

The screenshot shows a dialog box titled "Add Schedule" with a close button (X) in the top right corner. The "Wireless Off Time" section has two rows of dropdown menus. The first row is "From" with "10" and "PM". The second row is "To" with "6" and "AM", followed by the text "(next day)". Below this is a "Repeat" section with seven circular buttons representing the days of the week: S, M, T, W, T, F, S. At the bottom of the dialog are two buttons: "CANCEL" and "SAVE".

Note:

- The Effective Time Schedule is based on the time of the router. You can go to [Advanced > System > Time & Language](#) to modify the time.
- The wireless network will be automatically turned on after the time period you set.

7.3. Use WPS for Wireless Connection

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

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Make sure the Wi-Fi of your router is on and go to [Advanced > Wireless > WPS](#).

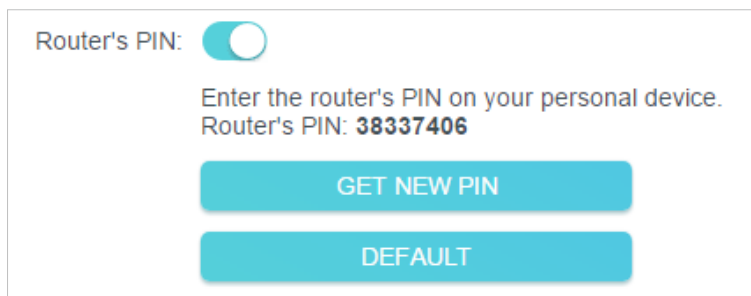
7.3.1. Connect via the Client's PIN

Enter the PIN of your device and click **Connect**. Then your device will get connected to the router.

The screenshot shows the WPS configuration interface. At the top, "WPS:" is followed by a toggle switch that is turned on. Below this, "Method 1: Using a PIN" is displayed. There are two radio button options: "Client's PIN" (which is selected) and "Router's PIN". Below the radio buttons, there is a text prompt: "Enter your personal device's PIN here and click **CONNECT**". Underneath the prompt is a text input field. At the bottom of the form is a large blue button labeled "CONNECT".

7.3.2. Connect via the Router's PIN

Select **Router's PIN** in **Method 1** to enable **Router's PIN**. You can use the default PIN or generate a new one.

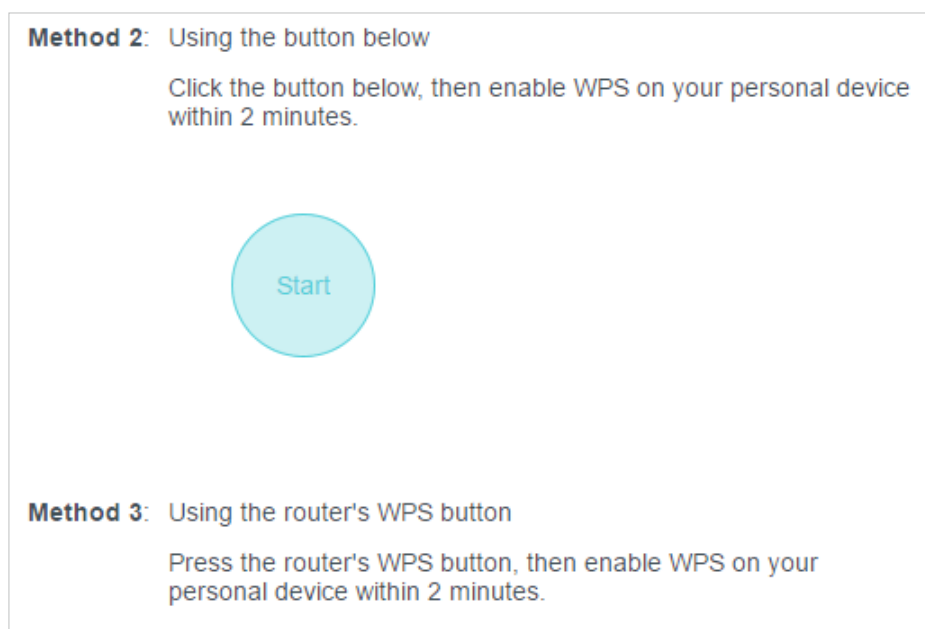


Note:

PIN (Personal Identification Number) is an eight-character identification number preset to each router. WPS supported devices can connect to your router with the PIN. The default PIN is printed on the label of the router.

7.3.3. Push the WPS Button

Click **Start** on the screen or directly press the router's WPS button. Within two minutes, enable WPS on your personal device. **Success** will appear on the screen and the WPS LED of the router should change from flashing to solid on, indicating successful WPS connection.



7.4. Advanced Wireless Settings

Check advanced wireless settings for your device.

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 > Wireless > Additional Settings**.
3. Configure advanced wireless settings.

Additional Settings
Check advanced wireless settings for your device.

WMM: Enable

AP Isolation: Enable

Airtime Fairness: Enable

Zero Wait DFS: Enable

Beacon Interval:

RTS Threshold:

DTIM Interval:

Group Key Update Period: s

- **WMM** - WMM function can guarantee the packets with high-priority messages being transmitted preferentially.
- **AP Isolation** - This function isolates all connected wireless stations so that wireless stations cannot access each other through WLAN.
- **Airtime Fairness** - This function can improve the overall network performance by sacrificing a little bit of network time on your slow devices.
- **Zero Wait DFS** - Zero Wait DFS (Dynamic Frequency Selection) allows the router to immediately reselect a new channel once the radar signal is detected on a channel allocated to radar devices to ensure lag-free network experience.
- **Beacon Interval** - Enter a value between 40 and 1000 in milliseconds to determine the duration between beacon packets that are broadcasted by the router to synchronize the wireless network. The default value is 100 milliseconds.
- **RTS Threshold**- Enter a value between 1 and 2346 to determine the packet size of data transmission through the router. By default, the RTS (Request to Send) Threshold size is 2346. If the packet size is greater than the preset threshold, the router will send RTS frames to a particular receiving station and negotiate the sending of a data frame.
- **DTIM Interval** - The value determines the interval of DTIM (Delivery Traffic Indication Message). Enter a value between 1 and 15 intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.

- **Group Key Update Period** - Enter a number of seconds (minimum 30) to control the time interval for the encryption key automatic renewal. The default value is 0, meaning no key renewal.

Chapter 8

Guest Network

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

It contains the following sections:

- [Create a Network for Guests](#)
- [Set Up Portal Authentication for the Guest Network](#)
- [Limit the Bandwidth of the Guest Network](#)
- [Specify the Effective Time of the Guest Network](#)
- [Customize Guest Network Options](#)

8.1. Create a Network for Guests

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Wireless](#) and locate the [Guest Network](#) section.
3. Create a guest network as needed.
 - 1) Enable [2.4GHz](#) and/or [5GHz](#).
 - 2) Customize the SSID. Don't select [Hide SSID](#) unless you want your guests to manually input the SSID for guest network access.
 - 3) Select the [Security](#) type and customize your own password. If [No security](#) is selected, no password is needed to access your guest network.

Guest Network
Enable the wireless bands you want your guests to use and complete the related information.

2.4GHz: Enable [Share Network](#)

Network Name (SSID): Hide SSID

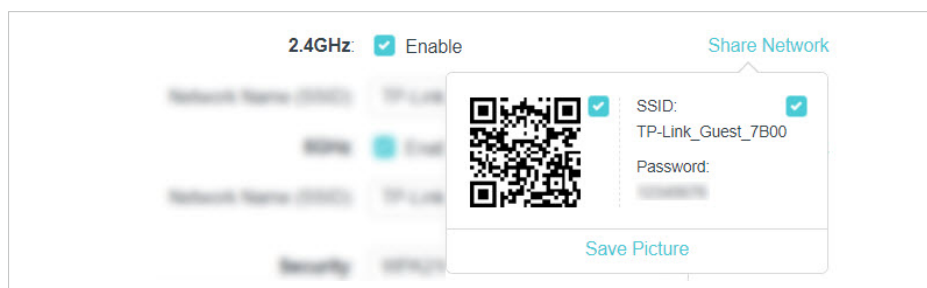
5GHz: Enable [Share Network](#)

Network Name (SSID): Hide SSID

Security: ▼

Password:

4. Click [SAVE](#). Now your guests can access your guest network using the SSID and password you set!
5. You can also click [Share Network](#) to share the SSID and password to your guests.



Tips:

To view guest network information, go to [Network Map](#) and locate the [Guest Network](#) section. You can turn on or off the guest network function conveniently.

8.2. Set Up Portal Authentication for the Guest Network

Imagine that you run a small shop and provide a guest network for your customers. You want to seize every opportunity to promote your shop, which makes portal authentication an excellent choice. Customers will be directed to a web page for access verification, on which your personalized promotion is displayed. Moreover, you can specify a web link so that newly connected guests will be redirected to, for example, the official website of your shop.

1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Wireless](#) and locate the [Guest Network](#) section.
3. Set [Security](#) to [Portal](#).

Guest Network

Enable the wireless bands you want your guests to use and complete the related information.

2.4GHz: Enable [Share Network](#)

Network Name (SSID): Hide SSID

5GHz: Enable [Share Network](#)

Network Name (SSID): Hide SSID

Security: ▼

Authentication Type: ▼

Password:

Authentication Timeout: ▼

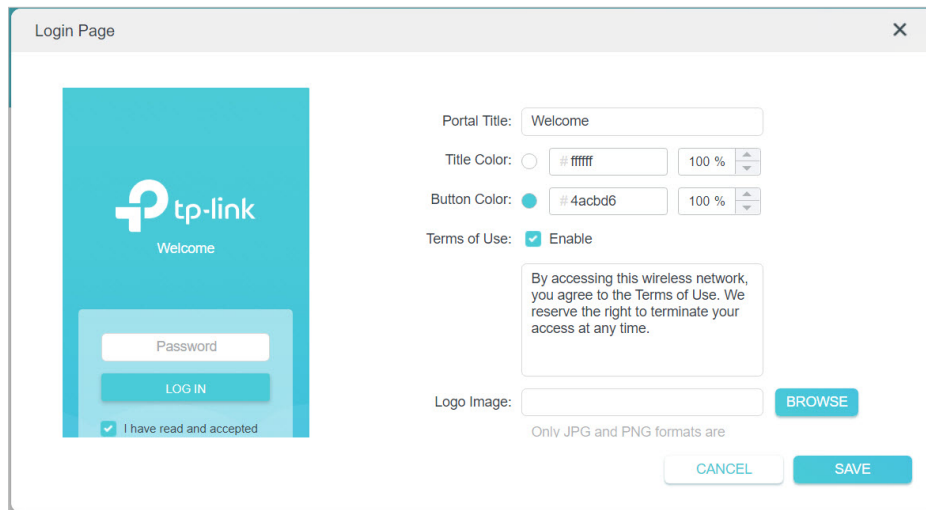
Redirect: Enable

Redirect URL:

Login Page: [Click to Edit](#)

4. Select the [Authentication Type](#).
 - If you select [No Authentication](#), guests can access the network without any authentication.
 - If you select [Simple Password](#), specify a password for authentication.
5. Specify the [Authentication Timeout](#). When a guest's authentication expires, they have to reconnect to the network. The default value [Always](#) indicates that authentication will never time out.

- (Optional) Enable **Redirect** and enter your desired web link. Newly connected guests will be redirected to the website you specify.
- (Optional) Click to edit the **Login Page**. You can customize the appearance and content of the login page.



The screenshot shows the 'Login Page' configuration window. On the left is a preview of the login page with the TP-Link logo, a 'Welcome' message, a 'Password' input field, a 'LOG IN' button, and a checked checkbox for 'I have read and accepted'. On the right are the configuration options:

- Portal Title:
- Title Color: #ffffff 100%
- Button Color: #4acbd6 100%
- Terms of Use: Enable
- Terms of Use Text:

By accessing this wireless network, you agree to the Terms of Use. We reserve the right to terminate your access at any time.
- Logo Image:
- Only JPG and PNG formats are
-

- Click **SAVE**.

8.3. Limit the Bandwidth of the Guest Network

- Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
- Go to **Advanced > Wireless > Guest Network**.
- Enable **Bandwidth Control** for one or all networks as you need.

Guest Network

Enable the wireless bands you want your guests to use and complete the related information.

2.4GHz: Enable [Share Network](#)

Network Name (SSID): Hide SSID

Bandwidth Control: Enable

Download Bandwidth: Mbps

Upload Bandwidth: Mbps

5GHz: Enable [Share Network](#)

Network Name (SSID): Hide SSID

Bandwidth Control: Enable

Download Bandwidth: Mbps

Upload Bandwidth: Mbps

Effective Time: ▼

Security: ▼

Password:

4. Limit the download and upload bandwidth for the network.

5. Click [SAVE](#). Now you can limit the bandwidth of the guest network.

8. 4. Specify the Effective Time of the Guest 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](#) > [Wireless](#) > [Guest Network](#).

Guest Network

Enable the wireless bands you want your guests to use and complete the related information.

2.4GHz: Enable [Share Network](#)

Network Name (SSID): Hide SSID

Bandwidth Control: Enable

5GHz: Enable [Share Network](#)

Network Name (SSID): Hide SSID

Bandwidth Control: Enable

Effective Time: ▼

Security: ▼

Password:

3. Specify the **Effective Time**. The guest network will be automatically turned off after the effective time. The default value **No Limit** indicates that the guest network will always remain on.

4. Click **SAVE**. Now you can keep the guest network on only when you need it.

8.5. Customize Guest Network Options

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 > Wireless > Guest Network**. Locate the **Guest Permissions** section.
3. Customize guest network options according to your needs.

Guest Permissions

Control the data that guests can access.

Allow guests to see each other

Allow guests to access your local network

- **Allow guests to see each other**

Tick this checkbox if you want to allow the wireless clients on your guest network to communicate with each other via methods such as network neighbors and Ping.

- **Allow guests to access your local network**

Tick this checkbox if you want to allow the wireless clients on your guest network to communicate with the devices connected to your router's LAN ports or main network via methods such as network neighbors and Ping.

4. Click **SAVE**. Now you can ensure network security and privacy!

Chapter 9

USB Settings

This chapter describes how to use the USB ports to share files and media from the USB storage devices over your home network locally, or remotely through the internet.

The router supports USB external flash drives and hard drives.

It contains the following sections:

- [Access the USB Storage Device](#)
- [Media Sharing](#)
- [Time Machine](#)

9. 1. Access the USB Storage Device

Insert your USB storage device into the router's USB port and then access files stored there locally or remotely.

 **Tips:**

- If you use USB hubs, make sure no more than 4 devices are connected to the router.
- If the USB storage device requires using bundled external power, make sure the external power has been connected.
- If you use a USB hard drive, make sure its file system is FAT32, exFat, NTFS or HFS+.
- Before you physically disconnect a USB device from the router, safely remove it to avoid data damage: Go to [Advanced > USB > USB Storage Device](#) and click [Remove](#).

9. 1. 1. Access the USB Device Locally

Insert your USB storage device into the router's USB port and then refer to the following table to access files stored on your USB storage device.

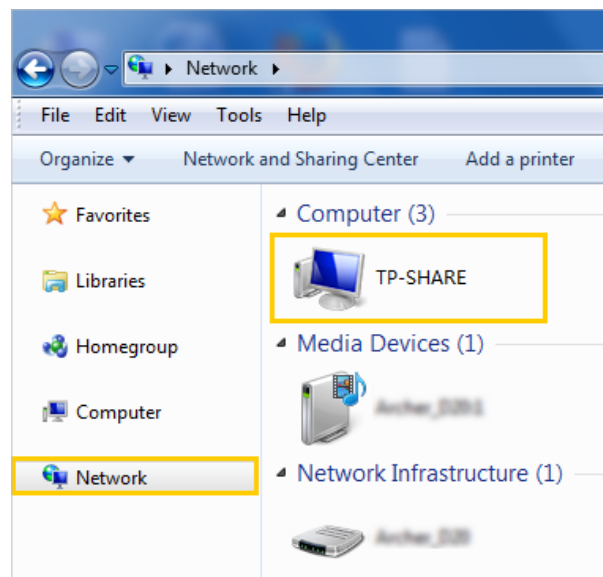
Windows computer

- **Method 1:**

Go to [Computer > Network](#), then click the Network Server Name ([TP-SHARE](#) by default) in the [Computer](#) section.

 **Note:**

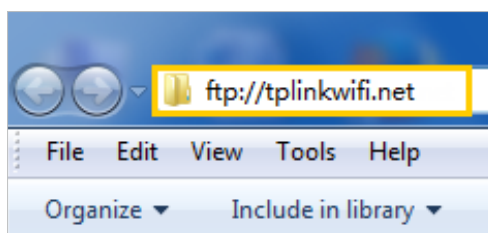
Operations in different systems are similar. Here we take Windows 7 as an example.



Windows
computer

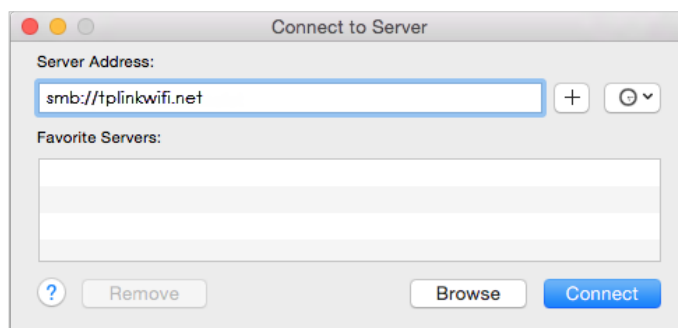
- **Method 2:**

Open the [Windows Explorer](#) (or go to [Computer](#)) and type the server address `\\tplinkwifi.net` or `ftp://tplinkwifi.net` in the address bar, then press [Enter](#).



Mac

- 1) Select [Go > Connect to Server](#).
- 2) Type the server address `smb://tplinkwifi.net`.
- 3) Click [Connect](#).



- 4) When prompted, select the [Guest](#) radio box. (If you have set up a username and a password to deny anonymous access to the USB disks, you should select the [Registered User](#) radio box. To learn how to set up an account for the access, refer to [To Set Up Authentication for Data Security](#).)

Tablet

Use a third-party app for network files management.

 **Tips:**

You can also access your USB storage device by using your Network/Media Server Name as the server address. Refer to [To Customize the Address of the USB Storage Device](#) to learn more.

9.1.2. Access the USB Device Remotely

You can access your USB disk outside the local area network. For example, you can:

- Share photos and other large files with your friends without logging in to (and paying for) a photo-sharing site or email system.
- Get a safe backup for the materials for a presentation.
- Remove the files on your camera's memory card from time to time during the journey.

Note:

If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), you cannot use this feature because private addresses are not routed on the internet.

Follow the steps below to configure remote access 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 > USB > USB Storage Device**.
3. Tick the **Internet FTP** checkbox, and then click **SAVE**.

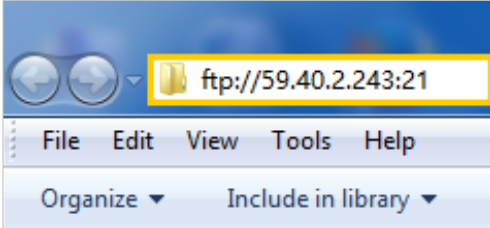
Access Method

Select the method for accessing your USB storage device. The device can then be reached via the access address.

Network/Media Server Name:

Enable	Access Method	Address	Port
<input checked="" type="checkbox"/>	Samba for Windows	\\TP-Share	---
<input checked="" type="checkbox"/>	Local FTP	ftp://192.168.0.1:21	21
<input checked="" type="checkbox"/>	Internet FTP	ftp://0.0.0.0:21 Set DDNS	<input type="text" value="21"/>

4. Refer to the following table to access your USB disk remotely.

Computer	<ol style="list-style-type: none"> 1) Open the Windows Explorer (or go to Computer, only for Windows users) or open a web browser. 2) Type the server address in the address bar: Type in ftp://<WAN IP address of the router>:<port number> (such as ftp://59.40.2.243:21). If you have specified the domain name of the router, you can also type in ftp://<domain name>:<port number> (such as ftp://MyDomainName:21) <div data-bbox="644 527 1134 753" style="text-align: center;">  </div> <ol style="list-style-type: none"> 3) Press Enter on the keyboard. 4) Access with the username and password you set in To Set Up Authentication for Data Security. <p><small>🔗 Tips:</small> You can also access the USB disk via a third-party app for network files management, which can resume broken file transfers.</p>
	Tablet

🔗 Tips:

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

9.1.3. Customize the Access Settings

By default, all the network clients can access all folders on your USB disk. You can customize your sharing settings by setting a sharing account, sharing specific contents and setting a new sharing address on the router's web management page.

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](#) > [USB](#) > [USB Storage Device](#).

- **To Customize the Address of the USB Storage Device**

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

1. In the [Access Method](#) session, make sure [Samba for Windows](#) is ticked, and enter a [Network/Media Server Name](#) as you like, such as [MyShare](#), then click [SAVE](#).

Access Method

Select the method for accessing your USB storage device. The device can then be reached via the access address.

Network/Media Server Name:

Enable	Access Method	Address	Port
<input checked="" type="checkbox"/>	Samba for Windows	\\TP-Share	---
<input checked="" type="checkbox"/>	Local FTP	ftp://192.168.0.1:21	21
<input type="checkbox"/>	Internet FTP	ftp://0.0.0.0:21 Set DDNS	<input type="text" value="21"/>

2. Now you can access the USB storage device by visiting <\\MyShare> (for Windows) or <smb://MyShare> (for Mac).

- **To Only Share Specific Content**

Focus on the [File Sharing](#) section. Specify sharing folders that you want to share and click [SAVE](#).

Sharing Contents:

Share Selected Folders

G:/Document
G:/Pictures

- **To Set Up Authentication for Data Security**

You can set up authentication for your USB storage device so that network clients will be required to enter username and password when accessing the USB storage device.

1. In the [File Sharing](#) section, enable [Secure Sharing](#).

Secure Sharing			
Customize the access settings to ensure data security.			
Username	Password	Permissions	Modify
admin	Read&Write	
visit	Read	

- Click to modify the access account. The username and password are both **admin** for default administrator account, and both **visit** for default visitor account. Accessing as an administrator can read and modify the shared folders while visitors can only read the shared folders.

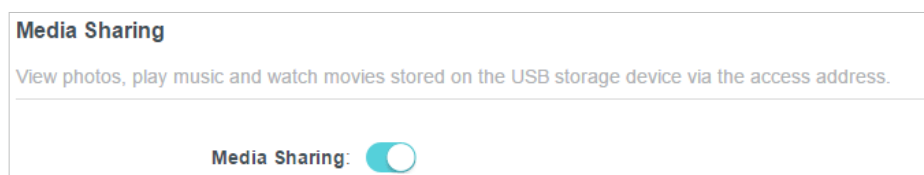
Note:

- For Windows users, do not set the sharing username the same as the Windows username. Otherwise, Windows credential mechanism may cause the following problems:
 - If the sharing password is also the same as the Windows password, authentication will not work since the Windows will automatically use its account information for USB access.
 - If the sharing password is different from the Windows password, the Windows will be unable to remember your credentials and you will always be required to enter the sharing password for USB access.
- Due to Windows credential mechanism, you might be unable to access the USB disk after changing Authentication settings. Please log out from the Windows and try to access again. Or you can change the address of the USB disk by referring to [To Customize the Address of the USB Storage Device](#).

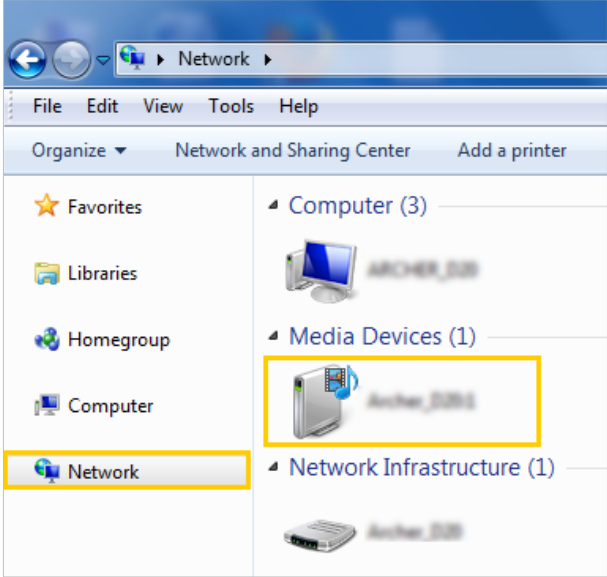
9.2. Media Sharing

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

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



- When your USB storage device is inserted into the router, your DLNA-supported devices (such as your computer and pad) connected to the router can detect and play the media files on the USB storage devices.
- Refer to the following table for detailed instructions.

Windows Computer	<ul style="list-style-type: none"> • Go to Computer > Network, then click the Media Server Name (Model number-share by default) in the Media Devices section. <p>Note: Here we take Windows 7 as an example.</p>  <p>The screenshot shows the Windows 7 Network folder. The 'Network' folder in the left sidebar is highlighted with a yellow box. In the main pane, the 'Media Devices (1)' section is expanded, and a device named 'Archos_2081' is highlighted with a yellow box. Other sections include 'Computer (3)', 'Network Infrastructure (1)', 'Favorites', 'Libraries', 'Homegroup', and 'Computer'.</p>
Tablet	<ul style="list-style-type: none"> • Use a third-party DLNA-supported player.

9.3. Time Machine

Time Machine backs up all files on your Mac computer to a USB storage device connected to 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 > 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: ---

● Please select a location for Time Machine backups

SELECT

Storage Limit for Backups: GB

(Enter "0" for no limit.)

3. Tick the checkbox to enable [Time Machine](#).
4. Click [Select](#) to select a location for Time Machine backups.
5. Set the [Size Limit for Backups](#).
■ Note: 0 means no limit for the space.
6. Click [SAVE](#).

Chapter 10

HomeShield

Customize your home network with enhanced security using a kit of features built in TP-Link HomeShield. Whether protecting your sensitive data or limiting the access of kids and guests, TP-Link HomeShield provides you the tools you need to fully manage your network.

It contains the following sections:

- [Network Security](#)
- [Parental Controls](#)
- [Network Analysis & Optimization](#)

10.1. Network Security

TP-Link HomeShield provides many tools to protect your network from malicious attacks.



Network Analysis

Analyze and optimize your network



IoT Protection

Get real-time security for your Internet of Things



Intrusion Prevention System

Identifies and block network intruders



Malicious Content Filter

Block malicious content



DDoS Protection

Protects your home network from DDoS attacks

- **To use this feature, download Tether to enjoy the HomeShield service**

1. Scan the QR code or get the Tether app from the Apple App Store or Google Play.



OR



2. Launch the Tether app and log in with your TP-Link ID. If you don't have an account, create one first.

3. Log in to your router and tap the HomeShield tab to use this feature.

10.2. 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.



Child Protection

Keep your child away from inappropriate content



Family Incentive Program

Manage screen time and create rewards



Family Time

Pause the internet to enjoy family time

- **To use this feature, download Tether to enjoy the HomeShield service**

1. Scan the QR code or get the Tether app from the Apple App Store or Google Play.



2. Launch the Tether app and log in with your TP-Link ID. If you don't have an account, create one first.

3. Log in to your router and tap the HomeShield tab to use this feature.

10.3. Network Analysis & Optimization

TP-Link HomeShield provides many tools for you to analyze and optimize your network.



Weekly and Monthly Reports

Get weekly and monthly reports of your network usage



Quality of Service (QoS)

Prioritizes devices to give faster performance



Scan

Run a scan for a better network performance and security anytime

- **To use this feature, download Tether to enjoy the HomeShield service**

1. Scan the QR code or get the Tether app from the Apple App Store or Google Play.



2. Launch the Tether app and log in with your TP-Link ID. If you don't have an account, create one first.
3. Log in to your router and tap the HomeShield tab to use this feature.



Chapter 11

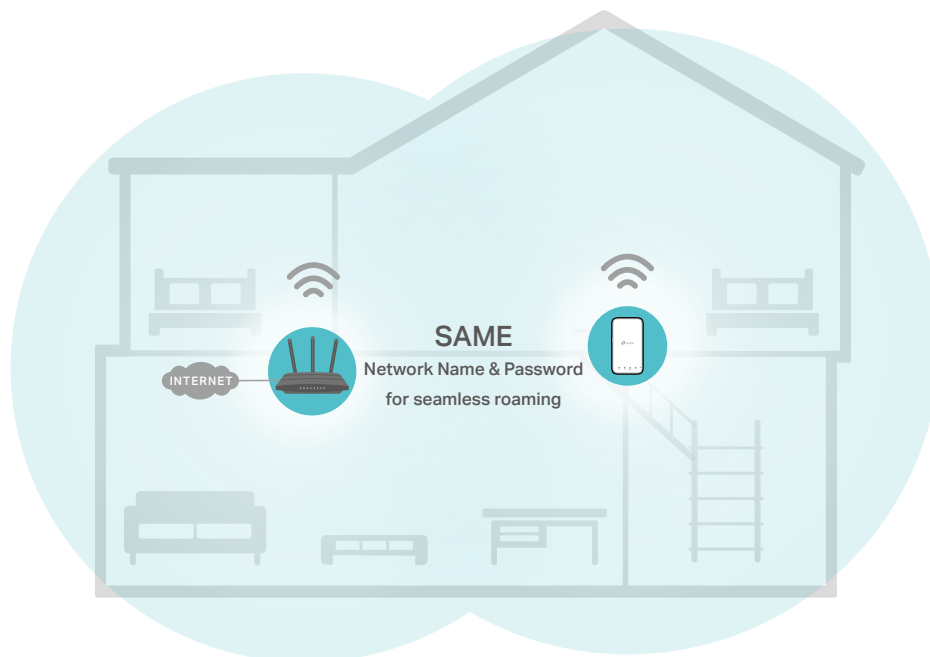
OneMesh with Seamless Roaming

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

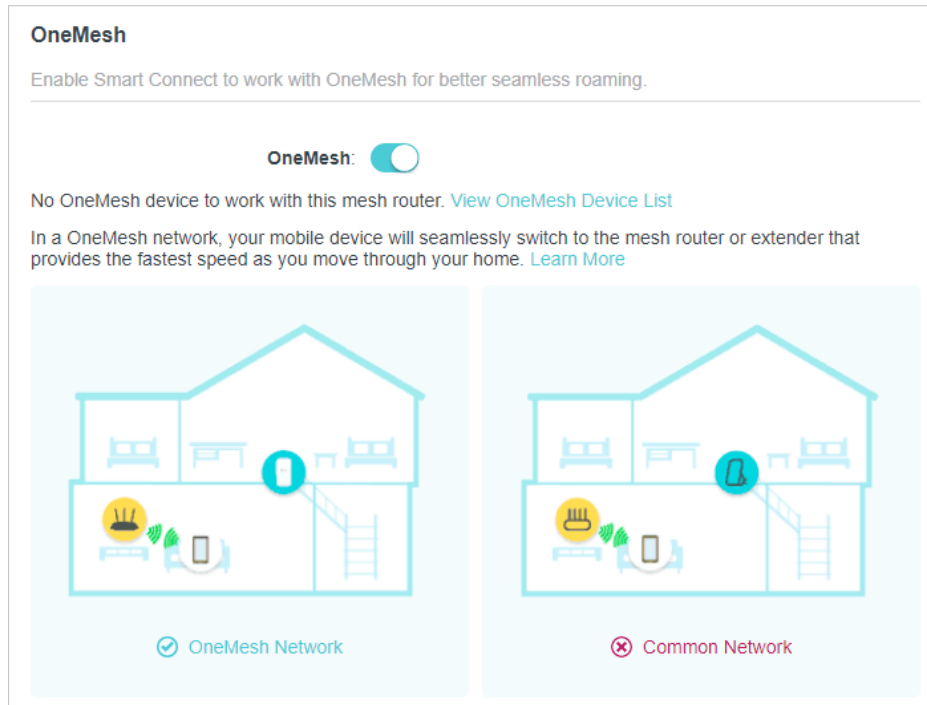
Devices automatically switch between your router and extenders as you move through your home for the fastest possible speeds.

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.

11.1. Set Up a OneMesh Network

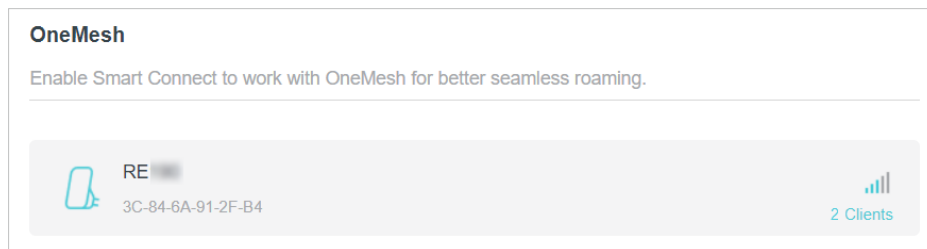
1. Visit <http://tplinkwifi.net>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > OneMesh**.
3. Enable **OneMesh**.



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.





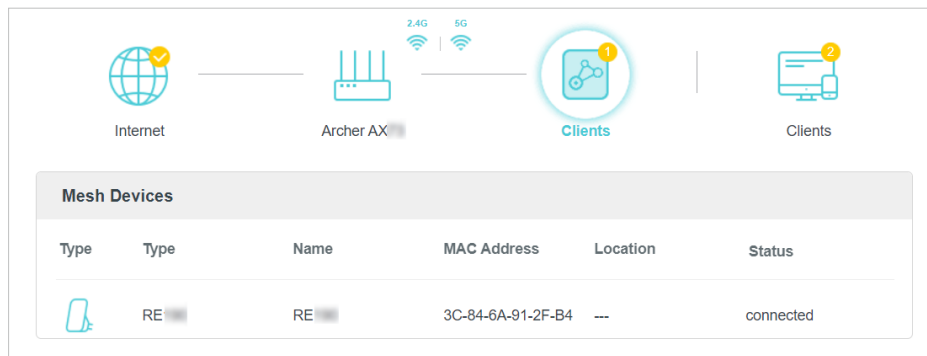
Done! Now your router and extender successfully form a OneMesh network!

11.2. 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.

The screenshot shows a web interface for managing a OneMesh device. The device name is 'RE'. The location is set to '- Please Select -'. The IP address is 192.168.0.50 and the MAC address is 3C-84-6A-91-2F-B4. The signal strength is shown as four bars, and the link speed is 130Mbps (2.4GHz) or 0Kbps (5GHz). There are two buttons: 'Leave OneMesh' and 'Manage Device'. A 'Clients' table is also visible, listing two devices: 'My-iPhone' and 'My-PC'.

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

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 12

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:

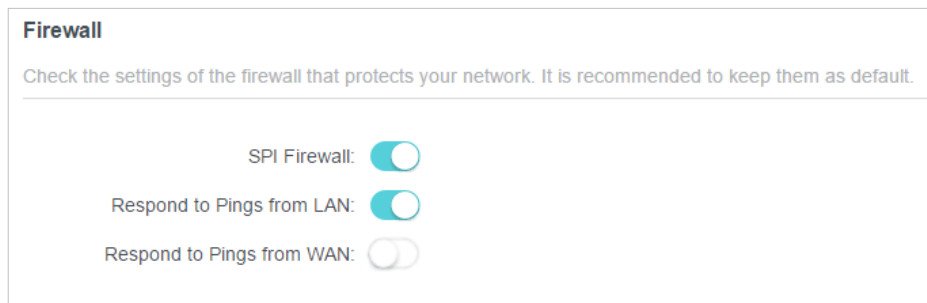
- [Protect the Network from Cyber Attacks](#)
- [Access Control](#)
- [IP & MAC Binding](#)

*For a more comprehensive home network protection system, refer to the [HomeShield](#) chapter.

12.1. 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.



12.2. 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:

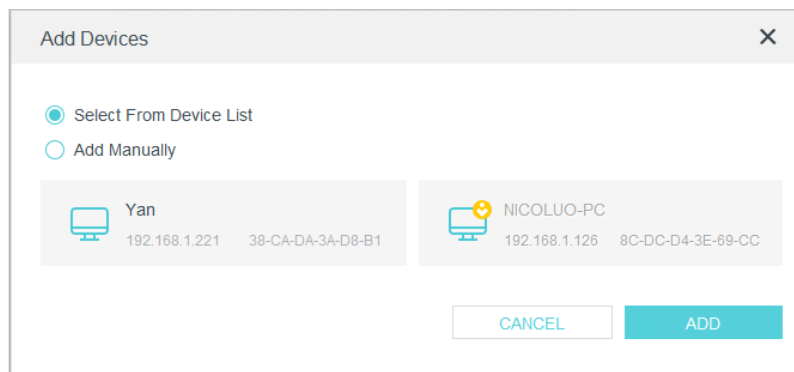
Access Mode: Blacklist
 Whitelist
 Configure a whitelist to only allow access to your network from the specified devices.

- 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**.

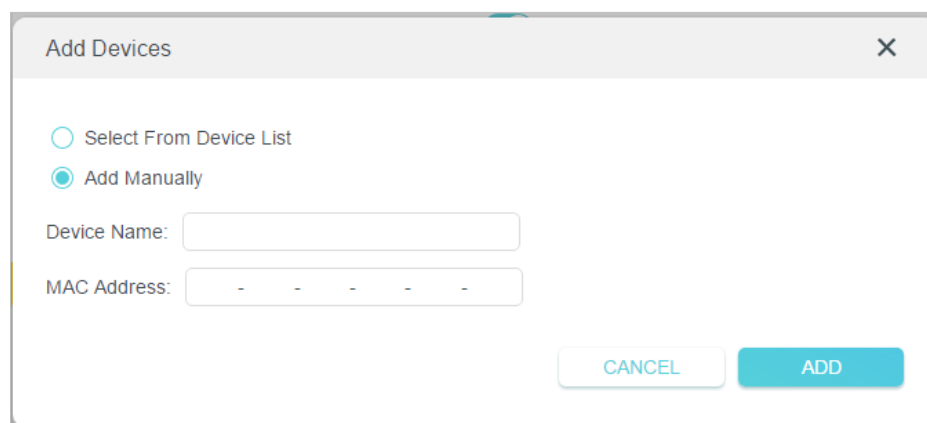


3) The **Operation Succeeded** message will appear on the screen, which means the selected devices have been successfully added to the whitelist.

- **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**.

12.3. IP & MAC Binding

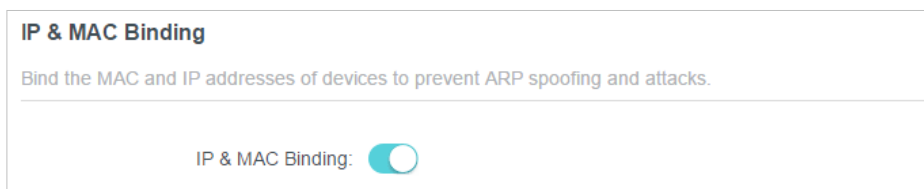
IP & MAC Binding, namely, ARP (Address Resolution Protocol) Binding, is used to bind network device's IP address to its MAC address. This will prevent ARP Spoofing and other ARP attacks by denying network access to an device with matching IP address in the Binding list, but unrecognized MAC address.

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

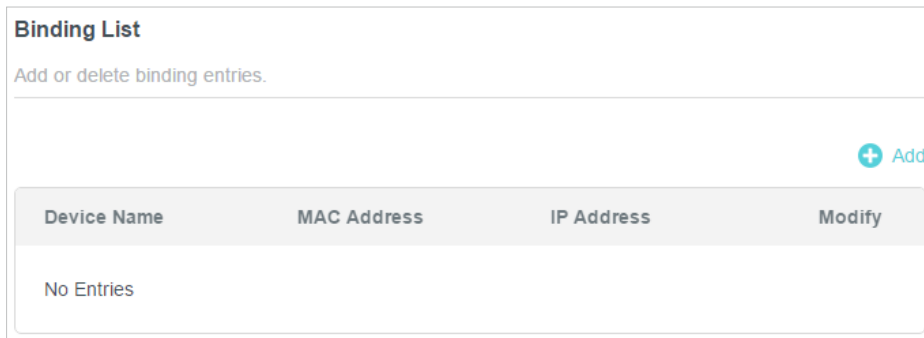
Bind the MAC and IP addresses of devices to prevent ARP spoofing and attacks.

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.



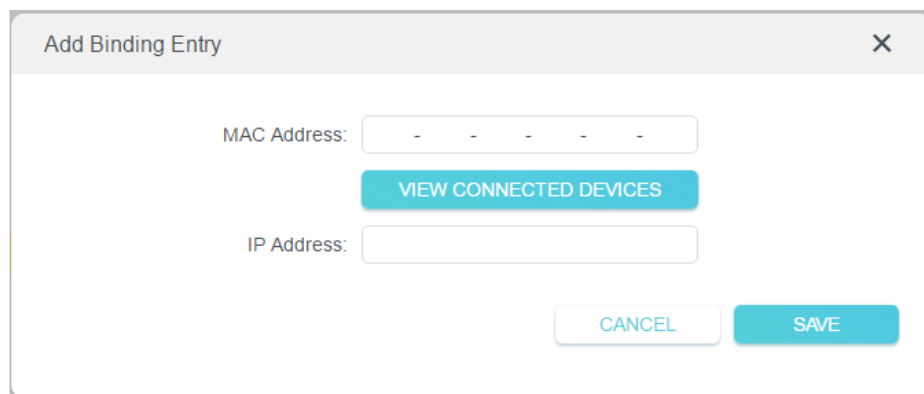
Binding List

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!

12.4. 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 13

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](#)

13. 1. Share Local Resources on the Internet by Port Forwarding

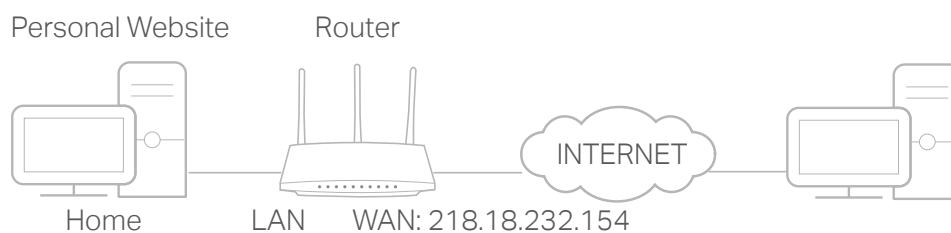
When you build up a server on the local network and want to share it on the internet, Port Forwarding can realize the service and provide it to internet users. At the same time Port Forwarding can keep the local network safe as other services are still invisible from the internet.

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						

5. Click [VIEW COMMON SERVICES](#) and select [HTTP](#). The [External Port](#), [Internal Port](#) and [Protocol](#) will be automatically filled in.
6. 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.
7. Click [SAVE](#).

Add a Port Forwarding Entry ✕

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](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.

13.2. 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.

13.3. 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.

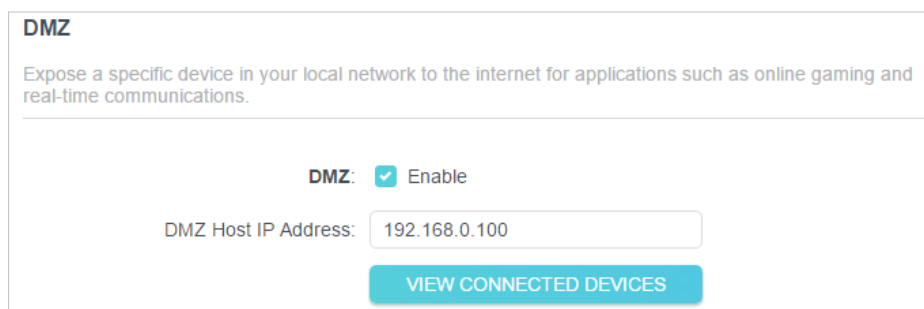
I want to:

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.



DMZ

Expose a specific device in your local network to the internet for applications such as online gaming and real-time communications.

DMZ: Enable

DMZ Host IP Address:

[VIEW CONNECTED DEVICES](#)

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.

13.4. Make Xbox Online Games Run Smoothly by UPnP

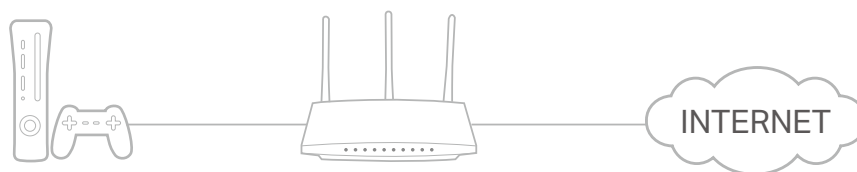
The UPnP (Universal Plug and Play) protocol allows applications or host devices to automatically find the front-end NAT device and send request to it to open the corresponding ports. With UPnP enabled, the applications or host devices on the local network and the internet can freely communicate with 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).

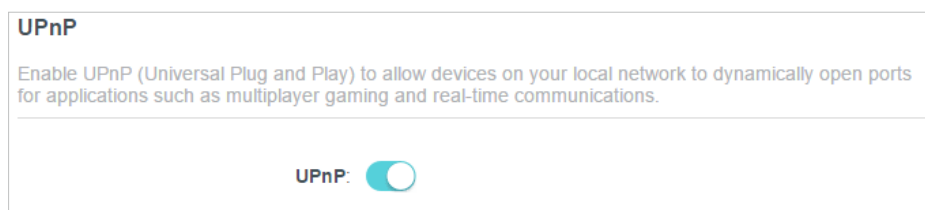
For example, when you connect your Xbox to the router which has connected to the internet to play online games, UPnP will send request to the router to open the

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 14

VPN Server&Client

The router offers several ways to set up VPN connections:

VPN Server allows remote devices to access your home network in a secured way through the internet. The router supports three types of VPN Server:

OpenVPN is somewhat complex but with higher security and more stability, suitable for restricted environments such as campus network and company intranet.

PPTP VPN is easy to use with the built-in VPN software of computers and mobile devices, but it is vulnerable and may be blocked by some ISPs.

L2TP/IPSec VPN is more secure but slower than PPTP VPN, and may have trouble getting around firewalls.

VPN Client allows devices in your home network to access remote VPN servers, without the need to install VPN software on each device.

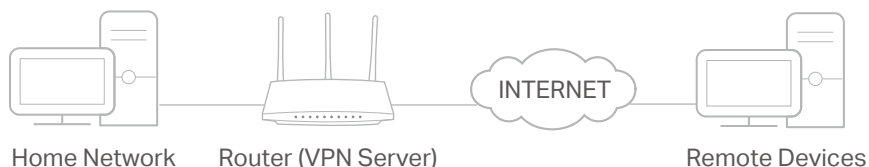
This chapter contains the following sections:

- [Use OpenVPN to Access Your Home Network](#)
- [Use PPTP VPN to Access Your Home Network](#)
- [Use L2TP/IPSec VPN to Access Your Home Network](#)
- [Use VPN Client to Access a Remote VPN Server](#)

14. 1. Use OpenVPN to Access Your Home Network

OpenVPN Server is used to create an OpenVPN connection for remote devices to access your home network.

To use the VPN feature, you need to enable OpenVPN Server on your router, and install and run VPN client software on remote devices. 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.

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

PPTP VPN Server is used to create a PPTP VPN connection for remote devices to access your home network.

To use the VPN feature, you need to set up PPTP VPN Server on your router, and configure the PPTP connection on remote devices. 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](#).

PPTP

Set up a PPTP VPN and accounts for quick, remote access to your network.

PPTP: [Enable](#)

Client IP Address: -
(up to 10 clients)

[Allow Samba \(Network Place\) access](#)

[Allow NetBIOS passthrough](#)

[Allow Unencrypted connections](#)

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.

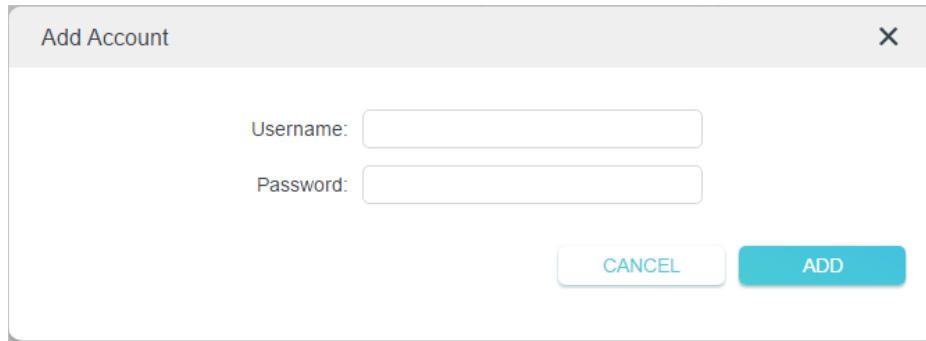
Account List

Configure accounts (up to 16) that can be used by remote clients to connect to the VPN server.

[+ Add](#)

Username	Password	Modify
admin	admin	✎ 🗑

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

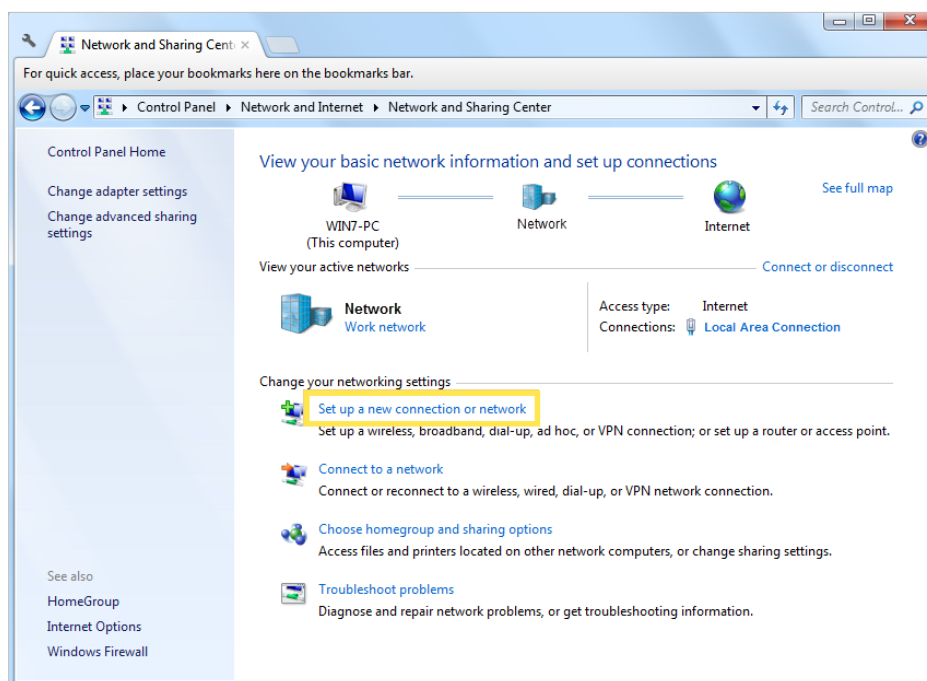


3) Click [ADD](#).

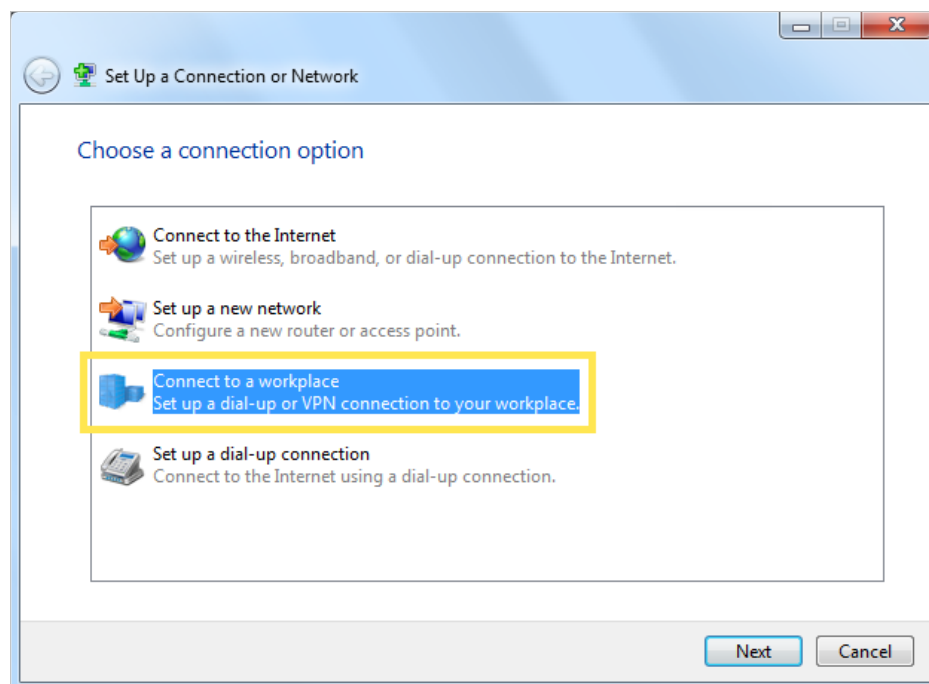
Step 2. Configure PPTP VPN Connection on Your Remote Device

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.

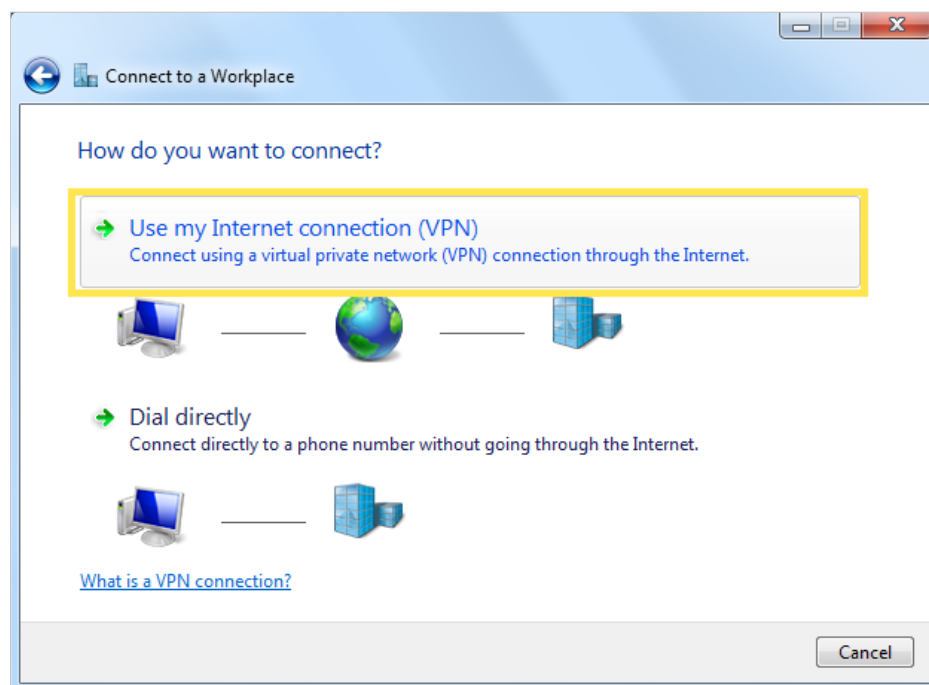
1. Go to [Start > Control Panel > Network and Internet > Network and Sharing Center](#).
2. Select [Set up a new connection or network](#).



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**.