

Archer C3200

User Guide

AC3200 Wireless Tri-Band Gigabit Router

Contents

About This Guide	1
Chapter 1. Get to Know About Your Router	2
1. 1. Product Overview.....	2
1. 2. Main Features.....	3
1. 3. Panel Layout	3
1. 3. 1. Front Panel.....	3
1. 3. 2. Rear Panel	5
Chapter 2. Connect the Hardware	6
2. 1. System Requirements	6
2. 2. Installation Environment Requirements.....	6
2. 3. Connect Your Router	6
Chapter 3. Log into Your Router	8
Chapter 4. Set Up Internet Connection	9
4. 1. Quick Setup.....	9
4. 2. Manually Configure Your Internet Connection Settings	12
4. 3. Setting Up an IPv6 Internet Connection.....	15
Chapter 5. Guest Network	19
5. 1. Create Guest Network	19
5. 2. Customize Guest Network Options	19
Chapter 6. NAT Forwarding	21
6. 1. Share Local Resources in the Internet by Virtual Server	21
6. 2. Open Ports Dynamically by Port Triggering	22
6. 3. Make Applications Free from Port Restriction by DMZ	23
6. 4. Make Xbox Online Games Run Smoothly by UPnP.....	24
Chapter 7. USB Application	25
7. 1. Local Storage Sharing	25
7. 1. 1. Access the USB disk	25
7. 1. 2. Customize Your Settings.....	25
7. 2. Remote Access via FTP Server	27
7. 2. 1. Access the USB disk	27
7. 2. 2. Customize Your Settings.....	29
7. 3. Media Sharing	29
7. 3. 1. Access the USB disk	29
7. 3. 2. Customize Your Settings.....	30
7. 4. Printer Sharing.....	31
Chapter 8. Parental Controls	35
Chapter 9. Bandwidth Control	37
Chapter 10. Network Security	39

10.1. Protect the Network from Cyber Attacks	39
10.2. Access Control	40
10.3. IP & MAC Binding	41

Chapter 11. Customize Your Network Settings 43

11.1. Change the LAN Settings	43
11.2. Configure to Support IPTV Service	43
11.3. Specify DHCP Server Settings	44
11.4. Set Up a Dynamic DNS Service Account	46
11.5. Create Static Routes	47
11.6. Specify Wireless Settings	48
11.7. Use WPS for Wireless Connection	51
11.7.1. Set the Router's PIN	51
11.7.2. Use the WPS Wizard for Wi-Fi Connections	51
11.8. Schedule Your Wireless Function	52
11.9. Set up a VPN Connection	53

Chapter 12. Manage the Router 56

12.1. Set Up System Time	56
12.2. Test the Network Connectivity	57
12.3. Upgrade the Firmware	58
12.4. Backup and Restore Configuration Settings	58
12.5. Change the Administrator Account	59
12.6. Local Management	60
12.7. Remote Management	60
12.8. System Log	61
12.9. SNMP Settings	63
12.10. Monitor the Internet Traffic Statistics	64
12.11. Control LEDs	64

Appendix A: Specifications 66




Appendix B: FAQ 68

About This Guide

This guide provides details of each function and shows how to configure the router appropriate to your needs. In addition to this guide, a Quick Installation Guide is also released with each TP-LINK router, you are suggested to configure your router for quick Internet setup by following the published Quick Installation Guide before you get started with a further configuration.

Conventions

In this guide the following conventions are used:

Convention	Description
router	Stands for AC3200 Wireless Tri-Band Gigabit Router without any explanation.
parameters	Parameters provided in the screenshots are just references for setting up the device, which may differ from the actual situation. You can set the parameters according to your demand.
screenshots	The demonstrated screenshots may look a little different from the actual web page of your device due to the various firmware versions. Please just configure your product based on the actual web page.
<i>Blue Italic</i>	Hyperlinks are in blue italic. You can click to redirect to a website or a specific section.
Blue	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	<ul style="list-style-type: none">•  click to edit the corresponding entry.•  click to delete the corresponding entry.•  click to enable or disable the corresponding entry.

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 AC3200 Wireless Tri-Band Gigabit Router integrates 4-port Switch, Firewall, NAT-router and Wireless AP. Powered by 3x3 MIMO technology, this router delivers exceptional range and speed, which can fully meet the need of Small Office/Home Office (SOHO) 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.

More Wi-Fi for More Devices

The Archer C3200 uses Tri-Band technology to run three separate Wi-Fi channels at once, creating a network that can connect to more devices without a trade-off in performance.

Smart Connect helps devices run even faster by assigning them to the best available channel to balance network demand.

Seamless Streaming and Gaming

With the fastest combined Wi-Fi speed of up to 3200Mbps, the Archer C3200 lets you simultaneously game online and stream video in 4K Ultra HD across multiple devices without lag.

Maximum Coverage and Stability

Six high-performance external antennas greatly increase the Archer C3200's range and signal stability. Beamforming technology further improves the router's coverage by helping it locate wireless devices to form stronger, more reliable connections.

Run All Your Devices At Once

A powerful 1GHz dual-core CPU and three co-processors easily handle the demand made on the Archer C3200's network when multiple users are browsing, streaming, and gaming all at the same time.

Lightning-Fast Wired Performance

External hard drives can connect directly to the Archer C3200 via its USB 3.0 and 2.0 ports, making it easy to share files, photos, music, and video across your network.

The Archer C3200 is also equipped with four Gigabit Ethernet ports that enable blazing wired speeds 10x greater than Fast Ethernet, helping connected gaming consoles, PCs, and smart TVs achieve their best performance.

Easy Setup and Use

Set up the Archer C3200 in minutes thanks to its intuitive web interface and the powerful Tether app. Tether also lets you manage its network settings from any Android or iOS device, including parental controls and media sharing.

1.2. Main Features

- 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 3200Mbps 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.


1.3. Panel Layout








1.3.1. Front Panel



The router's LEDs are located on the front 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
 Power	Flash	System initializing or firmware upgrading is in process. Do not disconnect or power off the router.
	On	System initialization complete.
	Off	Power is off. Please ensure that the power adapter is connected correctly.

Name	Status	Indication
 (2.4GHz)	On	2.4GHz wireless is working properly.
	Off	2.4GHz wireless is disabled.
 (5GHz-1)	On	5GHz-1 wireless is working properly.
	Off	5GHz-1 wireless is disabled.
 (5GHz-2)	On	5GHz-2 wireless is working properly.
	Off	5GHz-2 wireless is disabled.
 (Ethernet)	On	There is device(s) connected to the Ethernet (1/2/3/4) port(s).
	Off	No any device is connected to the Ethernet (1/2/3/4) port.
 (Internet)	Blue	The Internet port is connected, and the Internet is accessible.
	Orange	The Internet port is connected, but the Internet is inaccessible.
	Off	The Internet port isn't connected, and the Internet is inaccessible.
 (WPS)	Flash	WPS button on the router is pressed, and the router is trying to connect a wireless device to its network via WPS.
	On	The connection via WPS is successful.
	Off	The connection via WPS fails.
 (USB 1/USB 2)	Flash	The router is identifying the device connected to the USB 2.0 port/USB 3.0 port.
	On	The device is identified successfully.
	Off	No device is connected to the USB 2.0 port/USB 3.0 port.

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.

The following buttons are also located on the front panel (View from left to right). Refer to the following for detailed instructions.

Button	Description
 (Wi-Fi)	Pressing this button for 2 seconds enables or disables the Wi-Fi function.
 (WPS)	Pressing this button for less than 5 seconds enables the WPS function. If your client devices, such as wireless adapters, 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.
 (LED On/Off)	Pressing this button for 1 second turns all LEDs on or off.

1.3.2. Rear Panel



The following parts are located on the rear panel (View from left to right). Refer to the following for detailed instructions.

Item	Description
Reset button	Pressing this button for about 7 seconds enables the Reset function.
USB 2.0 port	The USB 2.0 port connects to a USB 2.0 storage device or a USB 2.0 printer.
Internet port	This port is where you will connect the DSL/cable Modem, or Ethernet.
Ethernet (1, 2, 3, 4) ports	These ports (1, 2, 3, 4) connect the router to the local PCs.
USB 3.0 port	The USB 3.0 port connects to a USB 3.0 storage device or a USB 3.0 printer.
Power On/Off button	This button powers on or off the router.
Power port	This port is where you will connect the power socket via the provided power adapter.

Connect the Hardware

This chapter contains the following sections:

- [System Requirements](#)
- [Installation Environment Requirements](#)
- [Connect Your Router](#)

2.1. System Requirements

- Broadband Internet Access Service (DSL/Cable/Ethernet)
- One DSL/Cable Modem that has an RJ45 connector (which is not necessary if the router is connected directly to the Ethernet)
- PCs with a working Ethernet adapter and an Ethernet cable with RJ45 connectors
- TCP/IP protocol on each PC
- Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari

2.2. Installation Environment Requirements

- Place the router in a well-ventilated place far from any heater or heating vent
- Avoid direct irradiation of any strong light (such as sunlight)
- Keep at least 2 inches (5 cm) of clear space around the router
- Operating Temperature: 0°C~40°C (32°F~104°F)
- Operating Humidity: 10%~90%RH, Non-condensing

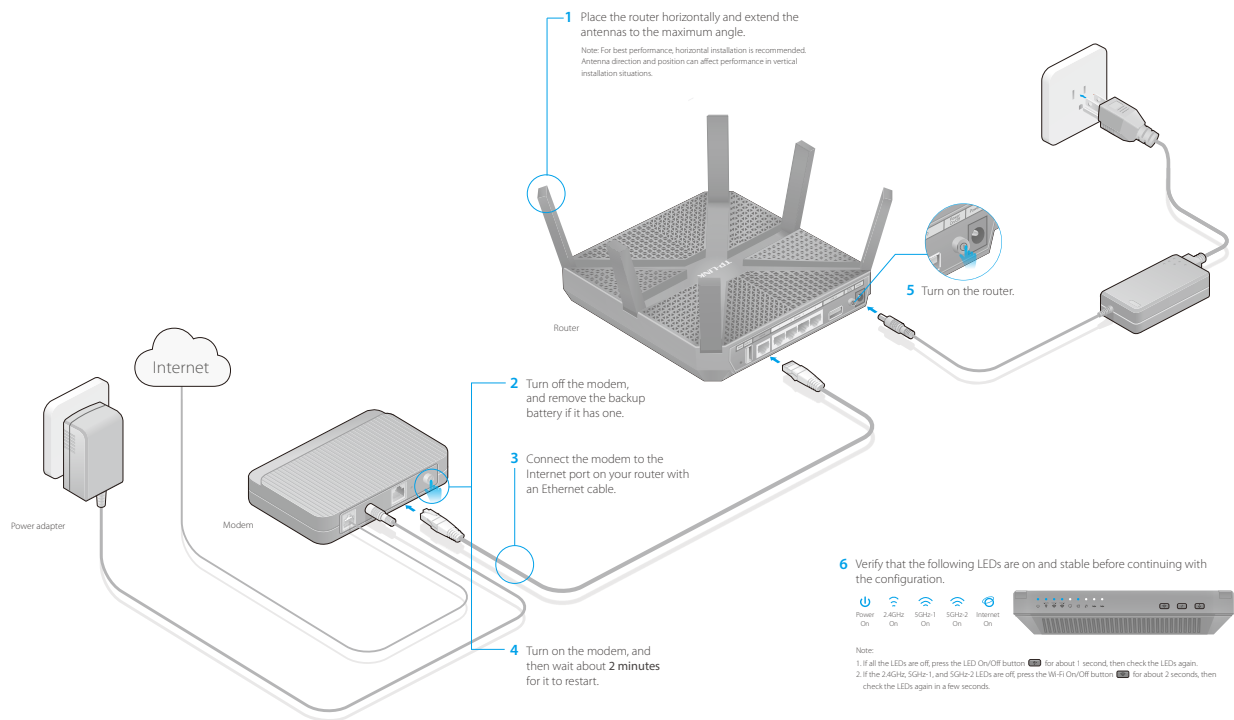
2.3. Connect Your Router

Follow the steps below to connect your router.

1. Connect your router as shown in the figure below. The electrical outlet shall be installed near the device and shall be easily accessible.

Note:

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.



2. Connect your computer to the router.

• **Method 1: Wired**

Connect your computer's Ethernet port to the router's Ethernet port via an Ethernet cable.

• **Method 2: Wirelessly**

Connect your computer to the router wirelessly by using the default SSID (Wireless Network Name) and Wireless Password printed on the product label of the router.

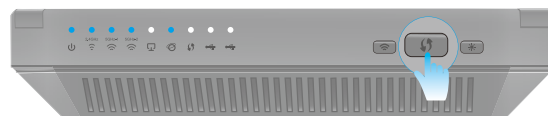
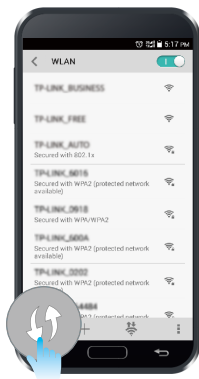
• **Method 3: Use the WPS button**

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. Tap the WPS icon on the device's screen.
2. Immediately press the WPS button on your router.
3. The WPS LED flashes for about two minutes during the WPS process.
4. When the WPS LED is on, the client device has successfully connected to the router.

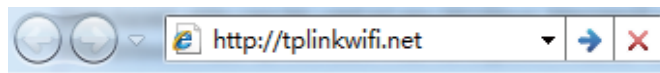


Log into Your Router

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](#).

A screenshot of a login page. On the left, there are two green icons: a person icon and a key icon. To the right of the person icon is a text input field containing the text "admin". Below the person icon is a key icon, and to its right is a password input field containing seven black dots. Below these two input fields is a green button with the text "Login".

Note:

If the login window does not appear, please refer to [Q3. I cannot login to the router's web management page, what can I do?](#)

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

A screenshot of a page titled "Set up a new username and password". The page has a close button (X) in the top right corner. Below the title, there are three input fields. The first is labeled "New Username:" and contains the text "example". The second is labeled "New Password:" and contains seven black dots. Below the "New Password:" field are three radio buttons labeled "Low", "Middle", and "High", with "High" selected. The third input field is labeled "Confirm New Password:" and contains seven black dots. Below these fields is a green button with the text "Confirm".

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

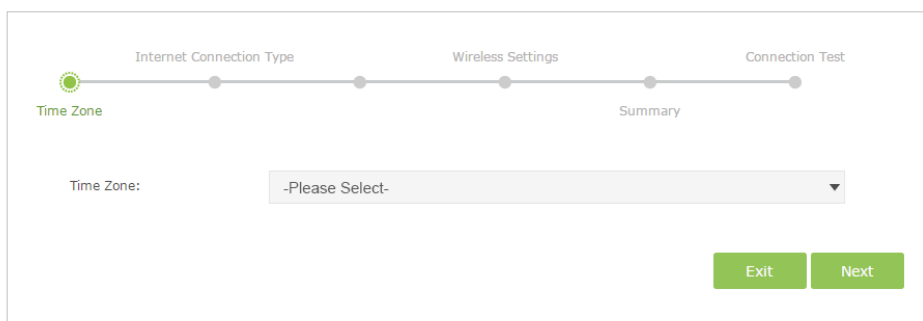
The Quick Setup Wizard will guide you through the process to set up your router to access the Internet.

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.

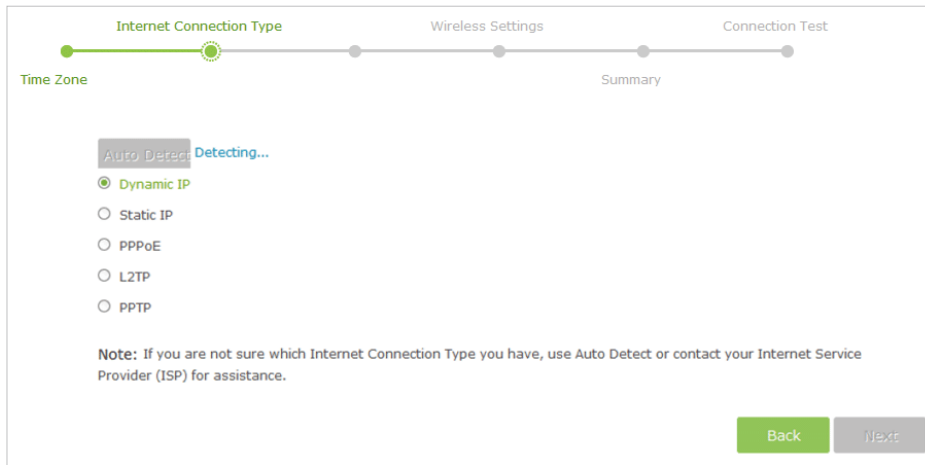
1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [Quick Setup](#) on the top of the page.
3. Select your time zone, and click [Next](#).



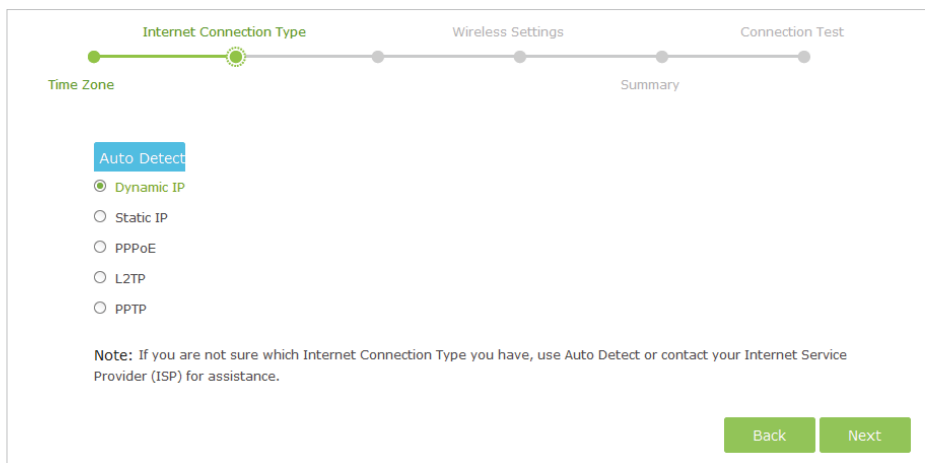
4. Click [Auto Detect](#) and the router will detect your connection type automatically.

Note:

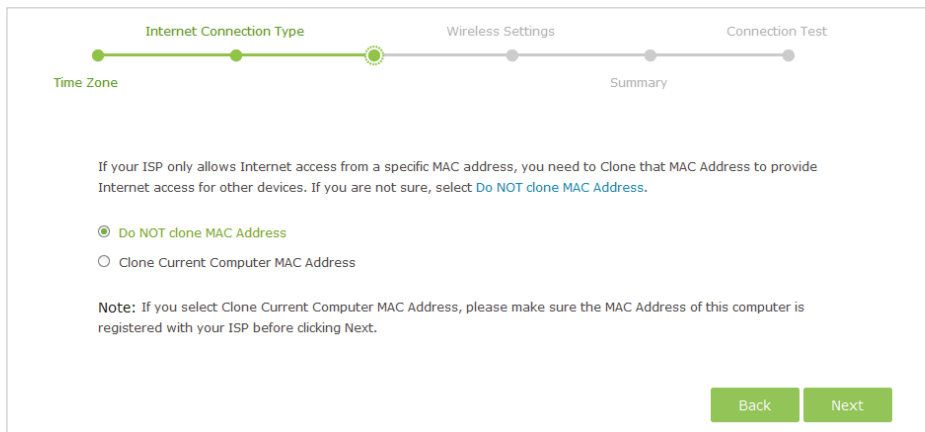
You can also choose the connection type manually. If you use DSL line and you are only provided an account name and a password by your ISP, choose PPPoE. If you use cable TV or fiber cable, choose Dynamic IP. If you are provided more information such as IP address, Subnet Mask and Default Gateway, choose Static IP. Contact your ISP if you are not sure about the Internet connection information.



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](#).

Internet Connection Type Wireless Settings Connection Test

Time Zone Summary

Please set the SSIDs and passwords for 2.4GHz and 5GHz wireless networks.

Wireless Network (2.4GHz): Enable

Wireless Network Name (SSID): TP-LINK_0969

Password: 12345670

Wireless Network (5GHz-1): Enable

Wireless Network Name (SSID): TP-LINK_0969_5G_1

Password: 12345670

Wireless Network (5GHz-2): Enable

Wireless Network Name (SSID): TP-LINK_0969_5G_2

Password: 12345670

Back Next

Note:

1. You may customize your 2.4GHz/5GHz-1/5GHz-2 SSID and password. Once done, the wireless connection will disconnect automatically, and you must then use the new SSID/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](#).

Internet Connection Type Wireless Settings Connection Test

Time Zone Summary

Time Zone: (GMT-08:00) Pacific Time (US & Canada); Tijuana

Internet Connection Type: Dynamic IP

Wireless Network (2.4GHz): Enabled

Wireless Network Name (SSID): TP-LINK_0969

Password: 12345670

Wireless Network (5GHz-1): Enabled

Wireless Network Name (SSID): TP-LINK_0969_5G_1

Password: 12345670

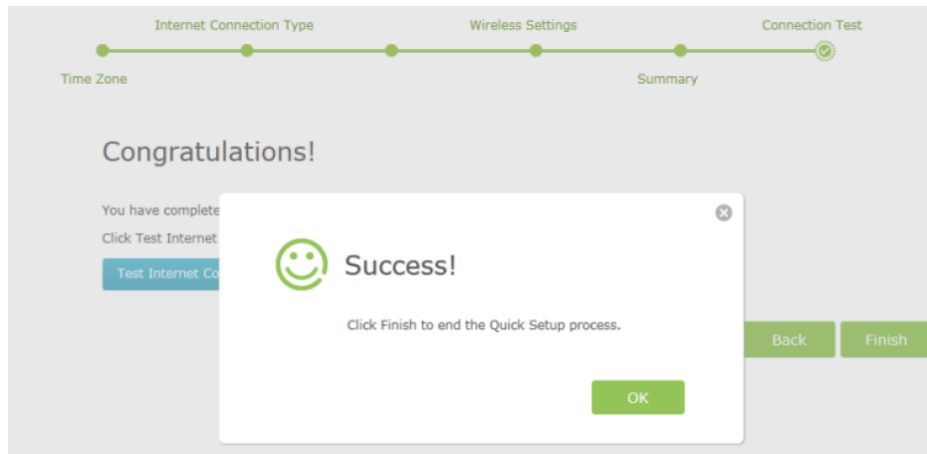
Wireless Network (5GHz-2): Enabled

Wireless Network Name (SSID): TP-LINK_0969_5G_2

Password: 12345670

Back 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 device can connect to the Internet!

tips:

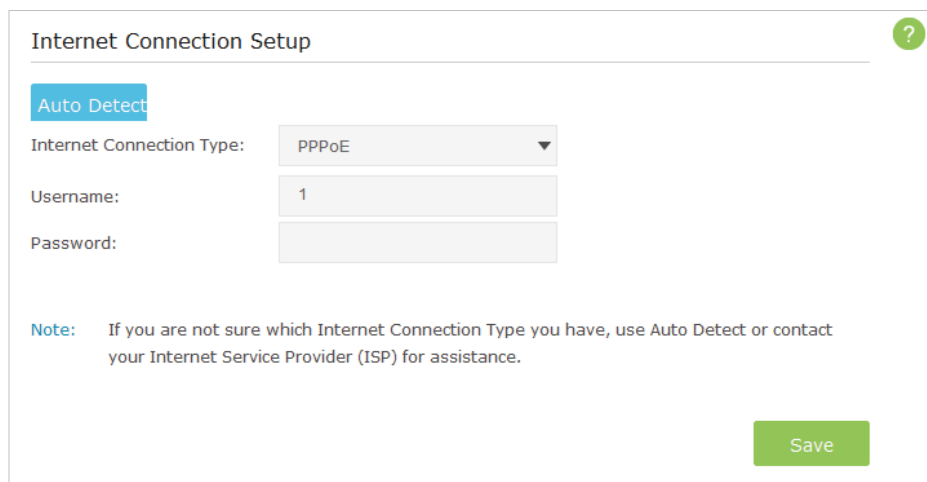
You can connect your computer to the router's LAN port using an Ethernet cable to join the local area network. You can also find and select the wireless network name on your Wi-Fi device to join the Wi-Fi network.

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](#) on the left to enter the setting page.
3. Select your Internet connection type from the drop-down list.



Note:

If you are unsure 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 3 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. Dynamic IP users are usually equipped with cable TV or fiber cable.

Internet Connection Setup ?

[Auto Detect](#)

Internet Connection Type:

Do NOT clone MAC Address

Clone Current Computer MAC Address

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

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

Internet Connection Setup ?

[Auto Detect](#)

Internet Connection Type:

IP Address:

Subnet Mask:

Default Gateway: (optional)

Primary DNS: (optional)

Secondary DNS: (optional)

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

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

Internet Connection Setup ?

Auto Detect

Internet Connection Type:

Username:

Password:

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

- 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.

Internet Connection Setup ?

Auto Detect

Internet Connection Type:

Username:

Password:

Secondary Connection: **Dynamic IP** Static IP

VPN Server IP/Domain Name

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

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

Internet Connection Setup ?

Auto Detect

Internet Connection Type: PPTP

Username: pptp

Password: ••••••

Secondary Connection: Dynamic IP Static IP

VPN Server IP/Domain Name: 192.168.202.254

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

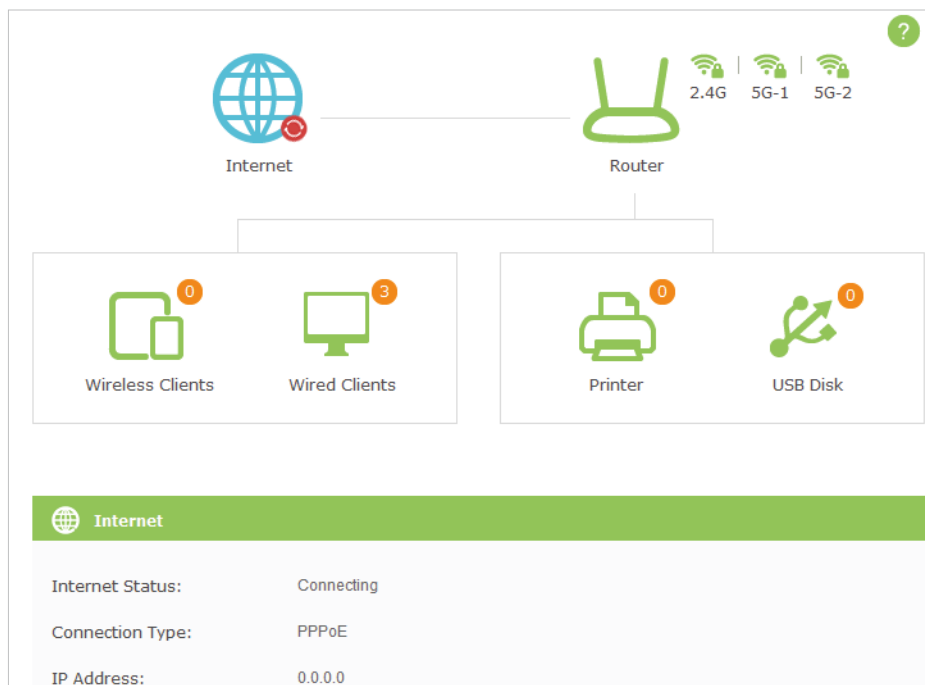
Save

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 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 [Appendix B: FAQ](#) for further instructions.

4.3. Setting Up an IPv6 Internet Connection

In this part, you can set up an IPv6 Internet connection if your ISP supports it and has provided related parameters.

1. Visit <http://tplinkwifi.net>, then log in with the username and password you set for the router.
2. Go to [Advanced](#) > [IPv6](#) to log into the configuration page.

IPv6 Internet

Enable IPv6

Internet Connection Type: Dynamic IP ▼

IPv6 Address: ::

IPv6 Gateway: ::

Addressing Type: DHCPv6 ▼

Advanced

Save

IPv6 LAN

Address Type: RADVD DHCPv6 Server

Enable RDNSS

Enable ULA Prefix

Site Prefix Type: Delegated Static

Save

3. Enable IPv6, and select the Internet connection type provided by your ISP.

Tips:

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

IPv6 Internet

Enable IPv6

Internet Connection Type: Dynamic IP ▼

Dynamic IP

Static IP

PPPoE

6to4 Tunnel

IPv6 Address:

IPv6 Gateway:

Addressing Type:

Advanced

Save

4. Fill in information provided by your ISP.
 - 1) **Static IP:** Fill in blanks. Click [Advanced](#) to have more configuration if your ISP requires. Click [Save](#).

IPv6 Internet

Enable IPv6

Internet Connection Type: Static IP ▼

IPv6 Address: ::

IPv6 Gateway: :: (Optional)

IPv6 DNS Server: :: (Optional)

Secondary IPv6 DNS Server: :: (Optional)

⌵ Advanced

Save

- 2) **Dynamic IP:** Select the [Addressing Type](#). Click [Advanced](#) to have more configuration if your ISP requires. Click [Save](#).

IPv6 Internet

Enable IPv6

Internet Connection Type: Dynamic IP ▼

IPv6 Address: ::

IPv6 Gateway: ::

Addressing Type: DHCPv6 ▼

⌵ Advanced

Save

- 3) **PPPoE:** Fill in the Username and Password, and select the [Addressing Type](#). Click [Advanced](#) to have more configuration if your ISP requires. Click [Save](#).

IPv6 Internet

Enable IPv6

Internet Connection Type: PPPoE ▼

Username:

Password:

Confirm Password:

Addressing Type: DHCPv6 ▼

⌵ Advanced

Save

- 4) **6to4 Tunnel:** An IPv4 Internet connection type is a prerequisite for this connection type. (Go to [Manually Configure Your Internet Connection Settings](#) for more information.) Click **Save**.

IPv6 Internet

Enable IPv6

Internet Connection Type: **6to4 Tunnel** ▼

IPv4 Address: 192.168.0.100

IPv4 Subnet Mask: 255.255.255.0

IPv4 Gateway: 192.168.0.1

Save

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

IPv6 LAN

Address Type: RADVD DHCPv6 Server

Enable RDNSS

Enable ULA Prefix

Site Prefix Type: Delegated Static

Save

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

Internet <input checked="" type="checkbox"/>		IPv4 IPv6
MAC Address:	00-0A-EB-AC-25-01	
IP Address:	2001:c68:202:2111::120/64	
Default Gateway:	fe80::edd0:80d2:7f5e:6be7	
Primary DNS:	2001:c68:202:2111::1	
Secondary DNS:	2001:c68:202:2111::2	
Connection Type:	PPPoE	

Tips:

Visit [Appendix B: FAQ](#) if there is no Internet connection.

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 Guest Network](#)
- [Customize Guest Network Options](#)

5.1. Create Guest Network

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

The screenshot shows the 'Wireless' configuration page for a guest network. At the top right, there are three tabs: '2.4GHz', '5GHz-1', and '5GHz-2'. Below the tabs, there is a section for enabling the guest network. The 'Enable' checkbox is checked. The 'Wireless Network Name (SSID)' is set to 'My_Guests' and the 'Hide SSID' checkbox is unchecked. The 'Security' is set to 'WPA/WPA2 Personal', the 'Version' is 'WPA2-PSK', and the 'Encryption' is 'AES'. The 'Password' is set to 'PassWord_1234'. A green 'Save' button is located at the bottom right of the form.

- 1) Click [2.4GHz](#), [5GHz-1](#), or [5GHz-2](#) and select [Enable](#).
- 2) Set an easy-to-identify SSID. Don't select [Hide SSID](#) unless you want your guests and other people to manually input this SSID for Wi-Fi access.
- 3) Set [Security](#) to [WPA/WPA2 Personal](#), keep the default [Version](#) and [Encryption](#) values, and set an easy-to-remember 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 find 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](#).
3. Customize guest network options according to your needs.

Settings

- Allow guests to see each other
- Allow guests to access my local network

[Save](#)

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

Select this checkbox if you want to allow the clients in your guest network to access each other.

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

Select this checkbox if you want to allow the clients in your guest network to access your local network, not just Internet access.

4. Click [Save](#). Now users in your guest network can enjoy only the network authorities you assigned!

🔗 Tips:

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

NAT Forwarding

6

Router's NAT (Network Address Translation) feature makes the devices in the LAN use the same public IP address to communicate in the Internet, which protect 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 in 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 in the Internet by Virtual Server](#)
- [Open Ports Dynamically by Port Triggering](#)
- [Make Applications Free from Port Restriction by DMZ](#)
- [Make Xbox Online Games Run Smoothly by UPnP](#)

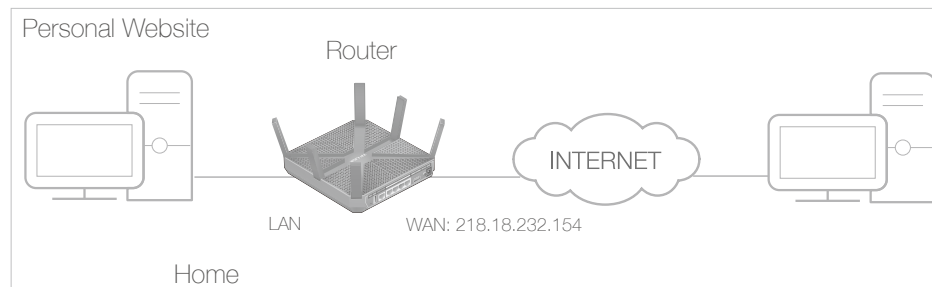
6.1. Share Local Resources in the Internet by Virtual Server

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

Virtual server 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 in my home PC (192.168.0.100). I hope that my friends in 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**, click **Add**.
4. Click **View Existing Application**, 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 in the **Internal IP** field.
5. Click **OK** to save the settings.

Virtual Servers
?

+ Add - Delete

☐	ID	Service Type	External Port	Internal IP	Internal Port	Protocol	Status	Modify
--	--	--	--	--	--	--	--	--

Service Name:

External Port: (XX-XX or XX)

Internal IP:

Internal Port: (XX or Blank, 1-65535)

Protocol: TCP ▼

Enable this Entry

View Existing Application

Cancel
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 need.
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 in the Internet can enter <http://WAN IP> (in this example: [http:// 218.18.232.154](http://218.18.232.154)) to visit your personal website.

🔗 Tips:

1. WAN IP should be a public IP address. For the WAN IP is assigned dynamically by ISP, it is recommended to apply and register a domain name for the WAN refer to [Set Up a Dynamic DNS Service Account](#). Then you 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.

6.2. 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](#) to save the settings.

Port Triggering ?

+ Add - Delete

<input type="checkbox"/>	ID	Application	Triggering Port	Triggering Protocol	External Port	External Protocol	Status	Modify
--	--	--	--	--	--	--	--	--

Application: View Existing Applications

Triggering Port: (XX,1-65535)

Triggering Protocol: ▼

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

External Protocol: ▼

Enable This Entry

Cancel
OK

Tips:

1. You can add multiple port triggering rules according to your network need.
2. 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.

6.3. 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:

DMZ is more applicable in the situation that users are not clear about which ports to open. When it 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 the checkbox to enable DMZ.

DMZ ?

DMZ: Enable DMZ

DMZ Host IP Address:

Save

4. Enter the IP address 192.168.0.100 in the [DMZ Host IP Address](#) filed.

5. Click [Save](#) to save the settings.

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.

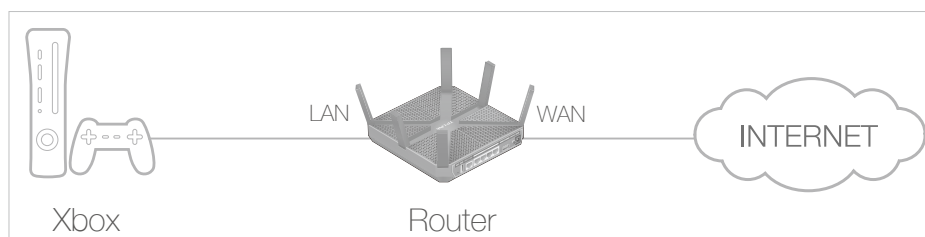
6.4. Make Xbox Online Games Run Smoothly by UPnP

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 in the 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:

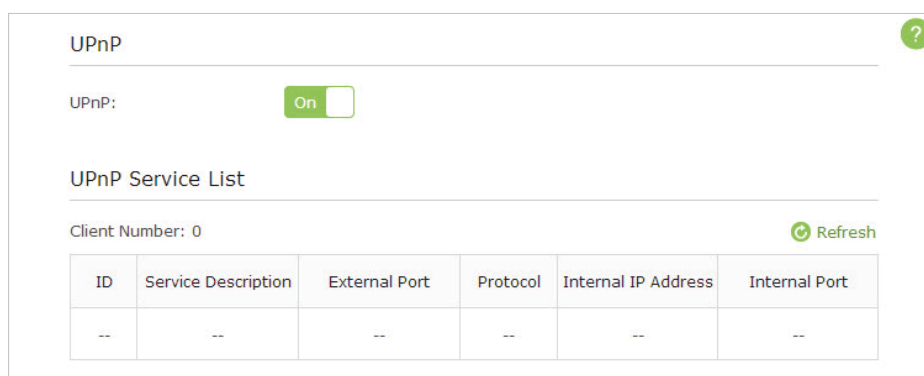
1. UPnP is enabled by default in this router.
2. Only the application supporting UPnP protocol can use this feature.
3. UPnP feature needs the support of operating system (e.g. Windows Vista/ Windows 7/ Windows 8, etc. Some of operating system need to install the UPnP components).

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.



The screenshot shows the UPnP configuration page. At the top right, there is a green question mark icon. The 'UPnP' section has a toggle switch set to 'On'. Below this is the 'UPnP Service List' section, which shows 'Client Number: 0' and a 'Refresh' button with a green circular arrow icon. A table with six columns is displayed below:

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

USB Application

7

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, and does not support USB 3G/4G modems.

This chapter contains the following sections:

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

7.1. Local Storage Sharing


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

7.1.1. 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 four 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 or NTFS.
- 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  [Safety 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 referring to [Customize Your Settings](#).

Windows computer	<ol style="list-style-type: none">1. Press Windows () + R on the keyboard (or select Start > Run).2. Type the server address \\tplinkwifi.net or ftp://tplinkwifi.net in the dialog box.3. Click OK.
Mac	<ol style="list-style-type: none">1. Select Go > Connect to Server.2. Type the server address smb://tplinkwifi.net or ftp://tplinkwifi.net.3. Click Connect.
pad	Use a third-party app for network files management.

Tips:

You can also access all folders by using your Network/Media Server Name. Refer to [To Customize the Address of the USB Disk](#) to learn more.

7.1.2. 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. Go to [Basic](#) or [Advanced](#) > [USB Settings](#) > [Sharing Access](#). Focus on the [Folder Sharing](#) section. Click the button to disable [Share All](#), then click [Add](#) to add a new sharing folder.

Folder Sharing

Share All:

+ Add - Delete

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

Volume Name: ▼

Folder Path:

Folder Name:

Enable Authentication

Enable Write Access

Enable Media Sharing

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](#): Select to enable authentication for this folder sharing, and you will be required to use a username and password to access the USB disk. Refer to [To Set up Authentication for Data Security](#) to learn more.
 - [Enable Write Access](#): If you select this check box, network clients can modify this folder.
 - [Enable Media Sharing](#): Select to enable media sharing for this folder, and you can view photos, play music and watch movies stored on the USB disk directly from DLNA-supported devices. Click [Media Sharing](#) to learn more.
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. Go to [Advanced](#) > [USB Settings](#) > [Sharing Access](#). Focus on the [Sharing Account](#) section.

Sharing Account ?

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

Account: Use Default Account Use New Account

Username:

Password: (Same as Login Password)

3. Choose to use the default account (admin) or use a 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.

Folder Sharing

Share All:

Enable Authentication:

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

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. Go to [Advanced](#) > [USB Settings](#) > [Sharing Access](#). Focus on the [Sharing Settings](#) section
3. Make sure [Network Neighborhood](#) is ticked, and enter a Network/Media Server Name as you like, such as [My-Share](#), then click [Save](#).

Sharing Settings

Network/Media Server Name:

Enable	Access Method	Link	Port
<input checked="" type="checkbox"/>	Network Neighborhood	\\My-Share	---
<input checked="" type="checkbox"/>	FTP	ftp://192.168.0.74:21	21
<input type="checkbox"/>	FTP (Via Internet)	ftp://0.0.0.0:21	<input type="text" value="21"/>

[Save](#)

4. Now you can access the USB disk with `\\My-Share` (`smb://My-Share` for Mac).

7.2. 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.


7.2.1. 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 four 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 or NTFS.

- 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  [Safety 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) Go to [Advanced](#) > [USB Settings](#) > [Sharing Access](#).
- 3) Choose to use the default account (admin) or use a new account, and click [Save](#).

Sharing Account ?

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

Account: Use Default Account
 Use New Account

Username:

Password: (Same as Login Password)

[Save](#)

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

Folder Sharing

Share All:

Enable Authentication:

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

3. Enable the FTP (via Internet)

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

Sharing Settings

Network/Media Server Name:

Enable	Access Method	Link	Port
<input type="checkbox"/>	Network Neighborhood	\\My-Share	---
<input checked="" type="checkbox"/>	FTP	ftp://192.168.0.74:21	21
<input checked="" type="checkbox"/>	FTP (Via Internet)	ftp://0.0.0.0:21	<input type="text" value="21"/>

[Save](#)

4. Access Your USB Disk via Internet

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



- To download, open a web browser and type the server address [ftp://<WAN IP address of the router>:<port number>](#) (such as [ftp://59.40.2.243:21](#)), or if you set up a domain name for your router you can type the server address [ftp://<domain name of the router>:<port number>](#) (such as [ftp://MyDomainName:21](#)) in the address bar, then press [Enter](#) on the keyboard.
- To upload, use a third-party app for network files management.

pad

- Use a third-party app for network files management.

Tips:

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

7.2.2. 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. Go to [Basic](#) or [Advanced](#) > [USB Settings](#) > [Sharing Access](#). Focus on the section of [Folder Sharing](#). 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. Select [Enable Authentication](#). If you allow network clients to modify this folder, select [Enable Write Access](#).

The screenshot shows the 'Folder Sharing' configuration page. At the top, there is a 'Share All' toggle switch which is currently turned off. To the right of the toggle are '+ Add' and '- Delete' buttons. Below this is a table with the following columns: ID, Folder Name, Folder Path, Media Sharing, Volume Name, Status, and Modify. The table contains one row with dashes in all cells. Below the table, there are three input fields: 'Volume Name' with a dropdown menu showing 'Select a folder', 'Folder Path' with a 'Browse' button, and 'Folder Name'. Below these fields are three checkboxes: 'Enable Authentication' (checked), 'Enable Write Access' (checked), and 'Enable Media Sharing' (unchecked). At the bottom right, there are 'Cancel' and 'OK' buttons.

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.

7.3. Media Sharing

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

7.3.1. 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 four 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 or NTFS.
- 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 [Safety Remove](#).

2. Play the Media 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.

1. Open the Windows Media Player.
2. Click the media server name (such as [Genie Media Servers](#)) under the list of [Other Libraries](#), then you can directly view photos, play music and watch movies that you share on the USB disks.



The screenshot shows the Windows Media Player interface. The left sidebar lists various media categories: English, Playlists, Music (selected), Artist, Album, Genre, Videos, Pictures, Recorded TV, Other Libraries, Genie Media Servers (expanded to show Music, Videos, Pictures, Recorded TV), Administrator (win7), and Genie Media Servers. The main area displays a list of music albums from the Genie Media Servers. The first album is 'Bob Acri' by Bob Acri, categorized as Jazz, released in 2004. The second album is 'Ninja Tuna' by Mr. Scruff, categorized as Electronic, released in 2008. The third album is 'Fine Music, Vol. 1' by Richard Stoltzman, categorized as Classical.

Windows computer

pad

- Use a third-party DLNA-supported player.

7.3.2. 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. Go to [Advanced](#) > [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. Select [Enable Media Sharing](#) and click [OK](#).

Folder Sharing

Share All:

+ Add - Delete

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

Volume Name:

Folder Path: Browse

Folder Name:

Enable Authentication

Enable Write Access

Enable Media Sharing

Cancel
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.

7.4. Printer Sharing

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

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.

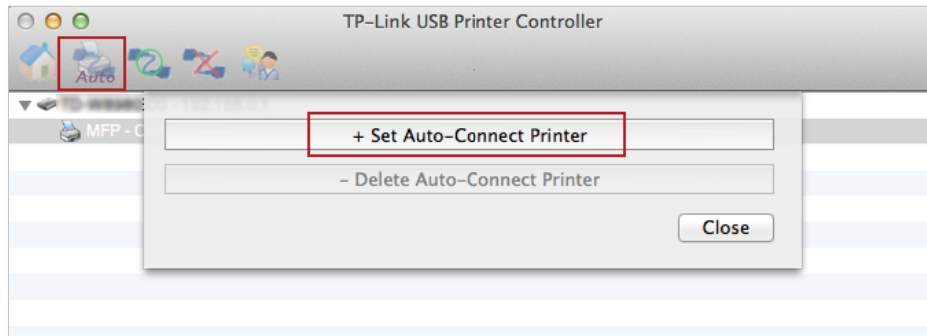
Note:

Printers unlisted may be incompatible with the router. You can check [Printer Compatibility List](http://www.tp-link.com/common/compatible/print-server/) to verify whether your printer is supported by the router: <http://www.tp-link.com/common/compatible/print-server/>.

3. Install the TP-LINK USB Printer Controller Utility

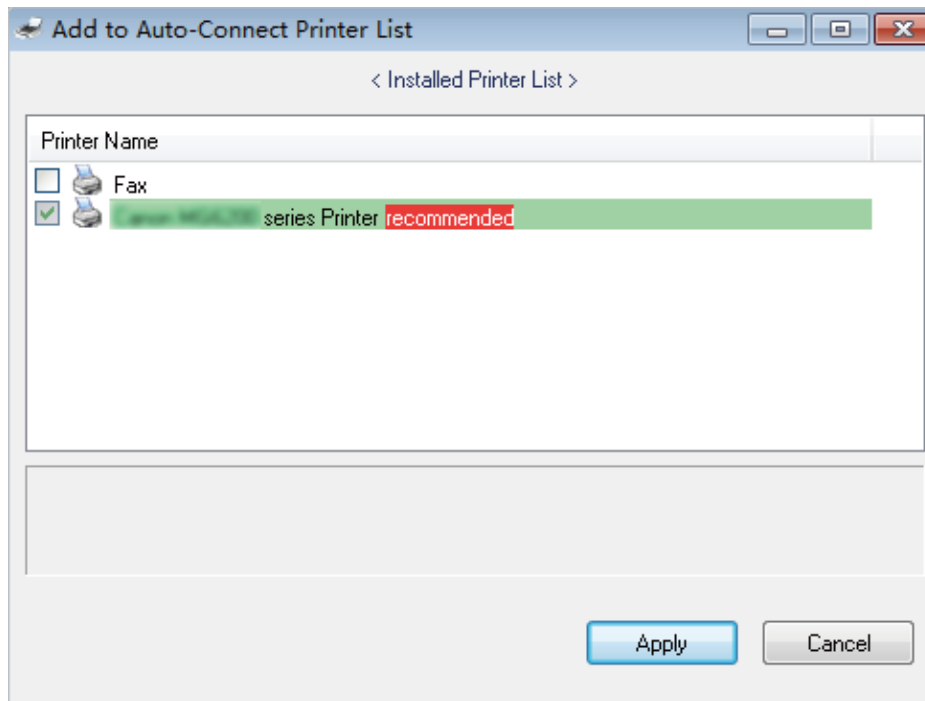
TP-LINK USB Printer Controller Utility helps you access the shared printer. Download and install the utility on each computer that needs printer service.

You can get the utility from <http://www.tp-link.com/app/usb/>. PC Utility is for Windows computer and Mac Utility is for Mac computer.

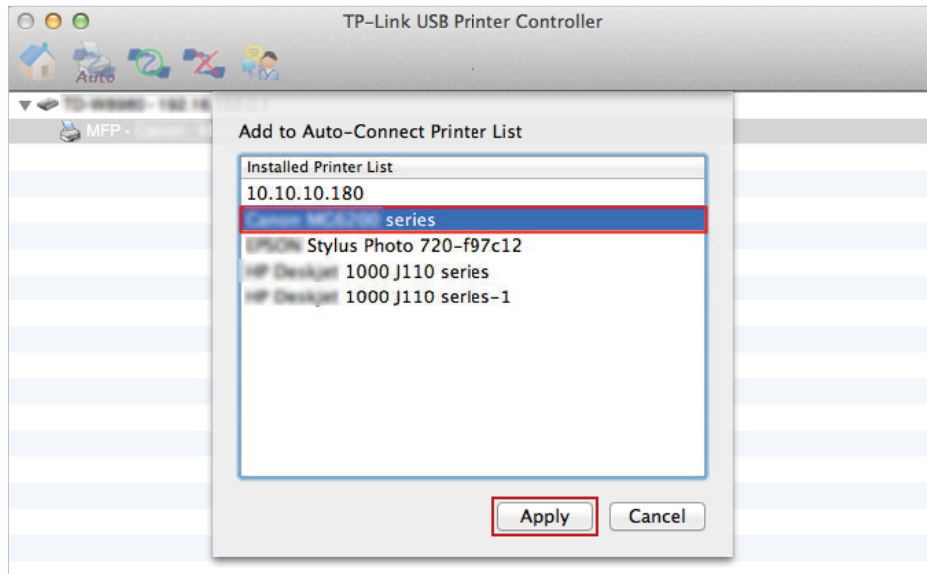


Mac

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

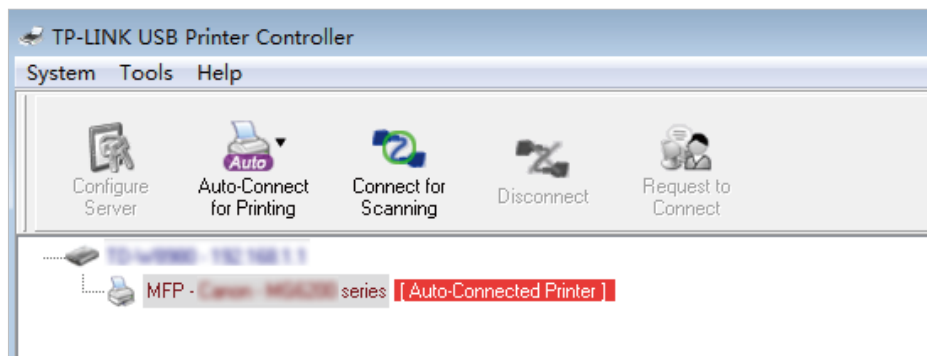


Windows

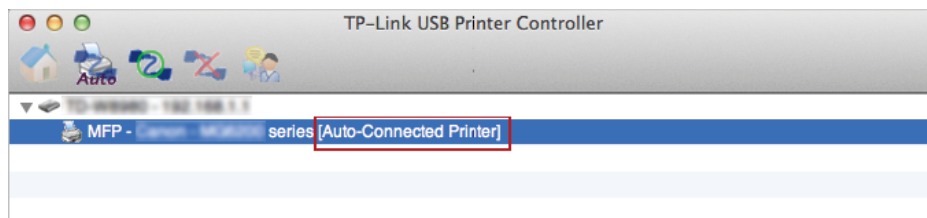


Mac

- 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 the on-screen instructions.

Parental Controls

8

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

I want to: control what types of websites my children or other home network users can visit and even the time of day they are allowed to access the Internet.

For example, I want to allow my children's devices (e.g. a computer or a tablet) to access only www.tp-link.com and Wikipedia.org from 18:00 (6PM) to 22:00 (10PM) 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](#).

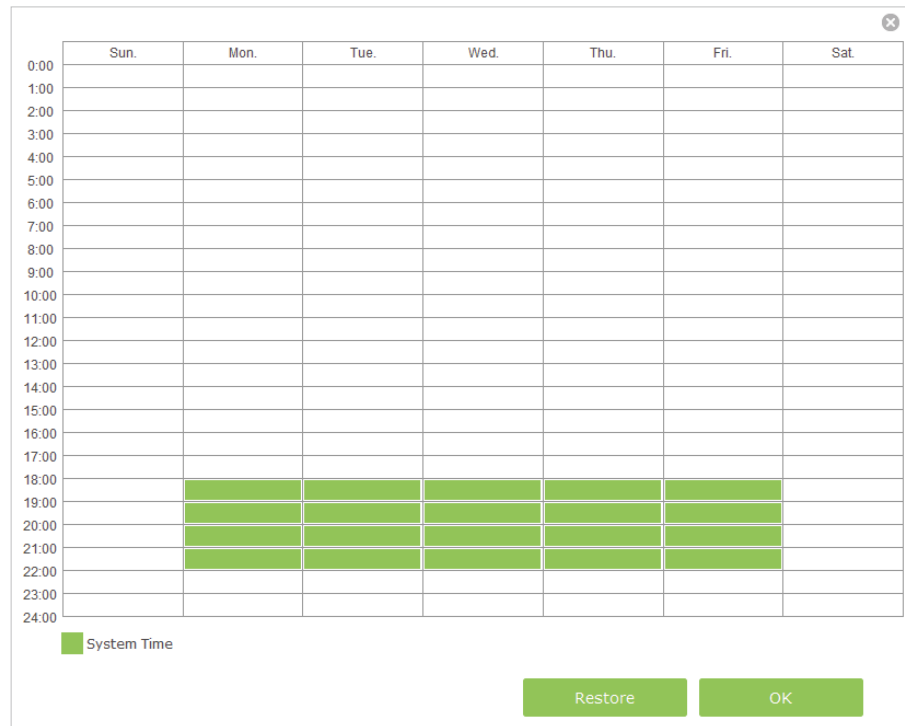
The screenshot shows the 'Parental Controls' settings page. At the top, there is a toggle switch for 'Parental Controls' which is currently turned on. Below this is a section titled 'Devices Under Parental Controls'. A note states: 'The Effective Time Schedule is based on the time of the Router. The time can be set in "Advanced -> System Tools -> Time Settings"'. There are '+ Add' and '- Delete' buttons. Below is a table with columns: ID, Device Name, MAC Address, Internet Access Time, Description, Status, and Modify. The table is currently empty. Below the table is a 'Content Restriction' section with radio buttons for 'Blacklist' (selected) and 'Whitelist'. There is a '+ Add a new keyword' button and a 'Save' button at the bottom right.

3. Click [Add](#).

The screenshot shows the 'Add' dialog box for adding a device to parental controls. It has a table with columns: ID, Device Name, MAC Address, Internet Access Time, Description, Status, and Modify. Below the table are input fields for 'Device Name', 'MAC Address', and 'Description (optional)'. There is a clock icon for 'Internet Access Time' and a checked 'Enable' checkbox. A 'View Existing Devices' button is next to the 'Device Name' field. At the bottom are 'Cancel' and 'OK' buttons.

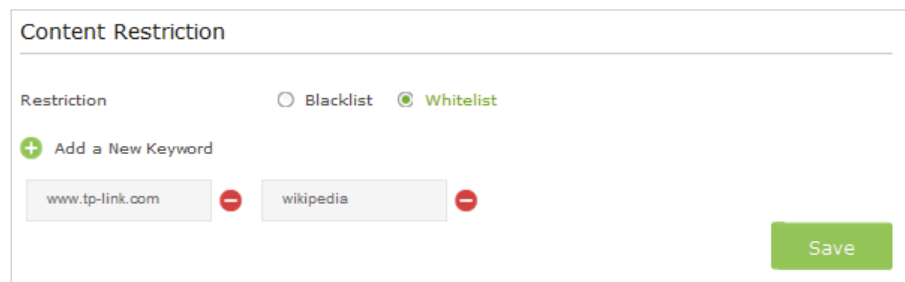
4. Click [View Existing Devices](#), and select the device to be controlled. Or, enter the [Device Name](#) and [MAC Address](#) manually.

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



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

6. Enter a **Description** for the entry.
7. Select the checkbox to enable this entry and click **OK**.
8. Select the restriction mode.
- 1) In **Blacklist** mode, the controlled devices cannot access any websites containing the specified keywords during the Internet Access Time period.
 - 2) In **Whitelist** mode, the controlled devices can only access websites containing the specified keywords during the Internet Access Time period.



9. Click **Add a New Keyword**. You can add up to 200 keywords for both Blacklist and Whitelist. Below are some sample entries to allow access.
- 1) Enter a web address (e.g. www.tp-link.com) or a web address keyword (e.g. [wikipedia](http://wikipedia.org)) to only allow or block access to the websites containing that keyword.
 - 2) Specify the domain suffix (eg. .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.

Bandwidth Control

9

The Bandwidth Control 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.

Bandwidth Control		
Bandwidth Control:	<input checked="" type="checkbox"/> Enable	
Total Upstream Bandwidth:	<input type="text" value="512"/>	kbps
Total Downstream Bandwidth:	<input type="text" value="8192"/>	kbps
<input type="button" value="Save"/>		

3. Enable [Bandwidth Control](#).
4. Enter the [Total Upstream Bandwidth](#) and the [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.

Controlling Rules

+ Add - Delete

<input type="checkbox"/>	Description	Priority	Up(min/max)	Down(min/max)	Enable	Modify
--	--	--	--	--	--	--

IP Range: -

Port Range: -

Protocol:

Priority: (1 means the highest priority.)

Upstream: to

Downstream: to

Enable this entry

- 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.

Controlling Rules

+ Add - Delete

<input type="checkbox"/>	Description	Priority	Up(min/max)	Down(min/max)	Enable	Modify
<input type="checkbox"/>	192.168.0.110	5	250/500 kbps	2000/4000 kbps		
<input type="checkbox"/>	192.168.0.101	5	250/500 kbps	2000/4000 kbps		

Done! Now you and your roommate have an independent bandwidth.

Network Security

10

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 function.

This chapter contains the following sections:

- [Protect the Network from Cyber Attacks](#)
- [Access Control](#)
- [IP & MAC Binding](#)

10.1. Protect the Network from Cyber Attacks

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

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

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](#).

DoS Protection:

Enable DoS Protection

ICMP-FLOOD Attack Filtering: Off

UDP-FLOOD Attack Filtering: Off

TCP-FLOOD Attack Filtering: Off

Forbid Lan Ping

Forbid Wan Ping

Save

Blocked DoS Host List

Refresh Delete

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

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 Internet Control Message Protocol (ICMP) flood attack.
 - [UDP-FLOOD Attack Filtering](#) - Enable to prevent the User Datagram Protocol (UDP) flood attack.
 - [TCP-SYN-FLOOD Attack Filtering](#) - Enable to prevent the Transmission Control Protocol-Synchronize (TCP-SYN) flood attack.

Tips:

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

5. Select [Forbid Lan Ping](#) if you want to ignore the ping packets from LAN port.
6. Select [Forbid Wan Ping](#) if you want to ignore the ping packets from WAN port.
7. Click [Save](#) to make the settings effective.

10.2. Access Control

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

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

- How can I do that?**
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](#).

Access Control

Access Control:

Access Mode

Default Access Mode: Blacklist Whitelist

Devices in Blacklist

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

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

Devices Online

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

<input type="checkbox"/>	ID	Device Name	IP Address	MAC Address	Connection Type
<input type="checkbox"/>	1	Unknown	192.168.0.200	50:E5:49:1E:06:80	Wired
<input type="checkbox"/>	2	C3200-SHARE	192.168.0.74	00:0A:EB:0C:26:42	Wired

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

Access Mode

Default Access Mode: Blacklist
 Whitelist

Devices in Whitelist

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

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

Device Name:

MAC Address:

Enable

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

- 3) Enter the [Device Name](#) and [MAC Address](#) (You can copy and paste the information from the following list if the device is connected to your network).
- 4) Click [OK](#).

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

10.3. IP & MAC Binding

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

I want to: Prevent ARP spoofing and ARP attacks.

- How can I do that?**
1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
 2. Go to [Advanced](#) > [Security](#) > [IP & MAC Binding](#).

Settings

IP & MAC Binding:

Binding List

+ Add - Delete

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

ARP List

Refresh Bind

<input type="checkbox"/>	ID	Device Name	MAC Address	IP Address	Bound	Modify
<input type="checkbox"/>	1	C3200-SHARE	00:0A:EB:0C:26:42	192.168.0.74	Unloaded	
<input type="checkbox"/>	2	Unknown	50:E5:49:1E:06:80	192.168.0.200	Unloaded	

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](#).

Binding List

+ Add - Delete

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

MAC Address:

IP Address:

Enable

- 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.

Customize Your Network Settings

11

This chapter guides you on how to configure advanced networking 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](#)

11.1. 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](#) page.
3. Type in a new IP address appropriate to your needs.

The screenshot shows the LAN configuration page. It includes the following fields and values:

MAC Address:	40:16:9F:BF:50:8B
LAN IPv4:	192.168.0.107
Subnet Mask:	255.255.255.0
IGMP Snooping:	<input checked="" type="checkbox"/> Enable IGMP Snooping

A green 'Save' button is located at the bottom right of the form.

4. Leave the [Subnet Mask](#) as the default settings.
5. 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.
6. 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.

11.2. 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 separating IPTV from Internet surfing, we guarantee you a high quality of video streaming and a high speed of Internet surfing.

I want to: Configure the router to enable Internet Protocol Television (IPTV) Services.

For example, I already bought IPTV service, but this service can only be delivered through the Internet. Therefore, I need to configure my router first.

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](#) to open the configuration page.
3. Configure IPTV settings:

The screenshot shows the 'IPTV Settings' configuration page. The 'IPTV' checkbox is checked and labeled 'Enable IPTV'. The 'Mode' dropdown is set to 'Bridge'. The 'IGMP Proxy' dropdown is set to 'V3'. The LAN ports are configured as follows: LAN1 is set to 'IPTV', LAN2 is set to 'Internet', LAN3 is set to 'Internet', and LAN4 is set to 'Internet'. A green 'Save' button is visible at the bottom right.

- 1) Select 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](#) mode, connect device to the predetermined LAN port. For [Bridge](#) and [Custom](#) mode, select a LAN port as the IPTV port 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.

11.3. 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 DHCP Server if necessary, and you can reserve LAN IP address for specified client device.

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](#).

DHCP Server

DHCP: Enable

IP Address Pool: -

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

Default Gateway: (Optional)

Primary DNS: (Optional)

Secondary DNS: (Optional)

[Save](#)

Client List

Client Number: 0 [Refresh](#)

ID	Client Name	MAC Address	Assigned IP	Lease Time
--	--	--	--	--

Address Reservation

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

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

Condition Pool

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

<input type="checkbox"/>	Vendor ID	Start IP Address/End IP Address	Facility	Group	Status	Modify
--	--	--	--	--	--	--

To specify the IP address that the router assigns

1. Make sure that the [Enable DHCP Server](#) checkbox is selected.
2. Enter the starting and ending IP address in the [IP Address Pool](#).
3. Enter other parameters if the ISP offers, the Default Gateway is automatically filled, which is the same as the LAN IP address of the router.
4. Click [Save](#) to make the settings effective.

To reserve an IP address for a specified client device

1. Click the [Add](#) button.

Address Reservation

+ Add - Delete

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

MAC Address:

Reserved IP:

Group:

Enable this entry

Cancel OK

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. Check to [Enable this entry](#) and click [OK](#) to make the settings effective.

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 to 192.168.0.80) to Camera devices, thus facilitating the network management.

11.4. 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 Internet IP address (such as 192.168.0.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](#).

Dynamic DNS Settings ?

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

Username:

Password:

Domain Name:

[Login](#) [Logout](#) Disconnected

[Save](#)

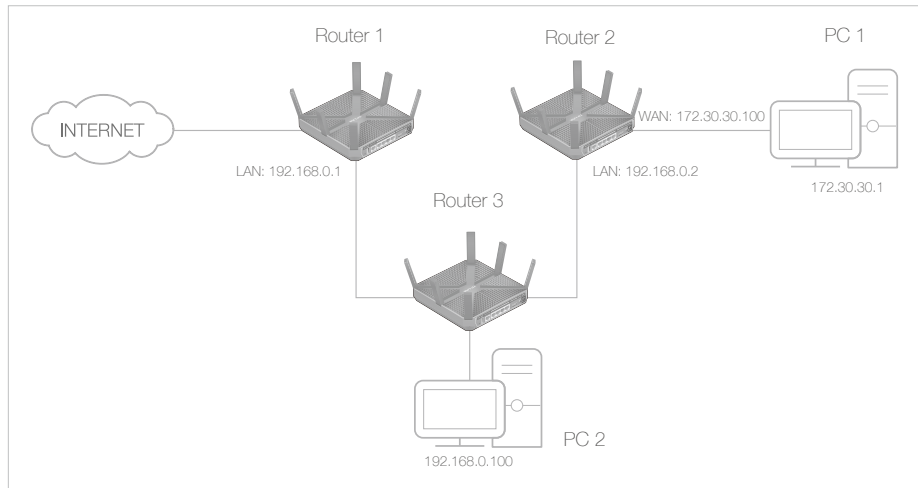
4. Enter the username, password and domain name of the account.
 5. Click [Login](#) and click [Save](#).
- Tips:** If you want to use a new DDNS account, please [Logout](#) first, then log in with the new account.

11.5. 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 set for the router.
3. Go to **Network > Advanced Routing**.
4. Click **Add** to add a new static routing entry.

Static Routing ?

+ Add - Delete

<input type="checkbox"/>	ID	Destination IP	Subnet Mask	Gateway	Enable	Modify
--	--	--	--	--	--	--

5. Finish the settings according to the following explanations:

<input type="checkbox"/>	ID	Destination IP	Subnet Mask	Gateway	Enable	Modify
--	--	--	--	--	--	--

Destination IP:

Subnet Mask:

Gateway:

Interface:

Status:

Destination IP: 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.

6. Click **OK** to save the settings.

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

System Routing Table				
ID	Destination Network	Subnet Mask	Gateway	Interface
1	172.30.30.1	255.255.255.255	192.168.0.2	LAN & WLAN
2	192.168.2.0	255.255.255.0	0.0.0.0	LAN & WLAN
3	192.168.0.0	255.255.255.0	0.0.0.0	LAN & WLAN

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

11.6. Specify Wireless Settings

The router's wireless network names (SSIDs) and passwords, and security options are preset in the factory. The preset SSIDs and passwords can be found on the product label. You can customize the wireless settings according to your needs.

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

- Go to [Basic](#) > [Wireless](#).

Wireless Settings ?

Wireless 2.4GHz: **Enable**

Wireless Network Name (SSID): Hide SSID

Password:

Wireless 5GHz-1: **Enable**

Wireless Network Name (SSID): Hide SSID

Password:

Wireless 5GHz-2: **Enable**

Wireless Network Name (SSID): Hide SSID

Password:

To enable or disable the wireless function:

The wireless radio is enabled by default, if you want to disable the 2.4GHz, 5GHz-1, or 5GHz-2 wireless function, just clear the corresponding [Enable](#) checkbox.

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

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, TP-LINK_XXXX_5G_1 for 5GHz-1, and TP-LINK_XXXX_5G_2 for 5GHz-2, 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:

Select [Hide SSID](#), and your SSID will not broadcast. Your SSID won't display when you scan for local wireless network list on your wireless device and you need to manually join the network.

Advanced Settings:

Go to [Advanced](#) > [Wireless](#) > [Wireless Settings](#).

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. Select the [Smart Connect](#) checkbox, and click [Save](#).
2. Keep the default or set a new SSID and password, and [click Save](#).

This SSID and password will be applied for 2.4GHz, 5GHz-1, and 5GHz-2 wireless networks.

The screenshot shows the 'Smart Connect' and 'Wireless' configuration sections. In the 'Smart Connect' section, the 'Enable' checkbox is unchecked, and a green 'Save' button is visible. The 'Wireless' section has a '2.4GHz | 5GHz-1 | 5GHz-2' indicator. The 'Wireless Radio' is checked and labeled 'Enable'. The 'Wireless Network Name (SSID)' is 'TP-LINK_0969' with a 'Hide SSID' checkbox. The 'Security' dropdown is set to 'WPA/WPA2 Personal(Recommended)'. The 'Version' has 'WPA2-PSK' selected. The 'Encryption' has 'AES' selected. The 'Password' field contains '12345670'. The 'Mode' is '802.11bgn mixed', 'Channel' is 'Auto', and 'Channel Width' is 'Auto'. The 'Transmit Power' has 'High' selected. A green 'Save' button is at the bottom right.

To change the security option:

In the [Wireless](#) section, select an option from the [Security](#) dropdown 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](#).

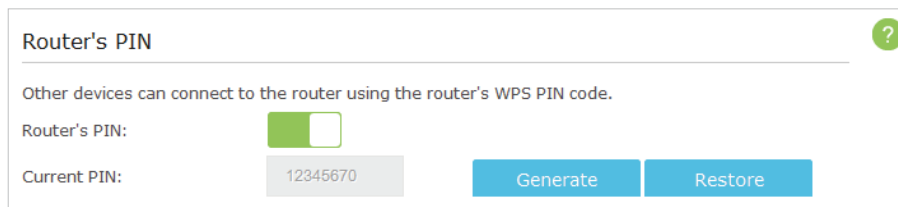
11.7. Use WPS for Wireless Connection

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](#) .

11.7.1. 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.

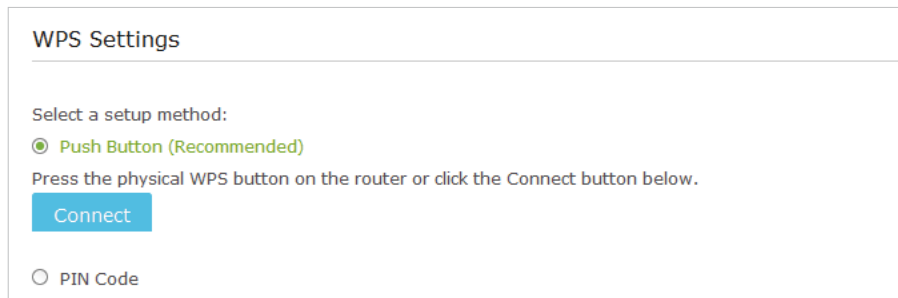


Note:

1. If you want to enable/disable the WPS feature, go to [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.

11.7.2. 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 Code:** Enter the client's PIN, and click [Connect](#).

WPS Settings

Select a setup method:

Push Button (Recommended)

PIN Code

Enter the client's PIN:

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

11.8. Schedule Your Wireless Function

You can automatically turn off your wireless network at the 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** page.
3. Select the 2.4GHz wireless network to configure. Toggle on the button to enable the Wireless Schedule feature.

Task Schedule 2.4GHz | 5GHz-1 | 5GHz-2

Drag the schedule table to choose the period on which you need the wireless off automatically!
 The Effective Time Schedule is based on the time of the Router. The time can be set in "System Tools -> Time Settings"

Enable Wireless Schedule:

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

System Time

4. Set the time. Drag the cursor to cover the time area and click [Save](#) to make the settings effective. The selected time will be in green.
5. Repeat steps 3 and 4 to set time for 5GHz-1 and 5GHz-2 wireless networks.

Note:

1. If you just set time for one wireless band, the other wireless band is still always on, so set time for both of the two bands to schedule your whole wireless network.
2. The wireless LED (2.4GHz, 5GHz-1, and 5GHz-2) will turn off if the corresponding wireless network is disabled.
3. The wireless network will be automatically turned on after the time period you set.

11.9. 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.

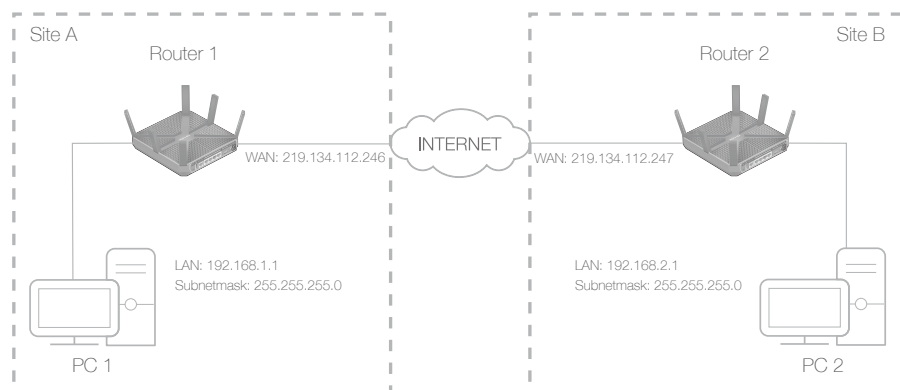
With the wide application of the Internet, more and more data are needed to be shared through the Internet. Connecting the local network to the Internet directly, though can allow the data exchange, will cause the private data to be exposed to all the users on the Internet.

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.

IPSec Settings

Dead Peer Detection:

+ Add - Delete

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

IPSec Connection Name:

Remote IPSec Gateway (URL): Site B's WAN IP

Tunnel access from local IP addresses: ▼

IP Address for VPN: LAN IP range of Site A

Subnet Mask:

Tunnel access from remote IP addresses: ▼

IP Address for VPN: LAN IP range of Site B

Subnet Mask:

Key Exchange Method: ▼

Authentication Method: ▼

Pre-Shared Key:

Perfect Forward Secrecy: ▼

Advanced

- 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.

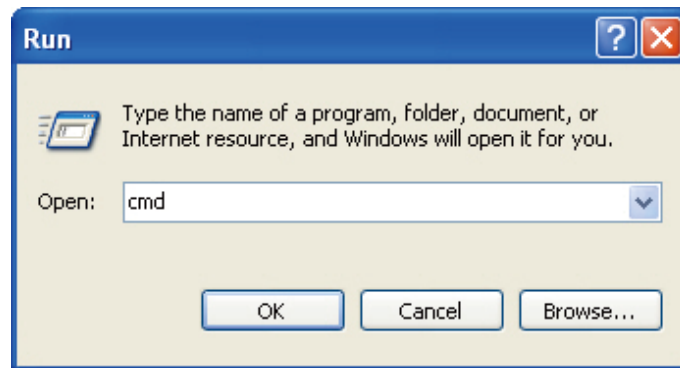
Note:

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

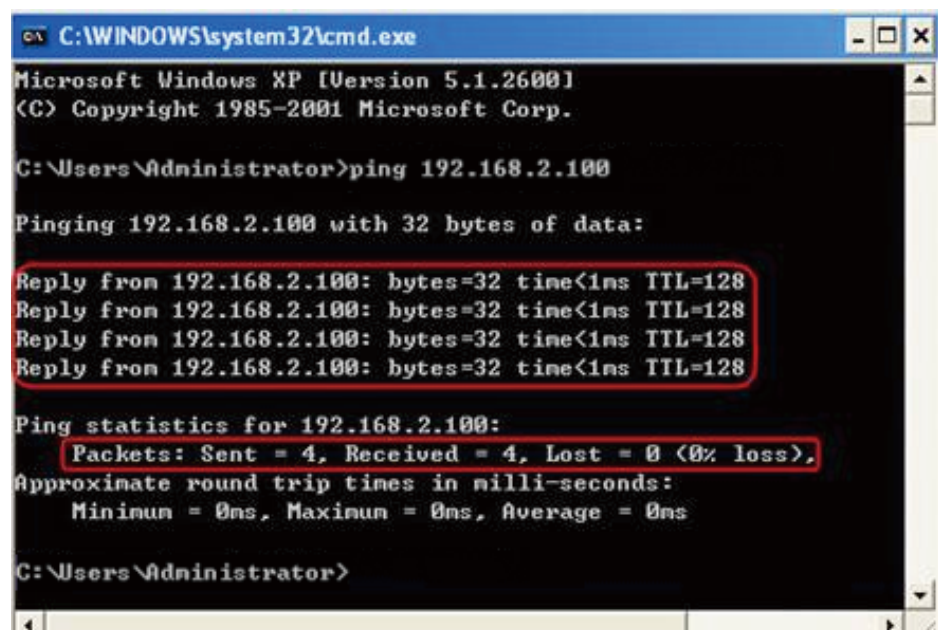
- 9) Leave the [Advanced](#) Settings as default value. Then click [OK](#) to save.
3. Configuration on Site B (remote network). Refer to step 2 configuration on Site A and make sure that Site A and Site B use the same [Pre-shared keys](#) and [Perfect Forward Secrecy](#) settings.
4. The [Status](#) 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.

Manage the Router

12

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](#)

12.1. Set Up System Time

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

The screenshot shows the 'Time Settings' page. It features a dropdown menu for 'Time Zone' set to '(GMT-08:00) Pacific Time (US & Canada); Tijuana'. Below this is a 'Date' field with '21/07/2015' and '(MM/DD/YY)' format. The 'Time' field is split into three dropdowns for hours (17), minutes (8), and seconds (45). There are two 'NTP Server' fields, both set to '0.0.0.0' and labeled '(optional)'. At the bottom, there are two buttons: 'Get from PC' and 'Get GMT', and a green 'Save' button on the right.

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](#), set the start and end time and then click [Save](#) to make the settings effective.

Daylight Saving

Daylight Saving: Enable Daylight Saving

Start: Mar ▼ M Last ▼ W Sun ▼ T 02:00 ▼

End: Oct ▼ M Last ▼ W Sun ▼ T 03:00 ▼

[Save](#)

12.2. 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](#).

Dagnostic Tools ?

Dagnostic tool: ping traceroute

Target IP Address/Domain Name:

[Start](#)

Advanced

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 packet count, 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](#).

```

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

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

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

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

12.3. Upgrade the Firmware

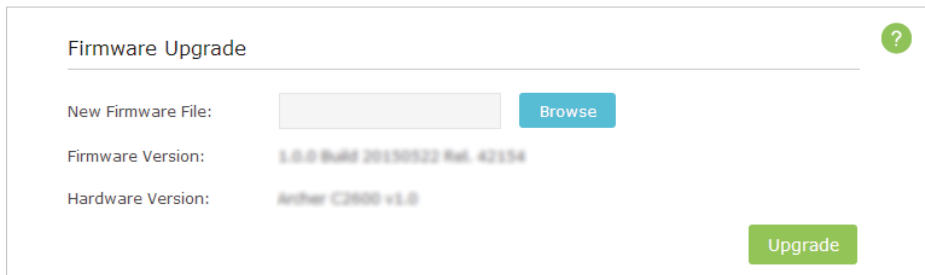
TP-LINK is dedicated to improving and enriching the product features, giving you a better network experience. We will release the latest firmware at TP-LINK official website, you can download the latest firmware file from the [Support](#) page of our website www.tp-link.com and upgrade the firmware to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

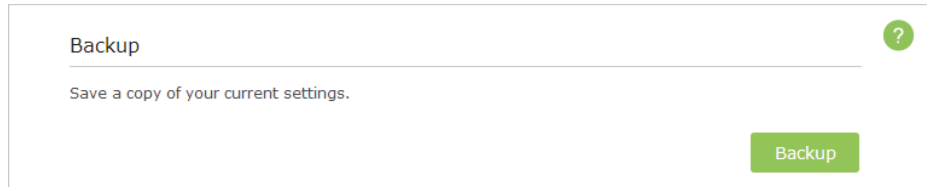
12.4. Backup and Restore Configuration Settings

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

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

To backup configuration settings:

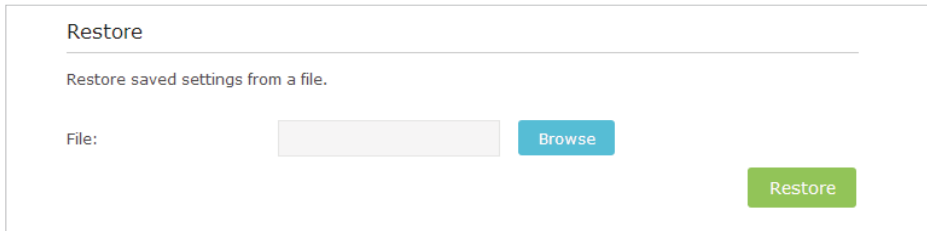
Click [Backup](#) to save a copy of the current settings to your local computer. A '.bin' file of the current settings will be stored to your computer.



The screenshot shows a web interface for the 'Backup' function. At the top, the word 'Backup' is displayed in a large font, followed by a horizontal line. Below the line, the text 'Save a copy of your current settings.' is centered. In the bottom right corner, there is a green button labeled 'Backup'. A small green circle with a white question mark is located in the top right corner of the panel.

To restore configuration settings:

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



The screenshot shows a web interface for the 'Restore' function. At the top, the word 'Restore' is displayed in a large font, followed by a horizontal line. Below the line, the text 'Restore saved settings from a file.' is centered. Underneath, there is a label 'File:' followed by a text input field and a blue button labeled 'Browse'. In the bottom right corner, there is a green button labeled 'Restore'.

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

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

To reset the router to factory default settings:

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



The screenshot shows a web interface for the 'Factory Default Restore' function. At the top, the text 'Factory Default Restore' is displayed in a large font, followed by a horizontal line. Below the line, the text 'Revert all the configuration settings to their default values.' is centered. In the bottom right corner, there is a green button labeled 'Factory Restore'.

2. Wait a few moments for the reset and reboot.

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.

12.5. Change the Administrator Account

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

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

Use the new username and password for the following logins.

12.6. 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.

12.7. 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.

Remote Management

Remote Management: Enable

Port:

IP/MAC Address:

[Save](#)

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.
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.

12.8. 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.

System Log

Type: ALL ▼

Level: Debug ▼

 Refresh  Delete All

ID	Time	Type	Level	Log Content
1	1970-01-01 00:46:15	IGMP	Warning	V2 igmp router occured! Not matching ours V3.
2	1970-01-01 00:45:15	IGMP	Warning	V2 igmp router occured! Not matching ours V3.
3	1970-01-01 00:44:10	IGMP	Warning	V2 igmp router occured! Not matching ours V3.
4	1970-01-01 00:43:10	IGMP	Warning	V2 igmp router occured! Not matching ours V3.
5	1970-01-01 00:42:41	DHCPD	Notice	Recv REQUEST from 48:43:7C:B0:B4:ED
6	1970-01-01 00:42:39	DHCPD	Notice	Send OFFER with ip 192.168.0.100
7	1970-01-01 00:42:39	DHCPD	Notice	Recv DISCOVER from 48:43:7C:B0:B4:ED
8	1970-01-01 00:42:05	IGMP	Warning	V2 igmp router occured! Not matching ours V3.

< 1 2 3 4 5 6 7 8 >

Log Settings Save Log

To view the system logs:

1. Select the log Type. Select **ALL** to view all kinds of logs, or select **IGMP** or **PPP** 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.

Log Settings

Save Locally

Minimum Level: Information ▼

Save Remotely

Minimum Level: Warning ▼

Server IP: 192.168.1.100

Server Port: 514

Local Facility Name: User ▼

Back Save

- **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.

12.9. 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.

SNMP Settings

Simple Network Management Protocol(SNMP) allows management applications to retrieve status updates and statistics from the SNMP agent within this device.

Enable SNMP Agent:

Read Community:	public
Set Community:	private
System Name:	Archer C3200
System Description:	Archer C3200 v00000000 Build 150803
System Location:	
System Contact:	
Trap Manager IP:	0.0.0.0

[Save](#)

- **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.
- **Set 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.

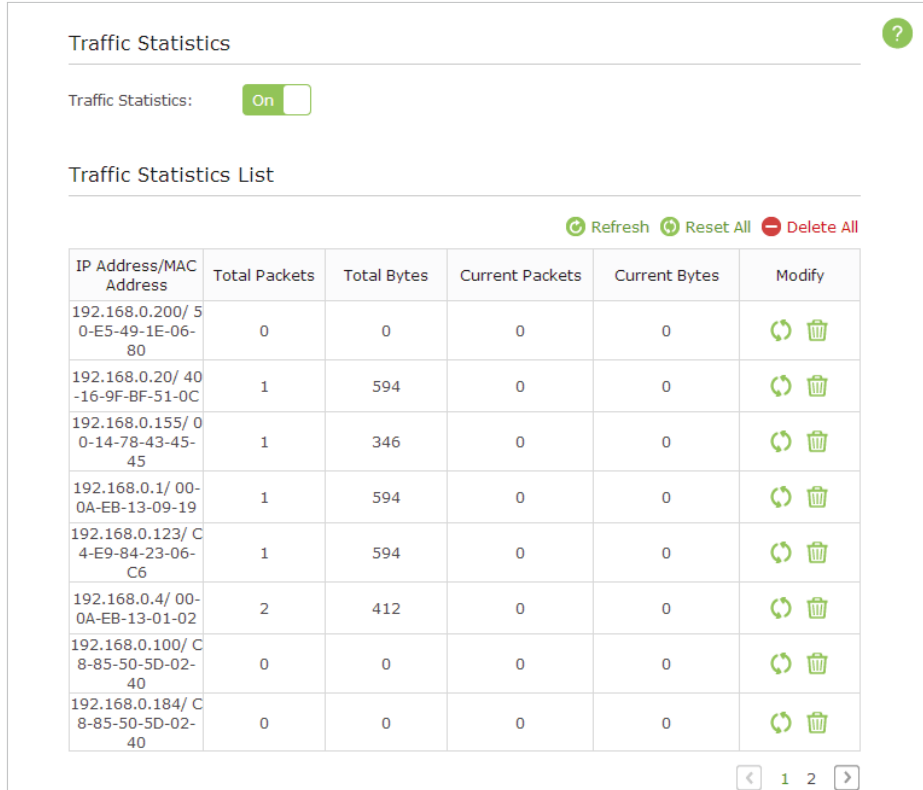
You are suggested to keep the default settings. Click **Save** to make the settings effective.

















12.10. Monitor the Internet Traffic Statistics

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

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [Advanced](#) > [System Tools](#) > [Traffic Statistics](#).
3. Toggle on [Traffic Statistics](#), and then you can monitor the traffic statistics in [Traffic Statistics List](#) section.

 **Tips:** This function is enabled by default.



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

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.

12.11. Control LEDs

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

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

LED

Night Mode: Enable

Period of Night Time: : to : (HH:MM)

Note: The time is based on the time of the Router which can be set in "System Tools -> Time Settings"

Save

Appendix A: 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	Wireless On/Off Button Power On/off Button LED On/off Button WPS Button Reset Button
External Power Supply	12V/5A
Dimensions (W X D X H)	7.9 X 7.9 X 1.5 in. (200 X 200 X 39mm)
Antenna	3 dual band Fixed antennas & 3 single band Fixed antennas

WIRELESS FEATURES

Wireless Standards	IEEE 802.11ac/n/a 5GHz IEEE 802.11b/g/n 2.4GHz
Frequency	2.4GHz, 5GHz Band1/Band4
Signal Rate	5GHz Band1: Up to 1300Mbps 5GHz Band2: Up to 1300Mbps 2.4GHz: Up to 600Mbps
Reception Sensitivity	5GHz: 11a 6Mbps: -94dBm 11a 54Mbps: -76dBm 11ac HT20: -68dBm 11ac HT40: -64dBm 11ac HT80: -60dBm 2.4GHz 11g 54M: -77dBm 11n HT20: -73dBm 11n HT40: -71dBm
Wireless Functions	Enable/Disable Wireless Radio, WMM, Wireless Statistics
Wireless Security	64/128-bit WEP, WPA/WPA2, WPA-PSK/WPA2-PSK encryption
Transmission Power	CE: <20dBm(2.4GHz) <23dBm(5GHz) FCC: <30dBm
Guest Network	2.4GHz guest network × 1 5GHz guest network × 2

OTHERS

Certification	FCC, RoHS
Package Contents	AC 3200 Wireless Tri-Band Gigabit Router Archer C3200 Power supply unit Ethernet Cable Quick Installation Guide
System Requirements	Microsoft Windows 98SE, NT, 2000, XP, Vista™ or Windows 7, Windows 8, MAC OS, NetWare, UNIX or Linux

HARDWARE FEATURES

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
-------------	--

* Only 2.412GHz~2.462GHz is allowed to be used in USA, which means only channel 1~11 is available for American users to choose.

Appendix B: FAQ

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

The default password is labeled at the back 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>, and log in with the username and password you set for the router.
2. Go to [Basic](#) > [Wireless](#) to obtain your wireless password.

Q2. How to retrieve the username and password of the web management page?

The default username and password of the web management page are [admin](#) (in lower case). If the password has been altered, please follow the steps below:

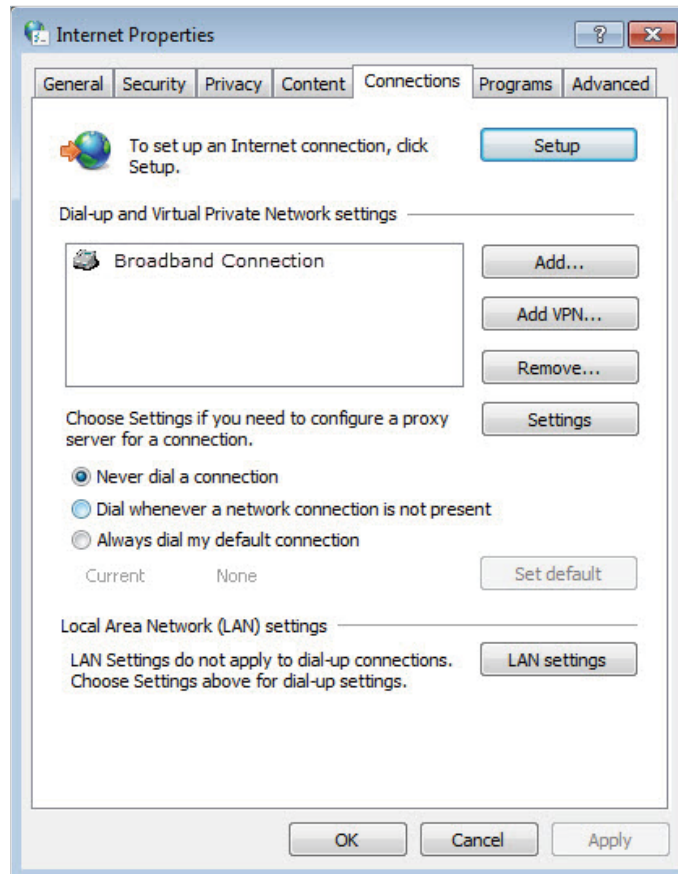
1. Reset the router to factory default settings: Press and hold the Reset button for about 7 seconds and then release;
2. Visit <http://tplinkwifi.net>;
3. Enter [admin](#) (in lower case) as both username and password to login.

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.

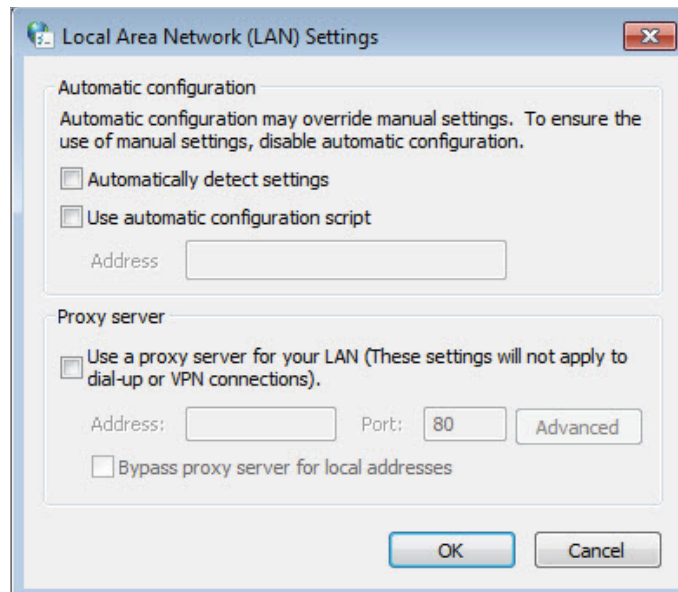
Q3. I cannot login to the router's web management page, what can I do?

This can happen for a variety of reasons, please try the methods below and try again.

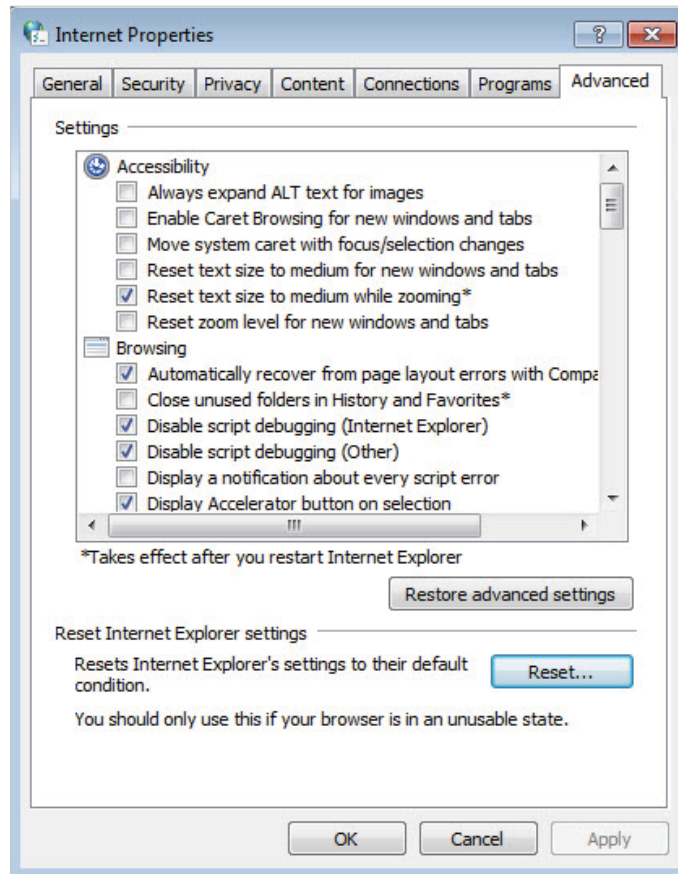
1. Make sure the router connects to the computer correctly and the corresponding LED indicator(s) light up.
2. Make sure the IP address of your computer is configured as [Obtain an IP address automatically](#) and [Obtain DNS server address automatically](#).
3. Make sure the <http://tplinkwifi.net> you input is right.
4. 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](#), select [Never dial a connection](#);



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



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




5. Change a web browser or computer and login again.
 6. Reset the router to factory default settings: Press and hold the Reset button for about 7 seconds and then release.
- Note:** You'll need to reconfigure the router to surf the Internet once the router is reset.
- Open a web browser and login again. If login still fails, please contact the technical support.

Q4. I cannot access the Internet even though the configuration is finished, what can I do?

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Advanced > Status** to check Internet status:
 - **If IP Address is a valid IP address, please try the methods below and try again:**

Internet ✖ IPv4 IPv6	
MAC Address:	00-0A-EB-AC-88-16
IP Address:	59.40.0.91
Subnet Mask:	255.255.255.0
Default Gateway:	59.40.0.1
Primary DNS:	202.96.128.166
Secondary DNS:	202.96.134.133
Connection Type:	Dynamic IP

1. 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.

DHCP Server ?

DHCP: **Enable**

IP Address Pool: -

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


Default Gateway: (Optional)

Primary DNS: (Optional)

Secondary DNS: (Optional)

[Save](#)

2. 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.
3. Reset the router to factory default settings and reconfigure.

 **Note:** You'll have to reconfigure the router to access the Internet once the router is reset.

 - 1) Reset the router to factory default settings: press and hold the RESET button for about 7 seconds and then release;
 - 2) Reconfigure the router with the help of [Quick Setup](#).
4. Please refer to [Upgrade the Firmware](#) to upgrade the firmware of the router.

• **If the IP Address is 0.0.0.0, please try the methods below and try again:**

Field	Value
MAC Address:	00-0A-EB-AC-88-16
IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Default Gateway:	0.0.0.0
Primary DNS:	0.0.0.0
Secondary DNS:	0.0.0.0
Connection Type:	None

1. Check the physical connection.
Make sure the physical connection between the router and the modem is proper.
2. 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](#);
 - 3) Choose an option to your need (Enter the MAC address if [Use Custom MAC Address](#) is selected), and click [Save](#).

MAC Clone

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

[Save](#)

Tips:

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

3. 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 be conflicting 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 the problem, we need to change the LAN IP address of the router to avoid such conflict, for example, 192.168.2.1.

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

LAN

MAC Address: 40:16:9F:BF:50:8B

LAN IPv4: 192.168.2.1

Subnet Mask: 255.255.255.0

IGMP Snooping: Enable IGMP Snooping

Save

4. 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.
5. Double check the Internet Connection Type.
 - 1) Confirm your Internet Connection Type, which can be learned from the ISP;
 - 2) Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router;
 - 3) Go to [Advanced](#) > [Network](#) > [Internet](#);
 - 4) Select your [Internet Connection Type](#) and fill in other parameters with the help of page tips;
 - 5) Click [Save](#).

WAN Interface

Internet Connection Type: Dynamic IP

IP Address: Dynamic IP

Subnet Mask: Static IP

Default Gateway: PPPoE

Renew Release

Advanced

MAC Clone

Use Default MAC Address

Use Current Computer MAC Address

Use Custom MAC Address

Save

- 6) Power cycle the modem and the TP-LINK router again.
3. Please refer to [Upgrade the Firmware](#) to upgrade the firmware of the router.
4. Check the TCP/IP settings on the particular device if all other devices can get Internet from 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:

1. Make sure the wireless function 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.
2. 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](#).
- 7) Connect to wireless network.

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

1. Check the wireless LEDs on your wireless router/modem;
2. Make sure your computer/device is still in the range of your router/modem, move closer if it is currently too far away;
3. Go to [Advanced](#) > [Wireless](#) > [Wireless Settings](#), and check the wireless router settings, double check your Wireless Network Name, make sure the wireless is not hidid;

Settings
?

Region: United States ▼

Smart Connect

Smart Connect: Enable

Save

Wireless 2.4GHz | 5GHz-1 | 5GHz-2

Wireless Radio: Enable

Wireless Network Name (SSID): TP-LINK_508B Hide SSID

Security: WPA/WPA2 Personal(Recommended) ▼

Version: Auto WPA2-PSK

Encryption: Auto TKIP AES

Password: 12345670

Mode: 802.11bgn mixed ▼

Channel: Auto ▼

Channel Width: Auto ▼

Transmit Power: Low Middle High

Save

4. Connect to wireless network.

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

- Authenticating problem, password mismatch:

1. Sometimes it will ask you 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 on saying [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.
4. Connect to wireless network.

- Windows was unable to connect to XXXX /Can not join this network/Taking longer than usual to connect to this network:
 1. Check the wireless signal strength of your network, if it is weak (1~3 bars), please move the router closer and try again;
 2. Change the wireless Channel of the router to 1,6,or 11 to reduce interference from other networks;
 3. Re-install or update the driver for your wireless adapter of the computer;
 4. Connect to wireless network.

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.

<http://www.tp-link.com>

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

The device operates in 5.15 ~ 5.25GHz / 5.745 ~ 5.85 GHz frequency range. It is restricted in indoor environment only. This device meets all the other requirements specified in Part 15E, Section 15.407 of the FCC Rules.

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.

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.

Restricted to indoor use.

Canadian Compliance Statement

This device complies with Industry Canada license-exempt RSSs. 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, et
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

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.

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 32cm 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 32 cm de distance entre la source de rayonnement et votre corps.

Industry Canada Statement

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

Korea Warning Statements:

당해 무선설비는 운용중 전파혼신 가능성이 있음.

NCC Notice & BSMI Notice:

注意！

依據 低功率電波輻射性電機管理辦法

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


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

減少電磁波影響，請妥適使用。

安全諮詢及注意事項

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

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.

This product can be used in the following countries:

AT	BG	BY	CA	CZ	DE	DK	EE
ES	FI	FR	GB	GR	HU	IE	IT
LT	LV	MT	NL	NO	PL	PT	RO
RU	SE	SG	SK	TR	UA	US	