

Create Profile [X]

Basic Info | Content Filter | **Time Controls**

Time Controls

Set internet access time for the profile.

Internet Allowed Time
Set the time period when internet access is allowed.

[+ Edit Time](#)

Time Limits
Set daily limits for the total time spent online.

Mon-Fri ☒ 30min 8h

Sat-Sun ☒ 30min 8h

[BACK](#) [SAVE](#)

- 1) Click [Edit Time](#) to select the [Internet Allowed Time](#), devices under this profile can only access internet during the specified period.

Edit Internet Allowed Time [X]

Click or drag to select timeslots.

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
12 AM							
1 AM							
2 AM							
3 AM							
4 AM							
5 AM							
6 AM							
7 AM							
8 AM							
9 AM							
10 AM							
11 AM							
12 PM							
1 PM							
2 PM							
3 PM							
4 PM							
5 PM							
6 PM							
7 PM							
8 PM							
9 PM							
10 PM							
11 PM							
12 AM							

[Select All](#) [Revert](#)

SUN 6 PM - 10 PM [-](#)

MON 6 PM - 10 PM [-](#)

TUE 6 PM - 10 PM [-](#)

WED 6 PM - 10 PM [-](#)

THU 6 PM - 10 PM [-](#)

FRI 6 PM - 10 PM [-](#)

SAT 6 PM - 10 PM [-](#)

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

☒ Access Allowed ☐ Access Denied

- 2) Enable [Time Limits](#) on Monday to Friday and Saturday & Sunday, and set the total time limit for the profile each day.

Time Limits
Set daily limits for the total time spent online.

Mon-Fri ☒ 30min 1h 8h

Sat-Sun ☒ 30min 2h 8h

CANCEL SAVE

3) Save the settings.

Done!

The amount of time your child spends online is controlled and inappropriate content is blocked on their devices.

8.2. Monitoring Internet Usage

Parental Controls allows you to easily monitor the internet usage of you kids, you can pause the internet at any time, and check which websites your kids have visited and how much time they have spent online recently, then you can configure parental controls rules accordingly to protect your kids from malicious content.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > Parental Controls**, locate the **Profiles** area, you can see how much time each profile has spent.

Note: If you have not set up a profile for your child yet, add a profile by referring to [Setting Up Access Restrictions](#).

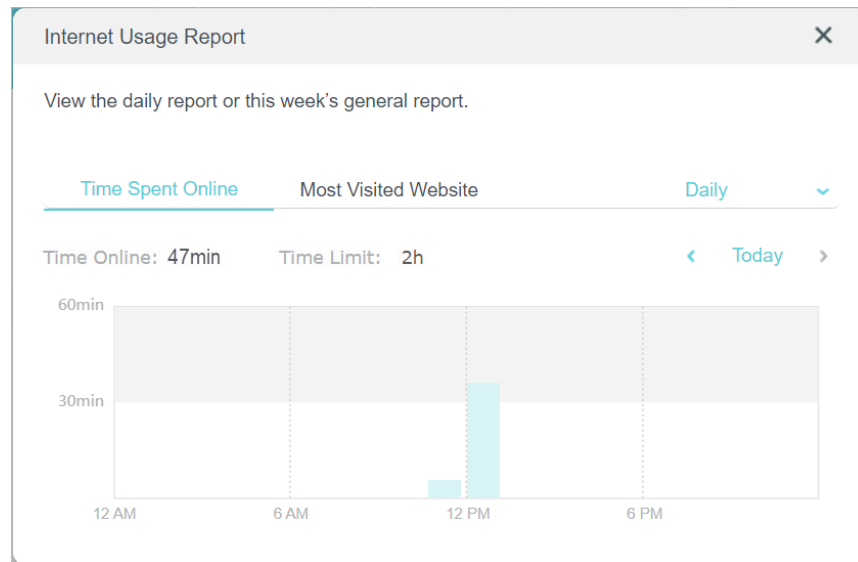
Profiles
Create a profile to manage devices of family members.

+ Add

Profile Name	Time Online/Limit	Internet Access	Action
Son	0 / 30min	Access Denied	
Daughter	0 / 2h	Access Allowed	

- Click / to pause/resume internet access for a profile at any time as you like.
- Click to edit the profile like adding devices, filtering content and changing time limits.

- Click  to view the detailed reports of internet usage like time spend online and most visited websites.



- Click the  to delete this profile.

Chapter 9

QoS

QoS (Quality of Service) allows you to prioritize the internet traffic of specific devices to guarantee a faster connection when you need it the most. Devices set as high priority will be allocated more bandwidth even when there is heavy traffic on the network.

I want to:

Ensure a fast connection for a device when I need it the most.

How can I do that?

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [QoS](#).
3. Configure global QoS settings.

Global Settings

Prioritize the Internet traffic of specific device to guarantee a faster connection.

QoS: ☒ Enable

Upload Bandwidth: Mbps

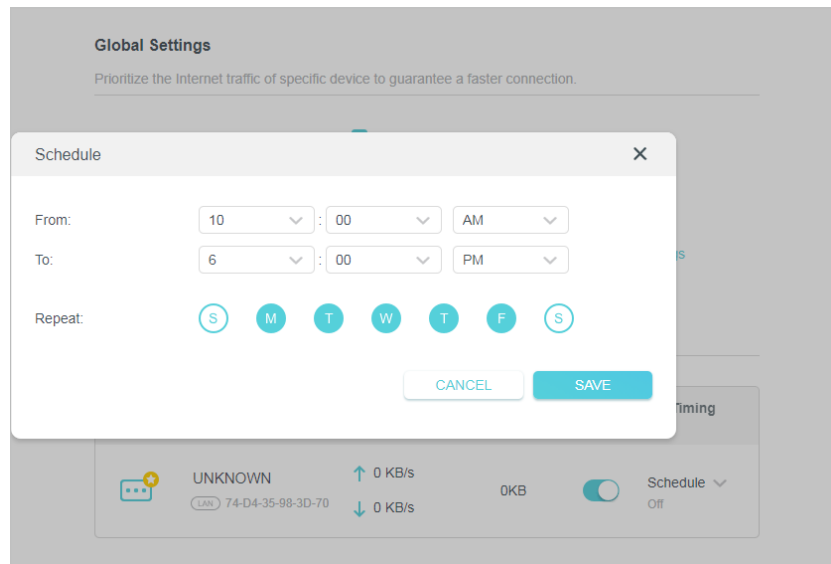
Download Bandwidth: Mbps

- 1) Enable [QoS](#).
- 2) Enter the maximum upload and download bandwidth provided by your internet service provider.
- 3) Save the settings.
4. Set the device priority.
 - 1) In the [Device Priority](#) section, find your desired device and toggle on [Priority](#).
 - 2) Set [Timing](#) according to your needs.

Type	Information	Real-time Rate	Traffic Usage	Priority	Timing
	 1A-1B-88-1C-10-96	↑ 0 KB/s ↓ 0 KB/s	0KB	☒	Always ▾
	 FC-AA-14-55-FB-5D	↑ 0 KB/s ↓ 0 KB/s	0KB	☒	2 hours ▾ 1 h 59 min Remaining
	 FC-AA-14-55-FB-5D	↑ 0 KB/s ↓ 0 KB/s	0KB	☒	Schedule ▾ Off

- To prioritize your device at any time, click the entry in the [Timing](#) column and choose [Always](#).
- To prioritize your device for next few hours, click the entry in the [Timing](#) column and choose the desired duration (like [2 hours](#)).

- To prioritize your device at specific time, click the entry in the **Timing** column and choose **Schedule**, then specify the time period and the days you wan to repeat.



Done! You can now enjoy using your device when you need it the most.

Chapter 10

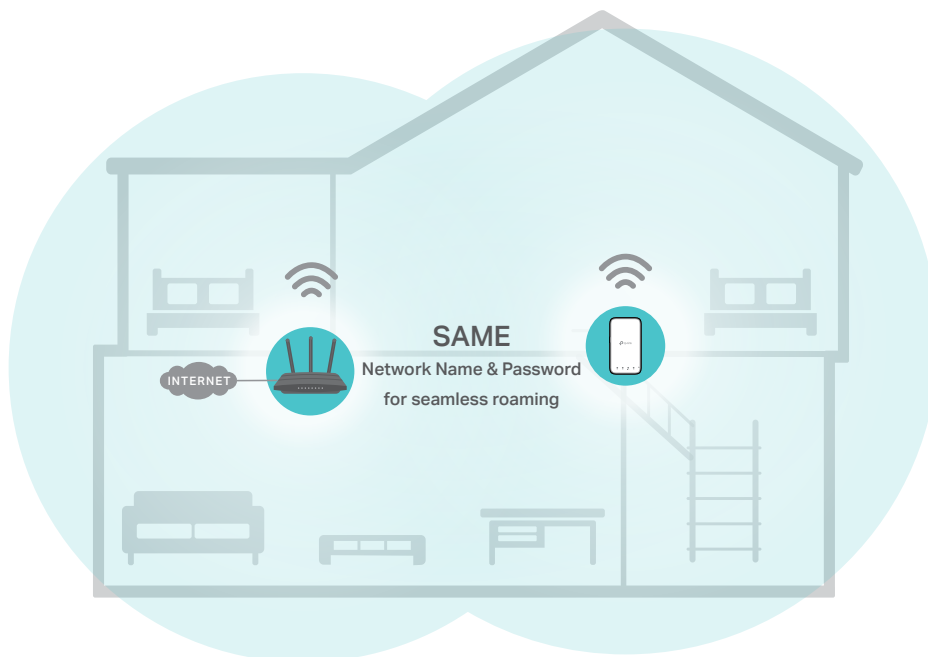
OneMesh with Seamless Roaming

This chapter introduces the TP-Link OneMesh™ feature.

It contains the following sections:

- [Set Up a OneMesh Network](#)
- [Manage Devices in the OneMesh Network](#)

TP-Link OneMesh  router and TP-Link OneMesh  extenders work together to form one unified Wi-Fi network. Walk through your home and stay connected with the fastest possible speeds thanks to OneMesh's seamless coverage.



Unified Wi-Fi Network

Router and extenders share the same wireless settings, including network name, password, access control settings and more.

Seamless Roaming

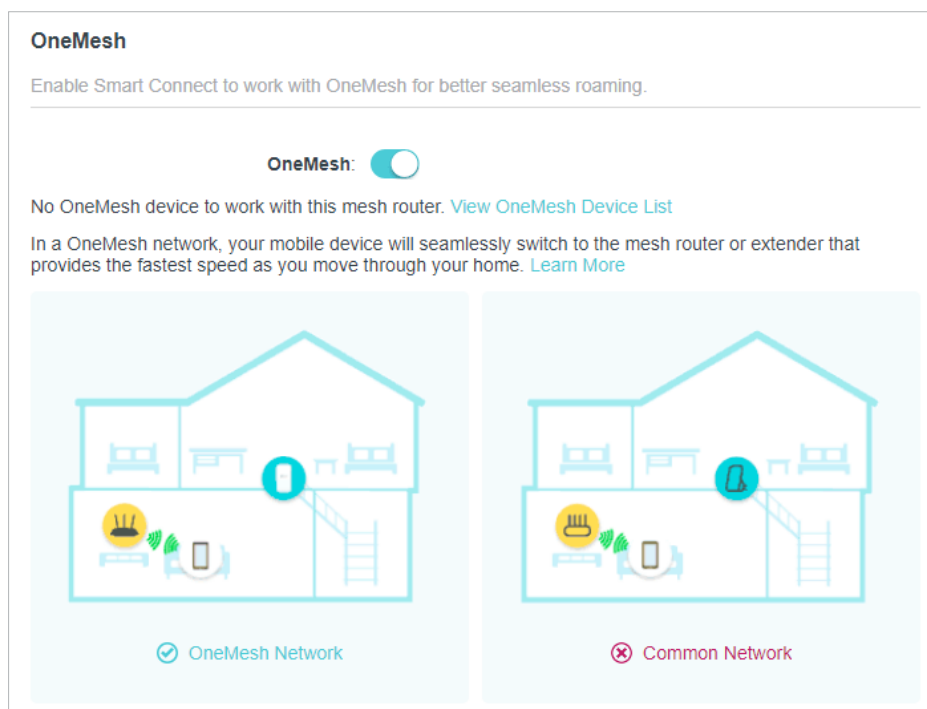
Devices automatically switch between your router and extenders as you move through your home for the fastest possible speeds.

Easy Setup and Management

Set up a OneMesh network with a push of WPS buttons. Manage all network devices on the Tether app or at your router's web management page.

10. 1. Set Up a OneMesh Network

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced > OneMesh](#).
3. Enable [OneMesh](#).



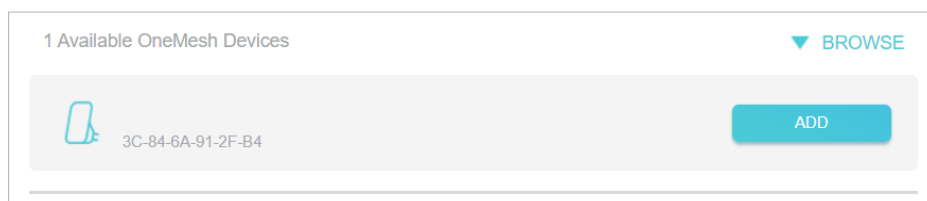
4. Connect a OneMesh extender to this router by following the setup instructions in the extender's manual. The extender will be listed on the router's [OneMesh](#) page.

■ Note: To check full list of TP-Link OneMesh devices, visit <https://www.tp-link.com/onemesh/compatibility>.

5. If you have set up the extender to join the OneMesh network, it will be listed on the router's [OneMesh](#) page.



Otherwise, you need to find it in the [Available OneMesh Devices](#) list and click [Add](#) to add it to the OneMesh network.



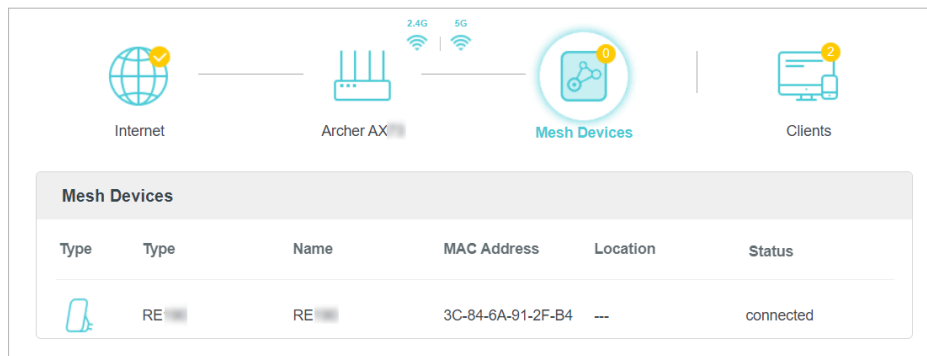
Done! Now your router and extender successfully form a OneMesh network!

10.2. Manage Devices in the OneMesh Network

In a OneMesh network, you can manage all mesh devices and connected clients on your router's web page.

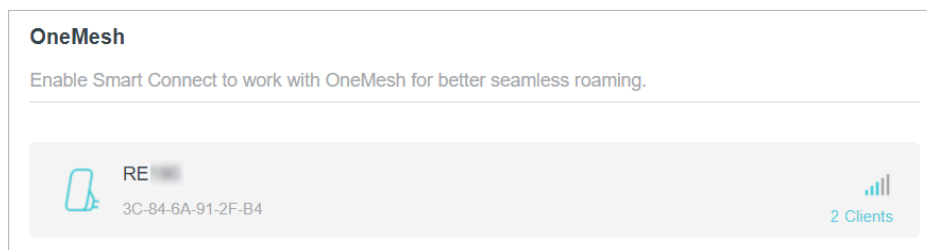
- **To view mesh devices and connected clients in the network:**

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Network Map](#).
3. Click  to view all mesh devices, and click  to view all connected clients.



- **To manage a OneMesh device in the network:**

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [OneMesh](#).



3. Click the OneMesh device to view detailed information.

RE

Name:

Location:

- Please Select -

SAVE

IP Address: 192.168.0.50

MAC Address: 3C-84-6A-91-2F-B4

Signal Strength:

Link Speed: 130Mbps (2.4GHz) 0Kbps (5GHz)

Leave OneMesh

Clients

ID	Device Name	IP Address/MAC Address
1	My-iPhone	C4-61-8B-CE-BF-32 192.168.0.56
2	My-PC	BB-C1-8E-BE-BF-33 192.168.0.58

Manage Device

4. Manage the OneMesh device as needed. You can:

- Change device information.
- Click [Manage Device](#) to redirect to the web management page of this device.
- Click [Leave OneMesh](#) to delete this device from the OneMesh network.

Chapter 11

Network Security

This chapter guides you on how to protect your home network from cyber attacks and unauthorized users by implementing these three network security functions. You can protect your home network from cyber attacks, block or allow specific client devices to access your network using Access Control, or you can prevent ARP spoofing and ARP attacks using IP & MAC Binding.

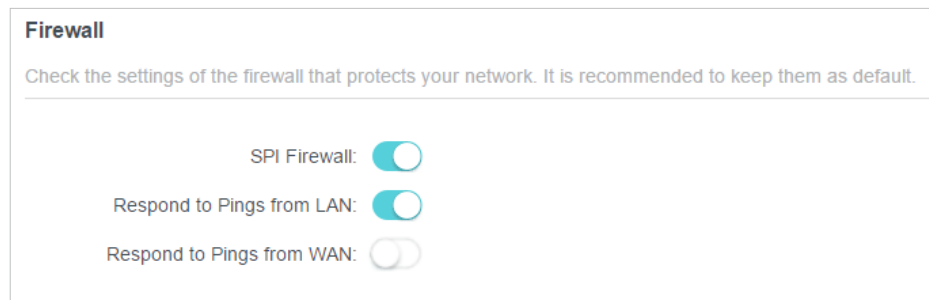
It contains the following sections:

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

11.1. Protect the Network from Cyber Attacks

The SPI (Stateful Packet Inspection) Firewall protects the router from cyber attacks and validate the traffic that is passing through the router based on the protocol. This function is enabled by default.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [Security](#) > [Firewall](#). It's recommended to keep the default settings.



11.2. 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 your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [Security](#) > [Access Control](#).
3. Toggle on to 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](#).

Access Control

Control the access to your network from the specified devices.

Access Control: ☒

Access Mode: ☒ Blacklist
 Configure a blacklist to only block access to your network from the specified devices.

☐ Whitelist

- 2) Click  **Add** and select devices you want to be blocked and Click **ADD**.
- 3) The **Operation Succeeded** message will appear on the screen, which means the selected devices have been successfully added to the blacklist.

Device Type	Device Name	MAC Address	Modify
	Yan	38-CA-DA-3A-D8-B1	

To allow specific device(s):

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

Access Control

Control the access to your network from the specified devices.

Access Control: ☒

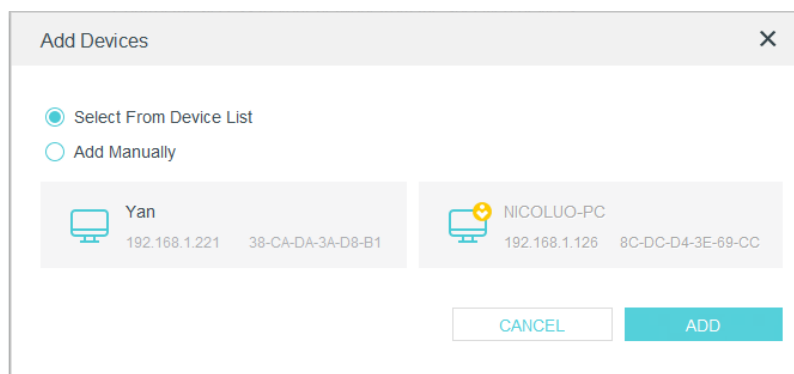
Access Mode: ☐ Blacklist
☒ Whitelist
 Configure a whitelist to only allow access to your network from the specified devices.

- 2) Your own device is in the whitelist by default and cannot be deleted. Click  **Add** to add other devices to the whitelist.

Device Type	Device Name	MAC Address	Modify
	UNKNOWN	00-19-66-35-E1-B0	

- **Add connected devices**

- 1) Click **Select From Device List**.
- 2) Select the devices you want to be allowed and click **ADD**.

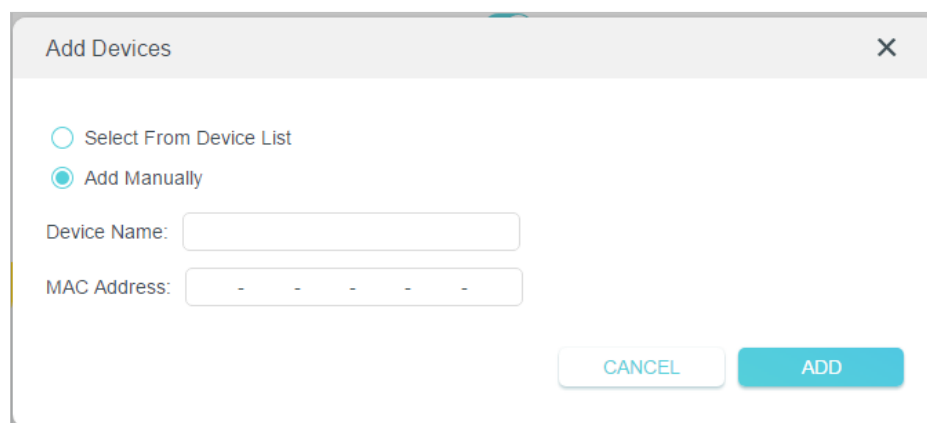


3) The **Operation Succeeded** message will appear on the screen, which means the selected devices have been successfully added to the whitelist.

- **Add unconnected devices**

1) Click **Add Manually**.

2) Enter the **Device Name** and **MAC Address** of the device you want to be allowed and click **ADD**.



3) The **Operation Succeeded** message will appear on the screen, which means the device has been successfully added to the whitelist.

Done!

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

11.3. IP & MAC Binding

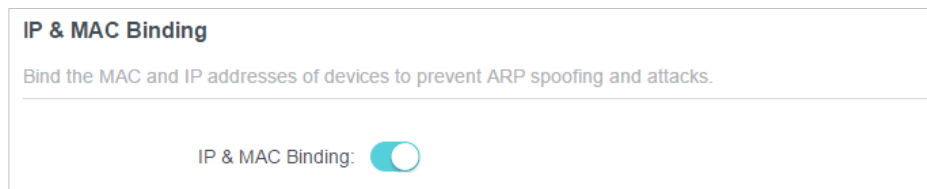
IP & MAC Binding, namely, ARP (Address Resolution Protocol) Binding, is used to bind network device's IP address to its MAC address. This will prevent ARP Spoofing and other ARP attacks by denying network access to an device with matching IP address in the Binding list, but unrecognized MAC address.

I want to:

Prevent ARP spoofing and ARP attacks.

How can I do that?

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



IP & MAC Binding

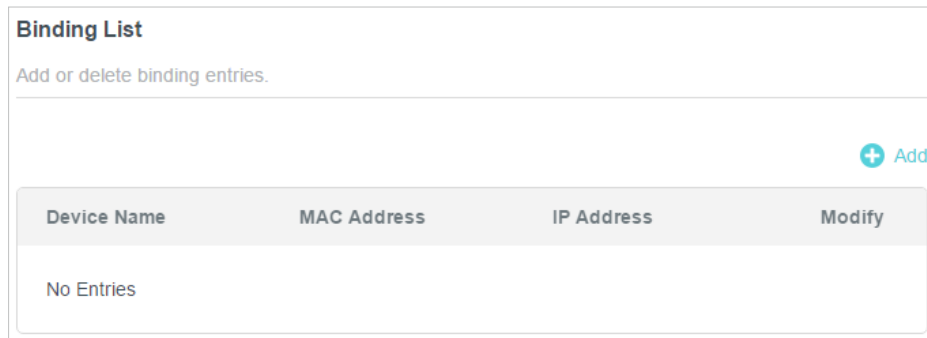
Bind the MAC and IP addresses of devices to prevent ARP spoofing and attacks.

IP & MAC Binding: ☒

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

To bind the connected device(s):

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



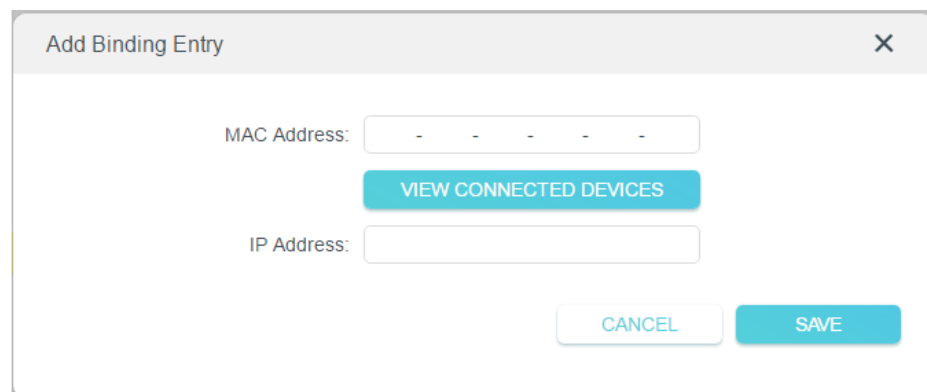
Binding List

Add or delete binding entries.

[+ Add](#)

Device Name	MAC Address	IP Address	Modify
No Entries			

- 2) Click [VIEW CONNECTED DEVICES](#) and select the device you want to bind. The [MAC Address](#) and [IP Address](#) fields will be automatically filled in.



Add Binding Entry ×

MAC Address:

[VIEW CONNECTED DEVICES](#)

IP Address:

[CANCEL](#) [SAVE](#)

- 3) Click [SAVE](#).

To bind the unconnected device:

- 1) Click  **Add** in the **Binding List** section.

Binding List
 Add or delete binding entries.

 **Add**

Device Name	MAC Address	IP Address	Modify
No Entries			

- 2) Enter the **MAC Address** and **IP Address** that you want to bind.
- 3) Click **SAVE**.

Done!

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

11.4. ALG

ALG allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc. It is recommended to keep the default settings.

You may need to disable SIP ALG when you are using voice and video applications to create and accept a call through the router, since some voice and video communication applications do not work well with SIP ALG.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > Security > ALG**.

ALG
 Check the ALG (Application Layer Gateway) settings. It is recommended to keep them as default.

PPTP Passthrough: 

L2TP Passthrough: 

IPSec Passthrough: 

FTP ALG: 

TFTP ALG: 

RTSP ALG: 

H323 ALG: 

SIP ALG: 

Chapter 12

NAT Forwarding

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

With the forwarding feature the router can penetrate the isolation of NAT and allows devices on the internet to initiatively communicate with devices on the local network, thus realizing some special functions.

The TP-Link router supports four forwarding rules. If two or more rules are set, the priority of implementation from high to low is Port Forwarding, Port Triggering, UPnP and DMZ.

It contains the following sections:

- [Share Local Resources on the Internet by Port Forwarding](#)
- [Open Ports Dynamically by Port Triggering](#)
- [Make Applications Free from Port Restriction by DMZ](#)
- [Make Xbox Online Games Run Smoothly by UPnP](#)

12.1. Share Local Resources on the Internet by Port Forwarding

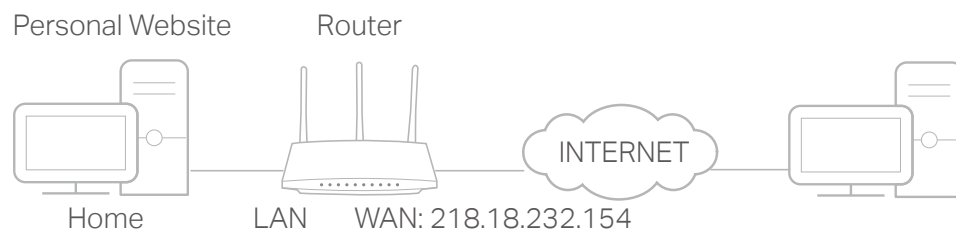
When you build up a server on the local network and want to share it on the internet, Port Forwarding can realize the service and provide it to internet users. At the same time Port Forwarding can keep the local network safe as other services are still invisible from the internet.

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

I want to:

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

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



How can I do that?

1. Assign a static IP address to your PC, for example 192.168.0.100.
2. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
3. Go to [Advanced](#) > [NAT Forwarding](#) > [Port Forwarding](#).
4. Click  [Add](#).

Port Forwarding

Specify ports to make specific devices or services on your local network accessible over the internet.

+ Add

Service Name	Device IP Address	External Port	Internal Port	Protocol	Status	Modify
No Entries						

- Click **VIEW COMMON SERVICES** and select **HTTP**. The **External Port**, **Internal Port** and **Protocol** will be automatically filled in.
- Click **VIEW CONNECTED DEVICES** and select your home PC. The **Device IP Address** will be automatically filled in. Or enter the PC's IP address 192.168.0.100 manually in the **Device IP Address** field.
- Click **SAVE**.

Add a Port Forwarding Entry X

Service Name:

VIEW COMMON SERVICES

Device IP Address:

VIEW CONNECTED DEVICES

External Port:

Internal Port:

Protocol: ▼

☒ Enable This Entry

Tips:

- It is recommended to keep the default settings of **Internal Port** and **Protocol** if you are not clear about which port and protocol to use.
- If the service you want to use is not in the common services list, you can enter the corresponding parameters manually. You should verify the port number that the service needs.
- You can add multiple port forwarding rules if you want to provide several services in a router. Please note that the **External Port** should not be overlapped.

Done!

Users on the internet can enter **http:// WAN IP** (in this example: **http:// 218.18.232.154**) to visit your personal website.

🔗 Tips:

- The WAN IP should be a public IP address. For the WAN IP is assigned dynamically by the ISP, it is recommended to apply and register a domain name for the WAN referring to [Set Up a Dynamic DNS Service Account](#). Then users on the internet can use [http:// domain name](#) to visit the website.
- 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.

12.2. Open Ports Dynamically by Port Triggering

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

Follow the steps below to configure the Port Triggering rules:

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

Port Triggering

Specify ports to allow devices on your local network to dynamically open specific external ports and forward packets (from the internet) to the device that triggered it.

 Add

Service Name	Triggering Port	Triggering Protocol	External Port	External Protocol	Status	Modify
No Entries						

3. Click **VIEW COMMON SERVICES**, and select the desired application. The **Triggering Port**, **Triggering Protocol** and **External Port** will be automatically filled in. The following picture takes application **MSN Gaming Zone** as an example.

4. Click **SAVE**.

Tips:

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

12.3. Make Applications Free from Port Restriction by DMZ

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

Note:

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

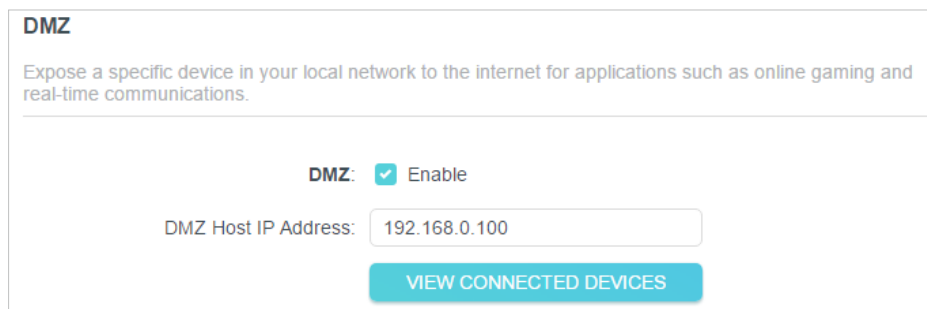
I want to:

Make the home PC join the internet online game without port restriction.

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

How can I do that?

1. Assign a static IP address to your PC, for example 192.168.0.100.
2. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
3. Go to **Advanced** > **NAT Forwarding** > **DMZ** and tick to enable DMZ.
4. Click **VIEW CONNECTED DEVICES** and select your PC. The **Device IP Address** will be automatically filled in. Or enter the PC's IP address 192.168.0.100 manually in the **DMZ Host IP Address** field.



5. Click **SAVE**.

Done!

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

12.4. Make Xbox Online Games Run Smoothly by UPnP

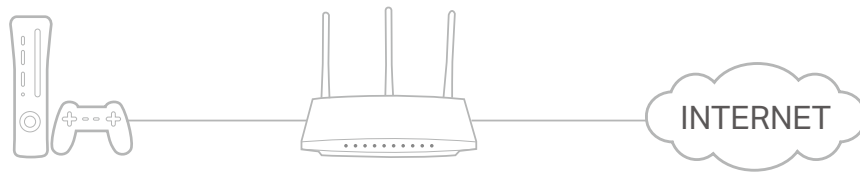
The UPnP (Universal Plug and Play) protocol allows applications or host devices to automatically find the front-end NAT device and send request to it to open the corresponding ports. With UPnP enabled, the applications or host devices on the local network and the internet can freely communicate with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

Tips:

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

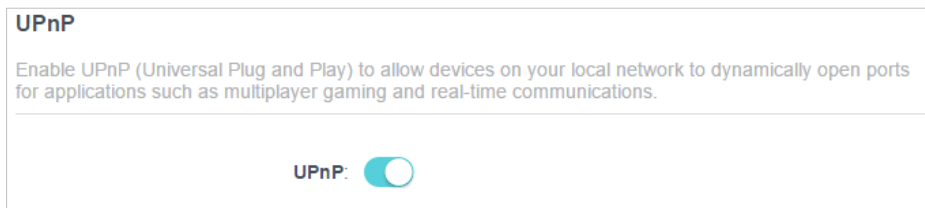
For example, when you connect your Xbox to the router which has connected to the internet to play online games, UPnP will send request to the router to open the

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



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

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



Chapter 13

VPN Server

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

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

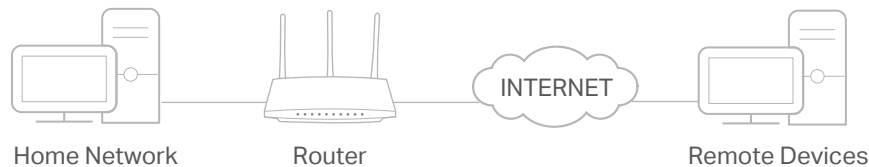
PPTP VPN is more easily used and its speed is faster, it's compatible with most operating systems and also supports mobile devices. Its security is poor and your packets may be cracked easily, and PPTP VPN connection may be prevented by some ISP.

It contains the following sections, please choose the appropriate VPN server connection type as needed.

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

13.1. Use OpenVPN to Access Your Home Network

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



Step1. Set up OpenVPN Server on Your Router

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > VPN Server > OpenVPN**, and tick the **Enable** box of **OpenVPN**.

OpenVPN
Set up an OpenVPN for secure, remote access to your network.

Note: No certificate has been created. Generate one below before enabling OpenVPN.

OpenVPN: ☒ Enable

Service Type: ☒ UDP
☐ TCP

Service Port:

VPN Subnet:

Netmask:

Client Access: ▼

Note:

- Before you enable VPN Server, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router's WAN port and synchronize your System Time with internet.
- The first time you configure the OpenVPN Server, you may need to [Generate](#) a certificate before you enable the VPN Server.

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

6. Select your **Client Access** type. Select **Home Network Only** if you only want the remote device to access your home network; select **Internet and Home Network** if you also want the remote device to access internet through the VPN Server.
7. Click **SAVE**.
8. Click **GENERATE** to get a new certificate.

Certificate
Generate the certificate.

GENERATE

■ **Note:** If you have already generated one, please skip this step, or click **GENERATE** to update the certificate.

9. Click **EXPORT** to save the OpenVPN configuration file which will be used by the remote device to access your router.

Configuration File
Export the configuration file.

EXPORT

Step 2. Configure OpenVPN Connection on Your Remote Device

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

■ **Note:** You need to install the **OpenVPN** client utility on each device that you plan to apply the VPN function to access your router. Mobile devices should download a third-party app from Google Play or Apple App Store.

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

13. 2. Use PPTP VPN to Access Your Home Network

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

Step 1. Set up PPTP VPN Server on Your Router

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.

2. Go to [Advanced](#) > [VPN Server](#) > [PPTP](#), and tick the [Enable](#) box of [PPTP](#).

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

3. In the [Client IP Address](#) field, enter the range of IP addresses (up to 10) that can be leased to the devices by the PPTP VPN server.

4. Set the PPTP connection permission according to your needs.

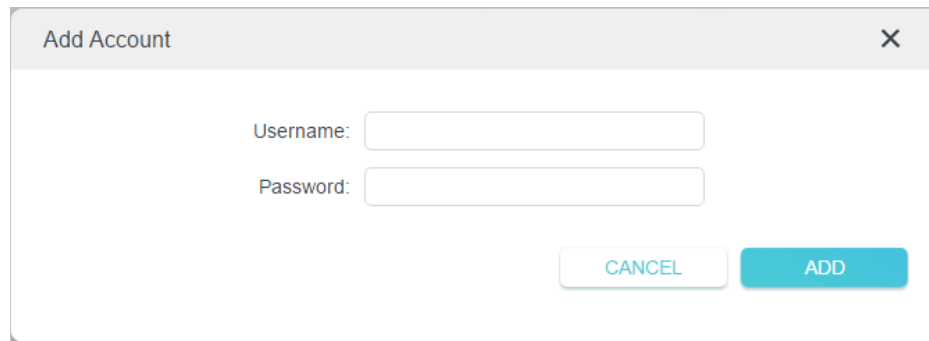
- Select [Allow Samba \(Network Place\) access](#) to allow your VPN device to access your local Samba server.
- Select [Allow NetBIOS passthrough](#) to allow your VPN device to access your Samba server using NetBIOS name.
- Select [Allow Unencrypted connections](#) to allow unencrypted connections to your VPN server.

5. Click [SAVE](#).

6. Configure the PPTP VPN connection account for the remote device. You can create up to 16 accounts.

1) Click [+ Add](#).

2) Enter the [Username](#) and [Password](#) to authenticate devices to the PPTP VPN Server.

A dialog box titled "Add Account" with a close button (X) in the top right corner. It contains two input fields: "Username:" and "Password:". Below the fields are two buttons: "CANCEL" and "ADD".

Add Account

Username:

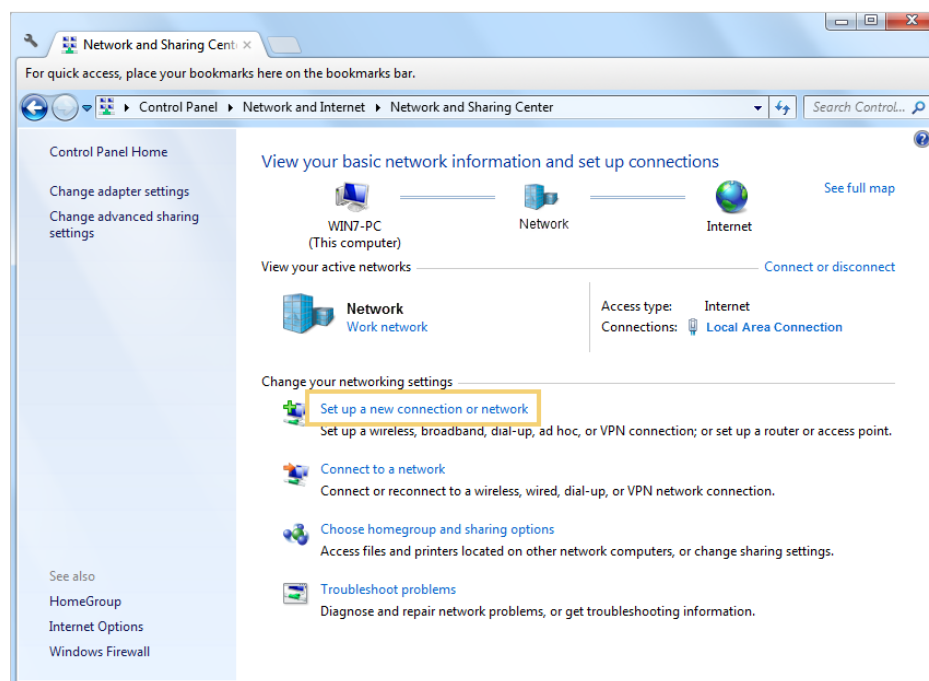
Password:

3) Click **ADD**.

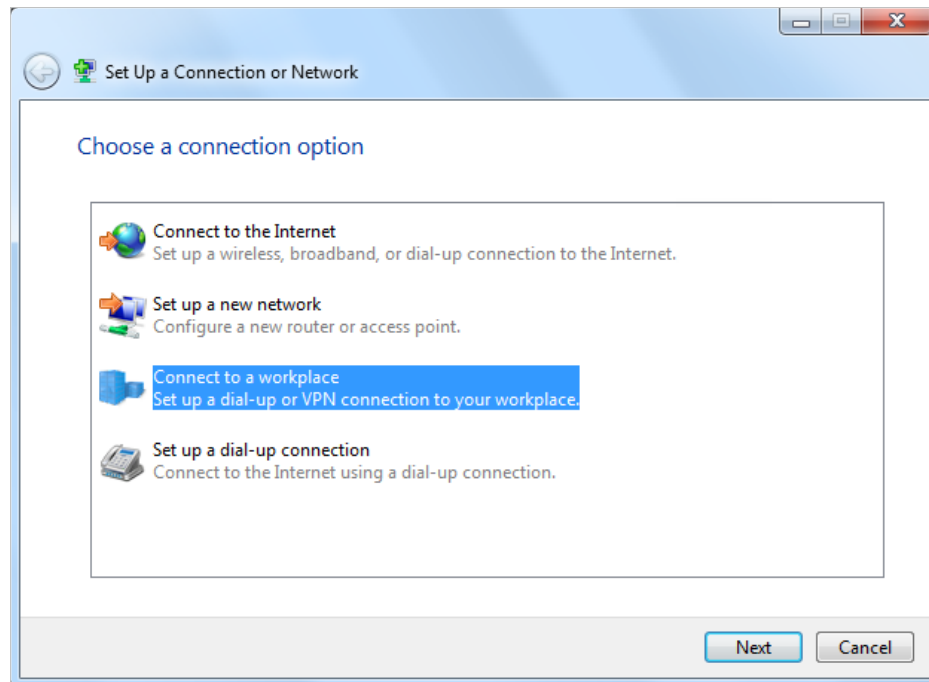
Step 2. Configure PPTP VPN Connection on Your Remote Device

The remote device can use the Windows built-in PPTP software or a third-party PPTP software to connect to PPTP Server. Here we use the [Windows built-in PPTP software](#) as an example.

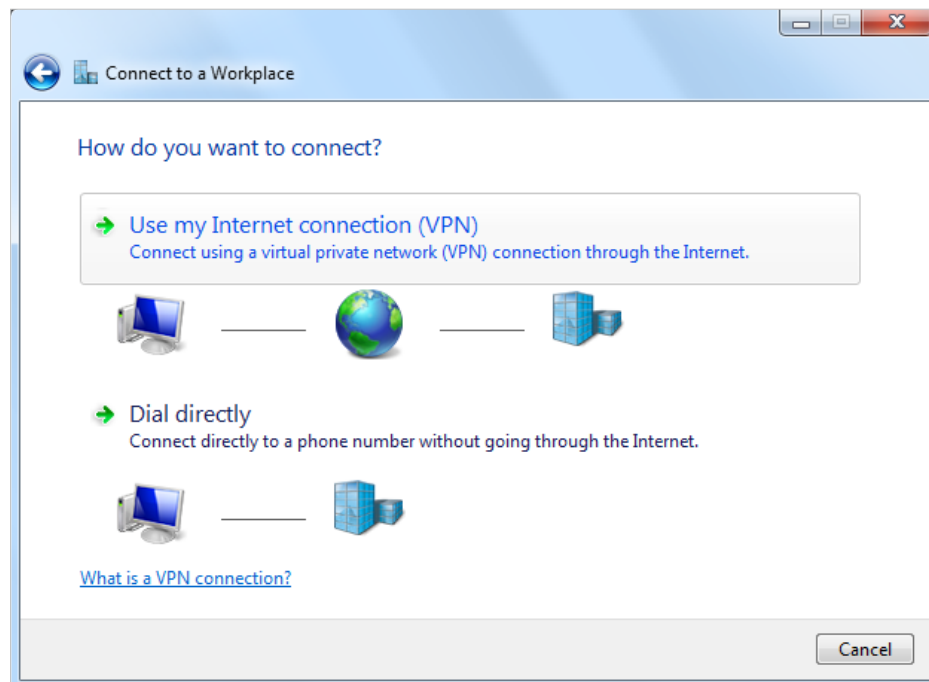
1. Go to [Start > Control Panel > Network and Internet > Network and Sharing Center](#).
2. Select [Set up a new connection or network](#).



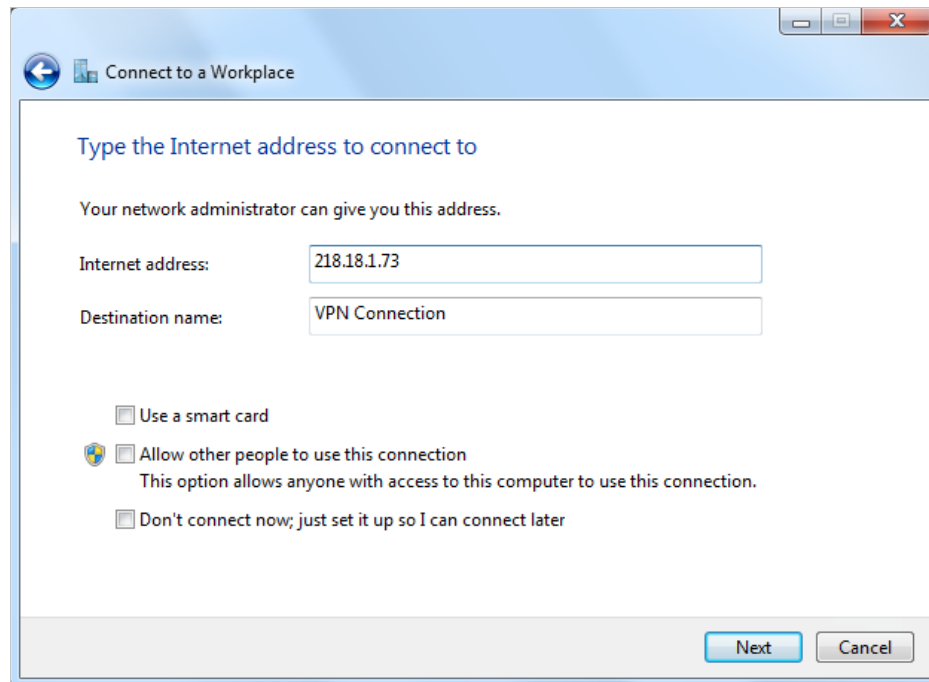
3. Select [Connect to a workplace](#) and click **Next**.



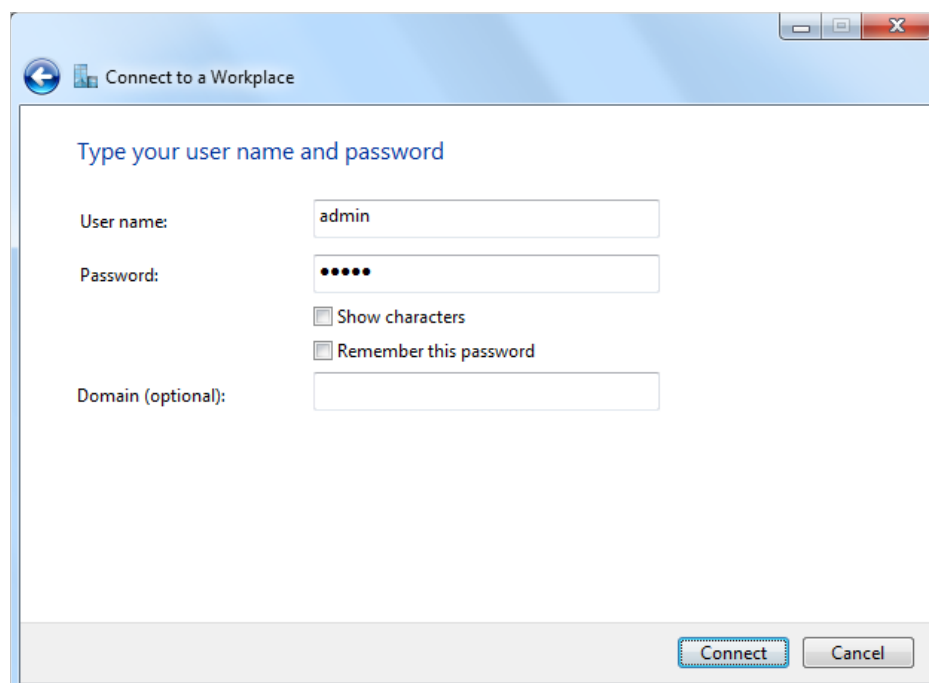
4. Select **Use my Internet connection (VPN)**.



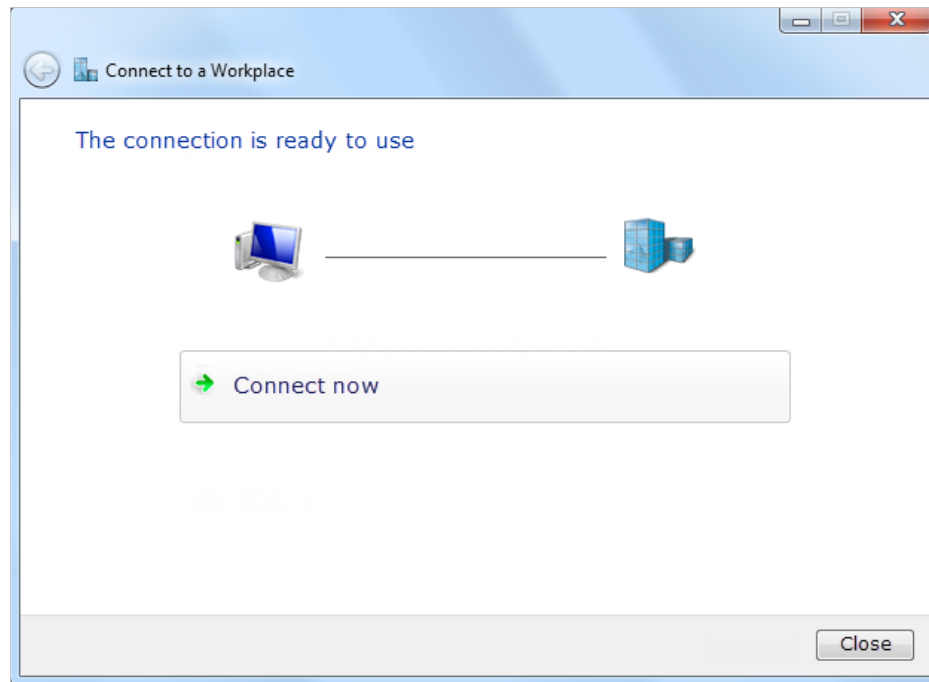
5. Enter the internet IP address of the router (for example: 218.18.1.73) in the **Internet address** field. Click **Next**.



6. Enter the **User name** and **Password** you have set for the PPTP VPN server on your router, and click **Connect**.



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



Chapter 14

Customize Your Network Settings

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

It 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](#)

14. 1. Change the LAN Settings

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

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



4. Click [SAVE](#).

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

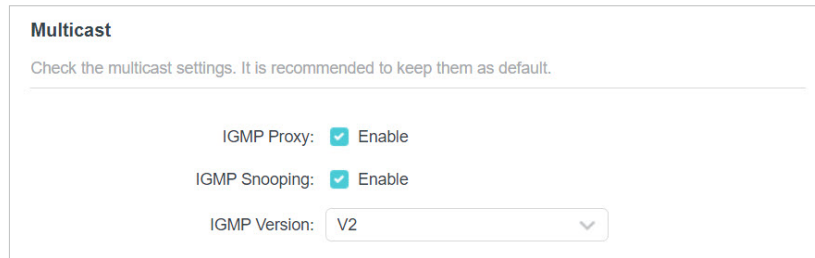
14. 2. Configure to Support IPTV Service

I want to:

Configure IPTV setup to enable Internet/IPTV/Phone service provided by my internet service provider (ISP).

How can I do that?

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



Multicast

Check the multicast settings. It is recommended to keep them as default.

IGMP Proxy: ☒ Enable

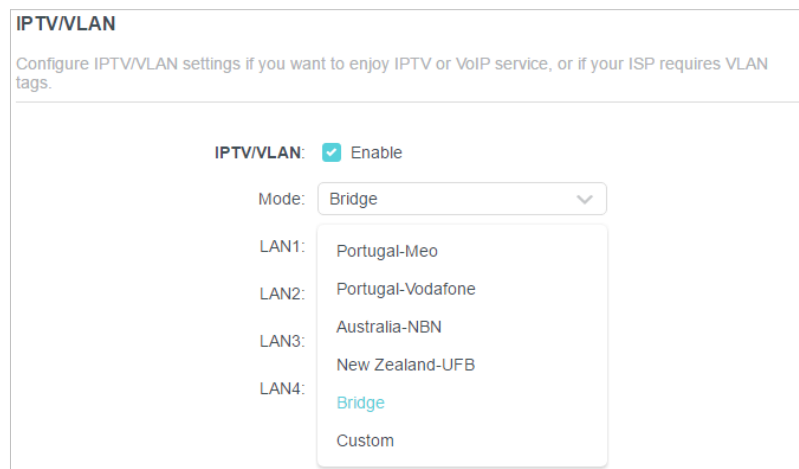
IGMP Snooping: ☒ Enable

IGMP Version: V2

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

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

- 1) Tick [Enable IPTV/VLAN](#).
- 2) Select the appropriate [Mode](#) according to your ISP.
 - Select [Bridge](#) if your ISP is not listed and no other parameters are required.
 - Select [Custom](#) if your ISP is not listed but provides necessary parameters.



IPTV/VLAN

Configure IPTV/VLAN settings if you want to enjoy IPTV or VoIP service, or if your ISP requires VLAN tags.

IPTV/VLAN: ☒ Enable

Mode: Bridge

LAN1: Portugal-Meo

LAN2: Portugal-Vodafone

LAN3: Australia-NBN

LAN4: New Zealand-UFB

Bridge

Custom

- 3) After you have selected a mode, the necessary parameters, including the LAN port for IPTV connection, are predetermined. If not, select the LAN type to determine which port is used to support IPTV service.
- 4) Click [SAVE](#).
- 5) Connect the set-top box to the corresponding LAN port which is predetermined or you have specified in Step 3.

Done!

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

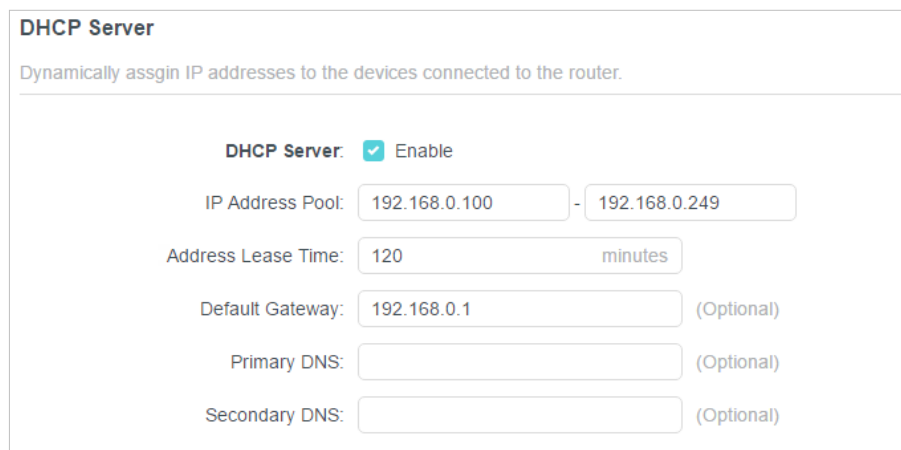
14.3. Specify DHCP Server Settings

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

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.

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

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



DHCP Server
Dynamically assign IP addresses to the devices connected to the router.

DHCP Server: ☒ Enable

IP Address Pool: 192.168.0.100 - 192.168.0.249

Address Lease Time: 120 minutes

Default Gateway: 192.168.0.1 (Optional)

Primary DNS: (Optional)

Secondary DNS: (Optional)

1. Tick the [Enable](#) checkbox.

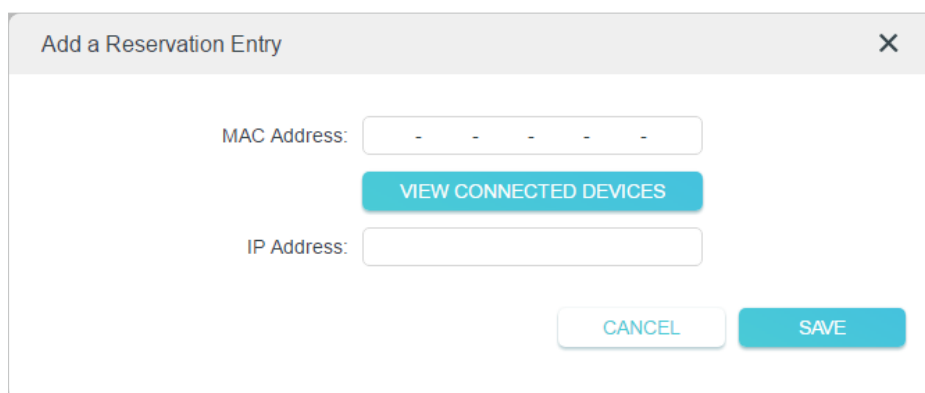
2. Enter the starting and ending IP addresses in the [IP Address Pool](#).

3. Enter other parameters if the ISP offers. The [Default Gateway](#) is automatically filled in and is the same as the LAN IP address of the router.

4. Click [SAVE](#).

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

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



Add a Reservation Entry X

MAC Address: - - - - -

[VIEW CONNECTED DEVICES](#)

IP Address:

[CANCEL](#) [SAVE](#)

2. Click [VIEW CONNECTED DEVICES](#) and select the you device you want to reserve an IP for. Then the [MAC Address](#) will be automatically filled in. Or enter the [MAC address](#) of the client device manually.
3. Enter the [IP address](#) to reserve for the client device.
4. Click [SAVE](#).

14.4. Set Up a Dynamic DNS Service Account

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

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

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [Network](#) > [Dynamic DNS](#).
3. Select the DDNS [Service Provider](#): TP-Link, NO-IP or DynDNS. It is recommended to select TP-Link so that you can enjoy TP-Link's superior DDNS service. Otherwise, please select NO-IP or DynDNS. If you don't have a DDNS account, you have to register first by clicking [Register Now](#).

Dynamic DNS
Assign a fixed host name (domain name) for remote access to your device, website, or server behind the router.

Service Provider: TP-Link 

Note: To enjoy TP-Link's DDNS service, you have to log in with a TP-Link ID. If you have not logged in with one, click [log in](#).

4. Click [Register](#) in the [Domain Name List](#) if you have selected TP-Link, and enter the [Domain Name](#) as needed.

Dynamic DNS

Assign a fixed host name (domain name) for remote access to your device, website, or server behind the router.

Service Provider:

TP-Link

Current Domain Name:

Domain Name List

+ Register

Domain Name	Registered Date	Status	Operation	Delete
No Entries				

If you have selected NO-IP or DynDNS, enter the username, password and domain name of your account.

Dynamic DNS

Assign a fixed host name (domain name) for remote access to your device, website, or server behind the router.

Service Provider:

NO-IP

Register Now

Username:

Password:

Domain Name:

WAN IP binding:
☐ Enable

Status: Not launching

LOGIN AND SAVE

LOGOUT

5. Click **LOGIN AND SAVE**.

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

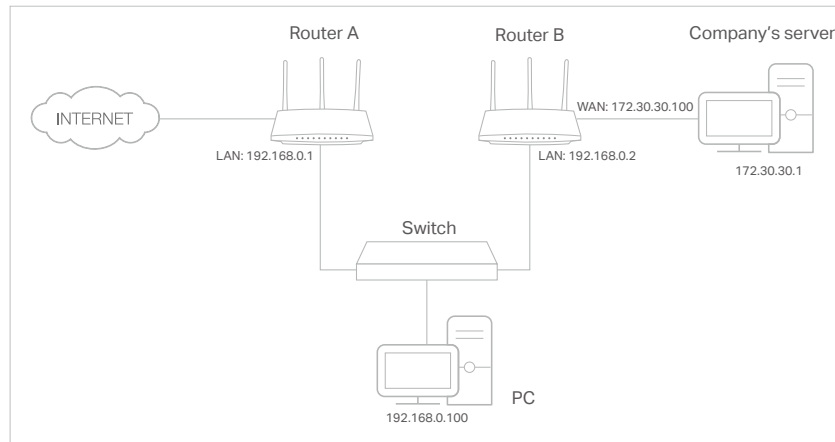
14.5. Create Static Routes

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

I want to:

Visit multiple networks and servers at the same time.

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



How can I do that?

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

Add a Routing Entry

Network Destination:

172.30.30.1

Subnet Mask:

255.255.255.255

Default Gateway:

192.168.0.2

Interface:

LAN/WLAN

Description:

Company

CANCEL

SAVE

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

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

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

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

Description: Enter a description for this static routing entry.

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

Routing Table			
View all valid routing entries that are currently in use.			
Active Route Number: 3			 Refresh
Network Destination	Subnet Mask	Gateway	Interface
172.30.30.1	255.255.255.255	192.168.0.2	LAN
192.168.0.0	255.255.255.0	0.0.0.0	LAN
0.0.0.0	0.0.0.0	0.0.0.0	WAN

Done!

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

Chapter 15

Manage the Router

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

It contains the following sections:

- [Update the Firmware](#)
- [Backup and Restore Configuration Settings](#)
- [Change the Login Password](#)
- [Password Recovery](#)
- [Local Management](#)
- [Remote Management](#)
- [System Log](#)
- [Test the Network Connectivity](#)
- [Set System Time and Language](#)
- [Set the Router to Reboot Regularly](#)
- [Control the LED](#)

15.1. Update the Firmware

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

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

Note:

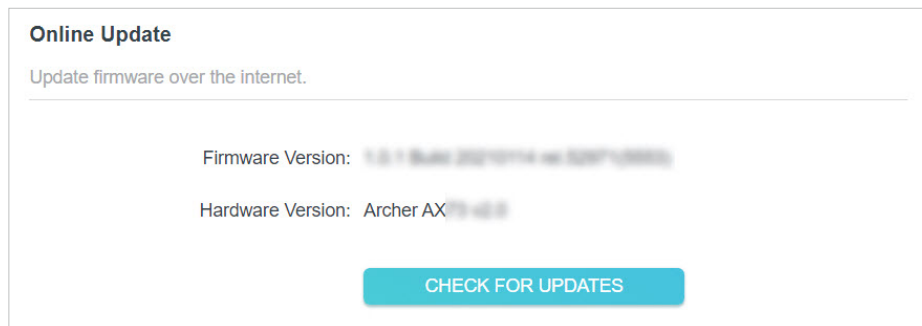
- Back up your router's configurations before firmware update.
- Do NOT turn off the router during the firmware update.

15.1.1. Online Update

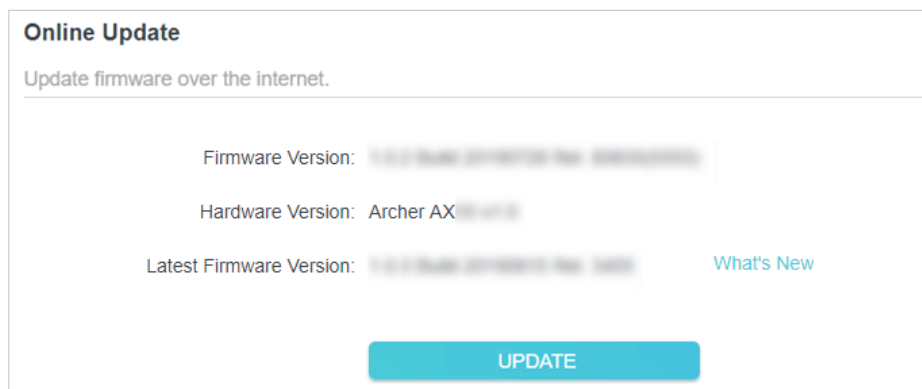
1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.

2. When the latest firmware is available for your router, the update icon  will display in the top-right corner of the page. Click the icon to go to the [Firmware Update](#) page.

Alternatively, you can go to [Advanced](#) > [System](#) > [Firmware Update](#), and click [CHECK FOR UPDATES](#) to see whether the latest firmware is released.



3. Focus on the [Online Update](#) section, and click [UPDATE](#) if there is new firmware.

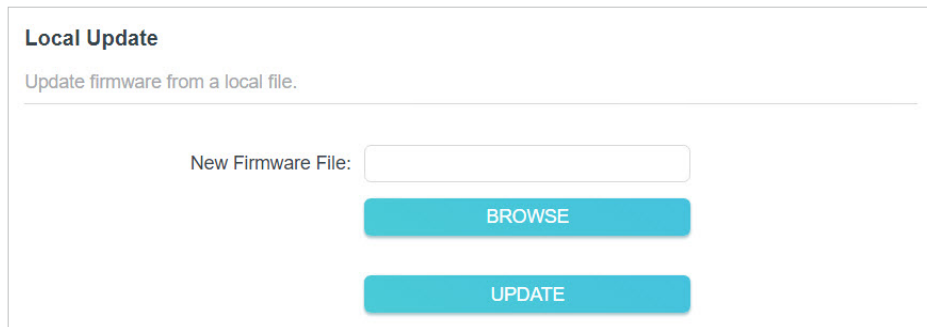


4. Wait a few minutes for the update and reboot to complete.

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

15.1.2. Local Update

1. Download the latest firmware file for the router from www.tp-link.com.
2. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
3. Go to [Advanced](#) > [System](#) > [Firmware Update](#).
4. Focus on the [Local Update](#) section. Click [BROWSE](#) to locate the downloaded new firmware file, and click [UPDATE](#).



The screenshot shows the 'Local Update' section of the router's web interface. It has a title 'Local Update' and a subtitle 'Update firmware from a local file.' Below this, there is a text input field labeled 'New Firmware File:'. Underneath the input field are two blue buttons: 'BROWSE' and 'UPDATE'.

5. Wait a few minutes for the update and reboot to complete.

■ **Note:** If you fail to update the firmware for the router, please contact our [Technical Support](#).

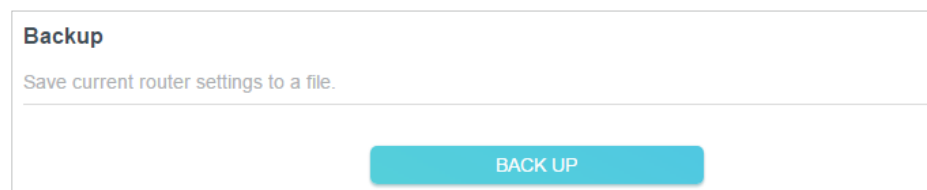
15.2. Backup and Restore Configuration Settings

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

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

- **To backup configuration settings:**

Click [BACK UP](#) 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 the 'Backup' section of the router's web interface. It has a title 'Backup' and a subtitle 'Save current router settings to a file.' Below this, there is a single blue button labeled 'BACK UP'.

- **To restore configuration settings:**