 3. 2. Back Panel



The router's back panel shows the connection ports, buttons and antennas (view from left to right). Refer to the following for detailed instructions.

Item	Description
Internet	This port is where you will connect the DSL/cable Modem, or Ethernet.
LAN1, LAN2, LAN3, LAN4	These ports (1, 2, 3, 4) connect the router to the local PC(s).
Power	For connecting the router to power socket via the provided power adapter.
Power On/Off	The switch for the power. Press it to power on or off the router.
Antennas	Used for wireless operation and data transmit. Upright them for the best Wi-Fi performance.

1. 3. 3. Side Panel



The router's side panel shows the USB ports and buttons (view from left to right). Refer to the following for detailed instructions.

Item	Description
WiFi On/Off	For turning on/off the WiFi function.
Reset	The switch for the reset function. There are two ways to reset the router's factory defaults. Method one: With the router powered on, press and hold the Reset button for at least 5 seconds until all LEDs light on (wireless LEDs may not light on if the WiFi on/off button is off). And then release the button and wait the router to reboot to its factory default settings. Method two: Restore the default setting from *13. 4. Backup and Restore Configuration Settings* of the router's Web-based Management.
WPS	The switch for the WPS function. Pressing this button for less than 5 seconds enables the WPS function. If your client devices, such as wireless adapters, that support Wi-Fi Protected Setup, then you can press this button to quickly establish a connection between the router and client devices and automatically configure wireless security for your wireless network.
USB 2.0	For connecting to a 2.0 USB storage device or a 2.0 USB printer.
USB 3.0	For connecting to a 3.0 USB storage device or a 3.0 USB printer. It is also compatible with USB 2.0 devices.

Chapter 2

Connect the Hardware

This chapter contains the following sections:

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

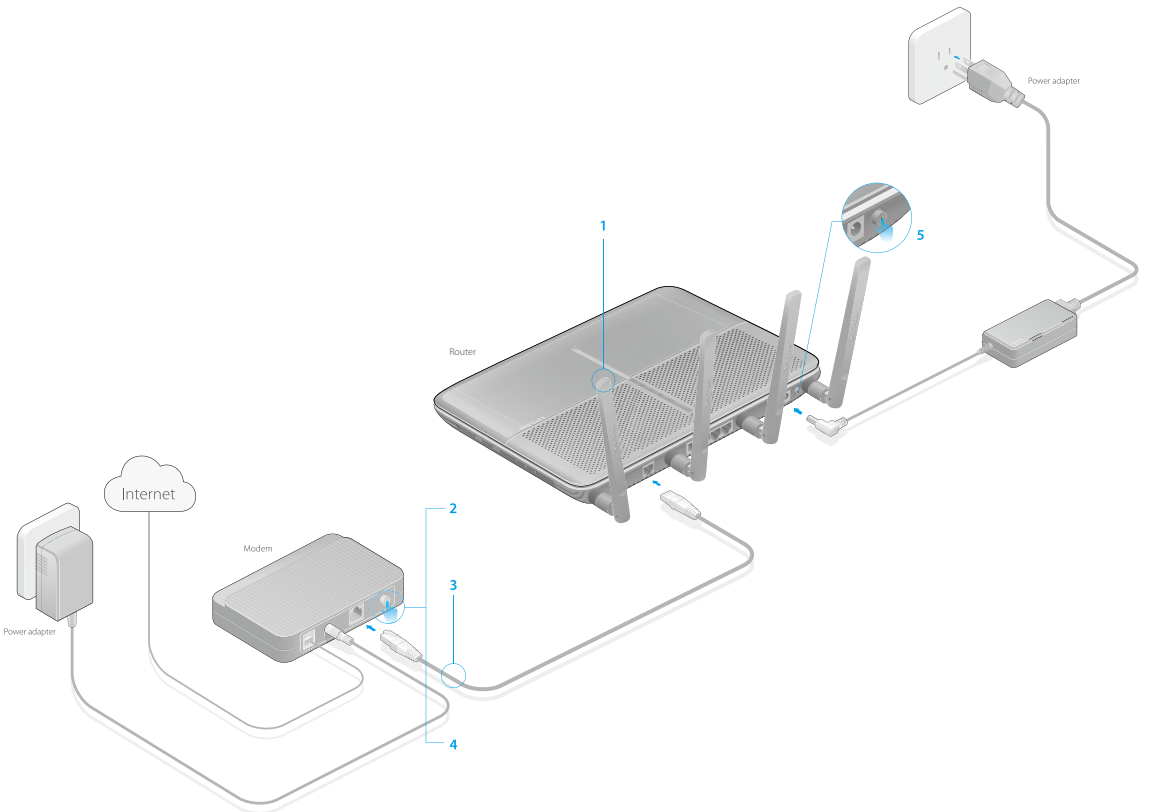
2. 1. Position Your Router

- 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.

2. 2. Connect Your Router

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 steps 5) and 6) to complete the hardware connection.



1. Install the antennas and position them vertically for best signal reception.
2. Turn off the modem, and remove the backup battery if it has one.
3. Connect the modem to the Internet port on your router with an Ethernet cable.

4. Turn on the modem, and then wait about 2 minutes for it to restart.
5. Turn on the router.
6. Verify that the following LEDs are on and solid before continuing with the configuration.

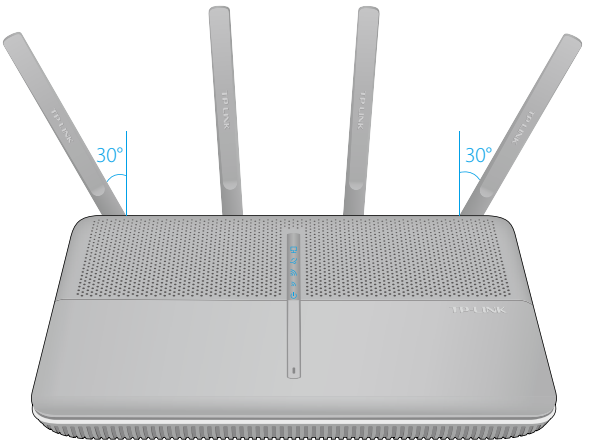


Note:

If the 2.4G LED and 5G LED are off, please press the Wi-Fi On/Off button on the side panel for 2 seconds and check the LEDs again in a few seconds later.

Tips:

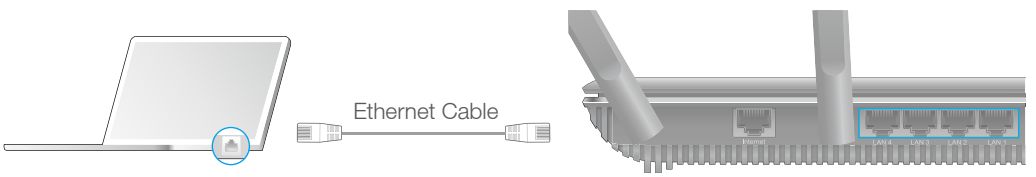
For optimum performance, orient the four antennas as shown in the drawing below.



7. Connect your computer to the router.

- **Method 1: Wired**

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



- **Method 2: Wirelessly**

Connect wirelessly by using the SSID (Network Name) and Wireless Password/PIN printed on the product label at the bottom of the router.



- **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.)

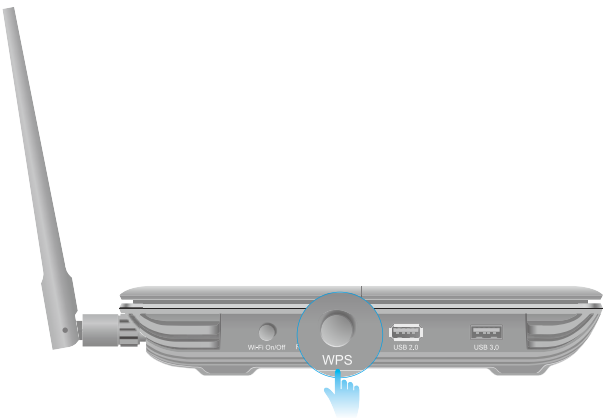
Note:

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) Tab the WPS icon on the device's screen.

2) Immediately press the WPS button on your router.





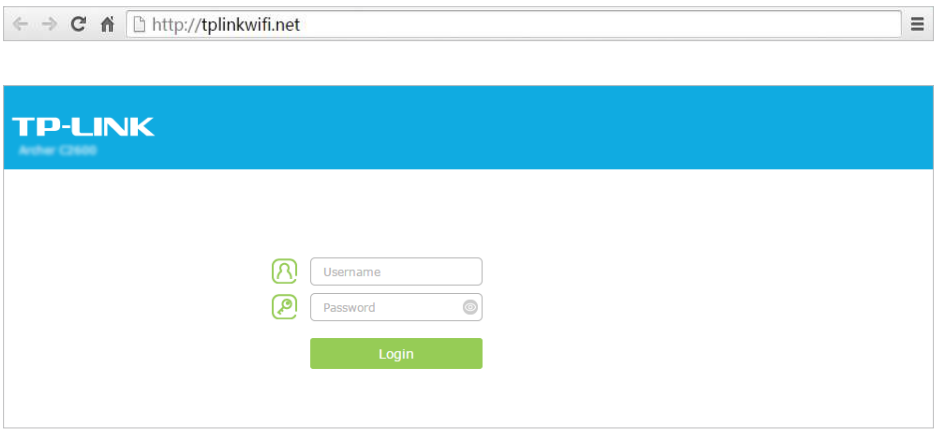
Chapter *3*

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.

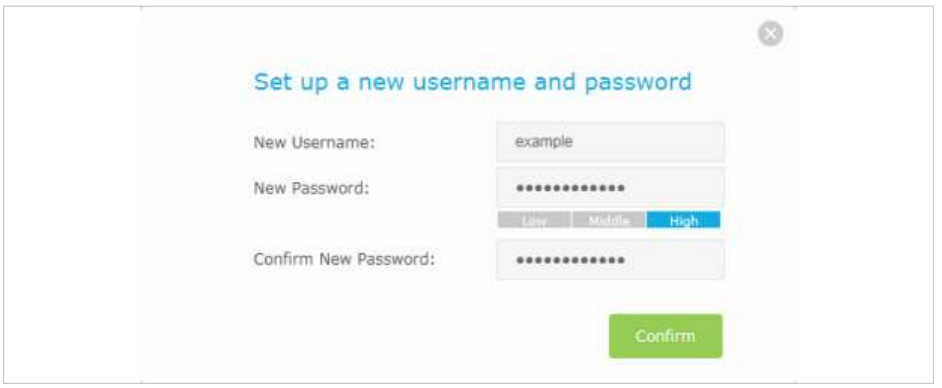
1. Set up the TCP/IP Protocol in Obtain an IP address automatically mode on your computer.
2. Launch a web browser and type in *http://tplinkwifi.net* or *http://192.168.0.1*. Use admin for both username and password, and click Login.



Note:

If the login window does not appear, please refer to *FAQ* > *Q3. I cannot log into the router's web management page, what can I do?*

3. Create a new username and password for subsequent login.



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 many 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:

- *Quick Setup*
- *Manually Configure Your Internet Connection Settings*
- *Setting Up an IPv6 Internet Connection*

4. 1. Quick Setup

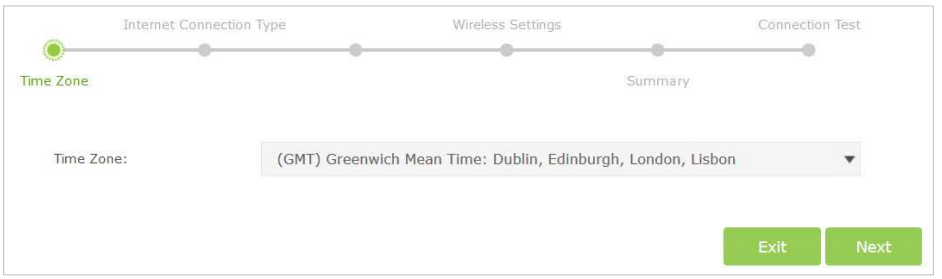
The Quick Setup Wizard will guide you through the process to set up your router to access the Internet.

Tips:

If you need the IPv6 Internet connection, please refer to the section of *Setting Up an IPv6 Internet Connection*.

Follow the steps below to set up your router to access the Internet.

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.
3. Select your Time Zone from the drop-down list and click Next.

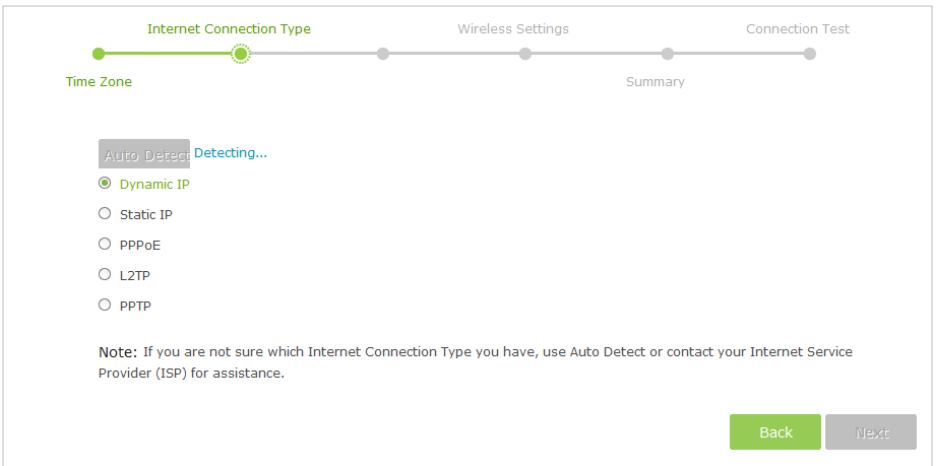


4. Click Auto Detect and the router will detect your connection type automatically.

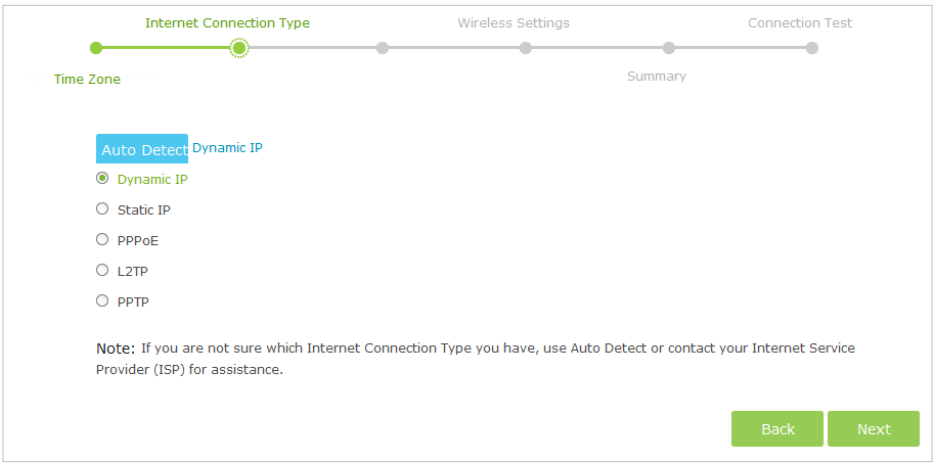
Note:

You can also choose the connection type manually. Contact your ISP if you are not sure about the Internet connection information.

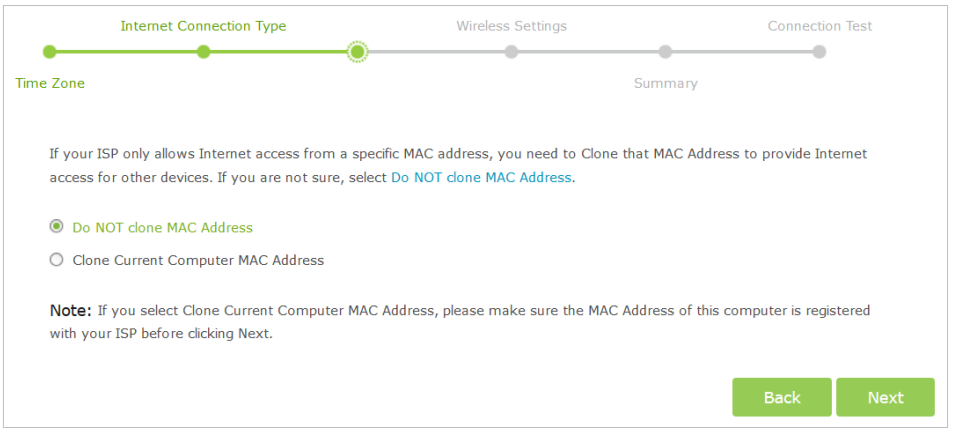
- If you use DSL line and you are only provided with an account name and a password by your ISP, choose PPPoE.
- If you use cable TV or fiber cable, choose Dynamic IP.
- If you are provided with more information such as IP address, Subnet Mask and Default Gateway, choose Static IP.



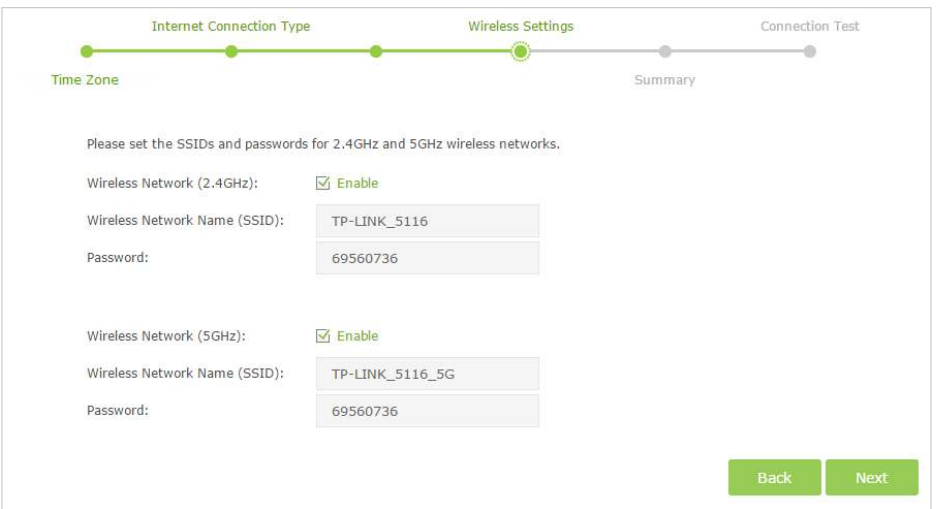
5. In this case, the router automatically detects Dynamic IP as the connection type. Click Next.



6. Follow the instructions on the page to decide whether to clone MAC Address. Click Next.



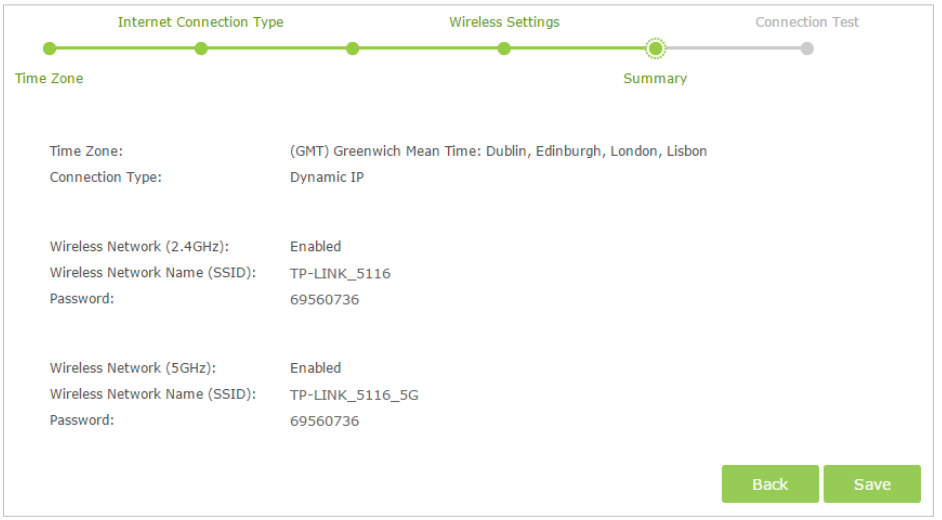
7. Configure your wireless settings and click Next.



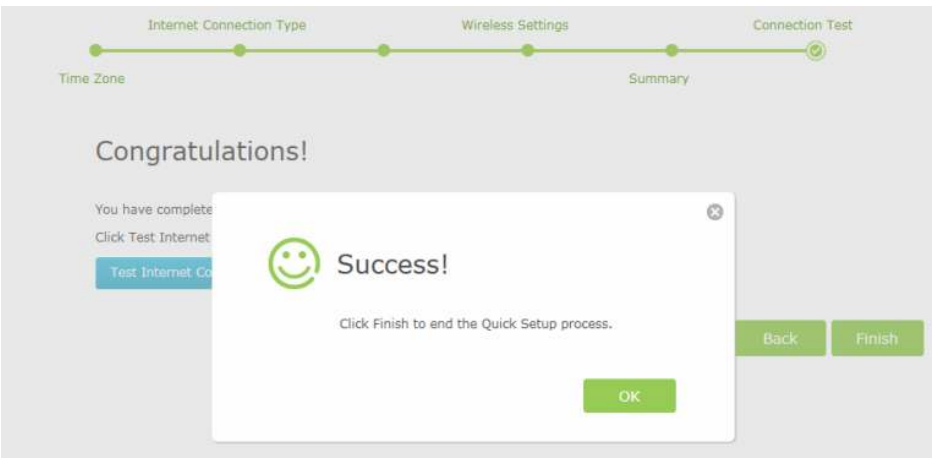
Note:

1. You may customize your 2.4GHz/5GHz SSID and password. Once done, the wireless connection will disconnect automatically, and you must then use the new SSID and password to regain access to the Internet.
2. Tick Hide SSID if you want to hide this wireless network name.

8. Confirm the information and click Save.



9. Click Test Internet Connection. If you successfully connect to the Internet, the screen will display as follows.



10. Now your computer and Wi-Fi devices can connect to the Internet!

Tips:

You can connect your computer to the router's Etherent port using an Ethernet cable to join the local area network. You can also find and select the wireless network name on your Wi-Fi device to join the Wi-Fi network.

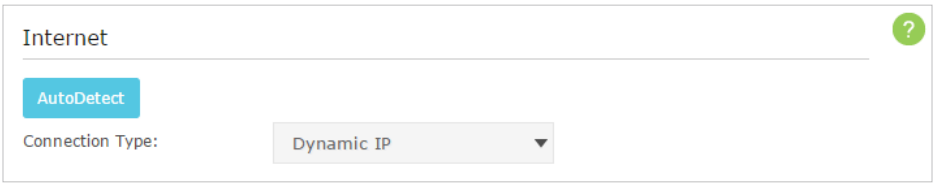
4. 2. Manually Configure Your Internet Connection Settings

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.

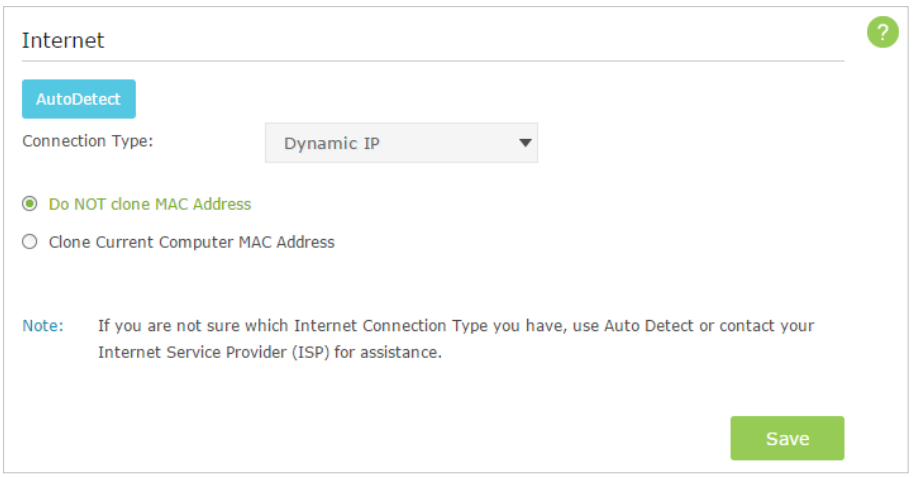
2. Go to Basic > Internet.
3. Select your Internet connection type from the drop-down list.



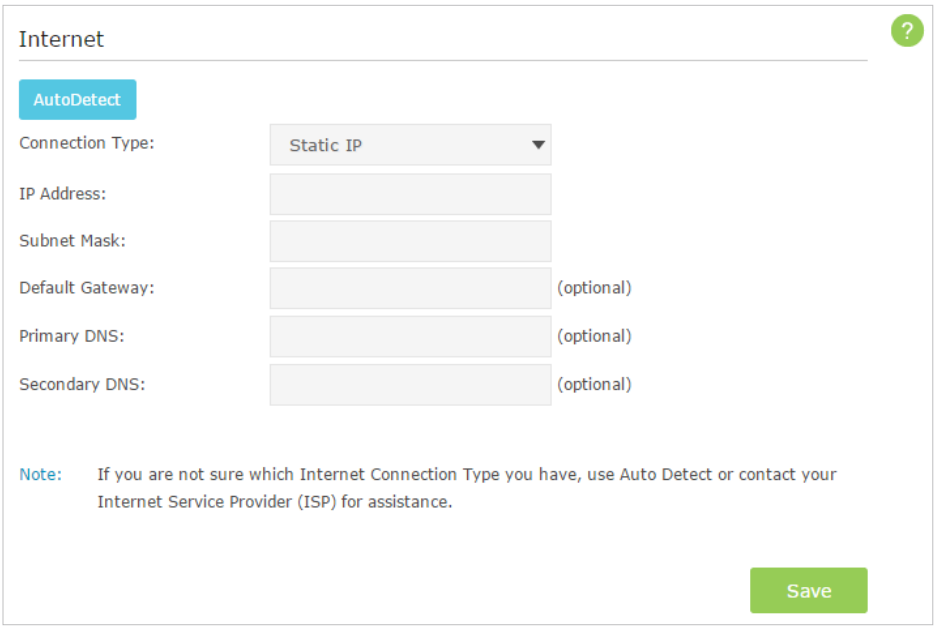
Note:
If you are unsure of what your connection type is, click Auto Detect. Since different connection types need different cables and connection information, you can also refer to the demonstrations in Step 4 to judge your connection type.

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

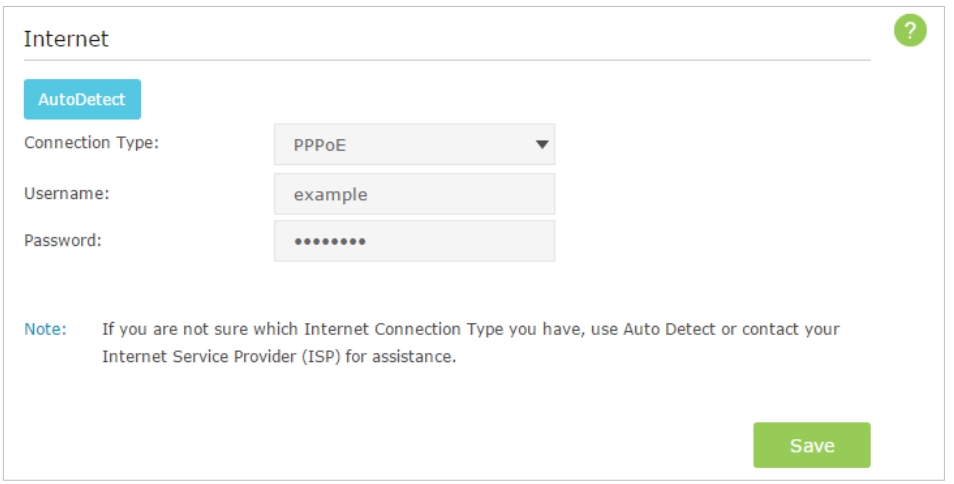
   1) If you choose Dynamic IP, you need to select whether to clone the MAC address or not. Dynamic IP users are usually equipped with cable TV or fiber cable.



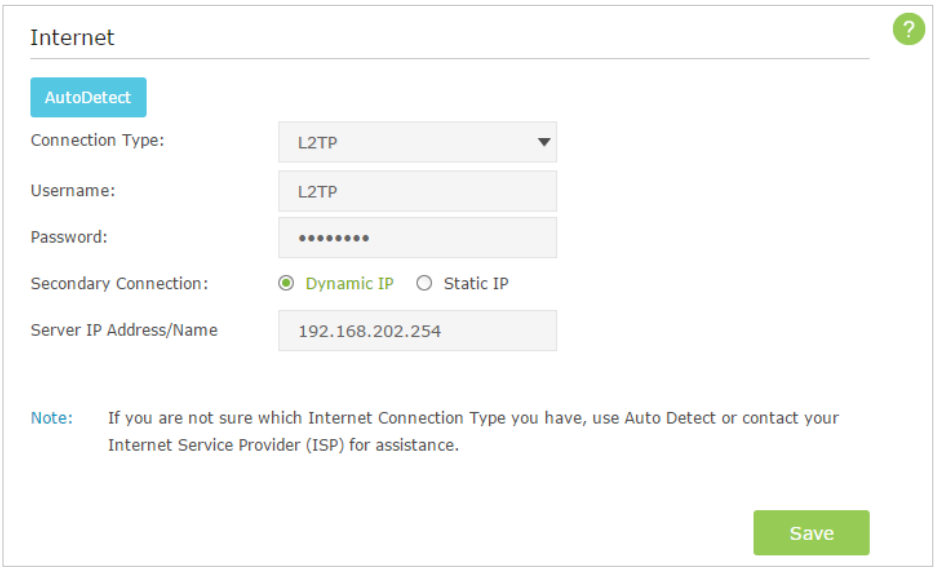
   2) If you choose Static IP, enter the information provided by your ISP in the corresponding fields.



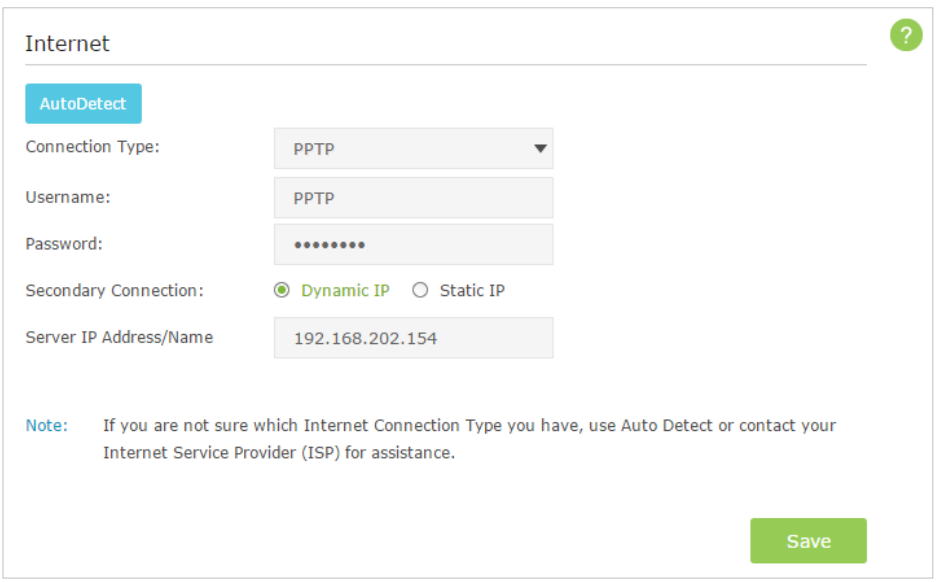
3) If you choose PPPoE, enter the username and password provided by your ISP. PPPoE users usually have DSL cable.



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.



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.

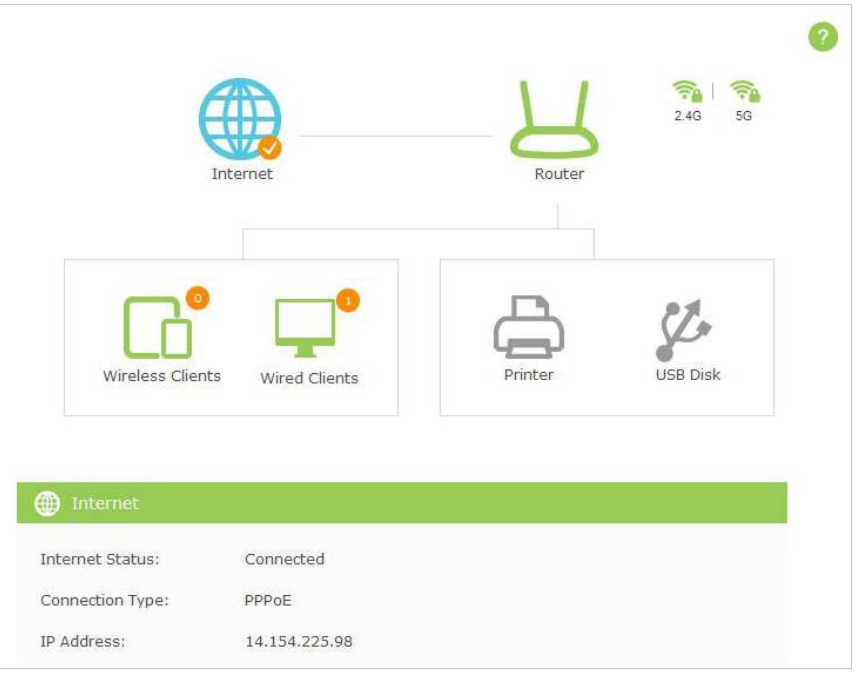


5. Click Save to make the settings take effect. To check your Internet connection, click Network Map on the left of the page.

Note:

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

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



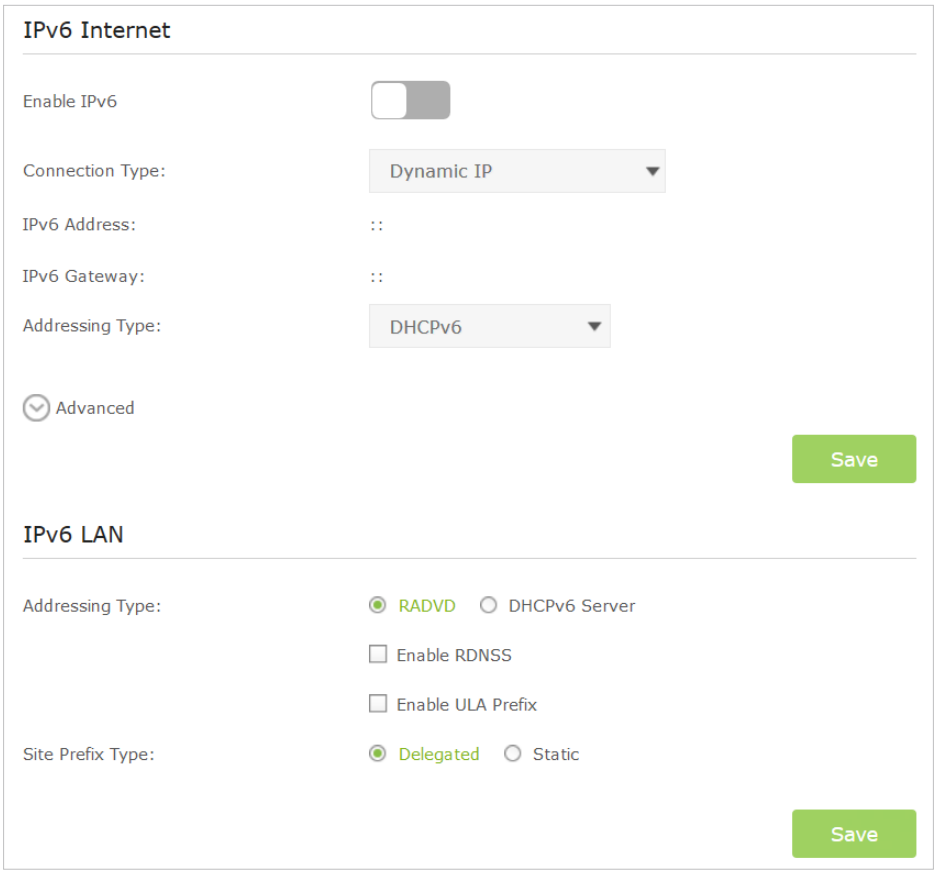
Tips:

1. 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.
2. If you still cannot connect to the Internet, refer to *FAQ* for further instructions.

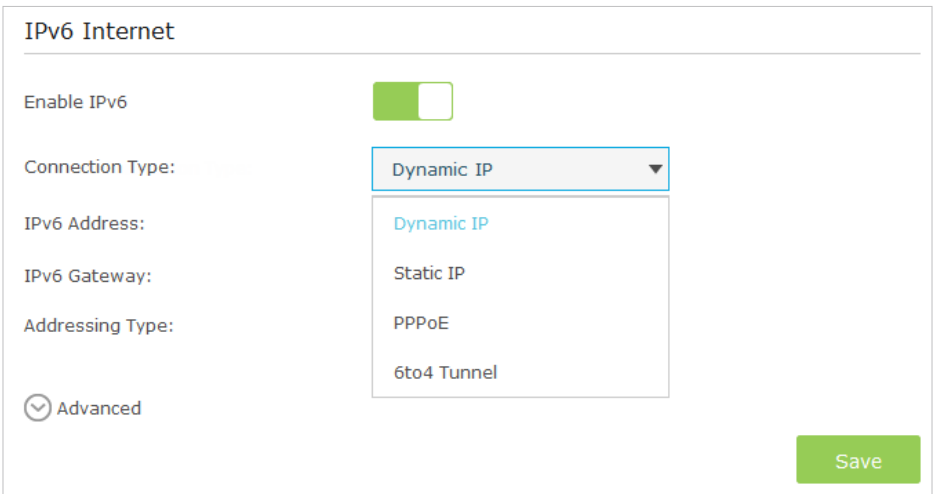
4. 3. Setting Up an IPv6 Internet Connection

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

1. Visit *http://tplinkwifi.net*, then log in with the username and password you set for the router.
2. Go to Advanced > IPv6.



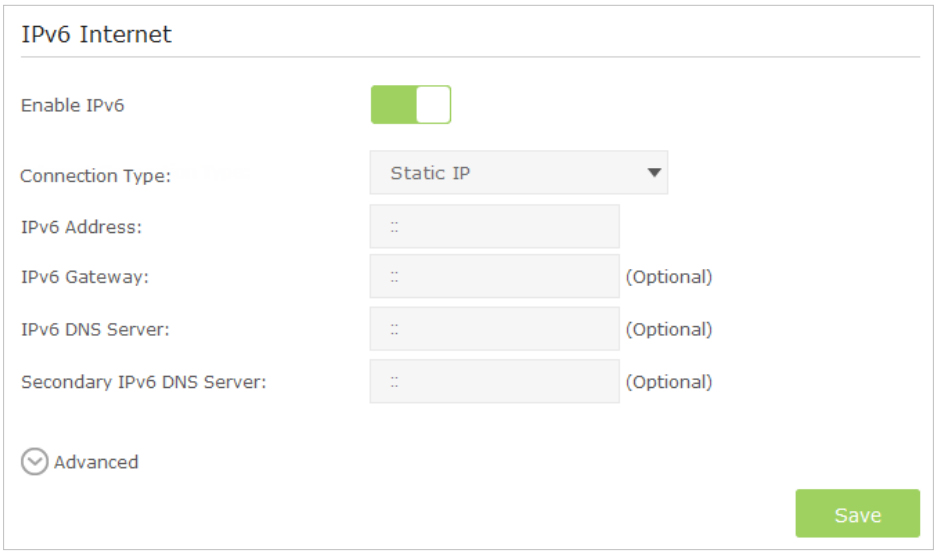
3. Select the Internet connection type provided by your ISP.



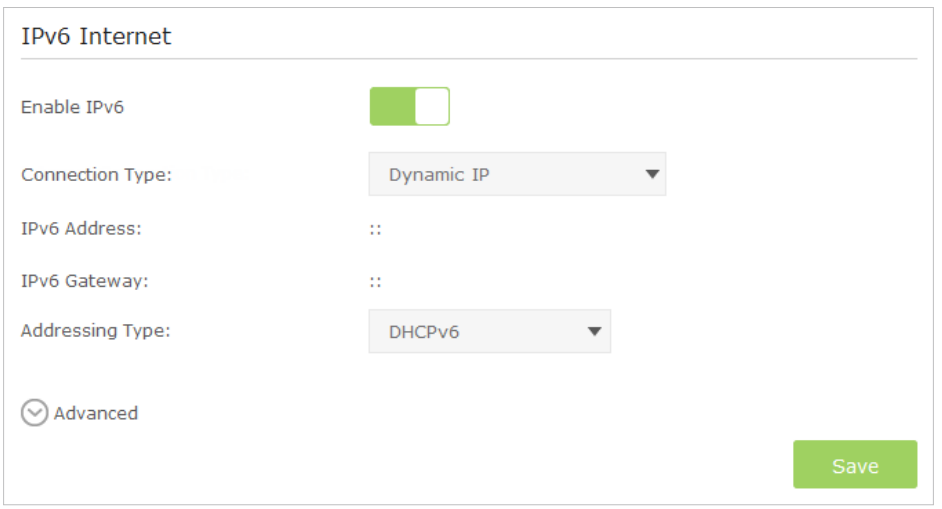
Tips:
If you do not know what your Internet connection type is, contact your ISP or judge according to the already known information provided by your ISP.

4. Fill in information as required by different connection types.

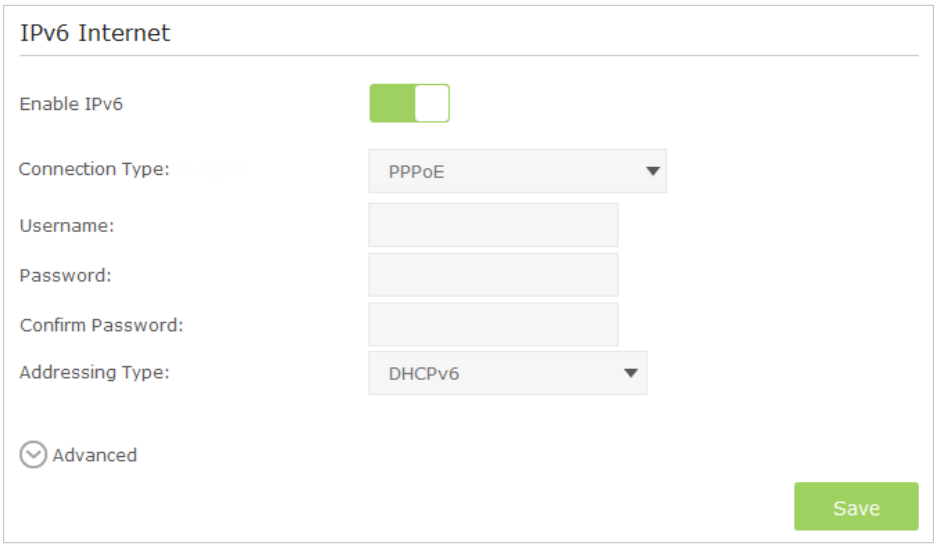
   1) Static IP: Fill in blanks and click Save.



2) Dynamic IP: Click Advanced to have more configuration if your ISP requires. Click Save to save the settings.



3) PPPoE: Fill in the Username and Password. Click Advanced to have more configuration if your ISP requires. Click Save to save the settings.



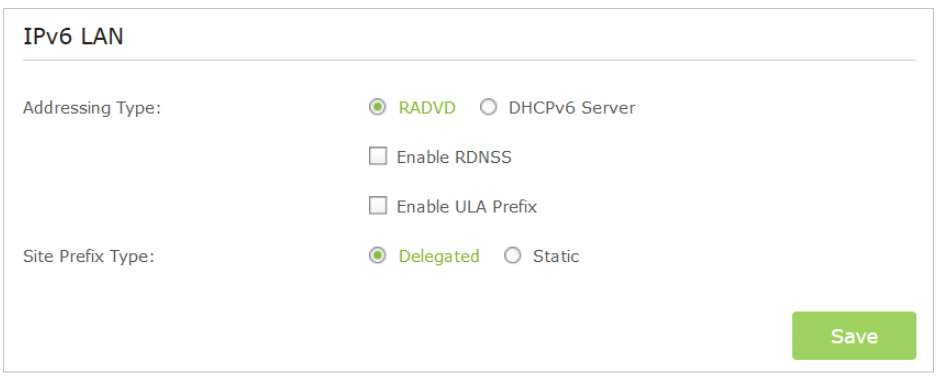
4) 6to4 Tunnel: An IPv4 Internet connection type is a prerequisite for this connection type (*Manually Configure Your Internet Connection Settings*). Click Advanced to have more configuration if your ISP requires. Click Save to save the settings.



5. Configure the IPv6 LAN settings. Leave the settings as default, and click Save.

Tips:

Find Help on the management interface to know more about items.



6. Click Status to check whether you succeed or not. The following figure is an example of a successful PPPoE configuration.



Tips:
Visit *FAQ* if there is no Internet connection.

Chapter 5

Guest Network

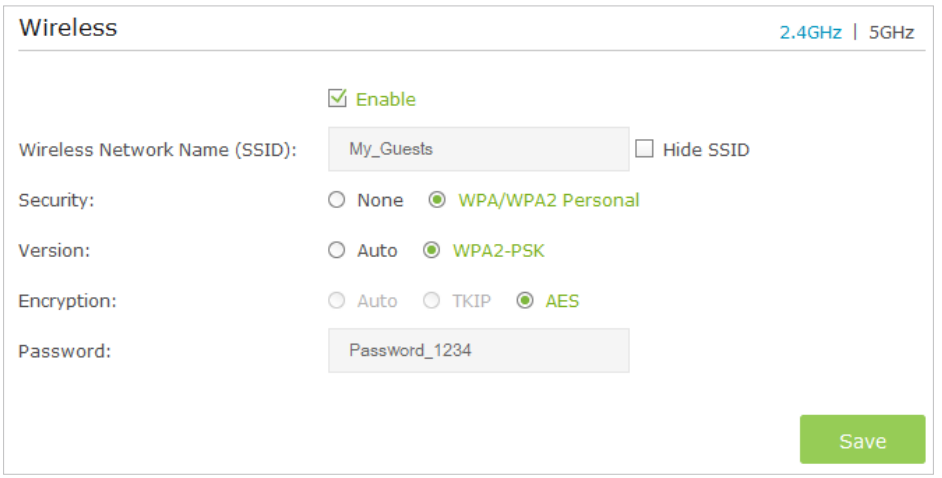
This function allows you to provide Wi-Fi access for guests without disclosing your main network. When you have guests in your house, apartment, or workplace, you can create a guest network for them. In addition, you can customize guest network options to ensure network security and privacy.

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) Click 2.4GHz or 5GHz, then select Enable.
   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.



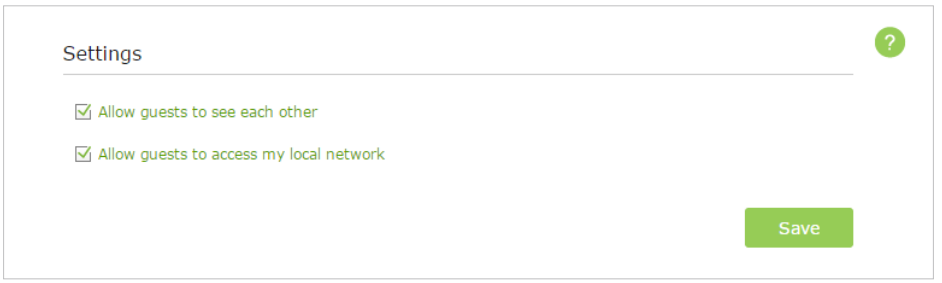
4. Click Save. Now your guests can access your guest network using the SSID and password you set!

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.



- 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 Settings

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.

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

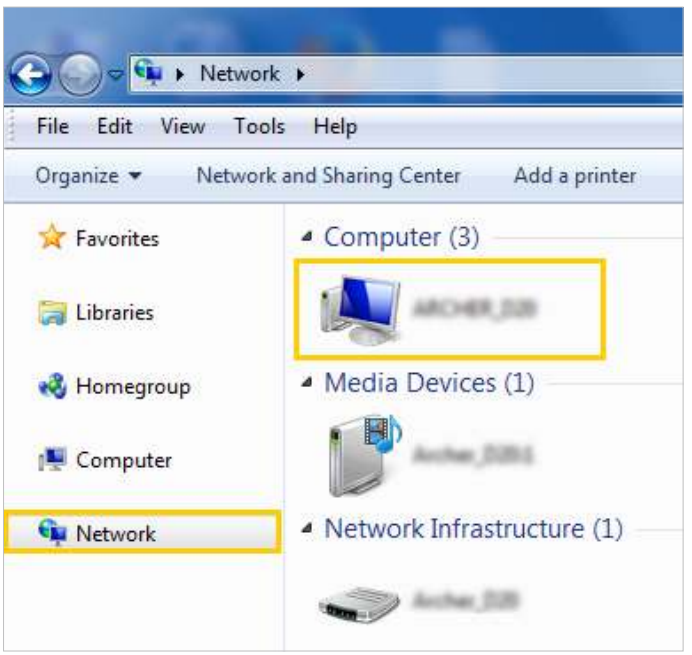
By default, all the network clients can access all folders on your USB disk. Refer to the following table for access instructions. You can also customize your sharing content and set a sharing account by referring to *Customize Your Settings*.

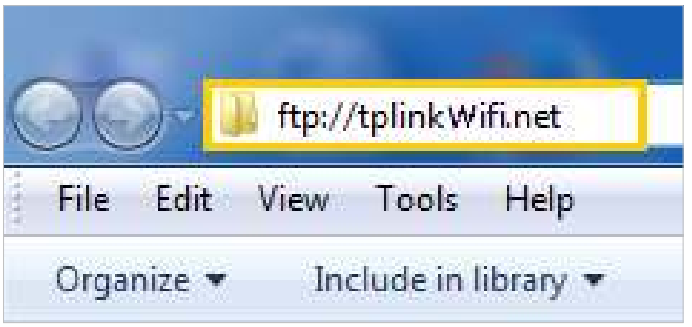
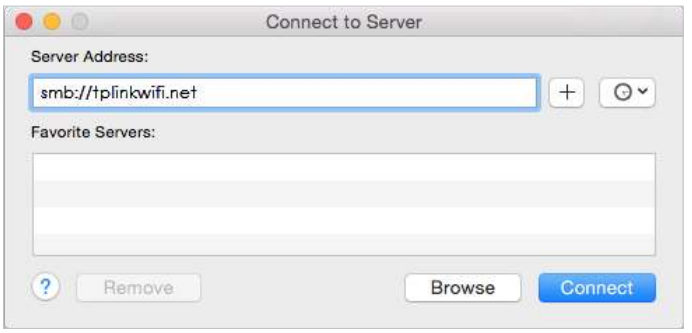
Windows computer

➢ **Method 1:**

Go to Computer > Network, then click the Network Server Name (Archer_C3150 by default) in the Computer section.

Note:
Operations in different systems are similar. Here we take Windows 7 as an example.



<table>
<tr><td>Windows computer</td><td>➢ 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].

</td></tr>
<tr><td>Mac</td><td>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.)</td></tr>
<tr><td>pad</td><td>Use a third-party app for network files management.</td></tr>
</table>

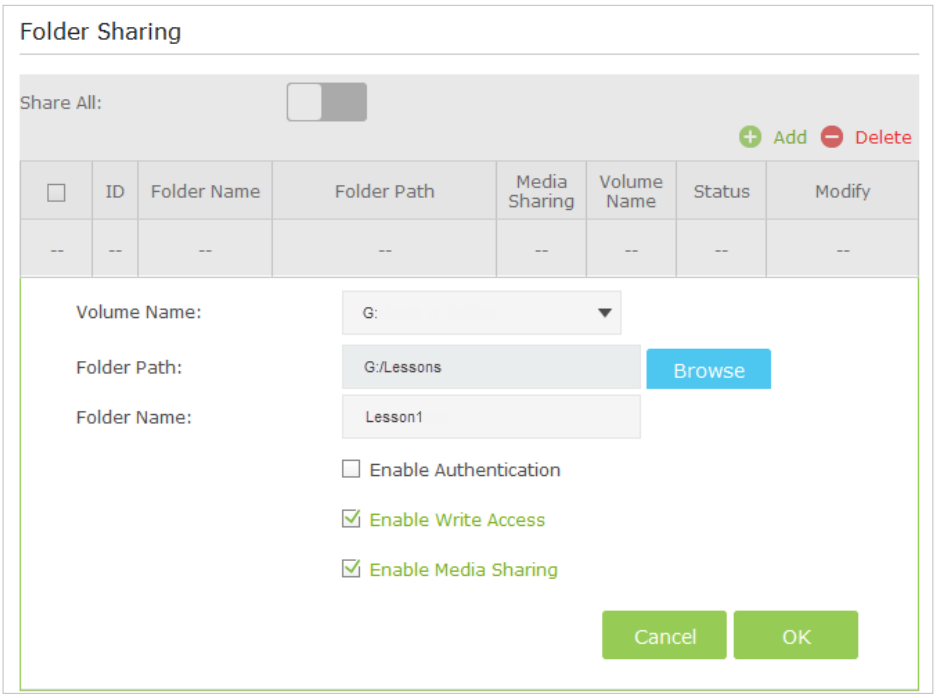
Tips:
You can also access your USB disk by using your Network/Media Server Name as the server address. Refer to *To Customize the Address of the USB Disk* to learn more.

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.



3. Select the Volume Name and Folder Path, then enter a Folder Name as you like.
4. Decide the way you share 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.

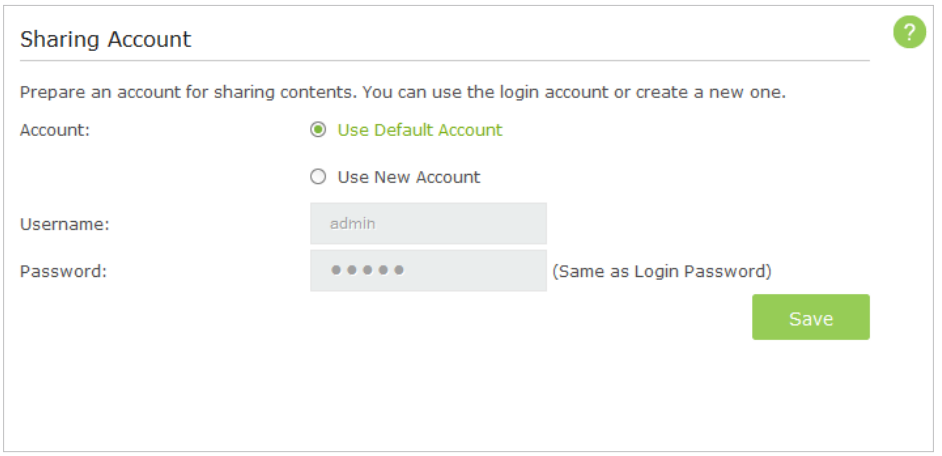
Tips:
The router can share 32 volumes at most. You can click on the page to detach the corresponding volume you do not need to share.



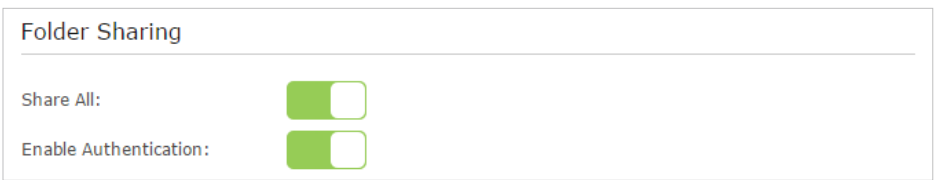
➢ To Set up Authentication for Data Security

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

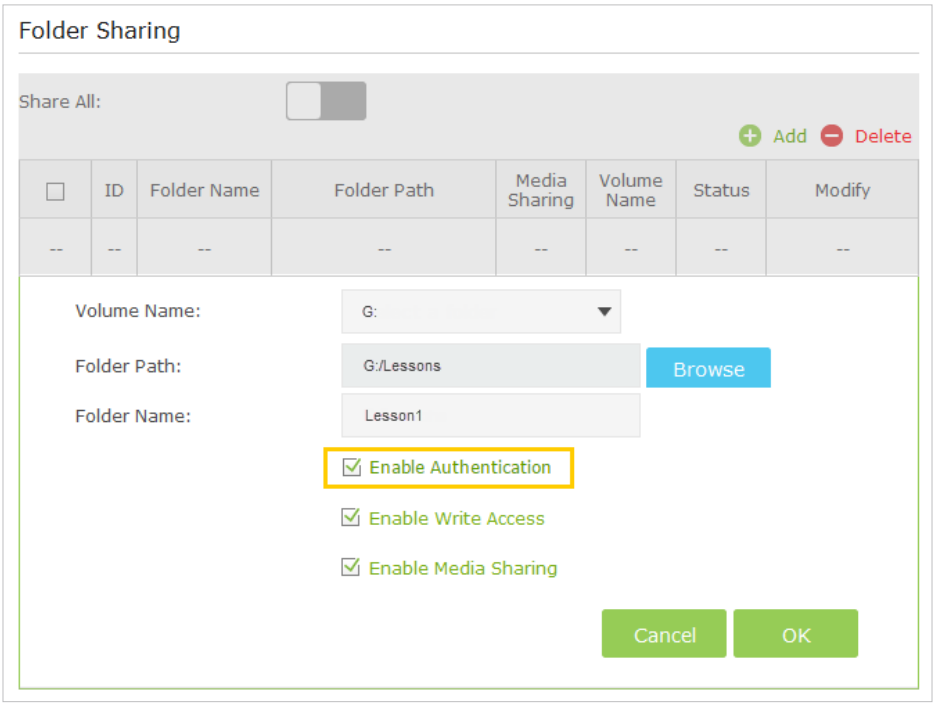
1. Visit *http://tplinkwifi.net*, then log in with the username and password you set for the router.
2. Select Advanced > USB Settings > Sharing Access. Focus on the Sharing Account section.



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



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



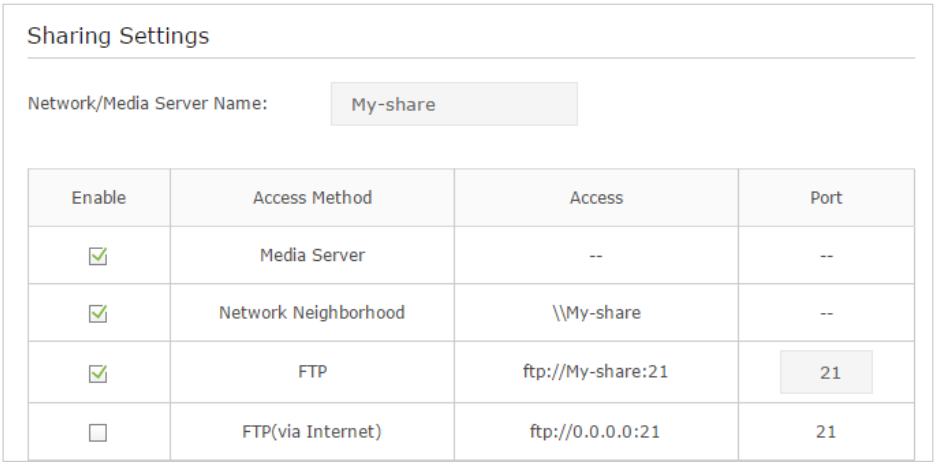
Note:

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. For more details, refer to *"Q6. What can I do if I cannot access the USB disk after I modify the Authentication settings?"*

➢ 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.



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.

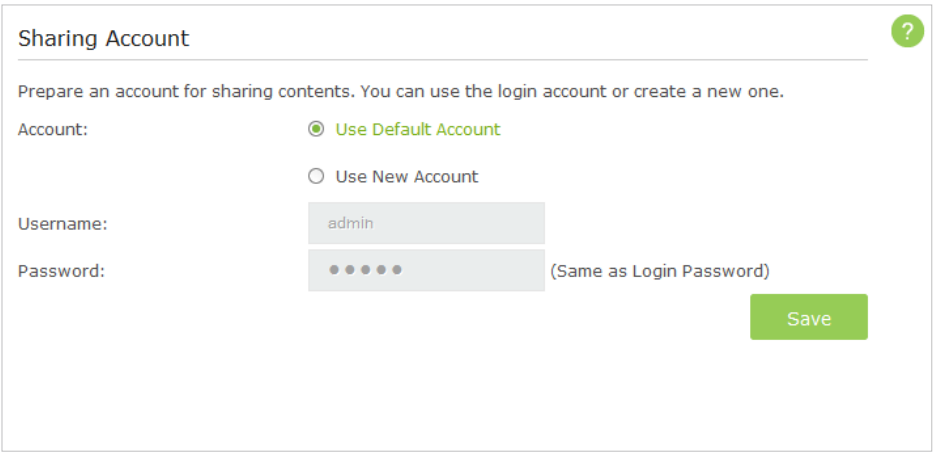
2. Enable Authentication for Data Security

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.

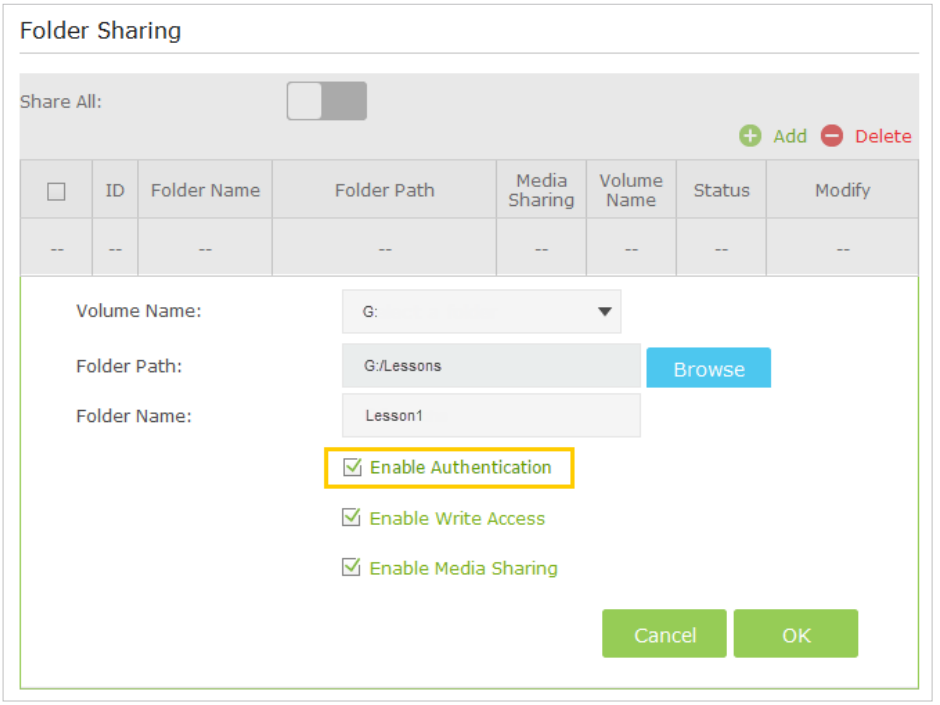


4) Enable Authentication to apply the sharing account.

- If you leave Share All enabled, click the button to enable Authentication for all folders.

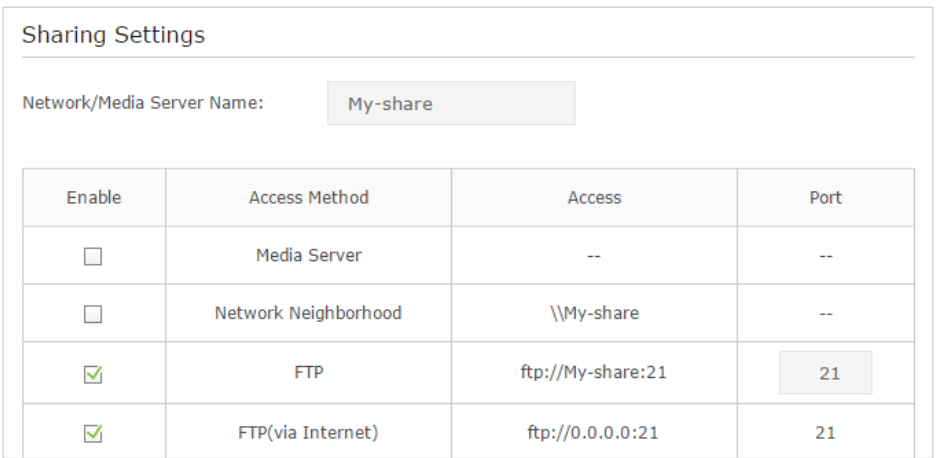


- If Share All is disabled, enable Authentication for specific folders.



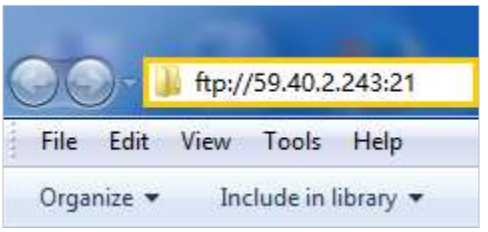
3. Enable the FTP(via Internet)

Select the check box to enable FTP(via Internet), then click 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 of 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.

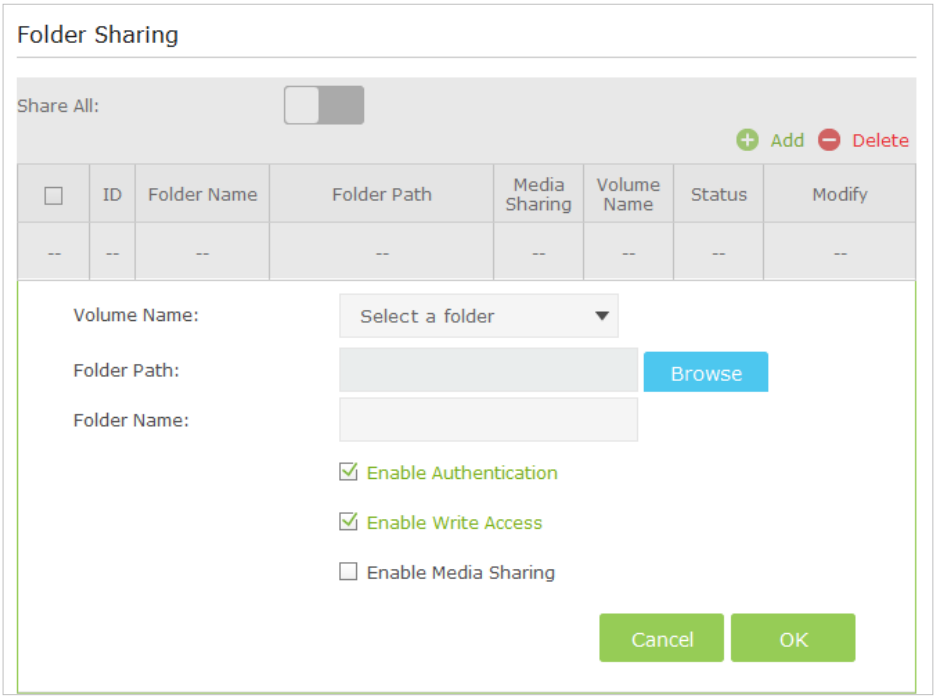
Tips:
Click *Set Up a Dynamic DNS Service Account* to learn how to set up a domain name for you router.

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.

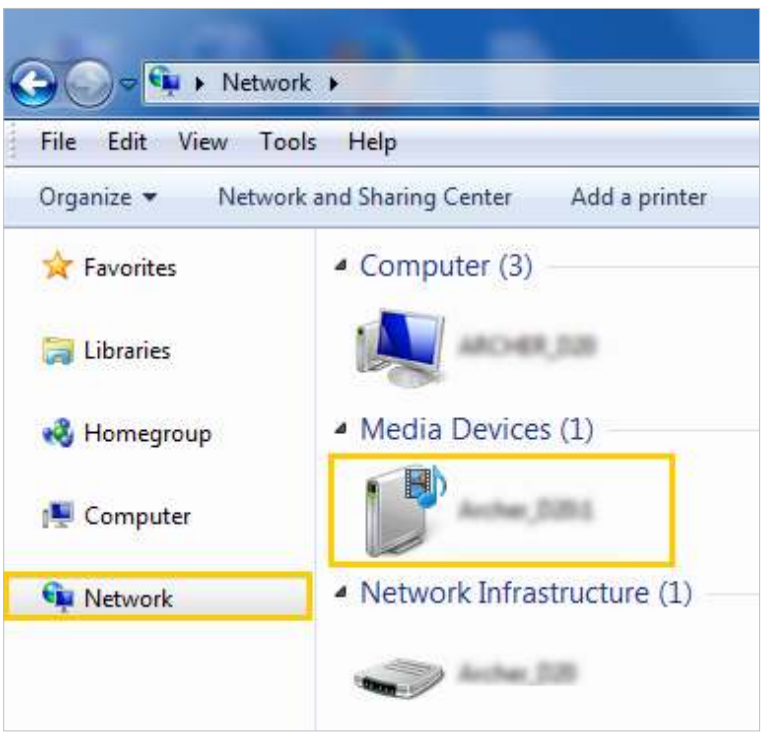
2. Access the Media Files on Your USB Disk

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 (Archer_C3150 by default) in the Media Devices section.

Note:
Here we take Windows 7 as an example.



Pad

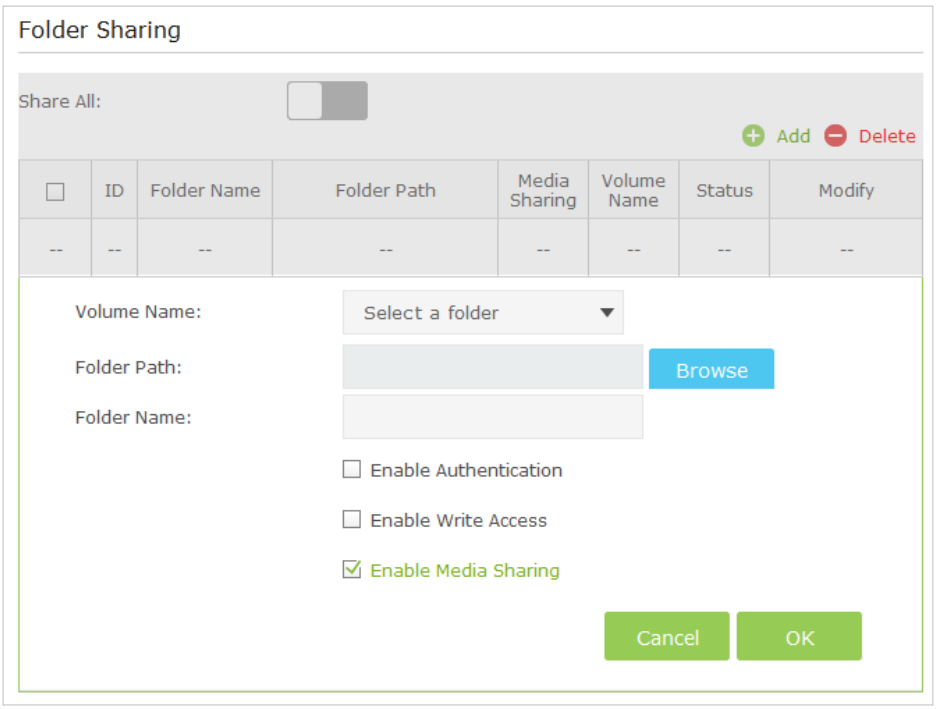
- Use a third-party DLNA-supported player.

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.



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

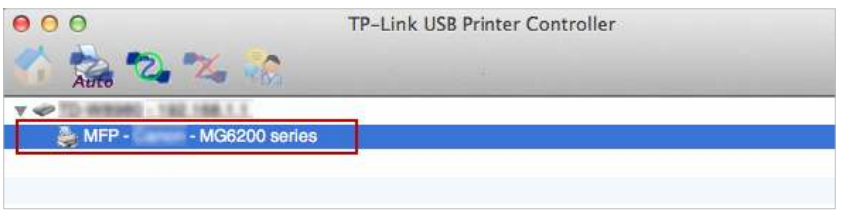
You should set the shared printer as Auto-Connect Printer on every computer that needs printer service.

1) Double-click the icon  on your desktop to launch the USB Printer Controller.

2) Highlight the printer you share.

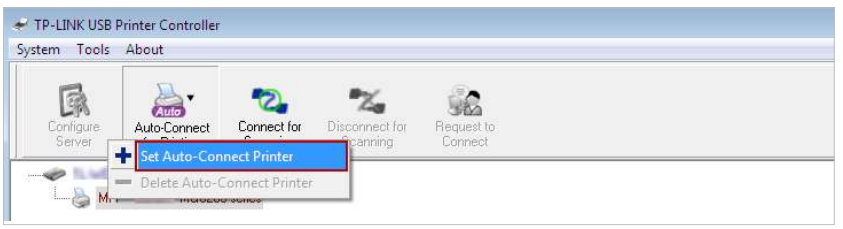


Windows

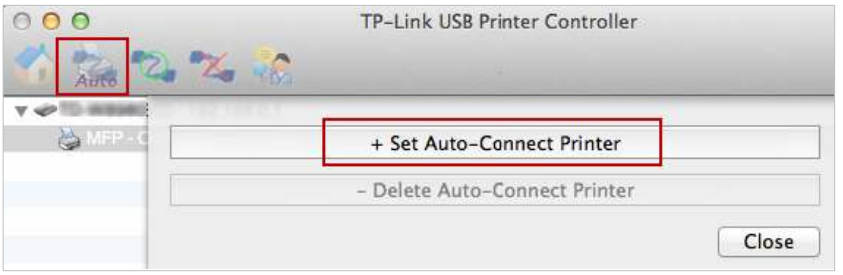


Mac

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

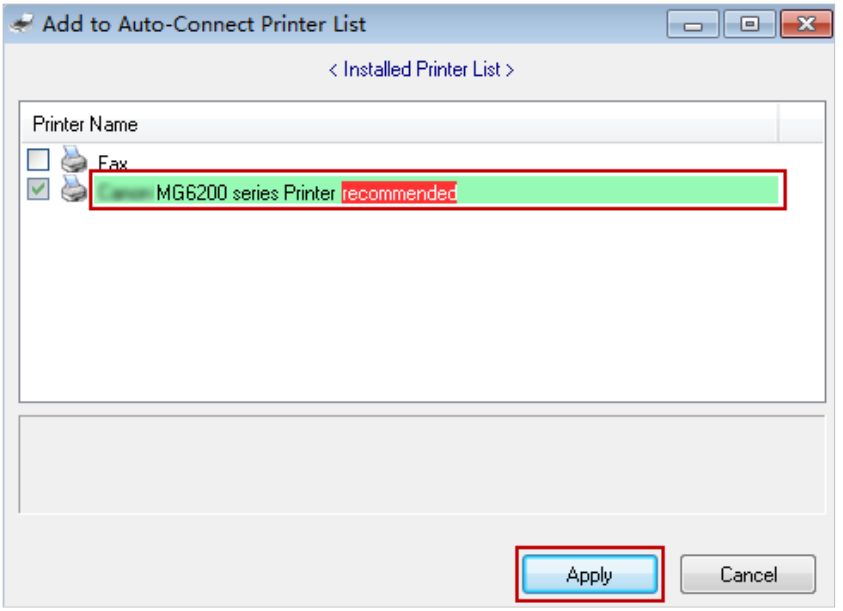


Windows

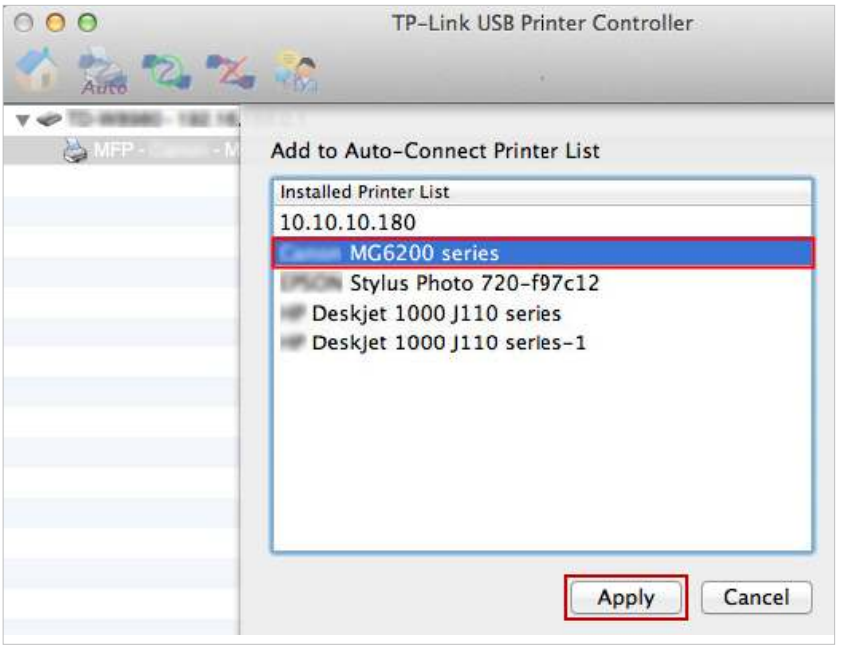


Mac

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 control access to specified websites at specified time.

I want to:

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

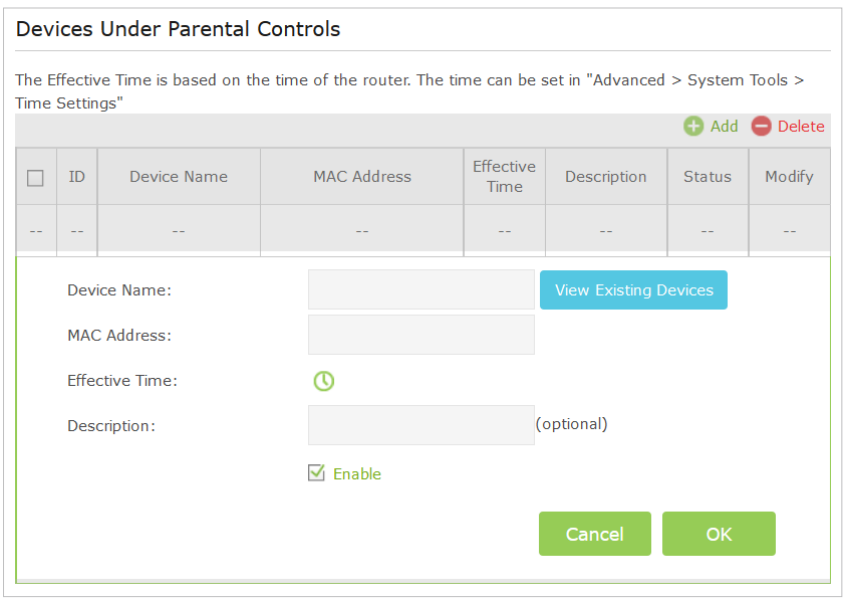
For example, I want to allow my children's devices (such as a computer or a tablet) to access only www.tp-link.com and Wikipedia.org from 18:00 (6PM) to 22:00 (10PM) on weekdays and not other time.

How can I do that?

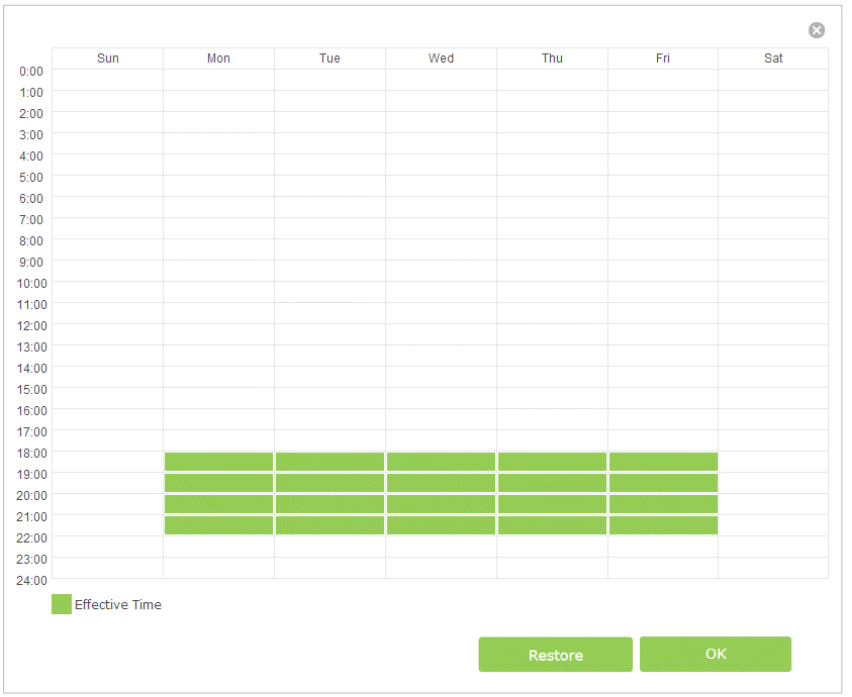
1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Basic or Advanced > Parental Controls and enable Parental Controls.



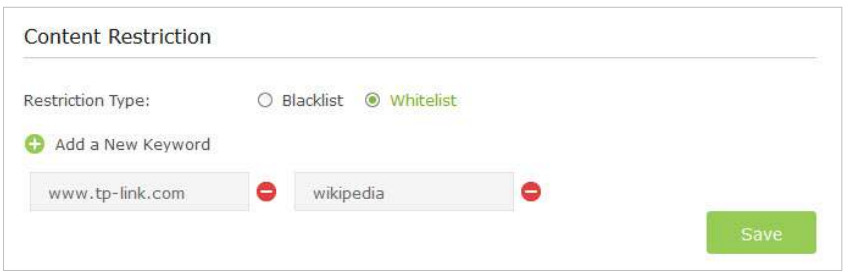
3. Click Add.



4. Click View Existing Devices, and select the device to be controlled. Or, enter the Device Name and MAC Address manually.
5. Click the icon to set the Effective Time. Drag the cursor over the appropriate cell(s) and click OK.



6. Enter a Description for the entry.
7. Select the checkbox to enable this entry and click OK.
8. Select the restriction type.
   1) With Blacklist selected, the controlled devices cannot access any websites containing the specified keywords during the Effective Time period.
   2) With Whitelist selected, the controlled devices can only access websites containing the specified keywords during the Effective Time period.



9. Click Add a New Keyword. You can add keywords for both Blacklist and Whitelist. Below are some sample entries to allow access.
   1) Enter a web address (such as www.tp-link.com) or a web address keyword (such as wikipedia) to only allow or block access to the websites containing that keyword.

2) Specify the domain suffix (such as .edu or .org) to allow access only to the websites with that suffix.

3) If you wish to block all Internet browsing access, do not add any keyword to the Whitelist.

10. Enter the keywords or websites you want to add and click Save.

Done!

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

Chapter *8*

Bandwidth Control

This feature is used to fully utilize your limit bandwidth and optimize the load respectively.

With this feature enabled, you can assign a specific minimum or maximum bandwidth for each computer, thus minimizing the impact caused when the connection is under heavy load.

I want to:

Use an independent bandwidth and enjoy a good Internet experience without being affected by other users who are sharing the same router.

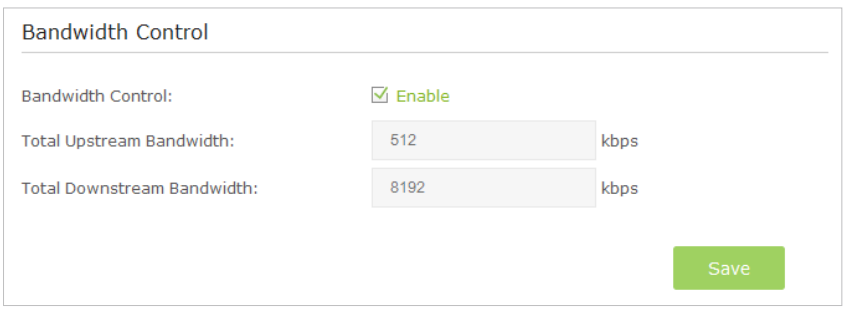
For example, my roommate and I share 512Kbps Upstream Bandwidth and 8Mbps Downstream Bandwidth via this router, she likes to watch live show and play online games, which may take up much bandwidth. I don't want to be affected, so we agree to equally distribute the bandwidth. Our IP addresses are 192.168.0.101 and 192.168.0.110.

Tips:

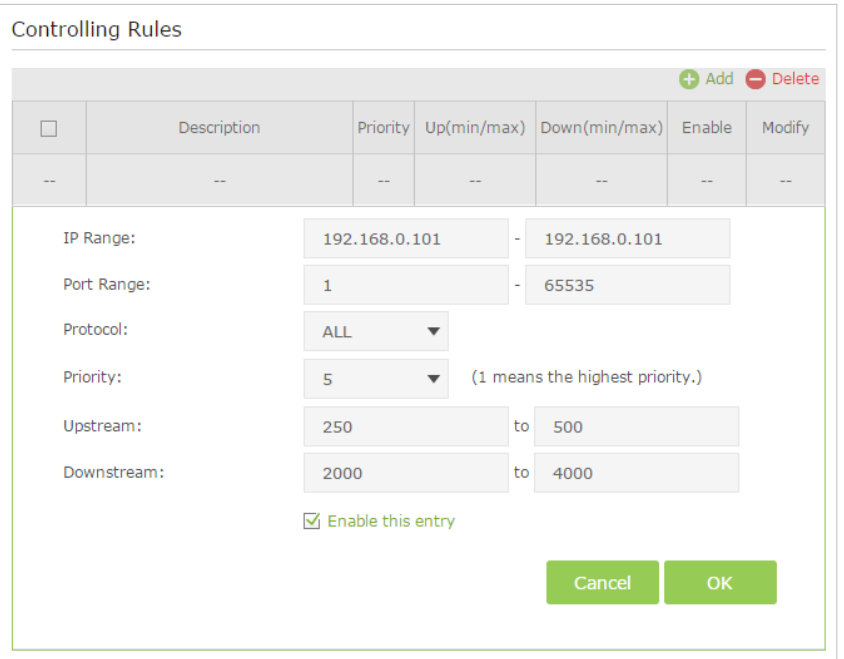
To use the bandwidth control feature, you'd better set static IP Address on each computer to be controlled or configure Address reservation on the router in order to manage easily. About how to configure address reservation, please refer to *To reserve an IP address for a specified client device*.

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 > Bandwidth Control page.



3. Enable Bandwidth Control.
4. Enter the Total Upstream Bandwidth and Total Downstream Bandwidth given by your ISP. (1Mbps=1024Kbps). Click Save to save the settings.
5. Click Add to add controlling rules for each computer respectively.



1) IP Range: Enter the IP address. The field can be single IP address or IP address range according to your demands. When you configure the single IP address, the computer with this IP address will get independent given bandwidth. When you configure the IP address range, all computers in the range will share the given bandwidth.

2) Port Range: Keep the default settings. The default port range of TCP protocol or UDP protocol is from 1 to 65535.

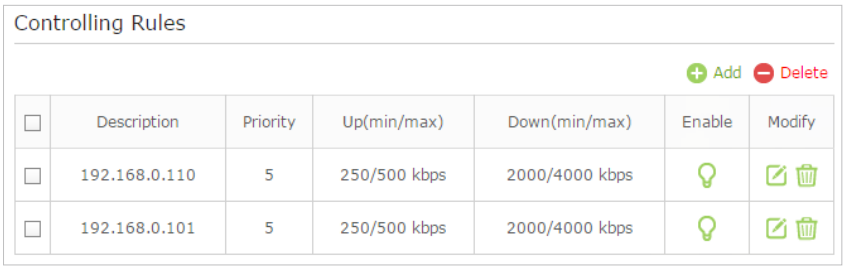
3) Protocol: Keep the default setting. Or you can choose the TCP protocol or UDP protocol or both of them.

4) Priority: Keep the default setting. You can change the value if you want to first guarantee the bandwidth for one computer. The smaller value has the higher priority.

5) Upstream/Downstream: Enter the bandwidth according to your division.

6) Check to enable this entry and click OK to save the settings.

6. Follow the steps above to add a rule for the other computer. And then you will get the following table.



Done!

Now you and your roommate have an independent bandwidth.

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*

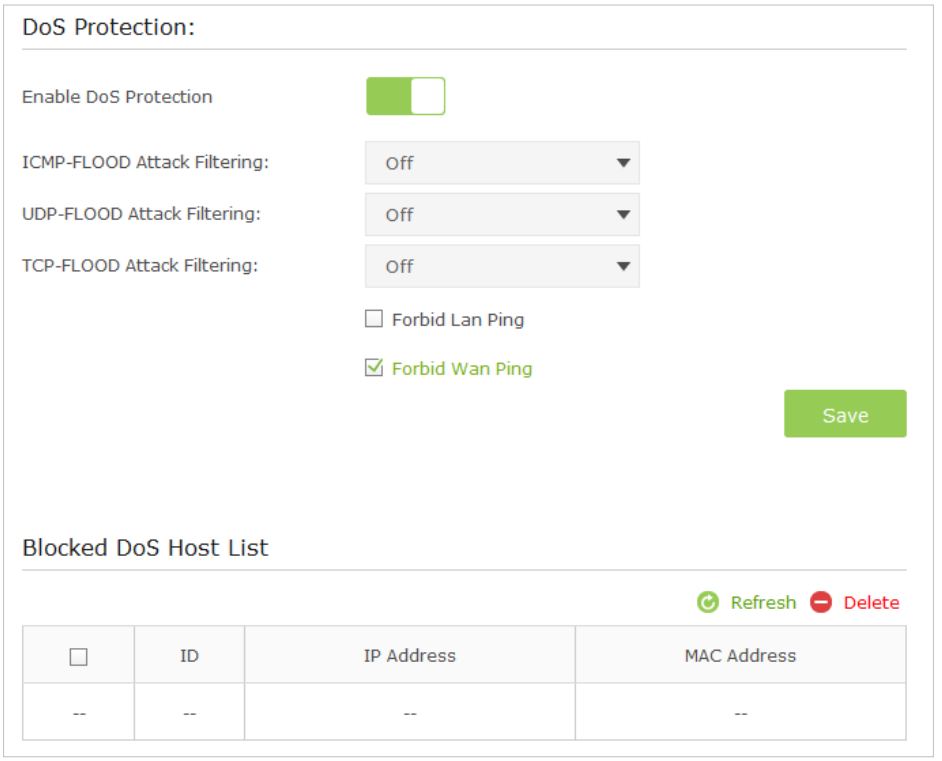
9. 1. Protect the Network from Cyber Attacks

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.

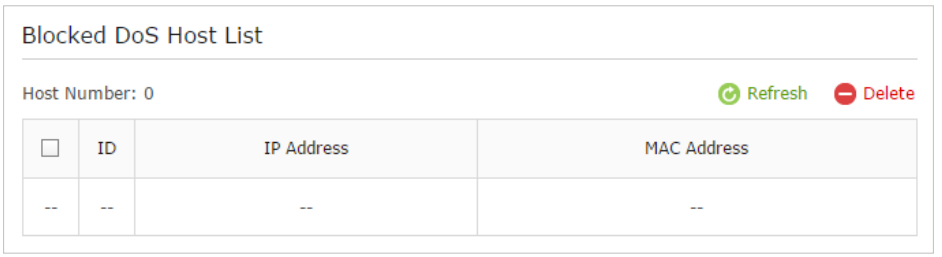


3. Enable DoS Protection.
4. Set the level (Off, Low, Middle or High) of protection for ICMP-FLOOD Attack Filtering, UDP-FlOOD Attack Filtering and TCP-SYN-FLOOD Attack Filtering.
   - ICMP-FLOOD Attack Filtering - Enable to prevent the ICM (PInternet Control Message Protocol) flood attack.
   - UDP-FlOOD 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 Settings), and the vicious host will be displayed in the Blocked DoS Host List.



5. If you want to ignore the ping packets from the WAN port, select Forbid Wan Ping; if you want to ignore the ping packets form the LAN port, select Forbid Lan Ping.
6. Click Save to make the settings effective.

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?

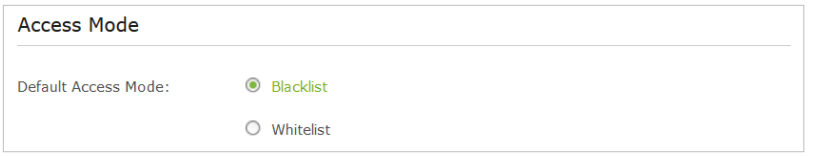
1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > Security > Access Control.
3. Enable Access Control.



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

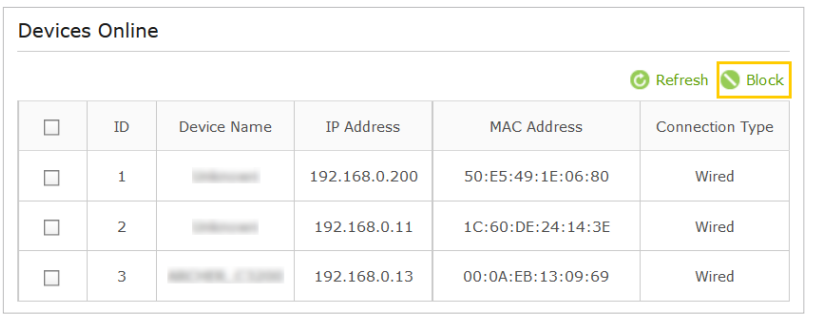
   To block specific device(s)

   1) Select Blacklist and click Save.



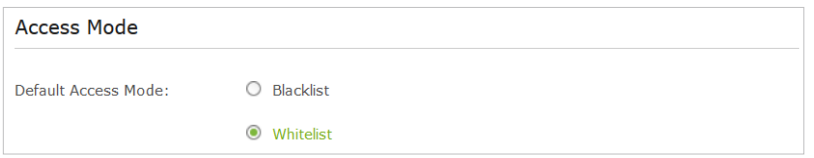
2) Select the device(s) to be blocked in the Devices Online table by ticking the box.

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

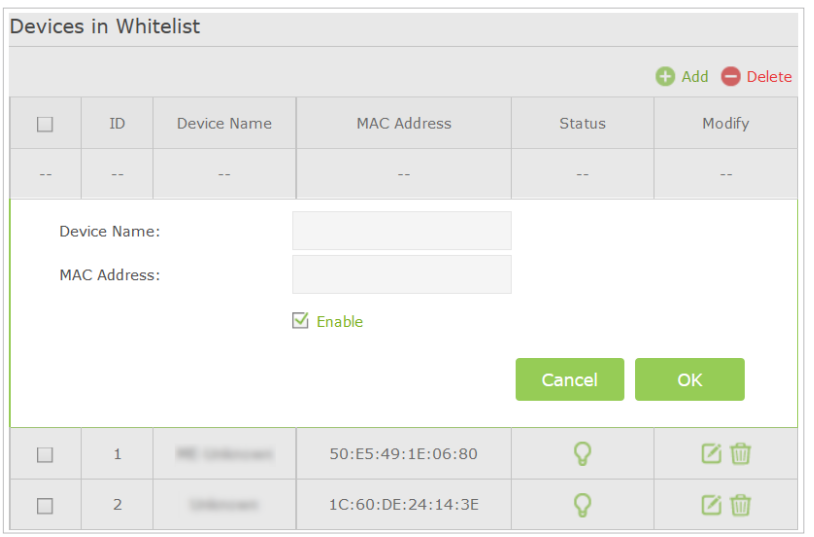


To allow specific device(s)

1) Select Whitelist and click 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 Devices Online list if the device is connected to your network).



3) Select the checkbox to enable the entry and 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

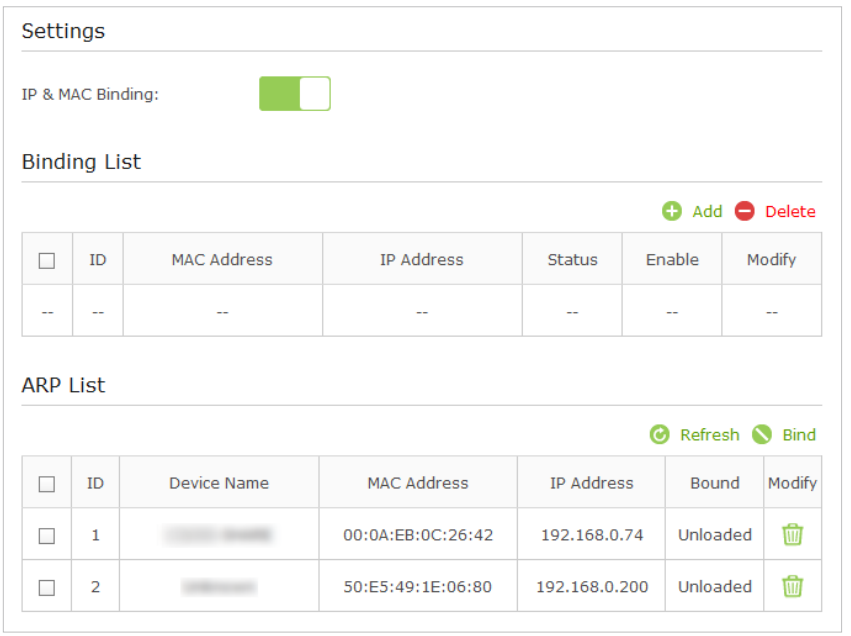
IP & MAC Binding, namely, ARP (Address Resolution Protocol) Binding, is used to bind network device's IP address to its MAC address. This will prevent ARP Spoofing and other ARP attacks by denying network access to an device with matching IP address in the Binding list, but unrecognized MAC address.

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 IP & MAC Binding.



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

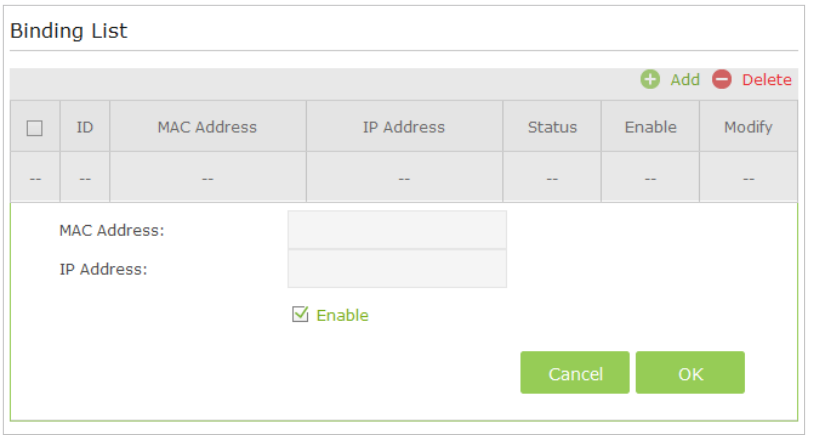
   To bind the connected device(s)

   1) Select the device(s) to be bound in the ARP List.

   2) Click Bind to add to the Binding List.

   To bind the unconnected device

   1) Click Add.



2) Enter the MAC address and IP address that you want to bind.

3) Select the checkbox to enable the entry 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

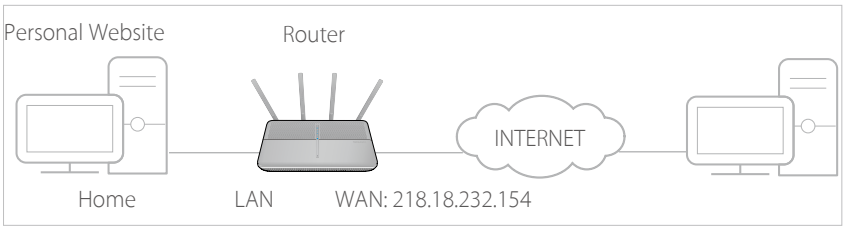
When you build up a server in the local network and want to share it on the Internet, Virtual Servers can realize the service and provide it to the Internet users. At the same time Virtual Servers can keep the local network safe as other services are still invisible from the Internet.

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:

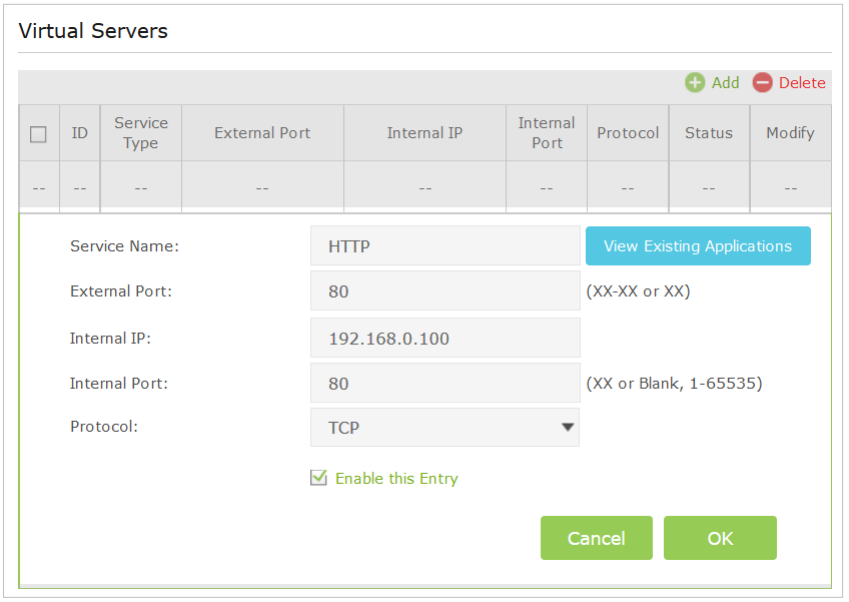
Share my personal website I've built in local network with my friends through the Internet.

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 Applications 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.



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 (in this example: 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 refer to *12. 4. Set Up a Dynamic DNS Service Account*. Then users on the Internet can use http:// domain name to visit the website.
2. If you have changed the default External Port, you should use http:// WAN IP: External Port or http:// domain name: External Port to visit the website.

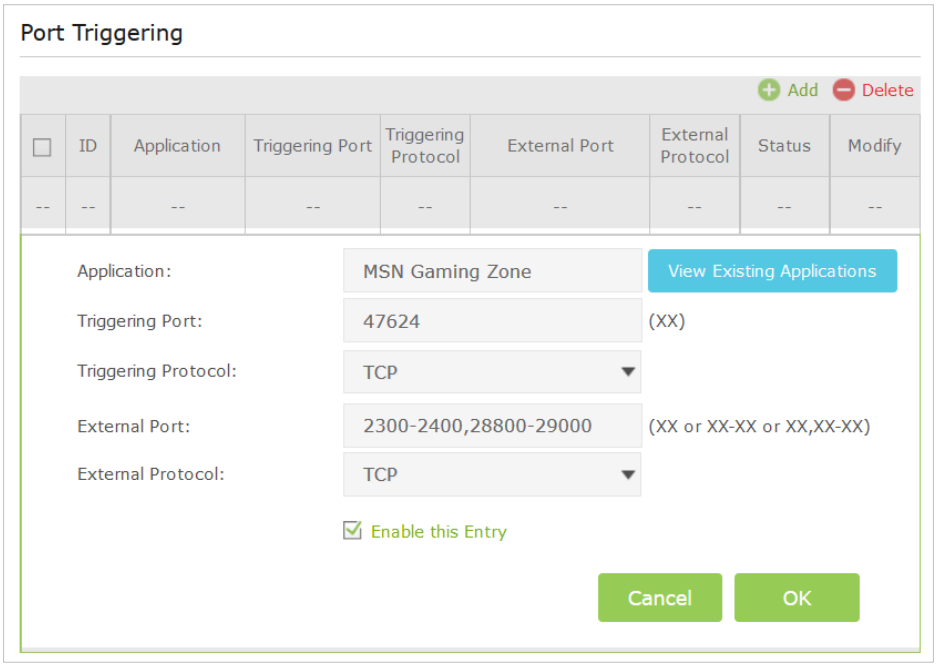
10. 2. Open Ports Dynamically by Port Triggering

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.



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.

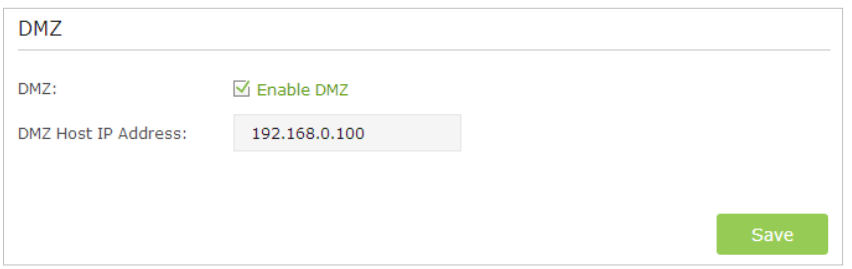
I want to:

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.



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.

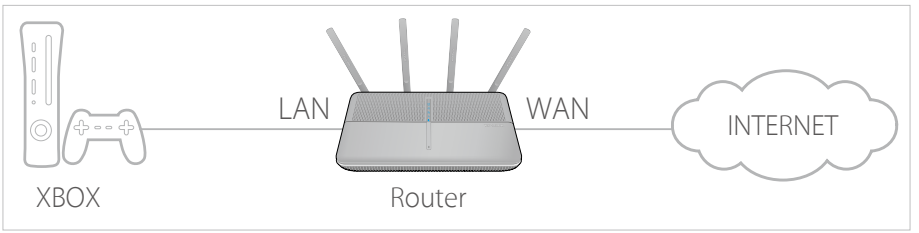
10. 4. Make Xbox Online Games Run Smoothly by UPnP

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:

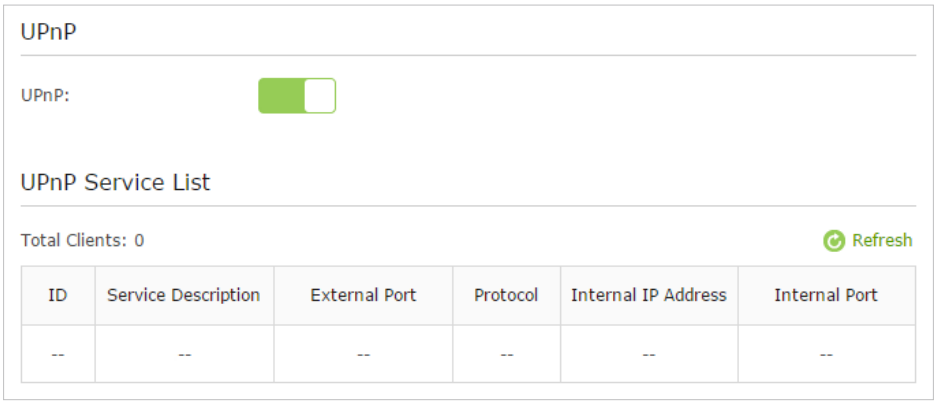
1. UPnP is enabled by default in this router.
2. Only the application supporting UPnP protocol can use this feature.
3. UPnP feature needs the support of operating system (e.g. Windows Vista/ Windows 7/ Windows 8, etc. Some of operating system need to install the UPnP components).

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.



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.

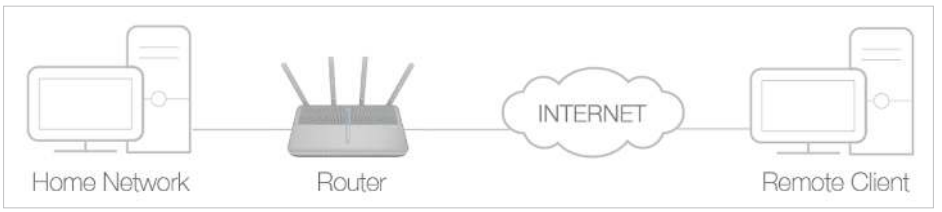
PPTP VPN is more easily used and its speed is faster, it's compatible with most operating systems and also supports mobile devices. Its security is poor and your packets may be cracked easily, and PPTP VPN connection may be prevented by some ISP.

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*

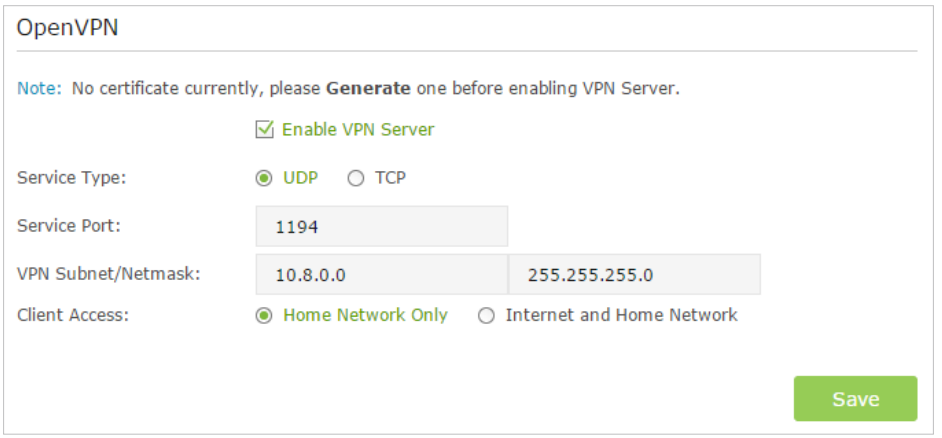
11. 1. Use OpenVPN to Access Your Home Network

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.

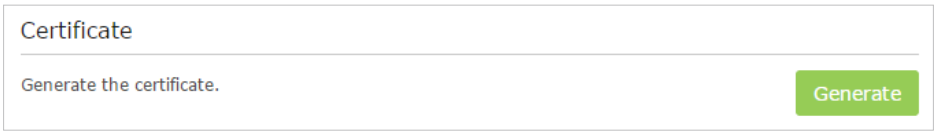


Note:

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.

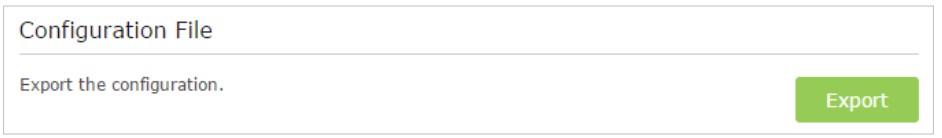
3. Select the Servive Type (communication protocol) for OpenVPN Server: UDP, TCP.
4. Enter a VPN Service Port to which a VPN client connects, and the port number should be between 1024 and 65535.
5. In VPN Subnet/Netmask field, enter the range of IP addresses that can be leased to the client by the OpenVPN 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.



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.



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 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.



Note:

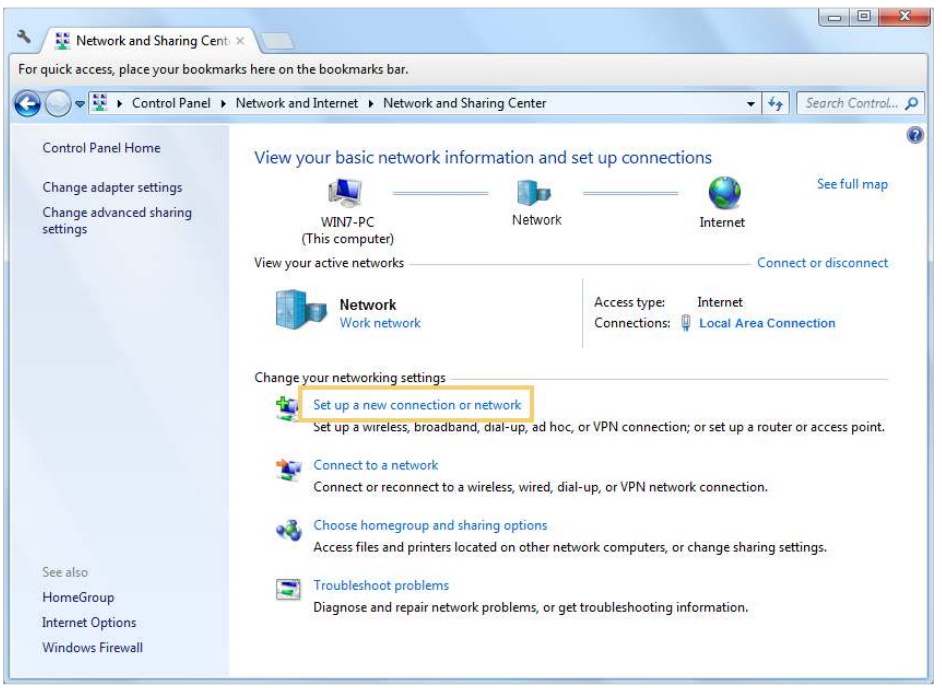
Before you enable VPN Server, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router's WAN port and synchronize your System Time with Internet.

3. In the Client IP Address filed, enter the range of IP addresses (up to 10 clients) that can be leased to the client by the PPTP VPN server.
4. Enter the Username and Password to authenticate clients to the PPTP VPN server.
5. Click Save.

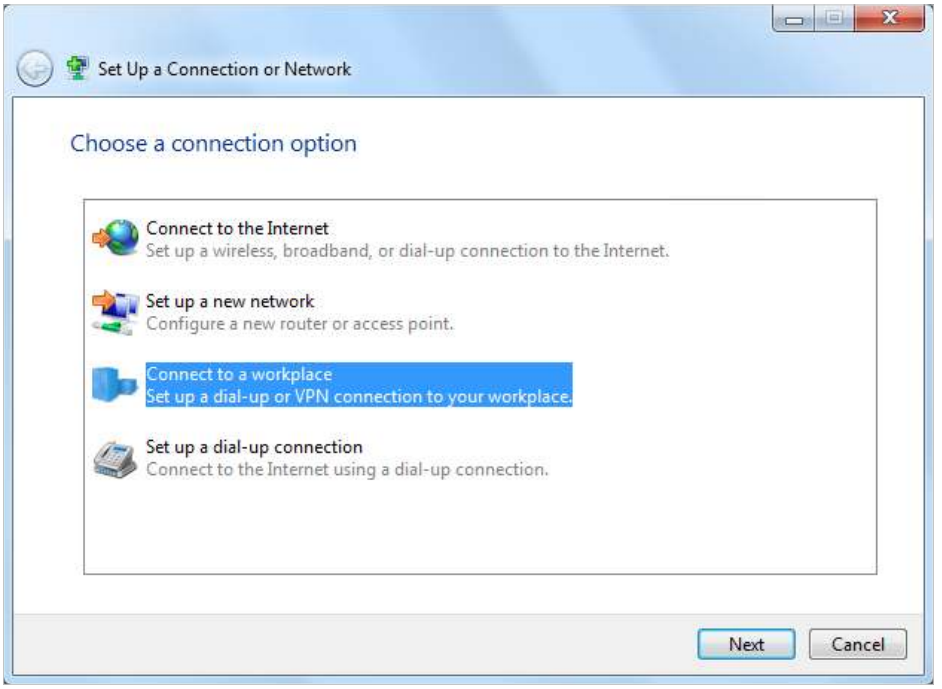
Step 2. Configure PPTP VPN Connection on Your Remote Client

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.

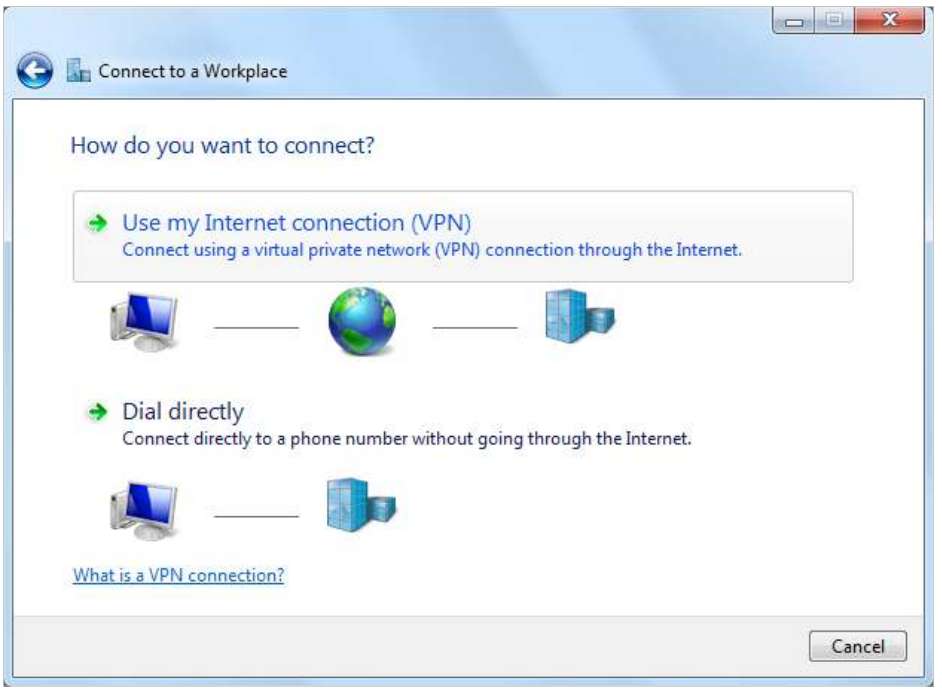
1. Go to Start > Control Panel > Network and Internet > Network and Sharing Center.
2. Select Set up a new connection or network.



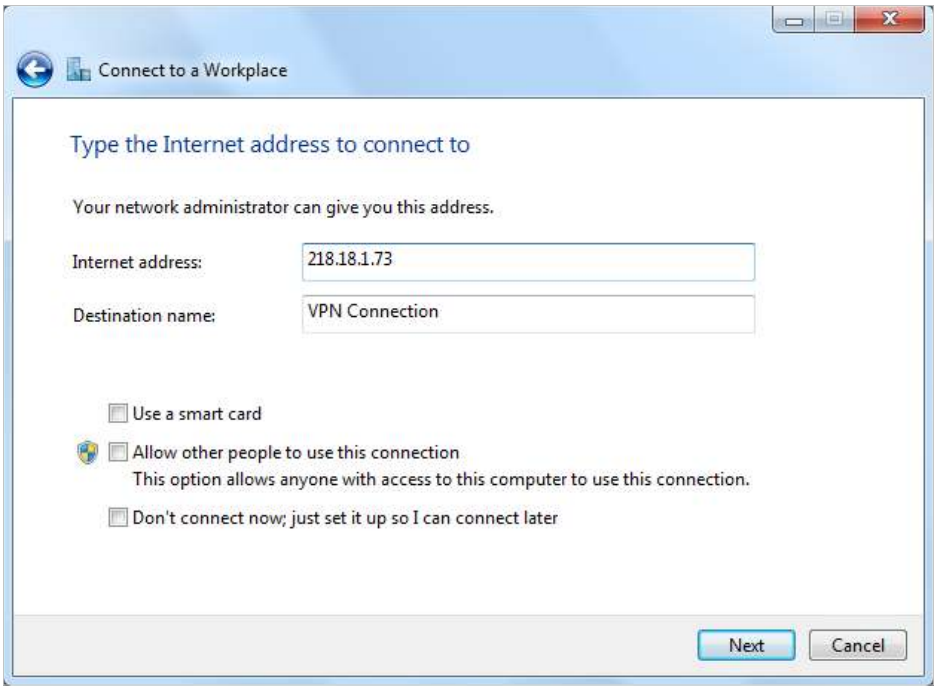
3. Select Connect to a workplace and click Next.



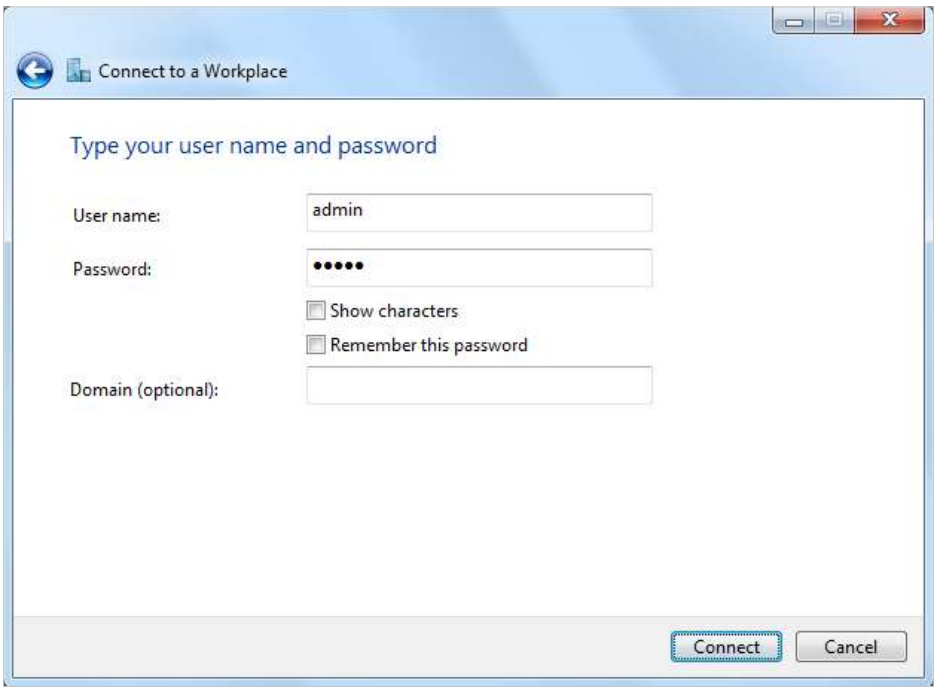
4. Select Use my Internet connection (VPN).



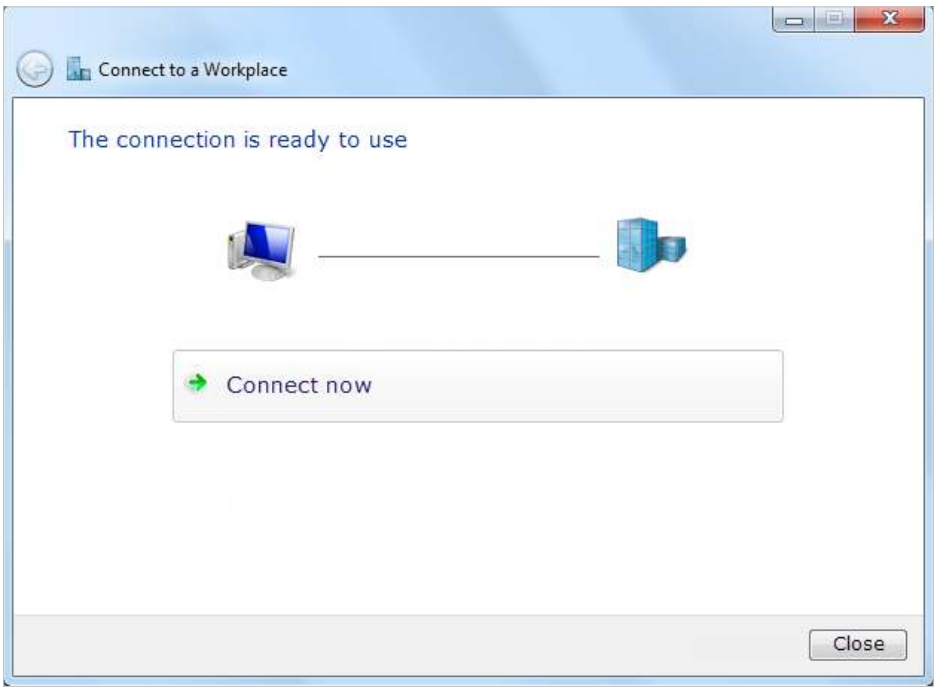
5. Enter the WAN IP address of the router (for example: 218.18.1.73) in the Internet address field. Click Next.



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



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 that are available for this router.

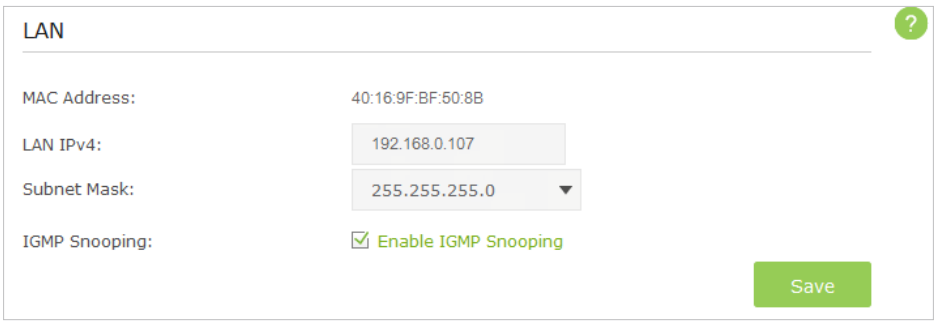
This chapter contains the following sections:

- *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*
- *Schedule Your Wireless Function*
- *Set up a VPN 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-based 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.



4. Keep IGMP Snooping as enabled by default. IGMP Snooping is the process of listening to IGMP (Internet Group Management Protocol) network traffic. The function prevents hosts on a local network from receiving traffic for a multicast group they have not explicitly joined.
5. 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 them.

12. 2. Configure to Support IPTV Service

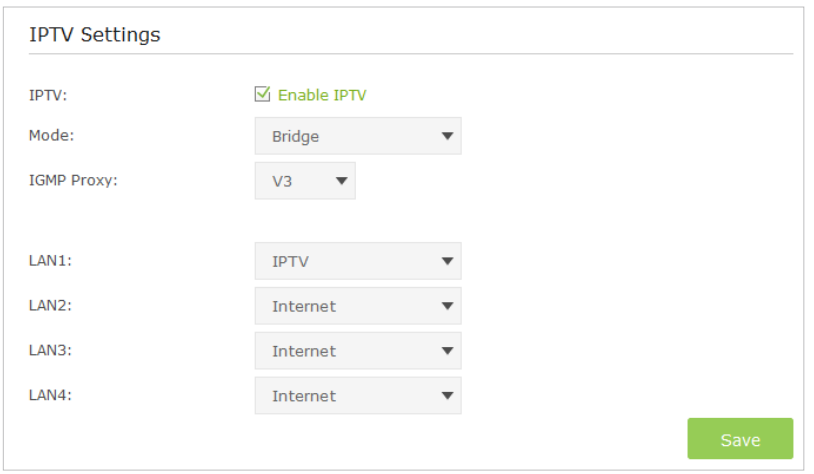
IPTV is the abbreviation of Internet Protocol Television. The service can only be delivered through the Internet, and our router provides a specific LAN port for IPTV.

By automatically seperating IPTV from Internet surfing, we guarantee you a high quality of vedio streaming and a high speed of Internet surfing.

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. Configure IPTV settings:



1) Tick the Enable IPTV check box.

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 substep 4. Select Custom if your ISP is not listed but provides necessary parameters.

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) Select the IGMP Proxy version, either V2 or V3, according to the information provided by your ISP.

5) For Russia, Singapore-ExStream, Malaysia-Unifi and Malaysia-Maxis modes, 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.

6) Click Save.

Done!

Your IPTV setup is done now! You may need other configurations on your set-top box before enjoying your TV.

Tips

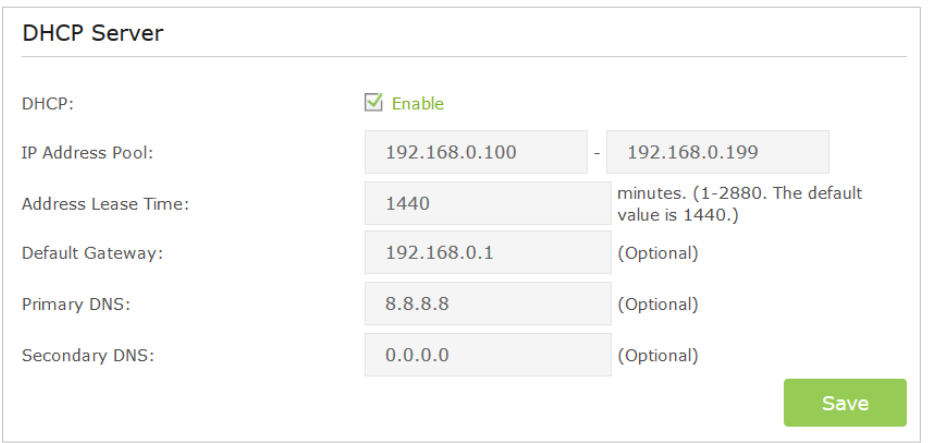
QoS and IPTV cannot be enabled at the same time.

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.

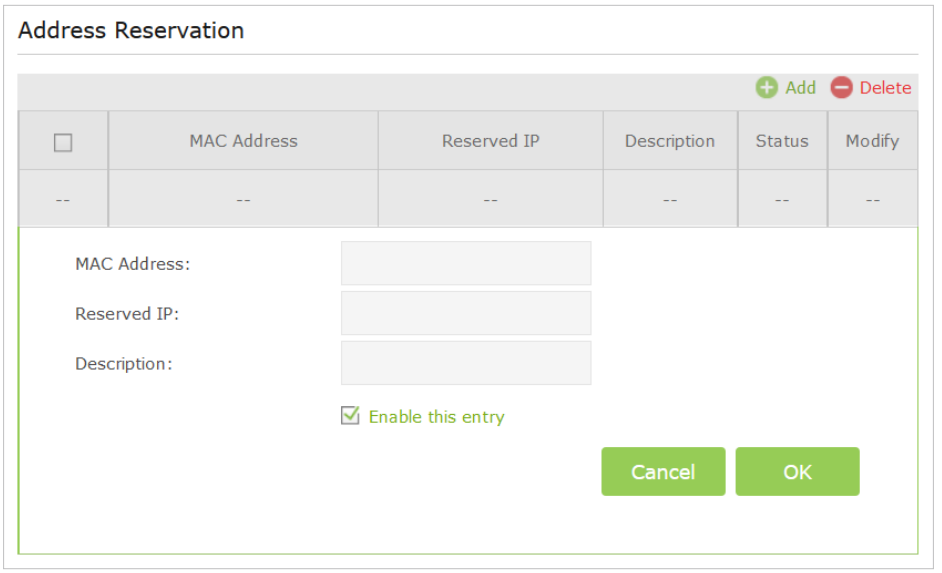
➢ **To specify the IP address that the router assigns**



3. Make sure that DHCP is enabled.
4. Enter the starting and ending IP addresses in the IP Address Pool.
5. 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.
6. Click Save to make the settings effective.

➢ **To reserve an IP address for a specified client device**

1. Click the Add button in Address Reservation section.



2. Enter the MAC address of the device for which you want to reserve IP address.
3. Specify the IP address which will be reserved by the router.
4. Enter the Description for the rule.
5. Tick the Enable This Entry checkbox and click OK.

Note:

You can also appoint IP addresses within a specified range to devices of the same type by using Condition Pool feature. For example, you can assign IP addresses within the range (192.168.0.50 to192.168.0.80) to Camera devices, thus facilitating the network management.

12. 4. Set Up a Dynamic DNS Service Account

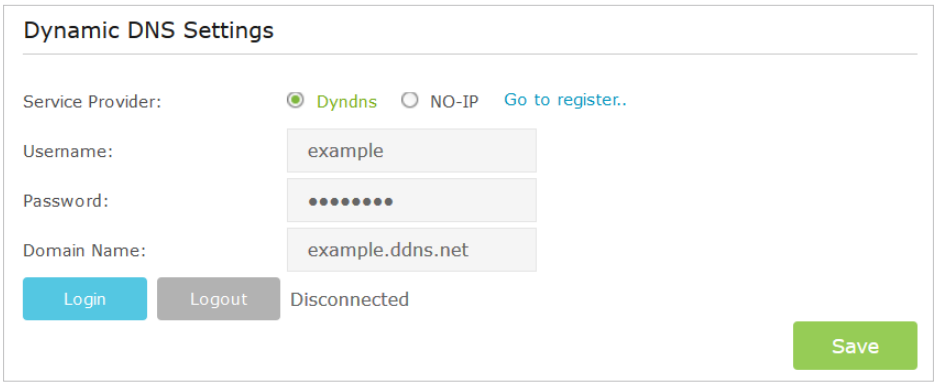
Most ISPs (Internet Service Providers) assign a dynamic IP address to the router and you can use this IP address to access your router remotely. However, the IP address can change any time and you don't know when it changes. In this case, you might need the DDNS (Dynamic Domain Name Server) feature on the router to allow you and your friends to access your router and local servers (FTP, HTTP, etc.) using domain name, in no need of 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 (Dyndns or NO-IP). If you don't have a DDNS account, select a service provider and click Go to register.



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

5. Click Login, then click Save.

Tips:

If you want to use a new DDNS account, please Logout first, then login with the new account.

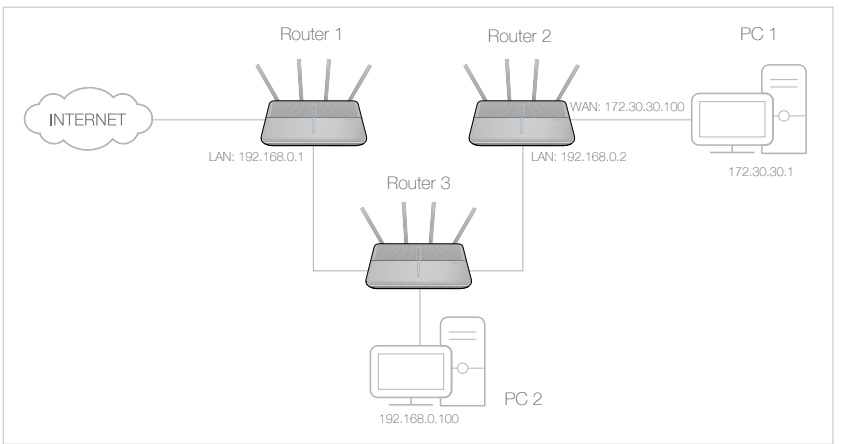
12. 5. Create Static Routes

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:

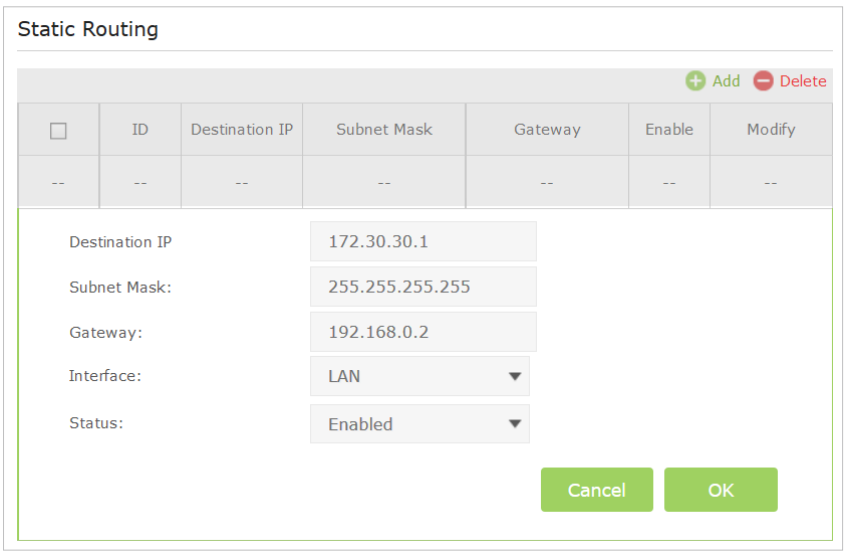
Visit multiple networks and multiple servers at the same time.

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 achieved. 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've set for the router.
3. Go to Advanced > Network > Advanced Routing.
4. Click Add and finish the settings according to the following explanations:



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 enters 172.30.30.1.

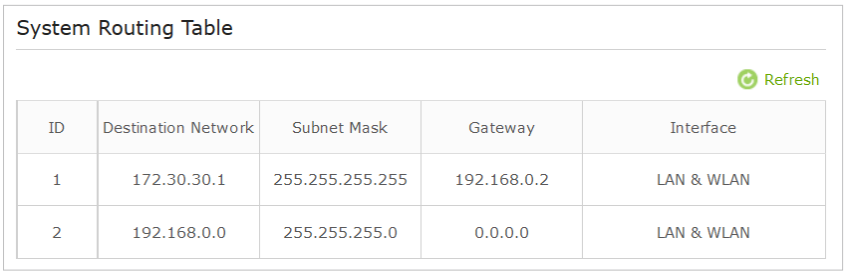
Subnet Mask: Determines the destination network with the destination IP address. If the destination is a single IP address, enter 255.255.255.255; otherwise, enter the subnet mask of the corresponding network IP. In the example, the destination network is a single IP, so here enters 255.255.255.255.

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 the 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 the data packets. In the example, the data is sent to the gateway through the LAN port, so LAN should be selected.

Status: Determines the status of the entry. In the example, Enabled should be selected.

5. Click OK to save the settings.
6. Check the System Routing Table below. If you can find the entry you've set in the System Routing Table, the static routing is set successfully.



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 product label. 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 of 2.4GHz or 5GHz:**

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 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 Wireless Network Name (SSID) and customize the password for the network in Password. The default SSID is TP-LINK_XXXX for 2.4GHz and TP-LINK_XXXX_5G for 5GHz, and the value is case-sensitive.

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

➢ **To hide SSID of 2.4GHz or 5GHz:**

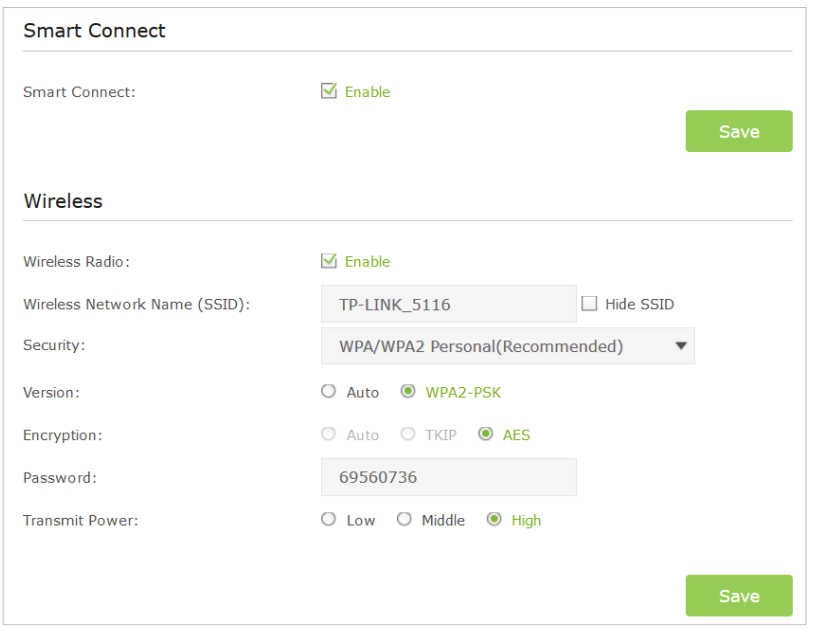
1. Go to Basic > Wireless.
2. Select Hide SSID, and your SSID will not be broadcast. Your SSID won't display when you scan for local wireless network on your wireless device and you need to manually join the network.

To use the smart connect function

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

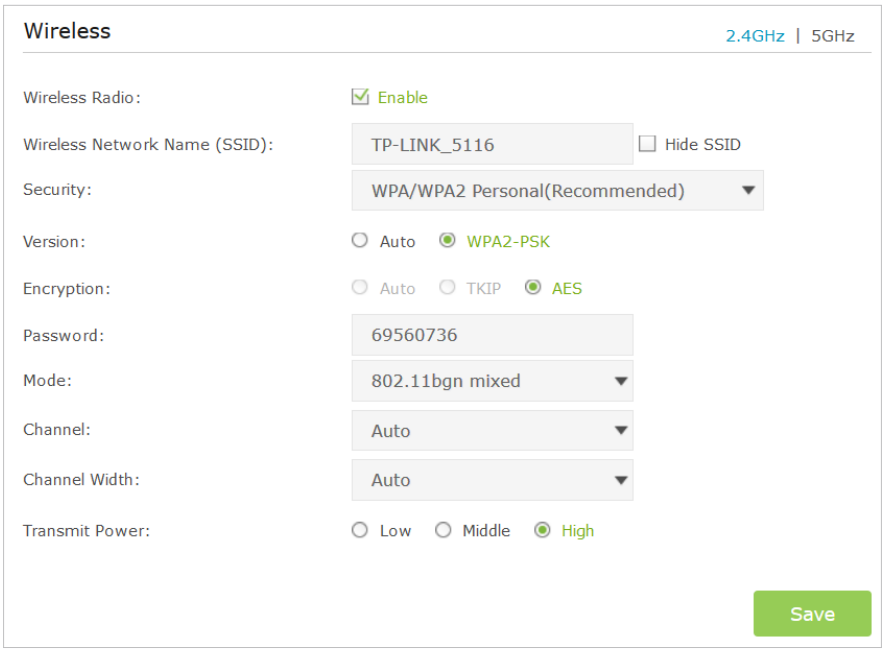
1. Go to Advanced > Wireless > Wireless Settings.
2. Select the Smart Connect checkbox, and click Save.
3. Keep the default or set a new SSID and password, and click Save.

This SSID and password will be applied for 2.4GHz and 5GHz wireless networks.



➢ **To change the security option:**

1. Go to Advanced > Wireless > Wireless Settings.



2. Select the wireless network 2.4GHz or 5GHz.
3. Select an option from the Security drop down list. The router provides four security options, No Security, WPA/WPA2 - Personal (Recommended), WPA/WPA2 - Enterprise and WEP. 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. 802.11b/g/n mixed, 802.11g/n mixed or 802.11n only for 2.4GHz; and 802.11a/n/ac mixed, 802.11n/ac mixed or 802.11ac only for 5GHz. 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

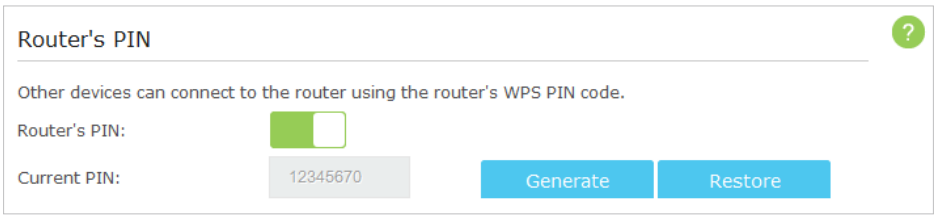
Wi-Fi Protected Setup (WPS) gives consumers an easier approach to set up a security-protected Wi-Fi connection.

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.



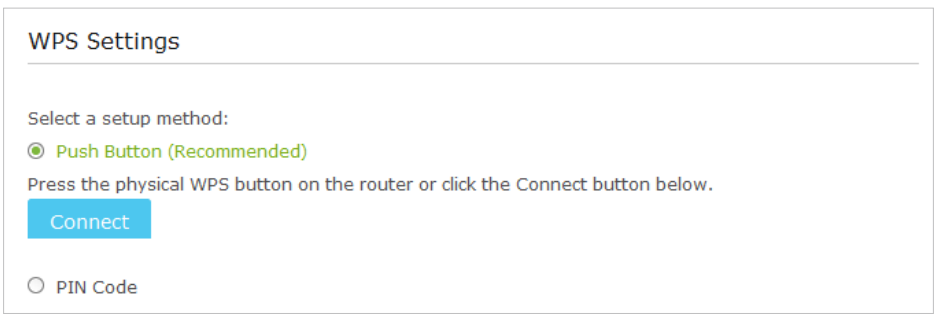
Note:

1. If you want to enable/disable the WPS feature, go to Advanced > 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 labeled on the bottom of the router.

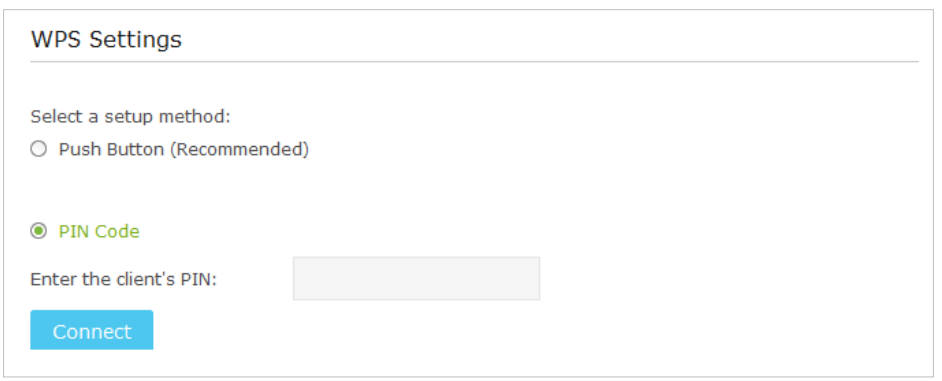
12. 7. 2. Use the WPS Wizard for Wi-Fi Connections

1. Select a setup method:

- **Push Button(Recommended)**: Click the Connect button on the screen. Within two minutes, push the WPS button on the client device.



- **PIN**: Enter the client's PIN, and click Connect.

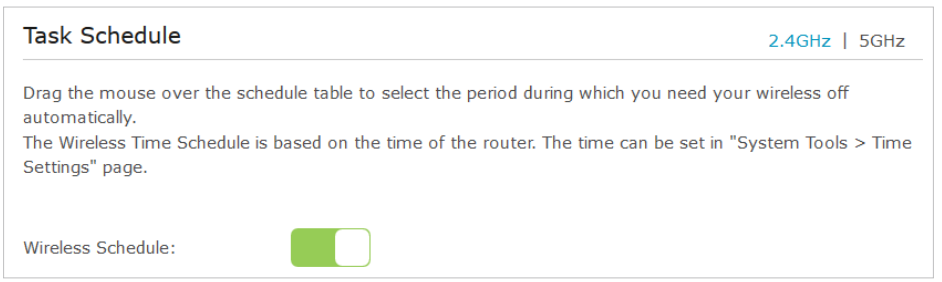


2. Success will appear on the above screen and the WPS LED on the router will keep on for five minutes if the client has been successfully added to the network.

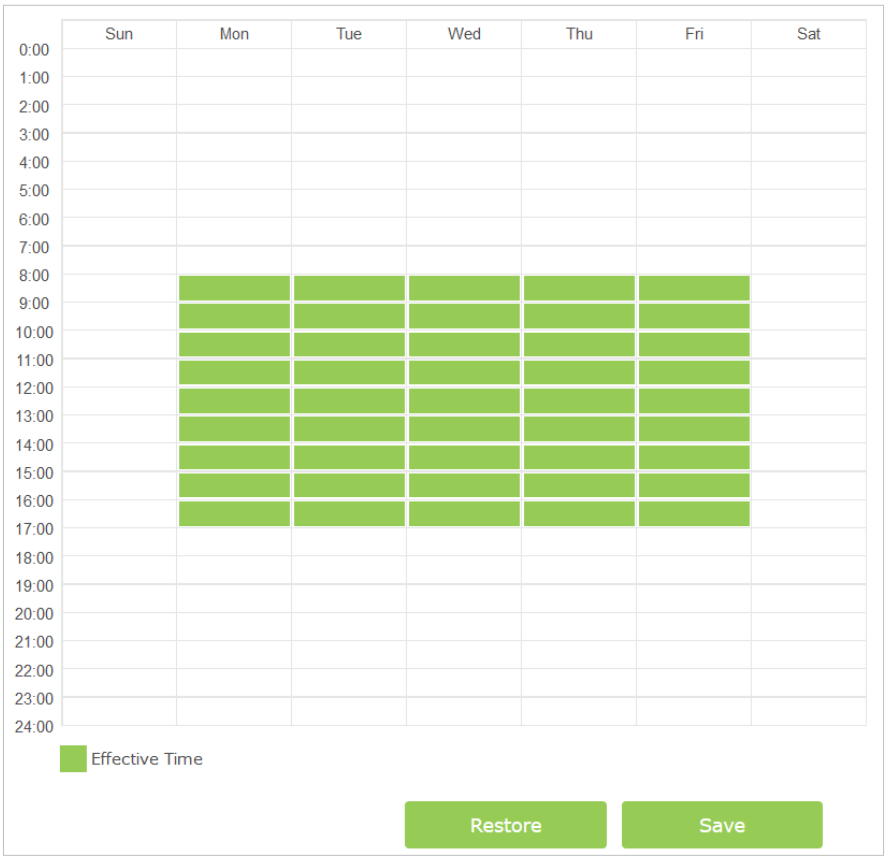
12. 8. Schedule Your Wireless Function

You can schedule to automatically turn off your 2.4GHz, 5GHz, or both wireless networks at a specific time when you do not need the wireless connection.

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Go to Advanced > Wireless > Wireless Schedule.
3. Select 2.4GHz or 5GHz to change the corresponding settings, then toggle on to enable the Wireless Schedule feature.



4. Set the Effective Time. Drag the cursor over the cells to choose the period during which you need the wireless off automatically, and click OK.



5. Click Save.

6. If you also want to set wireless off time for the other band, please repeat the steps above.

Note:

1. The Effective Time Schedule is based on the time of the router. You can go to Advanced > System Tools > Time Settings to modify the time.
2. The wireless LED will be off if the corresponding wireless network is disabled.
3. The wireless network will be automatically turned on after the time period you set.

12. 9. Set up a VPN Connection

VPN (Virtual Private Network) is a private network established across the public network, generally via the Internet. However, the private network is a logical network without any physical network lines, so it is called Virtual Private Network.

With the wide application of the Internet, more and more data are needed to be shared through the Internet. Connecting the local network to the Internet directly, though can allow the data exchange, will cause the private data to be exposed to all the users on the Internet.

The VPN (Virtual Private Network) technology is developed and used to establish the private network through the public network, which can provides a secure

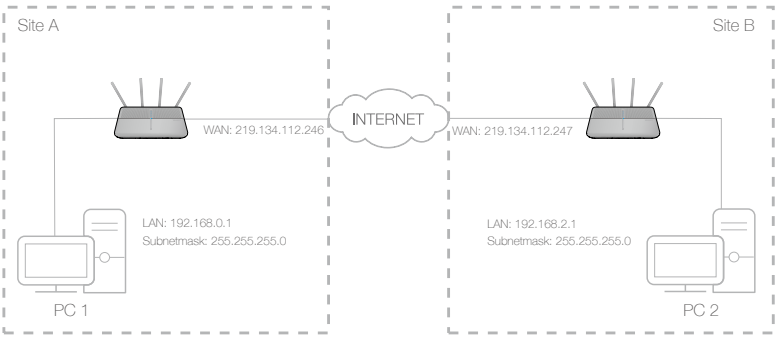
communication to a remote computer or remote network, and guarantee a secured data exchange. IPSec is one of the major implementations of VPNs.

I want to:

Establish an IPSec VPN tunnel to connect two LANs via Internet so that the hosts in different remote LANs are able to communicate with each as if they are in the same LAN.

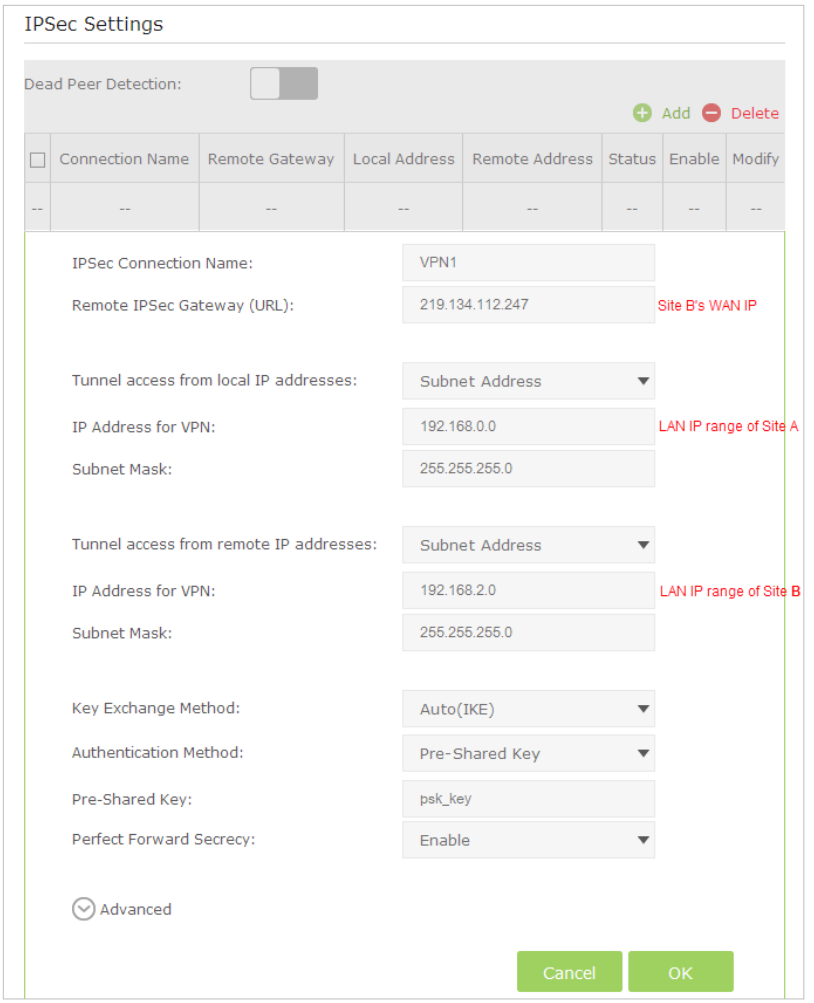
For example, I am the network administrator of a regional office, I need to let my office staff can visit the headquarter's servers and resources, and vice versa. I know that the router in my office and the device in headquarter both support IPSec VPN feature, so I decide to set up a VPN connection with the headquarter office.

The following diagram is a typical VPN topology. Here Site A refers to regional office's network (local network). And Site B refers to the headquarter's network (remote network) which I want to connect.



How can I do that?

1. Make sure of the topology you want to build and record site A (local network) and site B (remote network)'s LAN IP and WAN IP.
2. Configuration on site A (local network).
   1) Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
   2) Go to Advanced > Network > IPSec VPN to open the configuration page. Click Add to set up a VPN tunnel.



3) In the IPSec Connection Name column, specify a name.

4) In the Remote IPSec Gateway (URL) column, Enter Site B's WAN IP address.

5) To configure Site A's LAN:

In the Tunnel access from local IP addresses column, here we take Subnet Address as an example. Then input the LAN IP range of Site A in the IP Address for VPN column, and input Subnet Mask of Site A.

6) To configure Site B's LAN:

In the Tunnel access from remote IP addresses column, here we take Subnet Address as an example. Then input the LAN IP range of Site B in the IP Address for VPN column, and input Subnet Mask of Site B.

7) Select the Key Exchange Method for the policy. We select Auto(IKE) here.

8) Enter the Pre-Shared Key for IKE authentication. Then keep Perfect Forward Secrecy enabled.

Note:

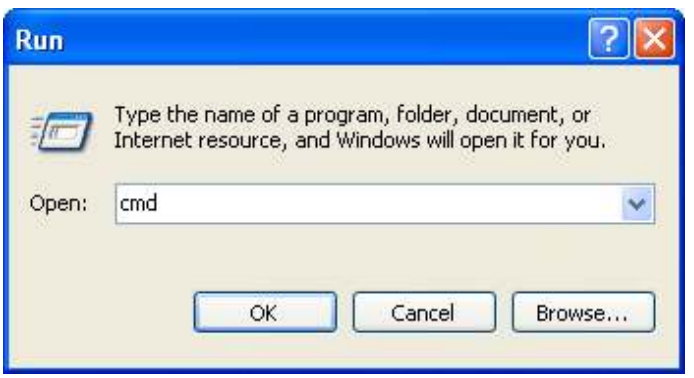
- The key should consist of visible characters without blank space.
- Make sure Site A and Site B use the same key.

9) Leave the Advanced Settings as default value. Then click OK to save.

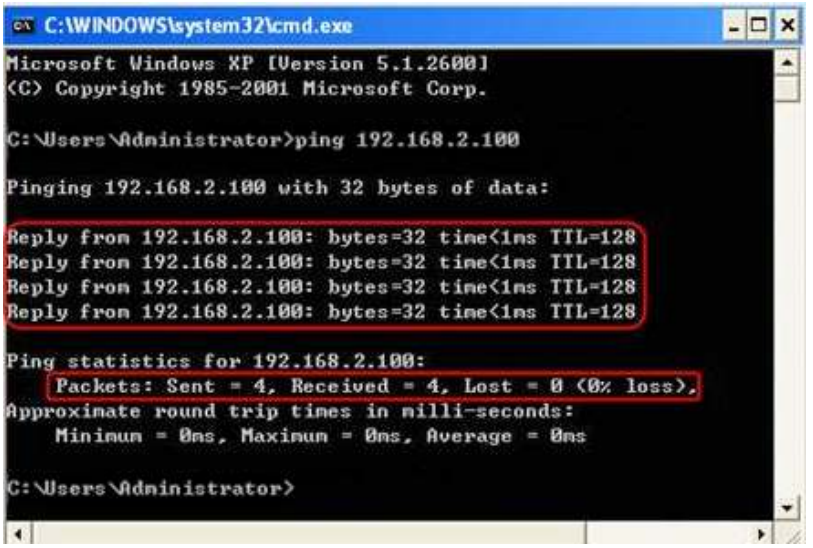
3. Configuration on Site B (remote network). Refer to step 2 configuration on Site A and make sure that Site A and Site B use the same Pre-shared keys and Perfect Forward Secrecy settings.
4. The Status column will change to UP if the VPN connection has been set up successfully.
5. Check the VPN connection. You can ping site B' LAN IP from your computer in site A to verify that the IPSec VPN connection is set up correctly.

Tips: To check the VPN connection, you can do the following.

a . On the host in Site A, press [Windows Logo] + [R] to open Run dialog. Input "cmd" and hit OK.



b . In the CLI window, type in "ping 192.168.2.x" ("192.168.2.x" can be IP address of any host in Site B). Then press [Enter].



If Ping proceeds successfully (gets replies from host in Site B), the IPSec connection is working properly now.

Done! Now IPSec VPN is implemented to establish a connection.

Note:

1. The product supports a maximum of ten simultaneous connections.
2. If one of the site has been off line for a while, for example, if Site A has been disconnected, on Site B you need to click Disable and then click Enable after Site A back on line in order to re-establish the IPSec tunnel.

Chapter *13*

Manage the Router

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

This chapter includes the following sections:

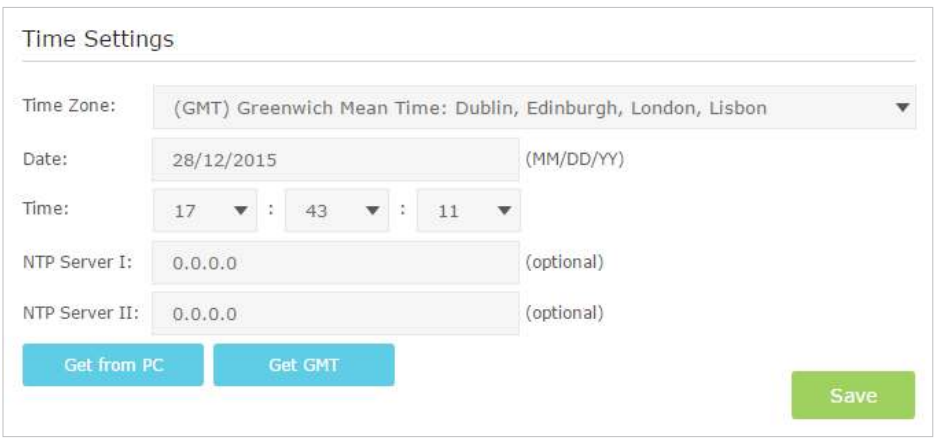
- *Set Up System Time*
- *Test the Network Connectivity*
- *Upgrade the Firmware*
- *Backup and Restore Configuration Settings*
- *Change the Administrator Account*
- *Local Management*
- *Remote Management*
- *System Log*
- *SNMP Settings*
- *Monitor the Internet Traffic Statistics*
- *Control LEDs*

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 and Wireless Schedule. You can manually set how to get the system time.

Follow the steps below to set your system time.

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



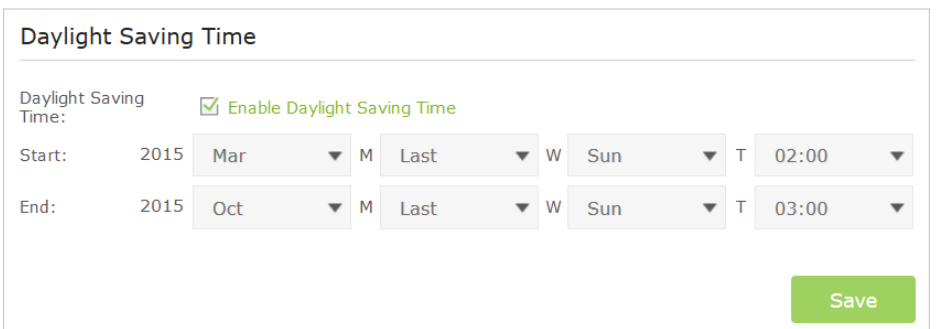
3. Configure the system time using the following methods :

   Manually: Select your time zone and enter your local time.

   Get from PC: Click this button if you want to use the current managing PC's time.

   Get GMT: Click this button if you want to get time from the Internet. Make sure your router can access the Internet before you select this way to get system time.

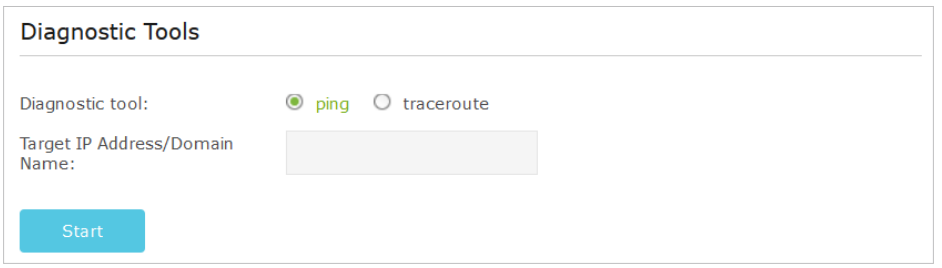
4. Click Save to make your settings effective.
5. After setting the system time, you can set Daylight Saving Time according to your needs. Tick the checkbox to enable Daylight Saving Time, set the start and end time and then click Save to make the settings effective.



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.

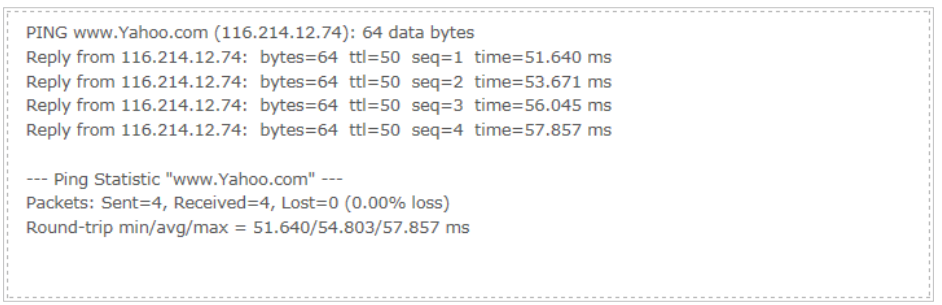
   2) Enter the Target IP Address/Domain Name of the tested host.

4. Click Start to begin the diagnostics.

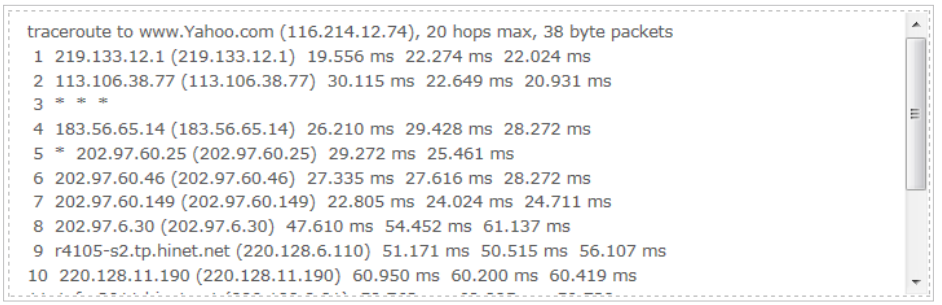
Tips:

Click Advanced, you can modify the ping count, ping packet size, test timeout time, or max hop. 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.



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



13. 3. Upgrade the Firmware

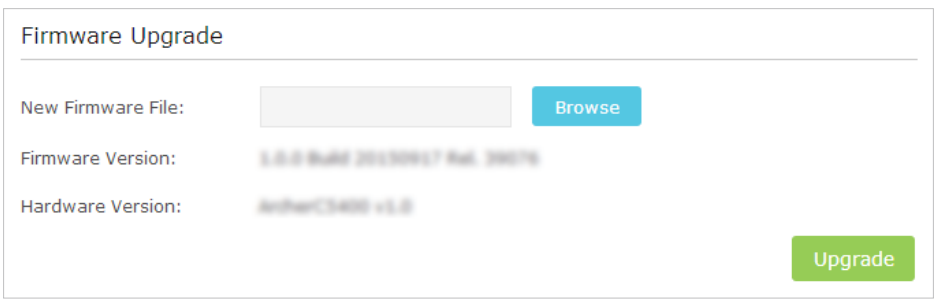
TP-LINK is dedicated to improving and richening the product features, giving you a better network experience. We will release the latest firmware at TP-LINK official website, you can download the latest firmware file from the Support page of our website *www.tp-link.com* and upgrade the firmware to the latest version.

Note:

1. Make sure the latest firmware file is matched with the hardware version (as shown in the webpage).
2. Make sure that you have a stable connection between the router and your computer. It is NOT recommended to upgrade the firmware wirelessly.
3. Make sure you remove any USB storage device connected to the router before the firmware upgrade to prevent data loss.
4. Backup your router configuration.
5. Do NOT turn off the router during the firmware upgrade.

Follow the steps to upgrade the firmware.

1. Download the latest firmware file for the router from our website *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. Click Browse to locate the downloaded new firmware file, and click Upgrade.



5. Wait a few moments for the upgrading and rebooting.

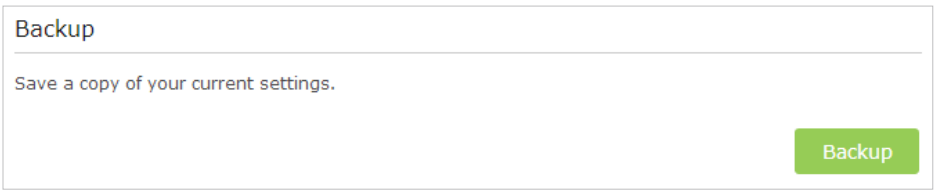
13. 4. Backup and Restore Configuration Settings

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.

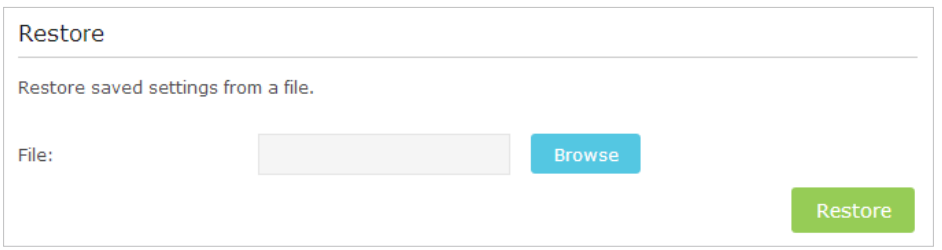
➢ **To backup configuration settings:**

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.



➢ **To restore configuration settings:**

1. Click Browse to locate the backup configuration file stored on your computer, and click Restore.

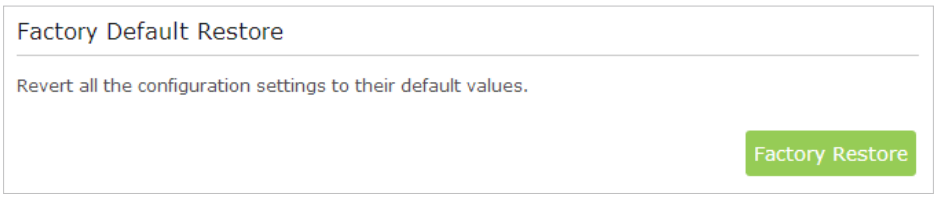


2. Wait a few moments for the restoring and rebooting.

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.



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

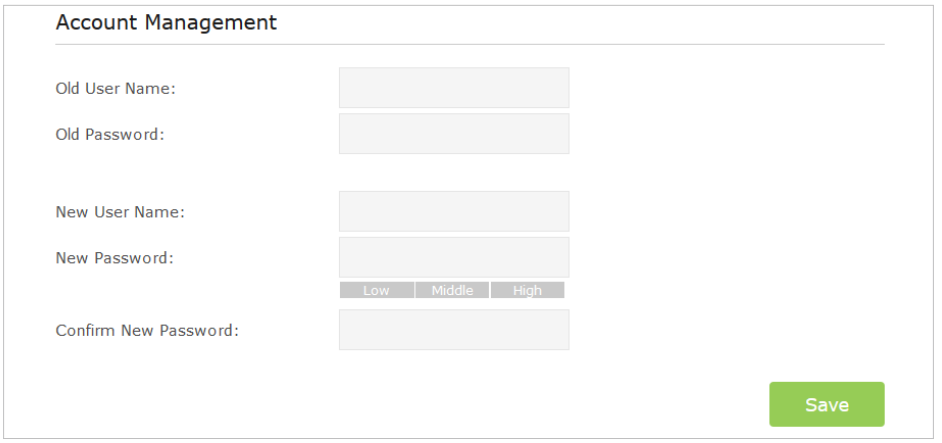
Note:

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 management web-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.



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. Local Management

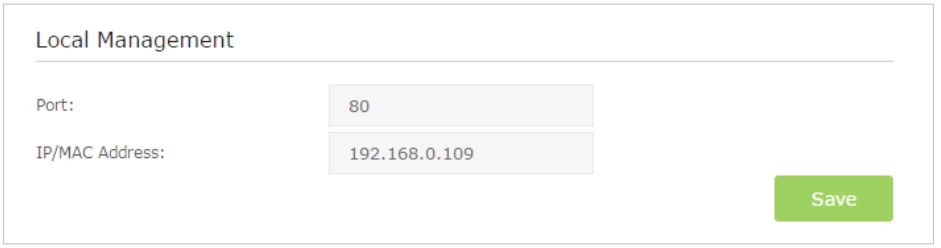
You can control the local devices' authority to manage the router via Local Management feature. By default all local connected devices are allowed to manage the router. You can also allow only one device to manage the router.

Follow the steps below to specify the local management.

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 page. Locate the Local Management section.
3. Keep the Port as the default setting. Enter the IP address or MAC address of the local device to manage the router.

Note:

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



4. Click Save to make the settings effective. Now only the device using the IP address or MAC address you set can manage the router.

13. 7. Remote Management

By default, the remote devices are not allowed to manage the router from the Internet.

Follow the steps below to allow remote devices 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 page. Locate the Remote Management section.



3. Tick the checkbox to enable Remote Management.
4. Keep the Port as the default setting. Enter the IP address or MAC address of the remote device to manage the router.

   Note: If you want that all remote devices can manage the router, just leave the IP/MAC Address field blank.

5. Click Save to make the settings effective. Now, only the device using the IP address or MAC address you set can log in to http://router's Internet IP address:port number (such as http://113.116.60.229:80) to manage the router remotely.

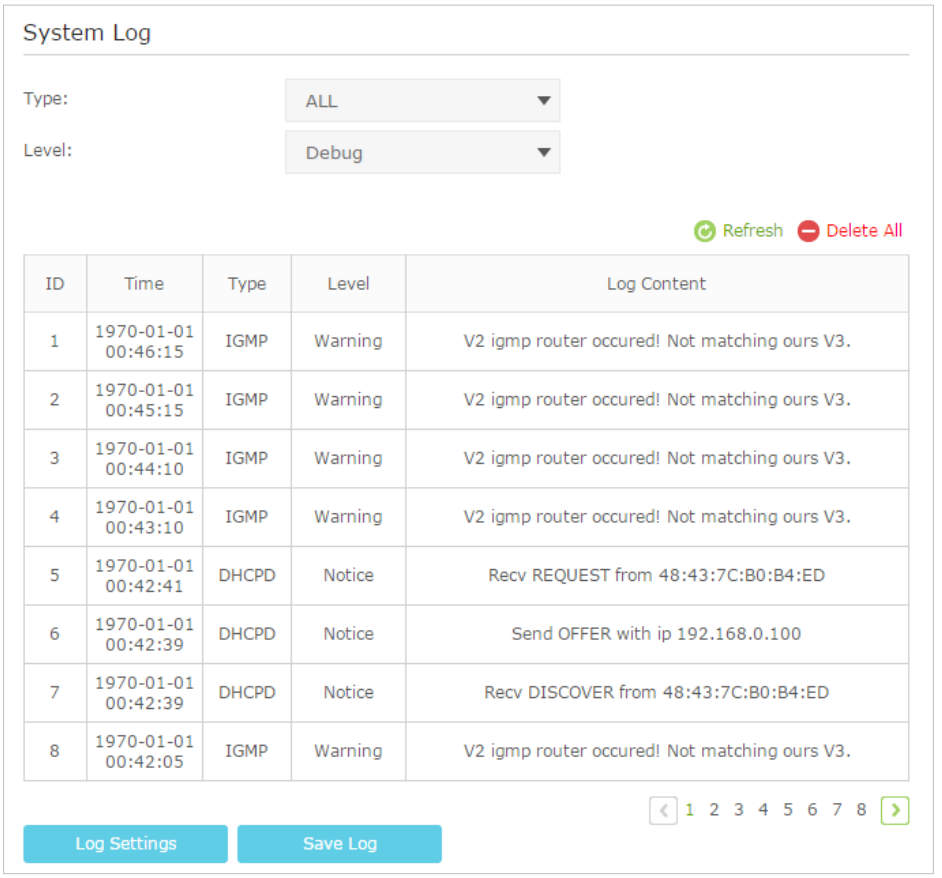
Tips:

1. You can find the Internet IP address of the router on Basic > Network Map > Internet.
2. The router's Internet 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. 8. System Log

System Log can help you know what happened to your router, facilitating you to locate the malfunctions. For example when your router does not work properly, you will need to save the system log and send it to the technical support for troubleshooting.

1. Visit *http://tplinkwifi.net*, and log in with the username and password you set for the router.
2. Click *Advanced* > *System Tools* > *System Log* page.



To view the system logs:

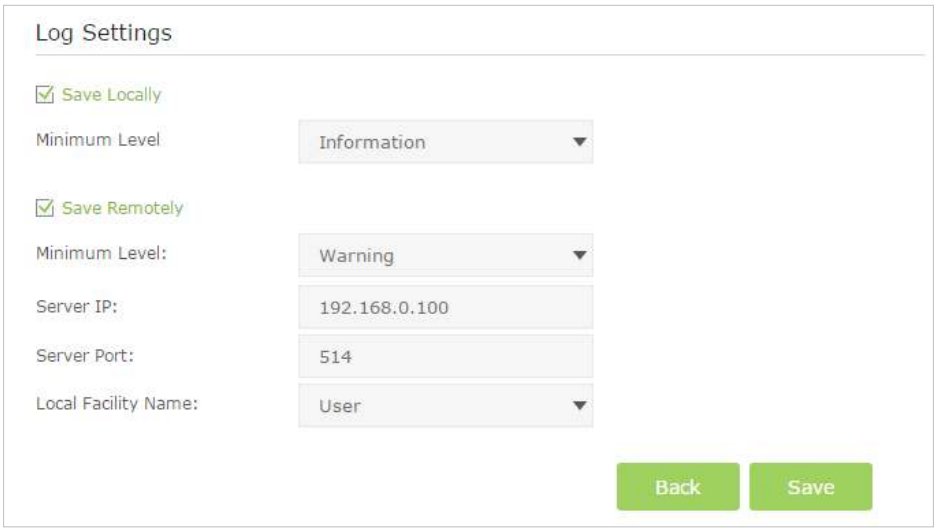
1. Select the log Type. Select ALL to view all kinds of logs, or select a specific type to view the specific logs.
2. Select the log Level and you will see the logs with the specific or higher levels.
3. Click Refresh to refresh the log list.

To save the system logs:

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

Click Save Log to save the logs in a txt file to your computer.

Click Log Settings to set the save path of the logs.



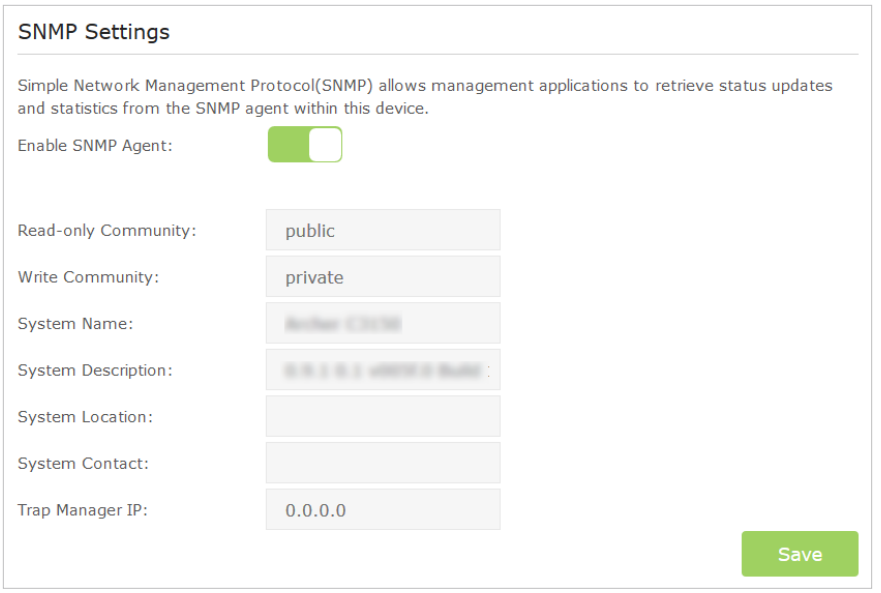
- Save Locally: Select this option to cache the system log to the router's local memory, select the minimum level of system log to be saved from the drop-down list. The logs will be shown in the table in descending order on the System Log page.
- Save Remotely: Select this option to send the system log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

13. 9. SNMP Settings

SNMP (Simple Network Management Protocol) has been widely applied in the computer networks currently, which is used for ensuring the transmission of the management information between two nodes. In this way, network administrators can easily search and modify the information on any node on the network. Meanwhile, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating.

An SNMP Agent is an application running on the router that performs the operational role of receiving and processing SNMP messages, sending responses to the SNMP manager, and sending traps when an event occurs. So a router contains SNMP "agent" software can be monitored and/or controlled by SNMP Manager using SNMP messages.

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



- Enable SNMP Agent: Toggle On to enable the built-in SNMP agent that allows the router to operate as the operational role in receiving and processing of SNMP messages, sending responses to the SNMP manager, and triggering SNMP traps when an event occurs.
- Read-only Community: Displays the default public community string that protects the router from unauthorized access.
- Write Community: Displays the default read and write community string that protects the router from unauthorized changes.
- System Name: Displays the administratively-assigned name for this managed device.
- System Description: Displays the textual description of the managed device. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software.
- System Location: Displays the physical location of this device (e.g., telephone closet, 3rd floor).
- System Contact: Displays the textual identification of the contact person for this managed device, together with information on how to contact this person.
- Trap Manager IP: Displays the IP address of the host to receive the traps.

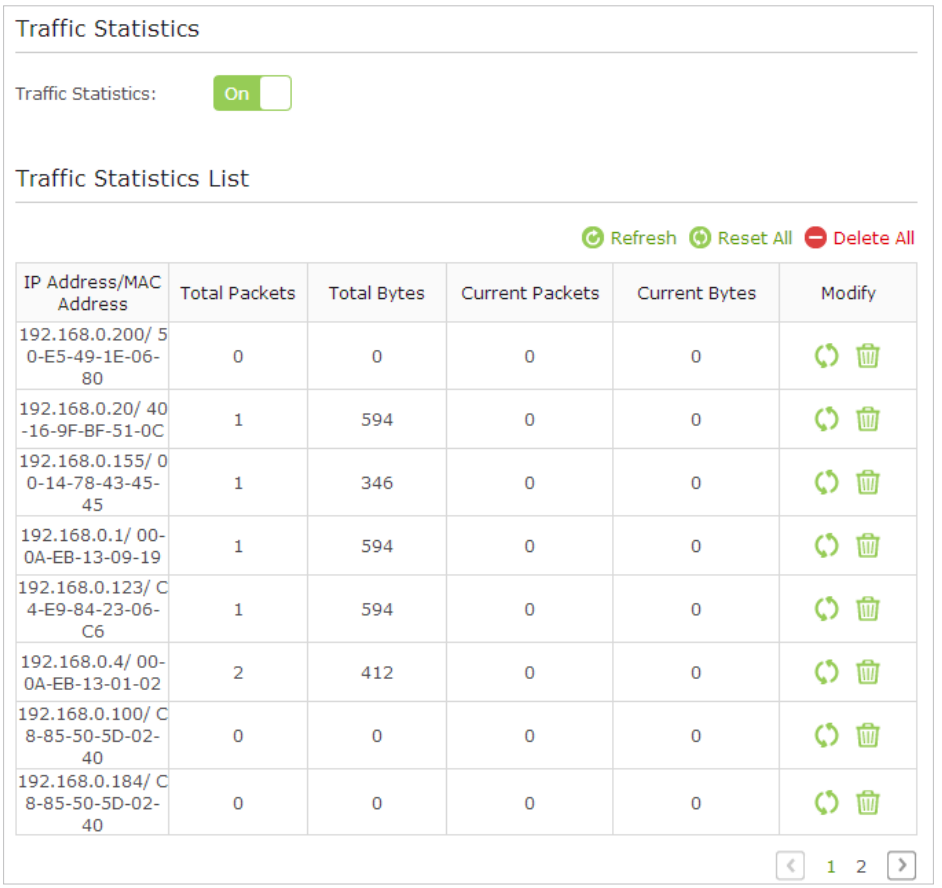
You are suggested to keep the default settings. Click Save to make the settings effective.

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. Enable traffic statistics, and then you can monitor the traffic statistics in Traffic Statistics List section.



Click Refresh to update the statistic information on the page.

Click Reset All to reset all statistic values in the list to zero.

Click Delete All to delete all statistic information in the list.

Click to reset the statistic information of the specific device.

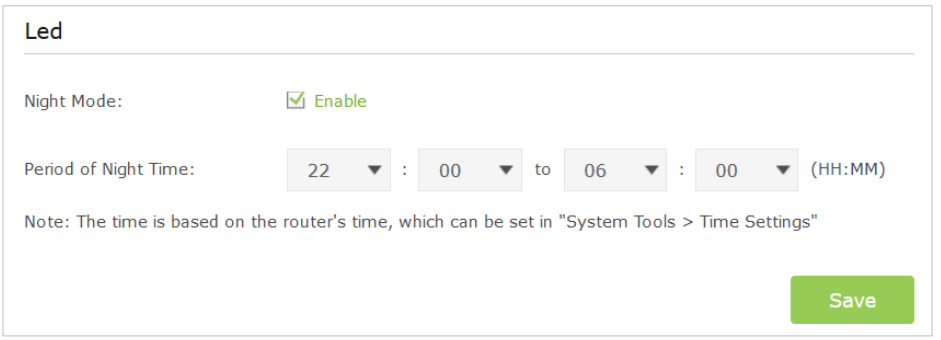
Click to delete the specific device item in the list.

13. 11. Control LEDs

The router LEDs indicate router activities and behavior. You can turn on or turn off the router from the management web-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 > System Parameters.
3. In the Led section, enable Night Mode.

4. Specify the Period of Night Mode according to your need, and the LEDs will be off during this period.
5. Click Save to make the settings effective.



FAQ

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

If it is your first time to connect the wireless network, use the password labeled at the bottom of the router. If the password has been altered, please connect the router to the computer using a cable and follow the steps below:

1. Visit *http://tplinkwifi.net*.
2. Go to Advanced > Wireless > Wireless Settings, locate the password , and mark down your new password for future use.

Q2. How to retrieve the default username and password of the web management page (without resetting the router) ?

The default username and password of the web management page are admin (in lower case).

If you have altered the username and password:

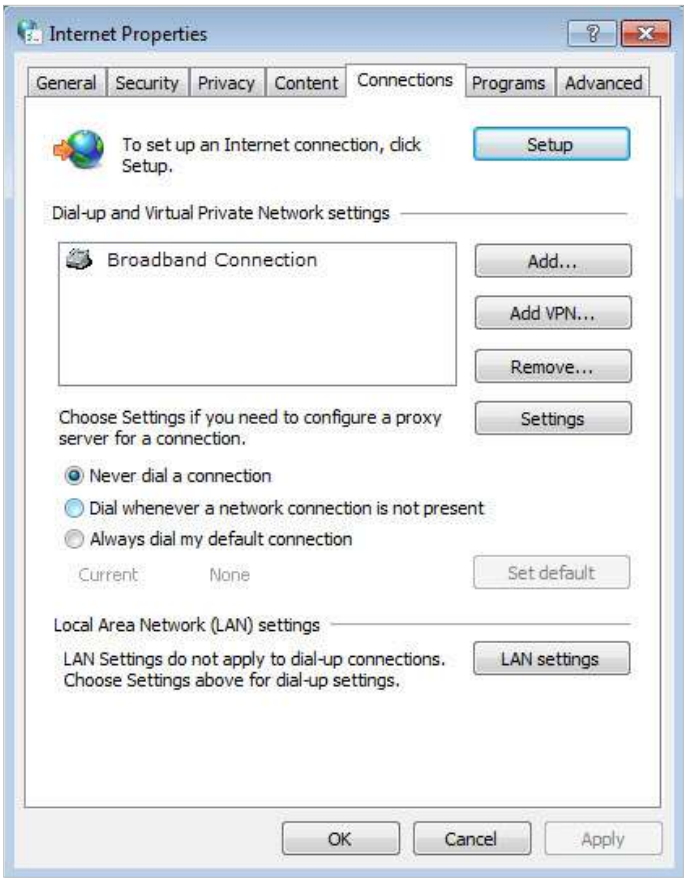
1. Reset the router to factory default settings.
2. Visit *http://tplinkwifi.net*, enter admin (in lower case) as both username and password to login.

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.

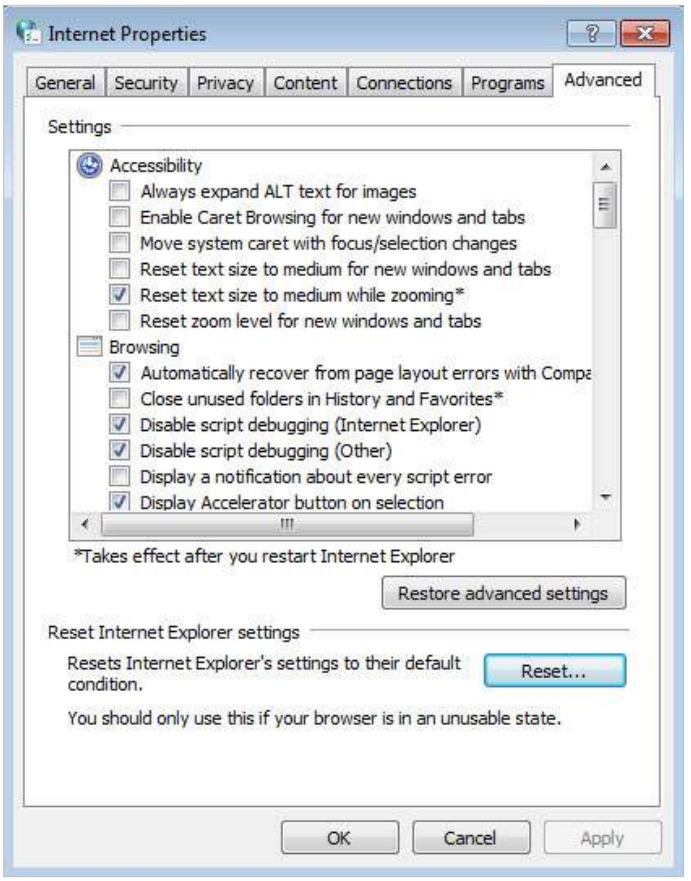
- Make sure the router connect to the computer correctly and the corresponding LED indicator(s) light up.
- Make sure the IP address of your computer is configured as Obtain an IP address automatically and Obtain DNS server address automatically.
- Make sure you enter the correct IP address to login: *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.



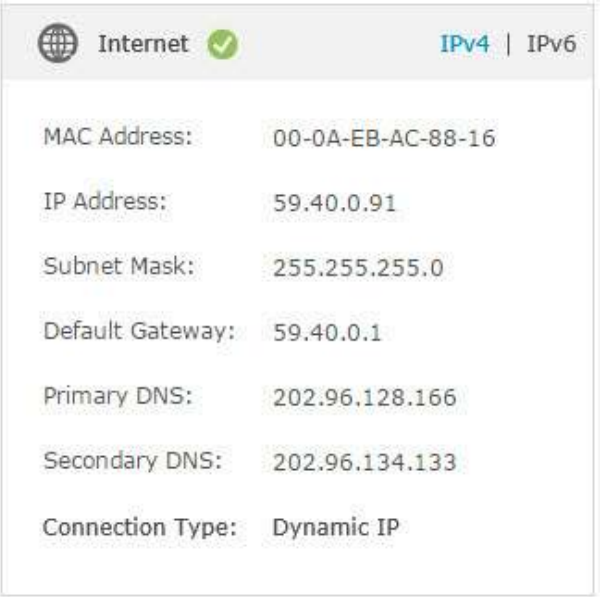
- Use another web browser or computer to login again.
- Reset the router to factory default settings and try again. If login still fails, please contact the technical support.

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

Q4. 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:

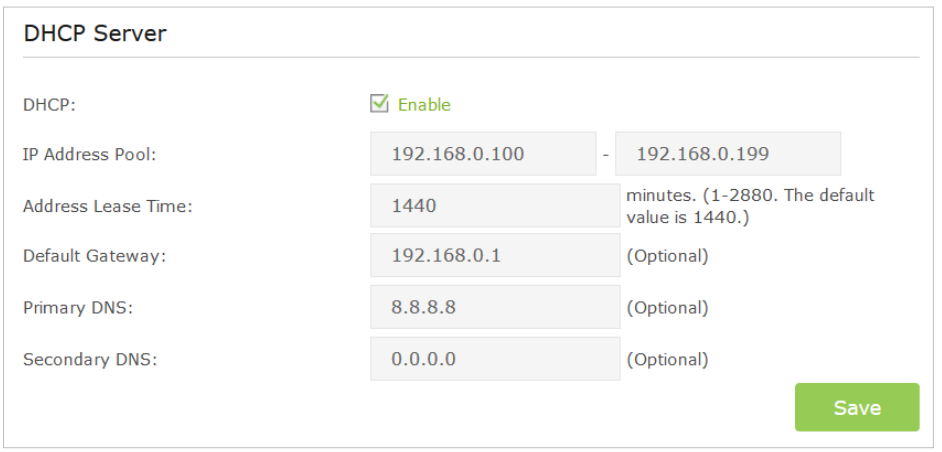


- Your computer might not recognize any DNS server addresses, please manually configure DNS server.

  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.



- 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 with the help of *Upgrade the Firmware*.

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

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

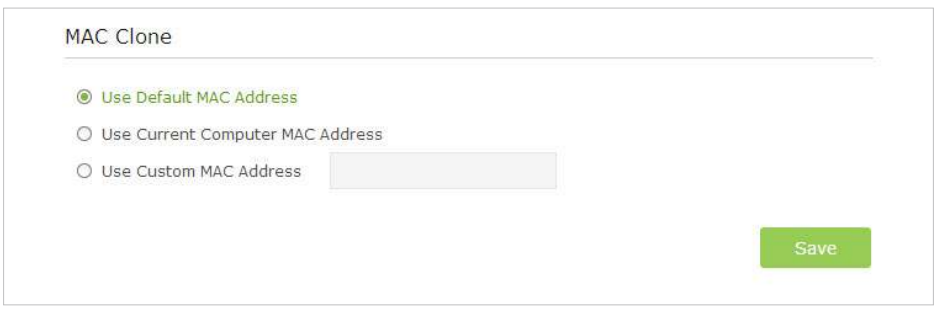


- Make sure the physical connection between the router and the modem is proper
- Clone the MAC address of your computer.

  1) Visit *http://tplinkwifi.net*, and log in with 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.



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:

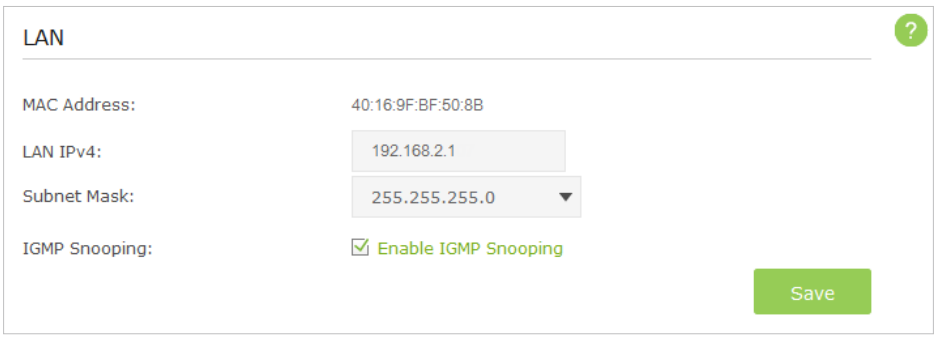
  Most TP-LINK routers use 192.168.0.1/192.168.1.1 as their default LAN IP address, it may conflict with the IP range of your existent ADSL modem/router. If so, the router is not able to communicate with your modem and cause you can't access the Internet. To resolve this problem, we need to change the 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've 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.



- 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.

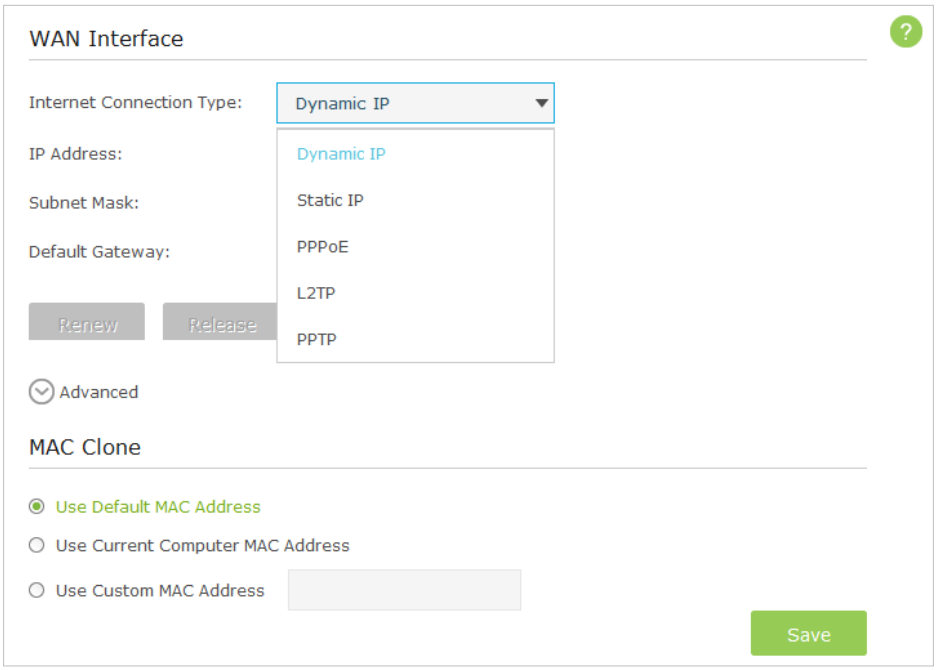
  1) Confirm your Internet Connection Type, which can be learned from the ISP.

  2) Visit *http://tplinkwifi.net*, and log in with the username and password you've 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.



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

- Please refer to *Upgrade the Firmware* to upgrade the firmware of the router.

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

Q5. 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.

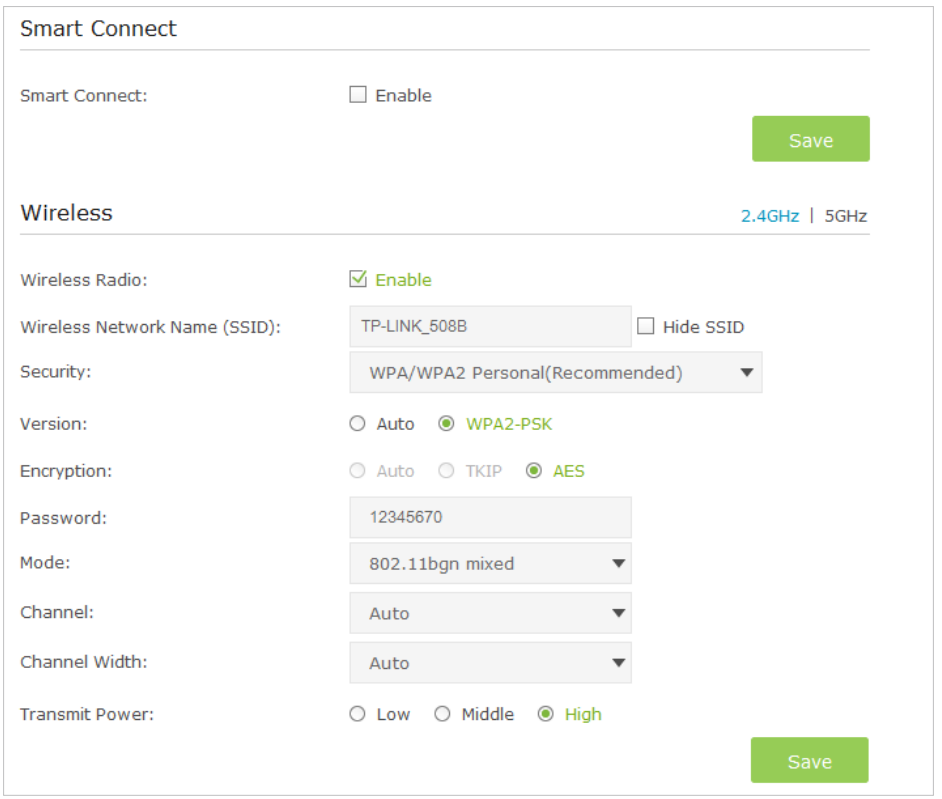
4) Expand Services and Applications > Services, find and locate Wireless Zero Configuration in the Services list on the right side.

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 router settings, double check your Wireless Network Name, make sure SSID is not hided.



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 back of your wireless 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.

Q6. What can I do if I cannot access the USB disk after I modify the Authentication settings?

This situation probably happens on your Windows computer due to its special credential mechanism. Once you successfully access the USB disk, the connection will be temporarily recorded and you will be refused to access the USB disk with another account.

You can follow either method below to solve this problem:

- **Method 1**: Log off (sign out) from the Windows to delete the temporary connection record.
- **Method 2: (Only for Local Storage Sharing)** Change the Address of the USB Disk by referring to *To Customize the Address of the USB Disk*.

Q7. What can I do if I am still required to enter the password for USB access even though I have selected Remember my credentials in my Windows computer?

Because of Windows special credential mechanism, if the USB access username you set is the same as the Windows account name, Windows will be unable to remember the password you set for the USB.

To solve this problem, you can set a different USB access username or make the USB access password the same as your Windows account. After you modify the access account, remember to log off (sigh out) from the Windows.

Q8. Why am I never required to enter the account information for USB access even though I have enabled the Authentication feature?

This situation probably happens to your Windows computer due to its special credential mechanism. If your USB access username and password are both the same as your Windows account, the Windows will automatically use its account information to access the USB disk. Therefore, you will have no need to enter the username and password.

Specifications

HARDWARE FEATURES	
Interfaces	4 10/100/1000Mbps LAN Ports, 1 10/100/1000Mbps WAN Port 1 USB 3.0 Port + 1 USB 2.0 Port
Button	WPS Button, Reset Button, Wireless On/Off Button, LED On/Off Button, Power On/Off Button
Antenna	4 Detachable Antennas
External Power Supply	12V/5A
Dimensions (W x D x H)	10.4×7.8×1.5 in. (263.8×197.8×37.3mm)
WIRELESS FEATURES	
Wireless Standards	IEEE 802.11ac/n/a 5GHz IEEE 802.11b/g/n 2.4GHz
Frequency	2.4GHz and 5GHz
Signal Rate	2167Mbps at 5GHz, 1000Mbps at 2.4GHz
Reception Sensitivity	5GHz: 11a 6Mbps: -91dBm 11a 54Mbps: -72dBm 11n HT20: -70dBm 11n HT40: -69dBm 11ac HT20: -60dBm 11ac HT40: -61dBm 11ac HT80: -56dBm 2.4GHz: 11g 54Mbps: -73dBm 11n HT20: -72dBm 11n HT40: -69dBm
Wireless Functions	Enable/Disable Wireless Radio, WMM, Wireless Statistics
Wireless Security	64/128-bit WEP, WPA/WPA2, WPA-PSK/WPA-PSK2 encryptions
Transmission Power	CE: <20dBm(2.4GHz), <23dBm(5GHz) FCC: <30dBm
Guest Network	2.4GHz guest network x 1, 5GHz guest network x 1
SOFTWARE FEATURES	
Quality of Service	WMM, Bandwidth Control
WAN Type	Dynamic IP/Static IP/PPPoE/ PPTP(Dual Access)/L2TP(Dual Access) /Bigpond
Management	Access Control, Local Management, Remote Management
DHCP	Server, Client, DHCP Client List, Address Reservation

Port Forwarding	Virtual Server, Port Triggering, UPnP, DMZ
Dynamic DNS	DynDns, Comexe, NO-IP
VPN Pass-Through	PPTP, Open VPN
Access Control	Parental Controls, Local Management Control, Host list, Access Schedule, Rule Management
Protocols	Supports IPv4 and IPv6
USB Sharing	Support Samba(Storage)/FTP Server/Media Server/ Printer Server
OTHERS	
Certification	**CE, FCC, RoHS**
Environment	Operating Temperature: 0°C~40°C (32°F ~104°F) Storage Temperature: -40°C~70°C (-40°F ~158°F) Operating Humidity: 10%~90% non-condensing Storage Humidity: 5%~90% non-condensing

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 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

This device is restricted in indoor environment only.

CE Mark Warning

CE 1588 !

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 (1999/5/EC Article 3.1a) on the limitation of exposure of the general public to electromagnetic fields by way of health protection.

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

National Restrictions

Restricted for 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.

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

1) l'appareil ne doit pas produire de brouillage;

2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, meme si le brouillage est susceptible d'en compromettre le fonctionnement.

This radio transmitter (IC: 8853A-C3150/ Model: Archer C3150) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain indicated. Antenna types not included in this list (Specifications), having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le présent émetteur radio (IC: 8853A-C3150/ Model: Archer C3150) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste (Specifications), et dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Caution:

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

2) For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and

The high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

Avertissement:

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

2) Le gain maximal d'antenne permis pour les dispositifs avec antenne(s) amovible(s) utilisant la bande 5725-5850 MHz doit se conformer à la limitation P.I.R.E spécifiée pour l'exploitation point à point et non point à point, selon le cas.

En outre, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Les produits utilisant la technique d'atténuation DFS (sélection dynamique des fréquences) sur les bandes 5250- 5350 MHz, 5470-5600MHz et 5650-5725MHz.

Radiation Exposure Statement:

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

Déclaration d'exposition aux radiations:

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

Industry Canada Statement

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

Korea Warning Statements

당해 무선설비는 운용중 전파혼신 가능성이 있음.

NCC Notice:

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。

BSMI Notice:

- 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

Explanation 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.