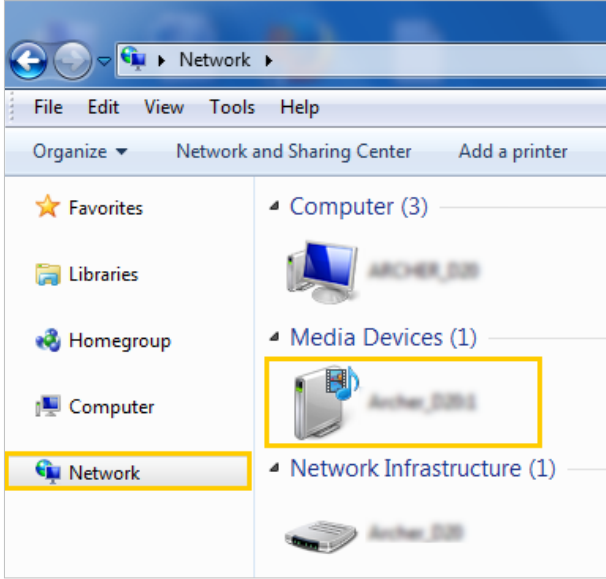


<p><b>Windows Computer</b></p>	<ul style="list-style-type: none"> <li>Go to <b>Computer</b> &gt; <b>Network</b>, then click the Media Server Name (<u>Model number-share</u> by default) in the <b>Media Devices</b> section.</li> </ul> <p>Note: Here we take Windows 7 as an example.</p> 
<p><b>Tablet</b></p>	<ul style="list-style-type: none"> <li>Use a third-party DLNA-supported player.</li> </ul>

## 7.3. Time Machine

Time Machine backs up all files on your Mac computer to a USB storage device connected to your router.

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

**Time Machine**

Back up all files on your Mac to a USB storage device connected to your router.

---

**Time Machine:** ☒ Enable


Backup Location:

**SELECT**

Storage Limit for Backups:  GB

(Enter "0" for no limit.)

- Tick the checkbox to enable **Time Machine**.

4. Click **SELECT** to select a location for Time Machine backups.
5. Set the **Storage Limit for Backups**.  
 **Note:** 0 means no limit for the space.
6. Click **SAVE**.

## Chapter 8

---

# HomeCare™ – Parental Controls, QoS, Antivirus

---

TP-Link HomeCare™ powered by Trend Micro™ provides a kit of features to help you create a personalized network that caters for the whole family. You can ensure appropriate internet access for everyone with Parental Controls, save bandwidth for the things that matter with QoS and keep your network secure with built-in Antivirus.

It contains the following sections:

- [Parental Controls](#)
- [QoS](#)
- [Antivirus](#)

## 8.1. Parental Controls


Parental Controls allows you to set up unique restrictions on internet access for each member of your family. You can block inappropriate content, set daily limits for the total time spent online and restrict internet access to certain times of the day.

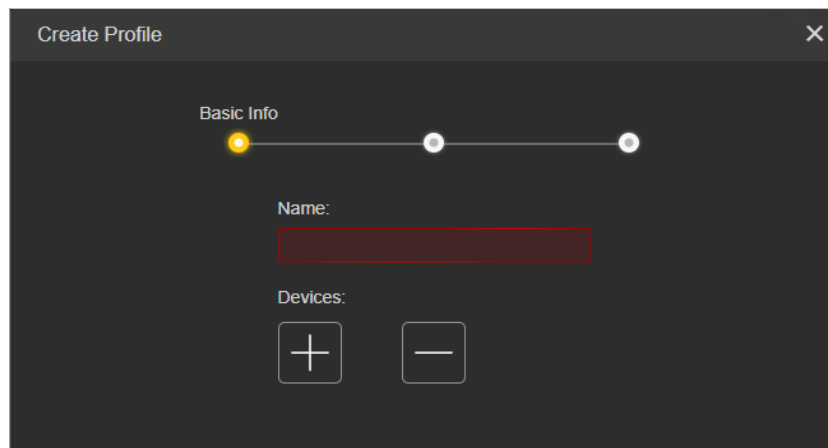
### 8.1.1. Scenario 1: Setting Up Access Restrictions



#### I want to:

Block access to inappropriate online content for my child's devices, restrict internet access to 2 hours every day and block internet access during bed time (10 PM to 7 AM) on school nights (from Thunday to Thursday).

#### 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](#) > [HomeCare](#) > [Parental Controls](#) or [Game Center](#) > [Game Protector](#) > [Parental Controls](#).
3. Click  to create a profile for a family member.
4. Add basic profile information.



- 1) Enter a [Name](#) for the profile to make it easier to identify.
- 2) Under [Devices](#), click .
- 3) Select the devices that belong to this family member. Access restrictions will be applied to these devices. Click [ADD](#) when finished.  
 **Note:** Only devices that have previously been connected to your router's network are listed here. If you are unable to find the device you want to add, connect it to your network and then try again.
- 4) Click [NEXT](#).
5. Block content for this profile.

Create Profile

Filter Level

Filter Level:

Child (0-7) Pre-Teen (8-12) Teen (13-17) Adult (>17)

Filter Content:

**Category Filter**  
Block more categories by selecting the corresponding content.

<input checked="" type="checkbox"/> Adult Content	<input type="checkbox"/> Pay to Surf
<input checked="" type="checkbox"/> Gambling	<input type="checkbox"/> Media
<input type="checkbox"/> Sex Education	<input type="checkbox"/> Download
<input type="checkbox"/> Online Communication	<input type="checkbox"/> Games
<input checked="" type="checkbox"/> Social Network	

**Keyword Filter**  
Block a website by adding a keyword/URL.

Input keyword/URL

BACK NEXT

- 1) Select a filter level based on the age of the family member this profile belongs to. Blocked content will then be displayed in the [Category Filter](#) list.
  - 2) If needed, you can edit the blocked content by selecting the categories in the [Category Filter](#) list.
  - 3) You can also block a specific website or application using the [Keyword Filter](#). Enter a keyword (for example, "Facebook") or a URL (for example, "www.facebook.com").
  - 4) Click [NEXT](#).
6. Set time restrictions on internet access.

The screenshot shows a 'Create Profile' window with a dark background. At the top, there's a progress bar with three yellow dots, and the text 'Time Controls' is visible. Below this, the 'Time Limits' section is active, with a subtitle 'Set daily time limits for the total time spent online.' It features a toggle for 'Mon to Fri:' which is turned on, a 'Daily Time Limit' dropdown set to '2 hours', and a toggle for 'Sat & Sun:' which is turned off. The 'Bed Time' section below it has a subtitle 'Block this person's internet access between certain times.' It includes a toggle for 'School Nights:' which is turned on, and time selection fields for 'Good Night:' (10:00 PM) and 'Good Morning:' (7:00 AM). A 'Weekend:' toggle is turned off. At the bottom right, there are 'BACK' and 'SAVE' buttons.

- 1) Enable [Time Limits](#) on Monday to Friday and Saturday & Sunday then set the allowed online time to 2 hours each day.
- 2) Enable [Bed Time](#) on School Nights and use the up/down arrows or enter times in the fields. Devices under this profile will be unable to access the internet during this time period.
- 3) Click [SAVE](#).

**Note:** The effective time limits are based on the time of the router. You can go to [Advanced > System > Time & Language](#) to modify the time.

## Done!

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

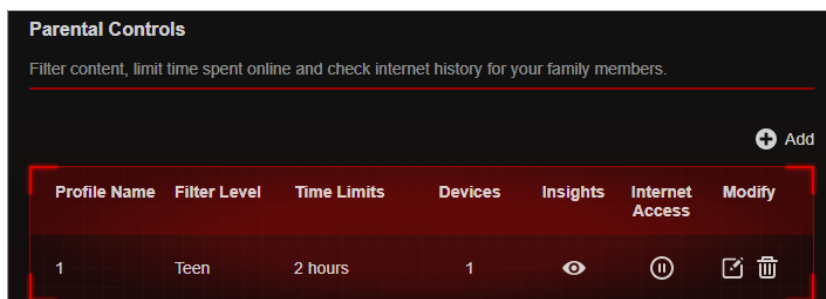
### 8. 1. 2. Scenario 2: Monitoring Internet Usage

#### I want to:

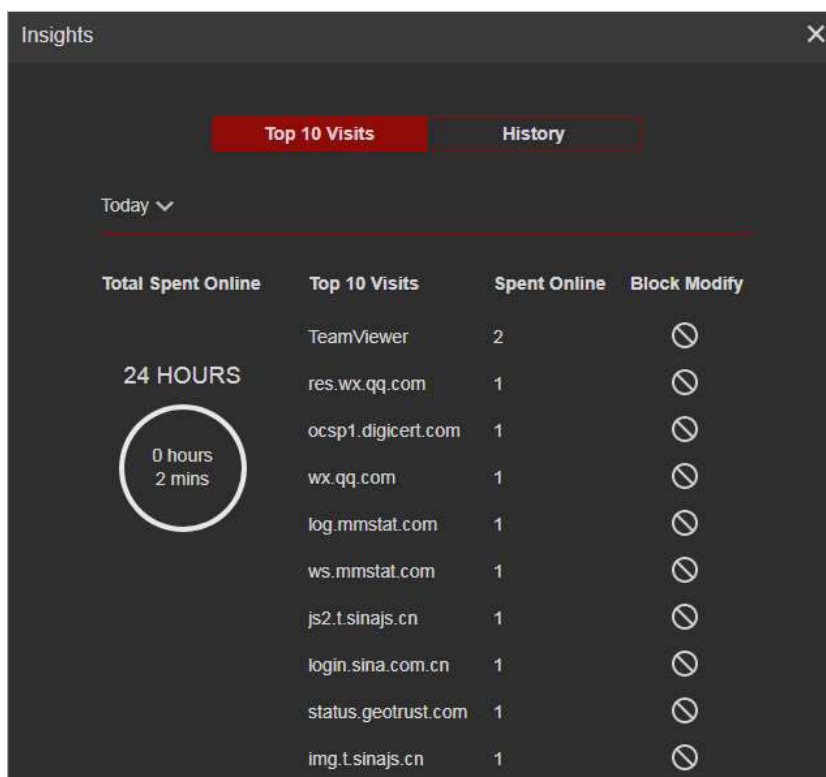
Check which websites my child has visited and how much time they have spent online recently.

## 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](#) > [HomeCare](#) > [Parental Controls](#) or [Game Center](#) > [Game Protector](#) > [Parental Controls](#).



3. Find the correct profile and click in the [Insights](#) column.  
**Note:** If you have not set up a profile for your child yet, you should do that first by clicking [Add](#), then follow the steps to create a profile. Refer to [Scenario 1: Setting Up Access Restrictions](#) for detailed instructions.
4. Use the drop-down menu to view the websites visited and time spent online for any of the last 7 days. Click [History](#) to view a complete history.



Tips: Click to block the corresponding content for this profile.

## Done!

You can now check up on your child's online activities.


## 8.2. QoS

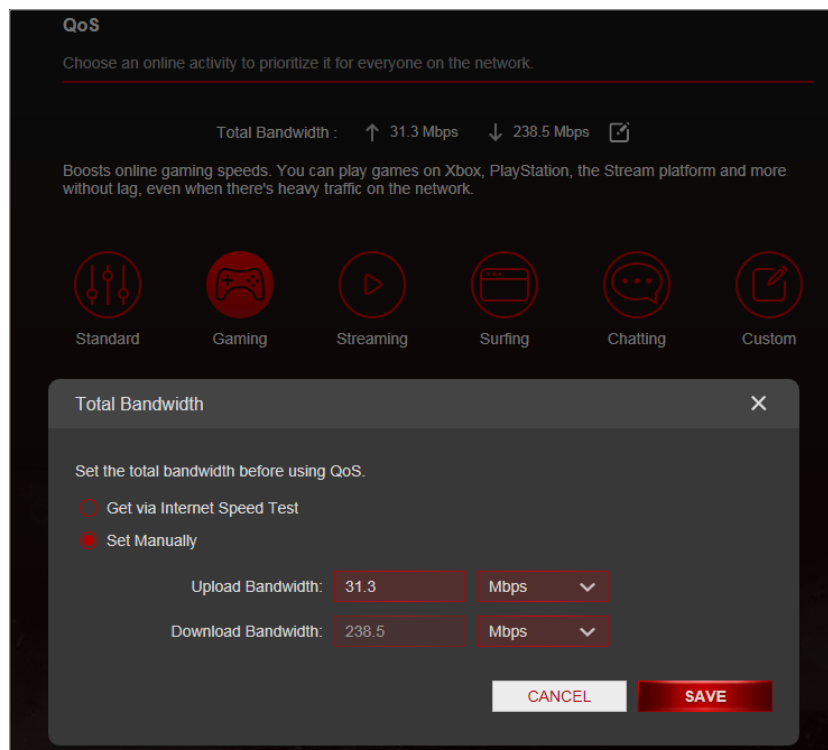
QoS (Quality of Service) allows you to prioritize the internet traffic of specific online activities, such as gaming or streaming. Activities set as high priority will be allocated more bandwidth and so continue to run smoothly even when there is heavy traffic on the network. You can also prioritize the connection of specific devices for a set duration.

### I want to:

Ensure a fast connection while I play online games with friends on my computer for the next 2 hours.

### 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](#) > [HomeCare](#) > [QoS](#).
3. If you already run a Speedtest® and get the bandwidth value, just skip to step 4. If not, click the edit button  to set the total bandwidth. You can choose to run a Speedtest® to get the value or manually enter the bandwidth provided by your internet service provider.

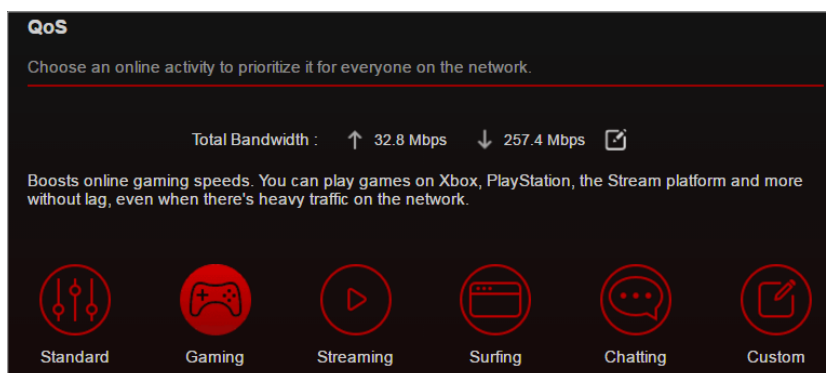


4. It's recommended to keep the Speedtest® result, but if you think the QoS rule you set does not achieve the expected result, you can manually set the upload

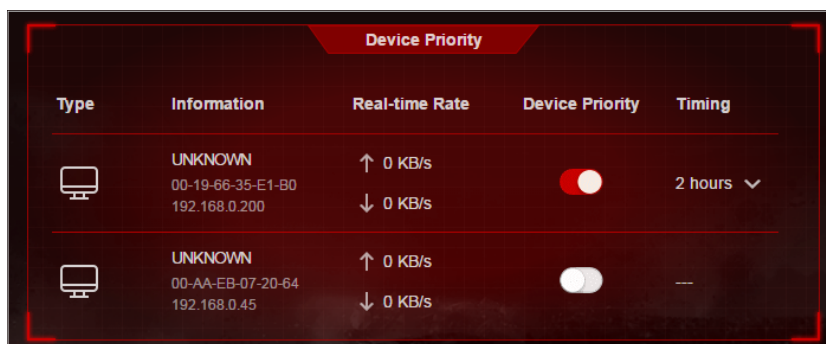


and download bandwidth to be a little bit lower than the value measured through Speedtest®.

5. Click **Gaming** to prioritize this online activity. The default is **Standard**, with no application prioritized.



6. Go to **Game Center > Dashboard** and locate the **Device Priority** section. Find your computer and toggle on **Device Priority**. Click the entry in the **Timing** column and select 2 hours as the duration you want the device to be prioritized for.



**Done!**

You can now enjoy playing games without lag on your computer for the next 2 hours.

### 8.3. Antivirus

Your router supports built-in Antivirus powered by Trend Micro™. It provides malicious content filtering and intrusion prevention for your home network, as well as a quarantine for infected devices. An active database protects every connected device from external threats.

Antivirus includes the following protection:

- Malicious Content Filter

Blocks malicious websites listed in Micro Trend's database. The database is automatically updated so new malicious websites are blocked when they go live.

- **Intrusion Prevention System**

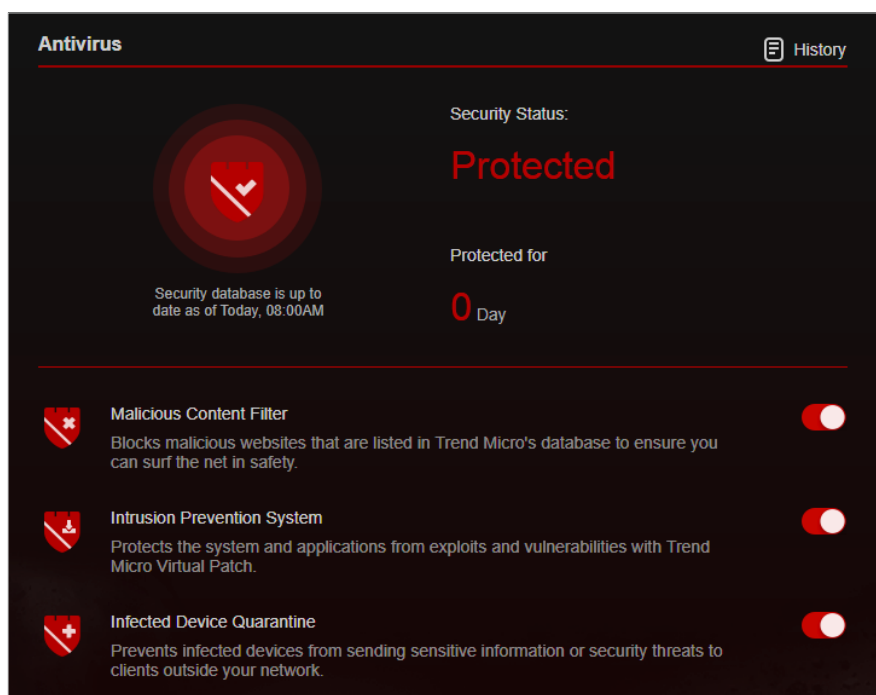
Identifies and blocks potential threats from attackers and fixes vulnerabilities in the network.

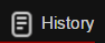
- **Infected Device Quarantine**

Prevents infected devices from sending your sensitive information to clients outside your network or spreading security threats.

- **To access your router's Antivirus 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](#) > [HomeCare](#) > [Antivirus](#) or [Game Center](#) > [Game Protector](#) > [Antivirus](#).



3. Choose the protection types you want to enable. It is recommended to keep them all enabled to ensure the best protection for your network.
4. Click  **History** to view threats that have been detected and resolved.

## Chapter 9

---

# Network Security

---

This chapter guides you on how to protect your home network from cyber attacks and unauthorized users by implementing these three network security functions. You can protect your home network against DoS (Denial of Service) attacks from flooding your network with server requests using DoS Protection, block or allow specific client devices to access your network using Access Control, or you can prevent ARP spoofing and ARP attacks using IP & MAC Binding.

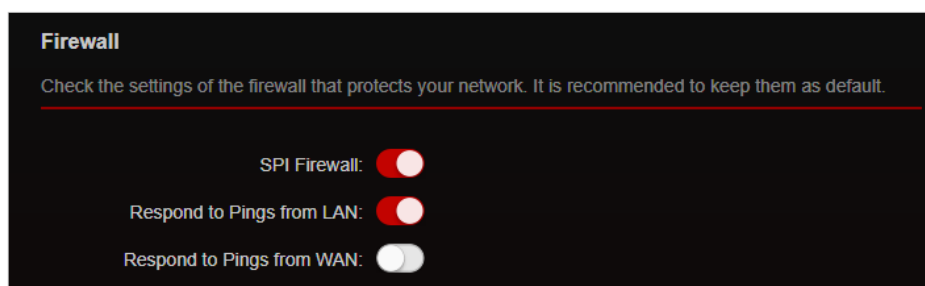
It contains the following sections:

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

## 9.1. Protect the Network from Cyber Attacks

The SPI (Stateful Packet Inspection) Firewall 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.



## 9.2. Access Control

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

### I want to:

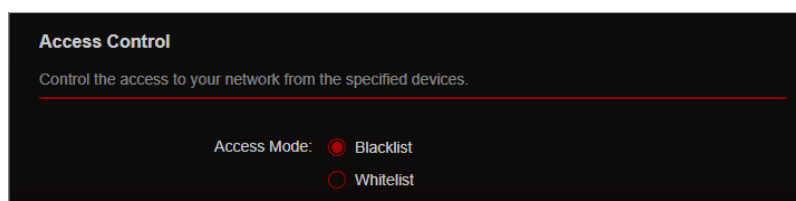
Block or allow specific client devices to access my network (via wired or wireless).

### How can I do that?

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [Security](#) > [Access Control](#).
3. Select the access mode to either block (recommended) or allow the device(s) in the list.

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

- 1) Select [Blacklist](#).

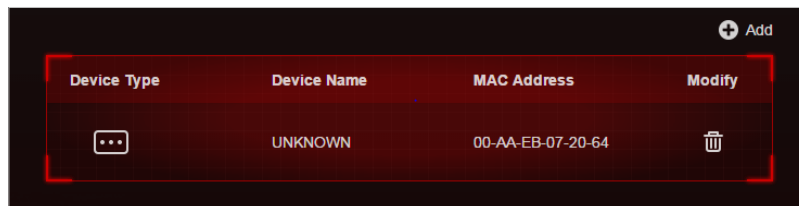


2) Click .



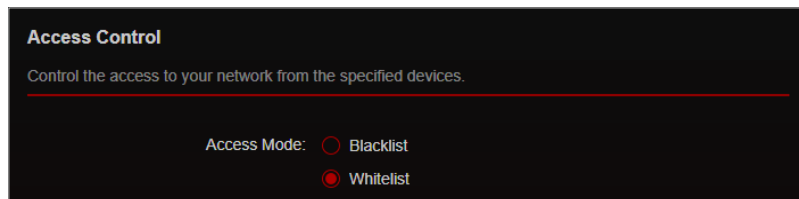
3) Select devices you want to be blocked and Click [ADD](#).


4) The [Operation Succeeded](#) message will appear on the screen, which means the selected devices have been successfully added to the blacklist.

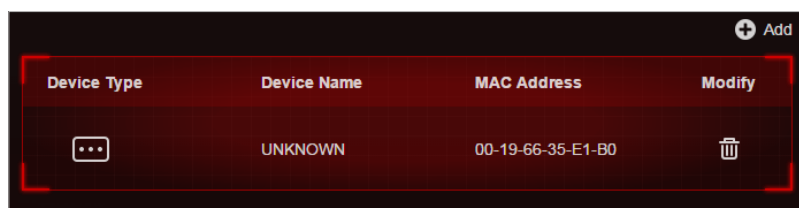


To allow specific device(s):

1) Select [Whitelist](#) and click [SAVE](#) in the lower page.



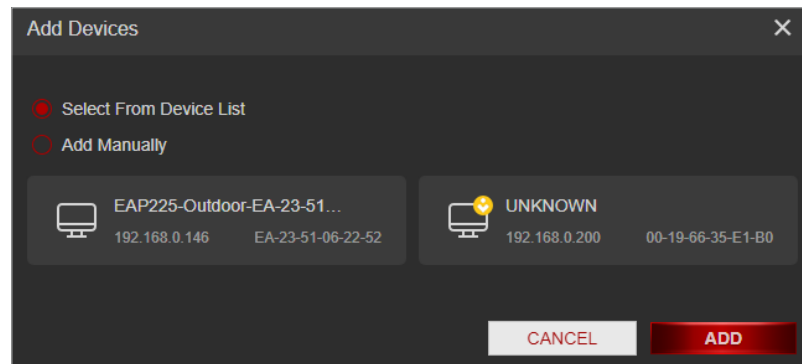
2) Your own device is in the whitelist by default and cannot be deleted. Click  to add other devices to the whitelist.



- **Add connected devices**

1) Click [Select From Device List](#).

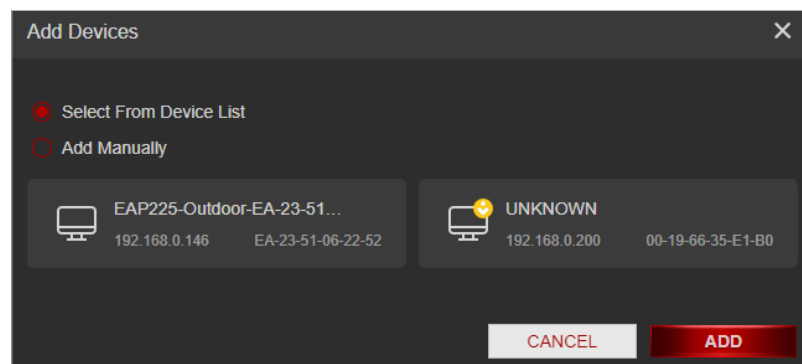
2) Select the devices you want to be allowed and click [ADD](#).



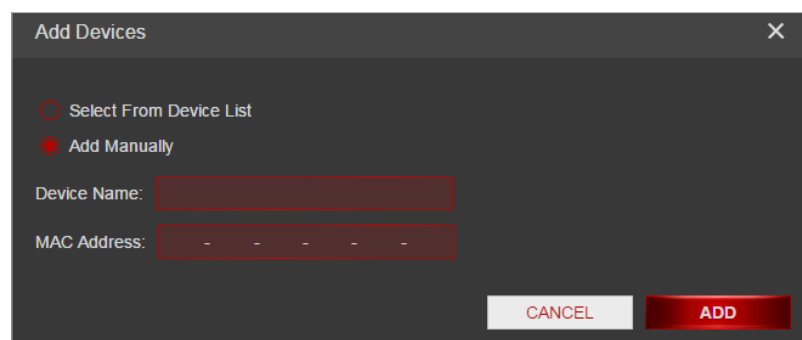
3) The **Operation Succeeded** message will appear on the screen, which means the selected devices have been successfully added to the whitelist.

- **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**.

## 9.3. IP & MAC Binding

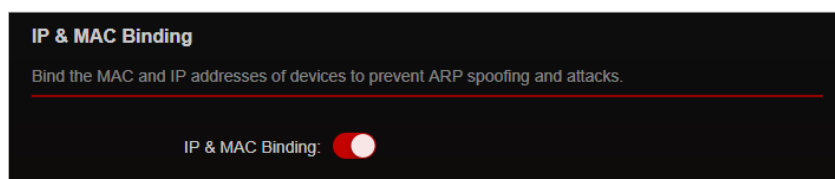
IP & MAC Binding, namely, ARP (Address Resolution Protocol) Binding, is used to bind network device's IP address to its MAC address. This will prevent ARP Spoofing and other ARP attacks by denying network access to an device with matching IP address in the Binding list, but unrecognized MAC address.

### I want to:

Prevent ARP spoofing and ARP attacks.

### How can I do that?

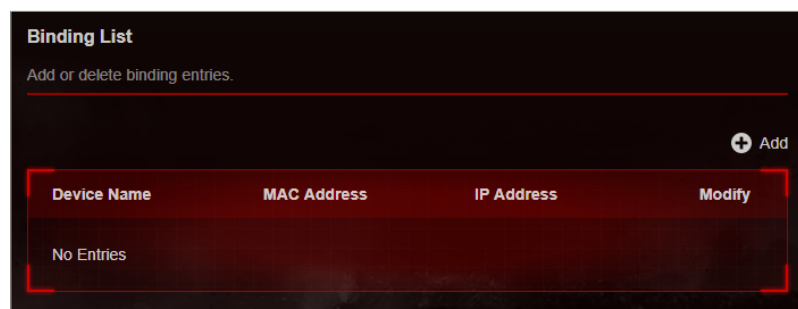
1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced** > **Security** > **IP & MAC Binding**.
3. Enable **IP & MAC Binding**.



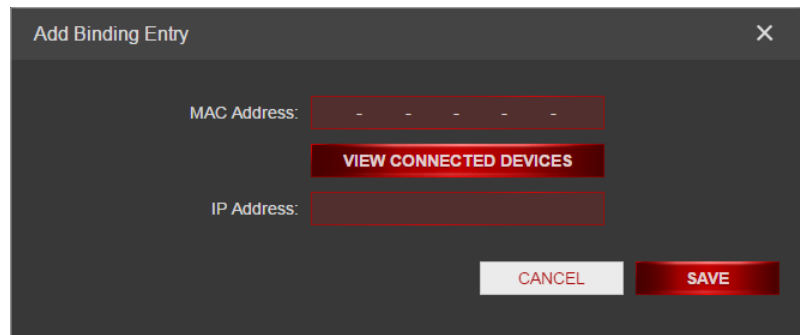
4. Bind your device(s) according to your need.

#### To bind the connected device(s):

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



- 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.

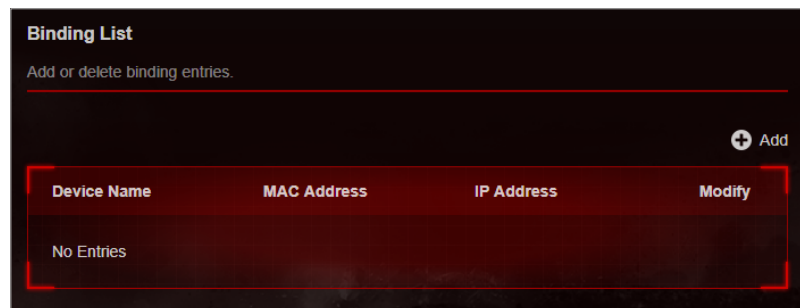


The 'Add Binding Entry' dialog box is shown. It has a title bar with a close button (X). Inside, there are two input fields: 'MAC Address' with a placeholder ' - - - - - ' and 'IP Address' which is empty. Between these fields is a red button labeled 'VIEW CONNECTED DEVICES'. At the bottom right are two buttons: 'CANCEL' and 'SAVE'.

3) Click [SAVE](#).

**To bind the unconnected device:**

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



The 'Binding List' section is shown. It has a title 'Binding List' and a subtitle 'Add or delete binding entries.' Below this is a red button with a plus icon and the text 'Add'. Below the button is a table with the following structure:

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!



## Chapter 10

---

# 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](#)

## 10.1. Share Local Resources on the Internet by Port Forwarding

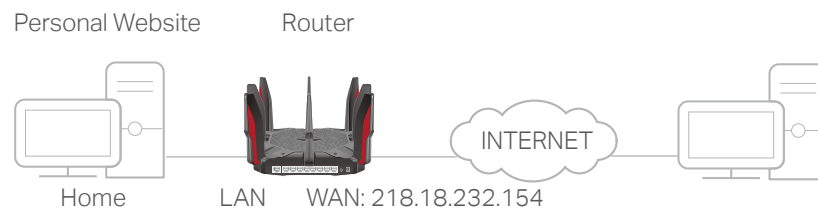
When you build up a server on the local network and want to share it on the internet, Port Forwarding can realize the service and provide it to internet users. At the same time Port Forwarding can keep the local network safe as other services are still invisible from the internet.

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](#) or [Game Center](#) > [Port Forwarding](#).
4. Click .

**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: All ▼

☐ Enable This Entry

CANCEL
SAVE

**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:**

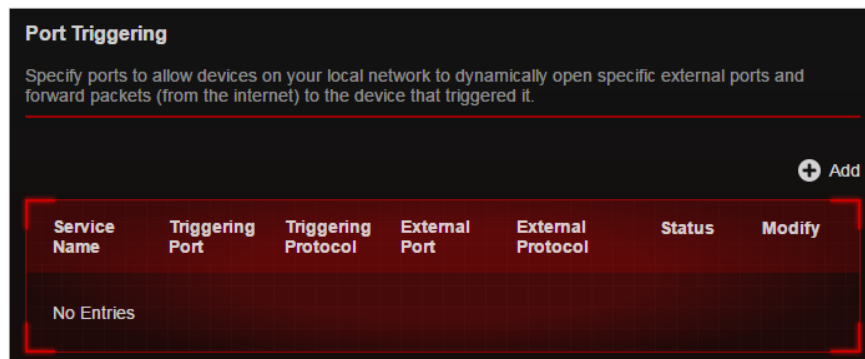
- The WAN IP should be a public IP address. For the WAN IP is assigned dynamically by the ISP, it is recommended to apply and register a domain name for the WAN referring to [Set Up a Dynamic DNS Service Account](#). Then users on the internet can use **http:// domain name** to visit the website.
- If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

## 10.2. 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 .



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.

## 10.3. Make Applications Free from Port Restriction by DMZ

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

##### Note:

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

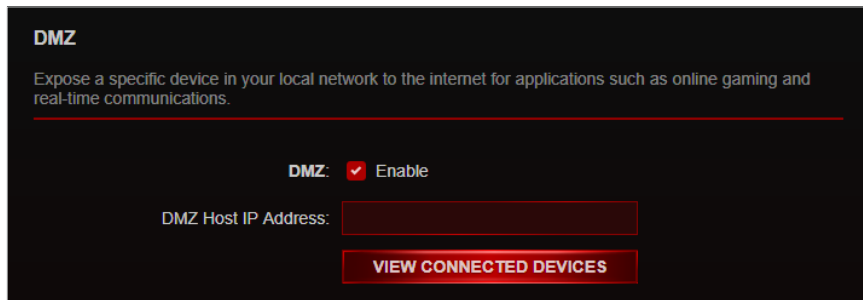
### I want to:

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

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

### How can I do that?

1. Assign a static IP address to your PC, for example 192.168.0.100.
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 select **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.

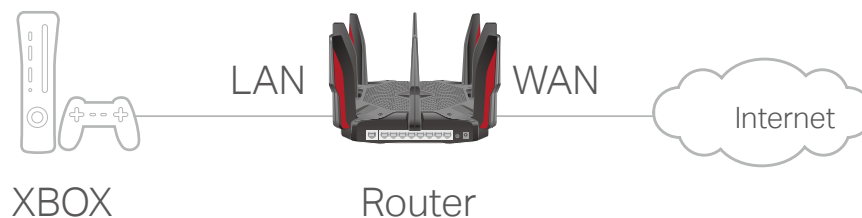
## 10.4. Make Xbox Online Games Run Smoothly by UPnP

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.

UPnP

Enable UPnP (Universal Plug and Play) to allow devices on your local network to dynamically open ports for applications such as multiplayer gaming and real-time communications.

UPnP: ☒

UPnP Client List

Displays the UPnP device information.

Total Clients: 0

Refresh

Service Description	External Port	Protocol	Client IP Address	Internal Port
No Entries				

## Chapter 11

---

# VPN Server

---

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

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

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

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](#)



## 11.1. 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

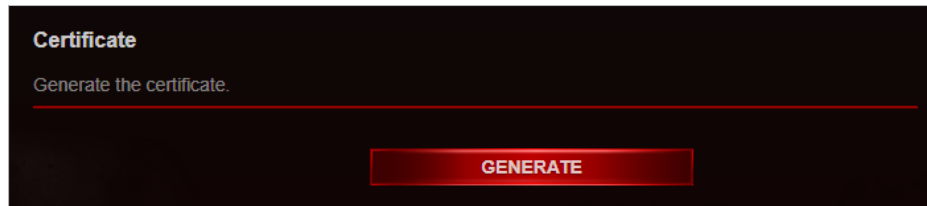
1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > VPN Server > OpenVPN** or **Game Center > VPN Server > OpenVPN**, and tick the **Enable** box of **VPN Server**.

**Note:**

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

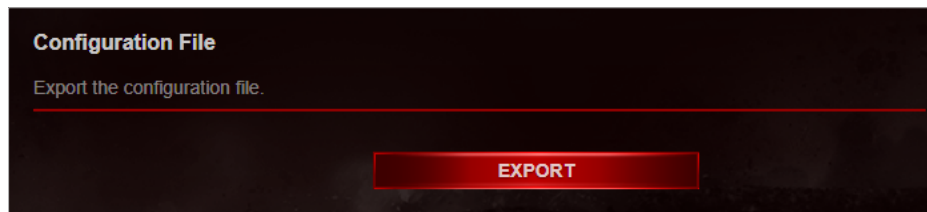
3. Select the **Service Type** (communication protocol) for OpenVPN Server: UDP, TCP.
4. Enter a VPN **Service Port** to which a VPN device connects, and the port number should be between 1024 and 65535.
5. In the **VPN Subnet/Netmask** fields, enter the range of IP addresses that can be leased to the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



■ **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.



## 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.

## 11.2. 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

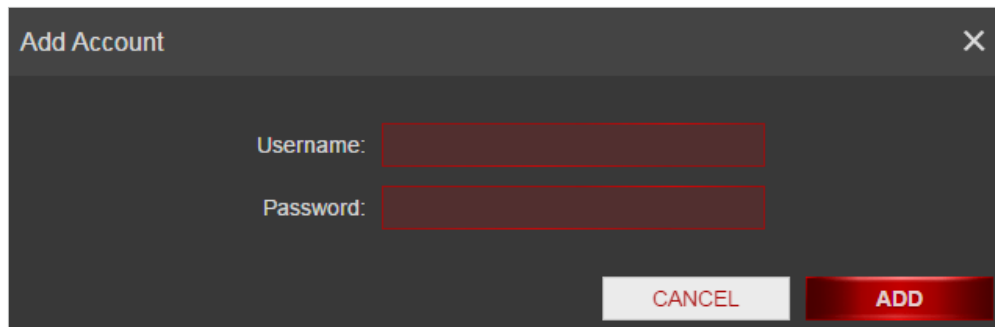
1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [VPN Server](#) > [PPTP](#) or [Game Center](#) > [VPN Server](#) > [PPTP](#), and tick the [Enable](#) box of [PPTP](#).

**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.

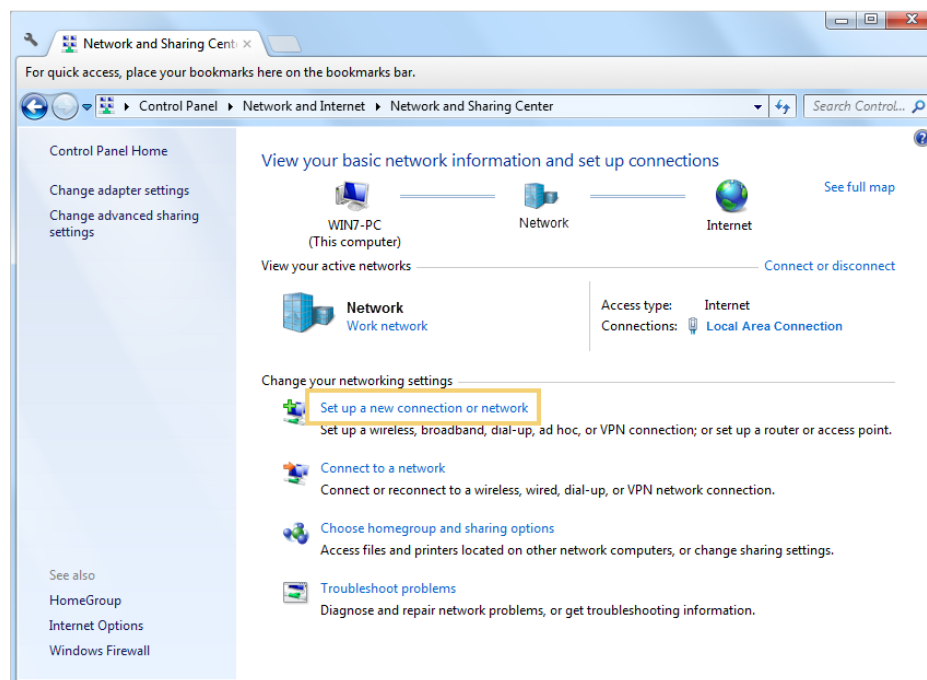


- 3) Click [ADD](#).

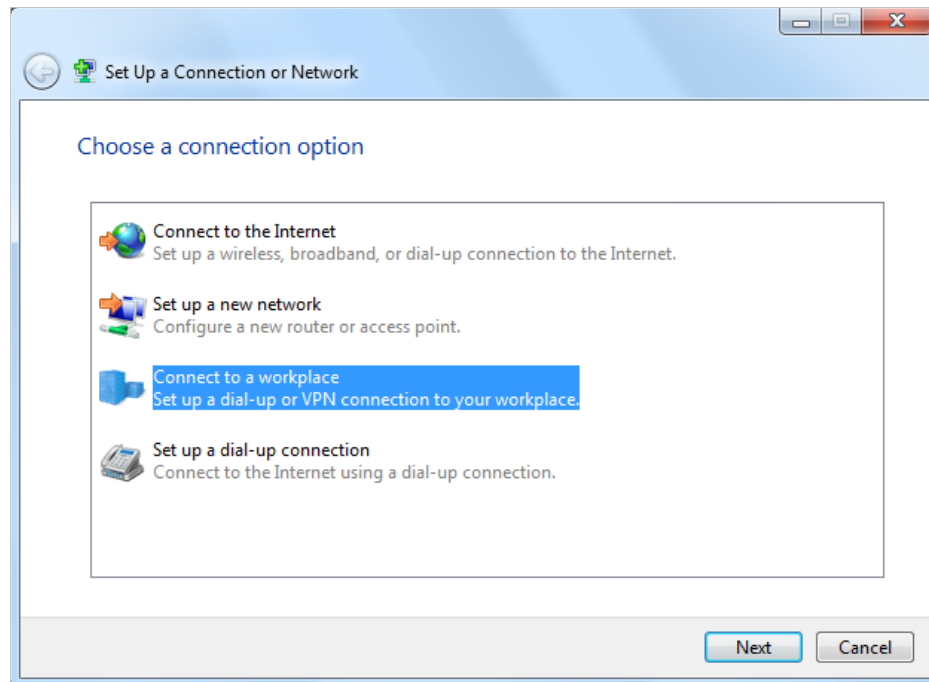
## Step 2. Configure PPTP VPN Connection on Your Remote Device

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.

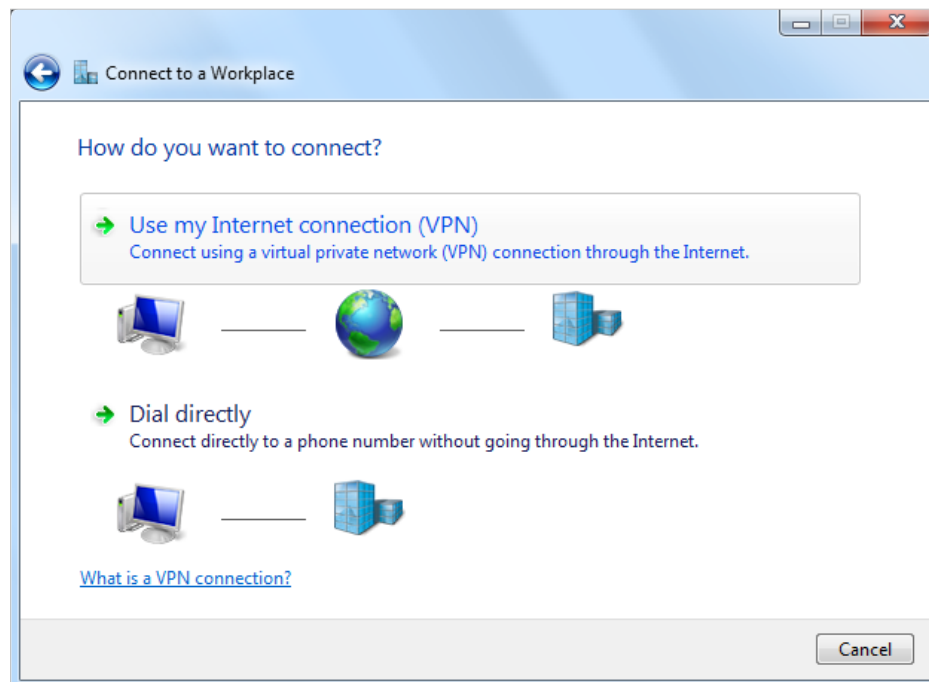
1. Go to [Start](#) > [Control Panel](#) > [Network and Internet](#) > [Network and Sharing Center](#).
2. Select [Set up a new connection or network](#).



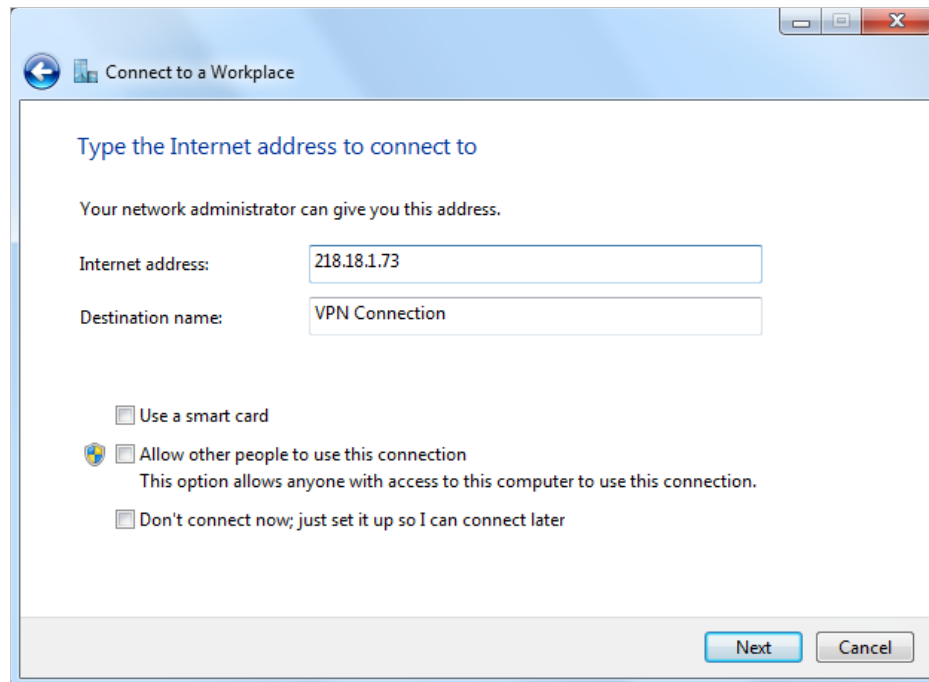
3. Select [Connect to a workplace](#) and click [Next](#).



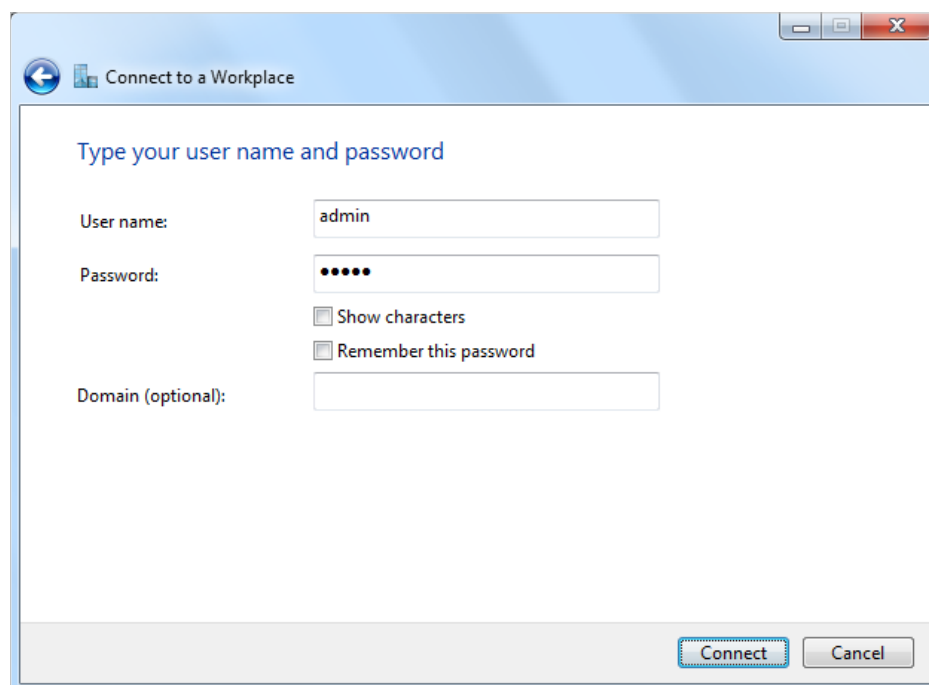
4. Select **Use my Internet connection (VPN)**.



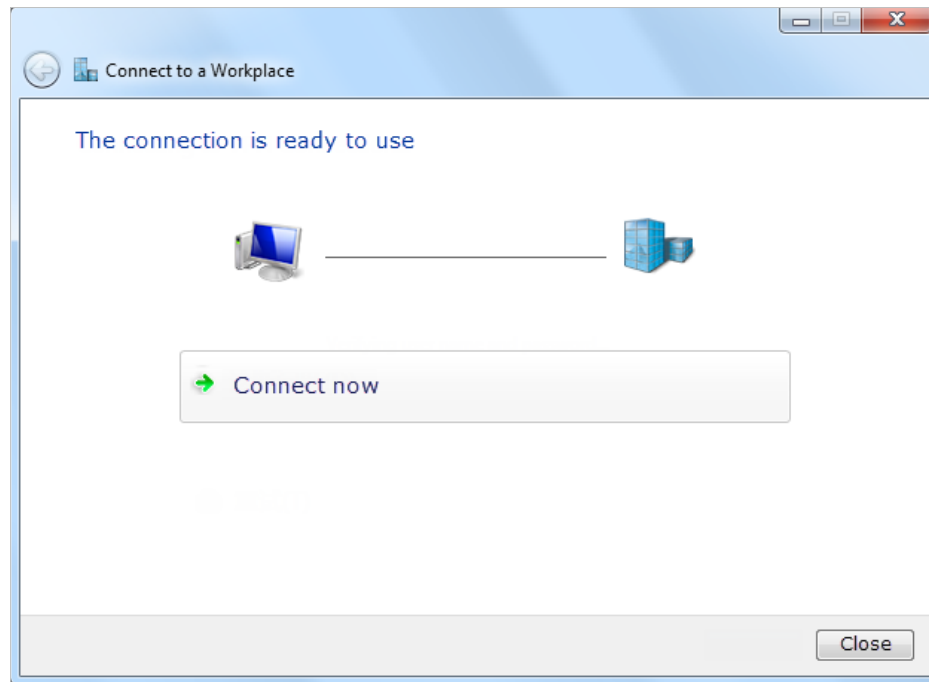
5. Enter the internet IP address of the router (for example: 218.18.1.73) in the **Internet address** field. Click **Next**.



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 12

---

# Customize Your Network Settings

---

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

It contains the following sections:

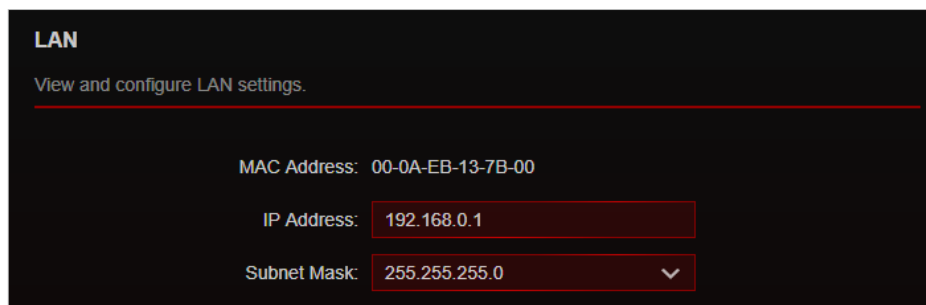
- [Change the LAN Settings](#)
- [Set Up Link Aggregation](#)
- [Configure to Support IPTV Service](#)
- [Specify DHCP Server Settings](#)
- [Set Up a Dynamic DNS Service Account](#)
- [Create Static Routes](#)
- [Specify Wireless Settings](#)
- [Schedule Your Wireless Function](#)
- [Use WPS for Wireless Connection](#)
- [Use WDS to Extend Network](#)
- [Advanced Wireless Settings](#)



## 12.1. Change the LAN Settings

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

1. Visit <http://tplinkwifi.net>, and log in with 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.



**LAN**

View and configure LAN settings.

MAC Address: 00-0A-EB-13-7B-00

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

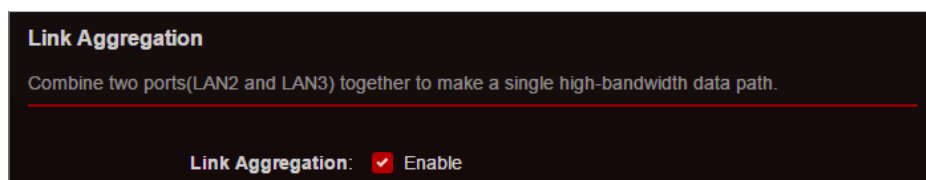
4. Click [SAVE](#).

**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.

## 12.2. Set Up Link Aggregation

The Link Aggregation feature combines two ports together to make a single highbandwidth data path, thus sustaining a higher-speed and more stable wired 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](#) > [Network](#) > [LAN](#).
3. Enable [Link Aggregation](#). The router will reboot to apply the settings and the LAN ports 2 and 3 will be used for Link Aggregation.



**Link Aggregation**

Combine two ports(LAN2 and LAN3) together to make a single high-bandwidth data path.

Link Aggregation: ☒ Enable

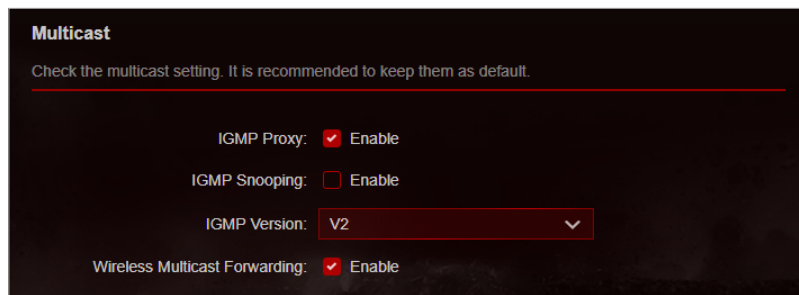
## 12.3. Configure to Support IPTV Service

### I want to:

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

### How can I do that?

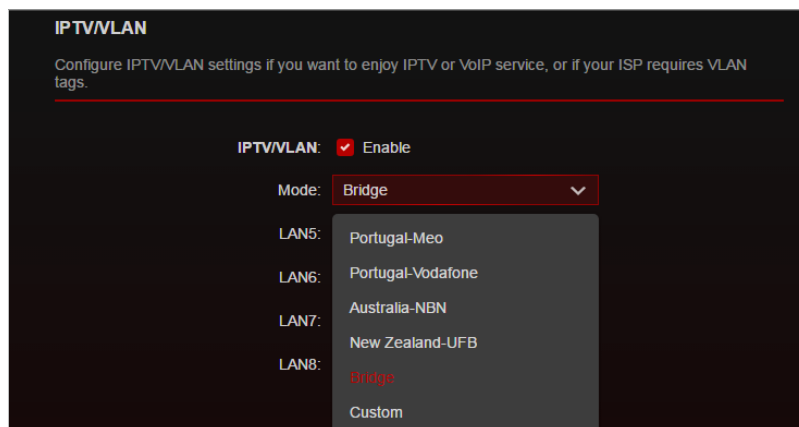
1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [Network](#) > [IPTV/VLAN](#).
3. If your ISP provides the networking service based on IGMP technology, e.g., British Telecom(BT) and Talk Talk in UK:
  - 1) Tick the [IGMP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



- 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.



- 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.

## 12.4. 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:**

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.

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.
3. Enter the [IP address](#) to reserve for the client device.
4. Click [SAVE](#).

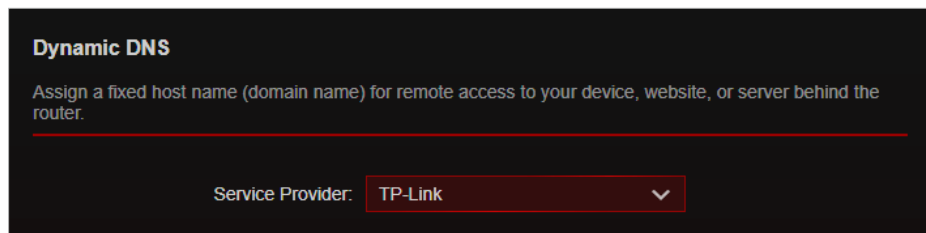
## 12.5. Set Up a Dynamic DNS Service Account

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](#).



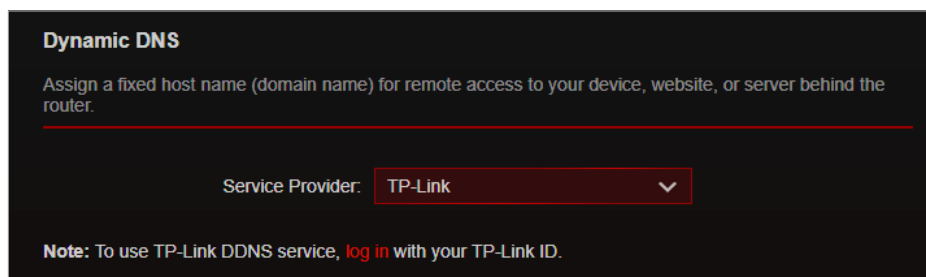
**Dynamic DNS**

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](#).



**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 use TP-Link DDNS service, [log in](#) with your TP-Link ID.

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

5. Click **SAVE**.

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

## 12.6. Create Static Routes

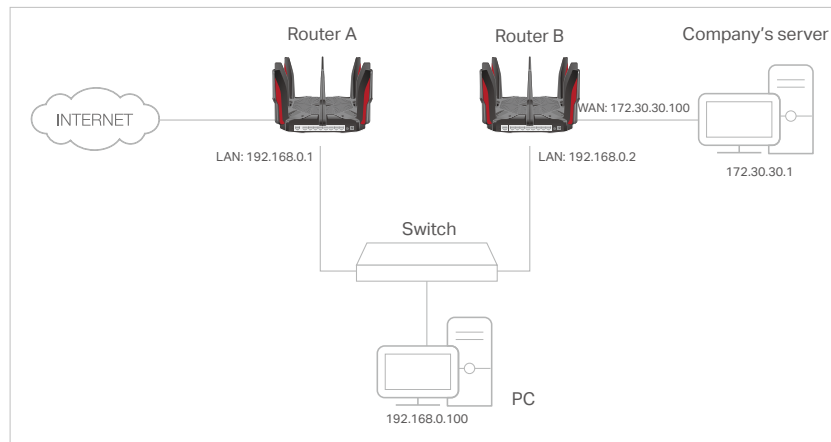
Static routing is a form of routing that is configured manually by a network administrator or a user by adding entries into a routing table. The manually-configured routing information guides the router in forwarding data packets to the specific destination.

### 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:

Subnet Mask:

Default Gateway:

Interface:

Description:

**CANCEL** **SAVE**

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

**Subnet Mask:** Determines the destination network with the destination IP address.

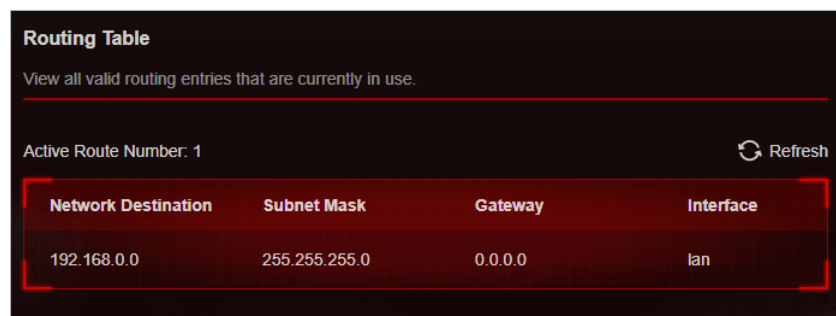
If the destination is a single IP address, enter 255.255.255.255; otherwise, enter the subnet mask of the corresponding network IP. In the example, the destination network is a single IP, so here enter 255.255.255.255.

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

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

**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.



The screenshot shows a web interface titled "Routing Table" with a subtitle "View all valid routing entries that are currently in use." Below this, it says "Active Route Number: 1" and has a "Refresh" button with a circular arrow icon. A table with four columns is displayed: "Network Destination", "Subnet Mask", "Gateway", and "Interface". The table contains one row with the values "192.168.0.0", "255.255.255.0", "0.0.0.0", and "lan".

Network Destination	Subnet Mask	Gateway	Interface
192.168.0.0	255.255.255.0	0.0.0.0	lan

**Done!**

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

## 12.7. Specify Wireless Settings

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

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

- **To enable or disable the wireless function:**

1. Go to **Wireless** or **Advanced > Wireless > Wireless Settings**.



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

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

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

**Note:**

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

- **To hide SSID:**

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

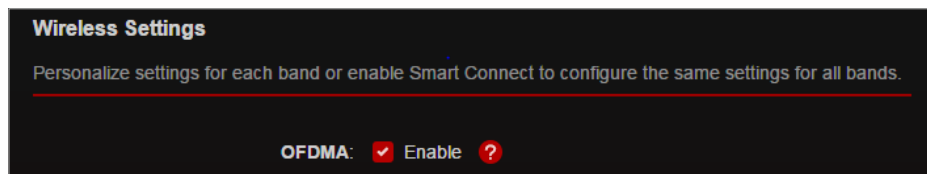
- **To use OFDMA function:**

The OFDMA feature enables multiple users to transmit data simultaneously, and thus greatly improves speed and efficiency.

**Note:**

Only when your clients also support OFDMA can you fully enjoy the benefits.

1. Go to [Wireless](#) or [Advanced](#) > [Wireless](#) > [Wireless Settings](#).
2. Enable [OFDMA](#).



- **To use the smart connect function:**

The smart connect function lets you to enjoy a more high-speed network by assigning your devices to best wireless bands based on actual conditions to balance network demands.

1. Go to [Wireless](#) or [Advanced](#) > [Wireless](#) > [Wireless Settings](#).
2. Enable [Smart Connect](#).