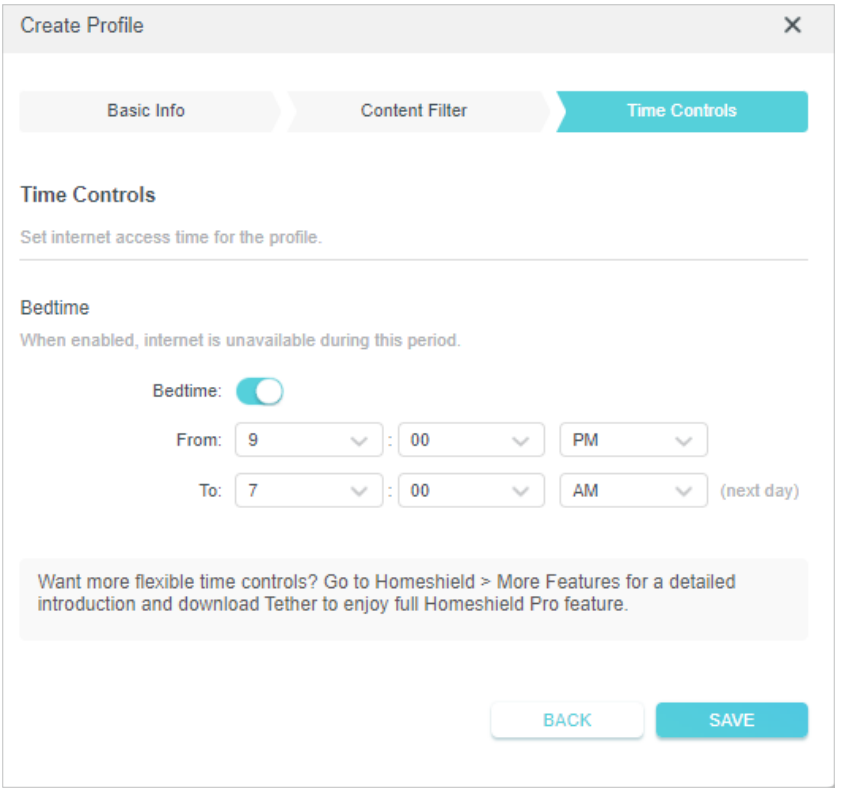
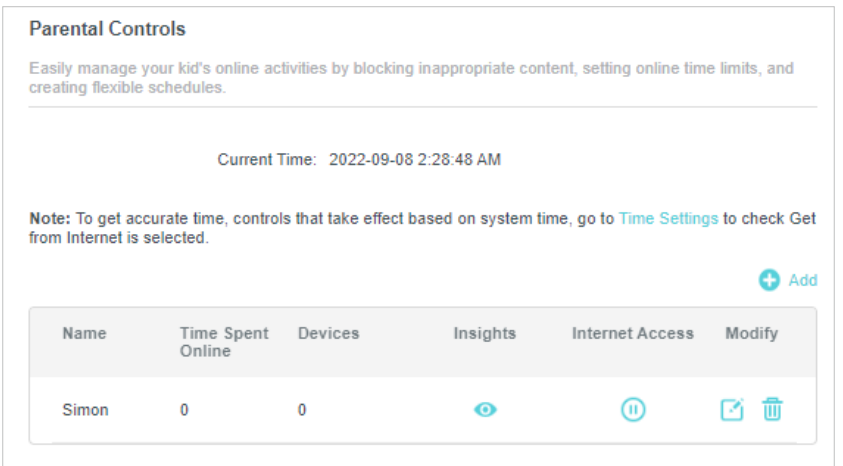


4) Enable Bed Time and use the up/down arrows or enter times in the fields. Devices under this profile will be unable to access the internet during this time period.

5) Click SAVE.

6) After adding a profile, you can click the Insight icon to check the detailed visited history, and click the pause the network for this profile anytime.

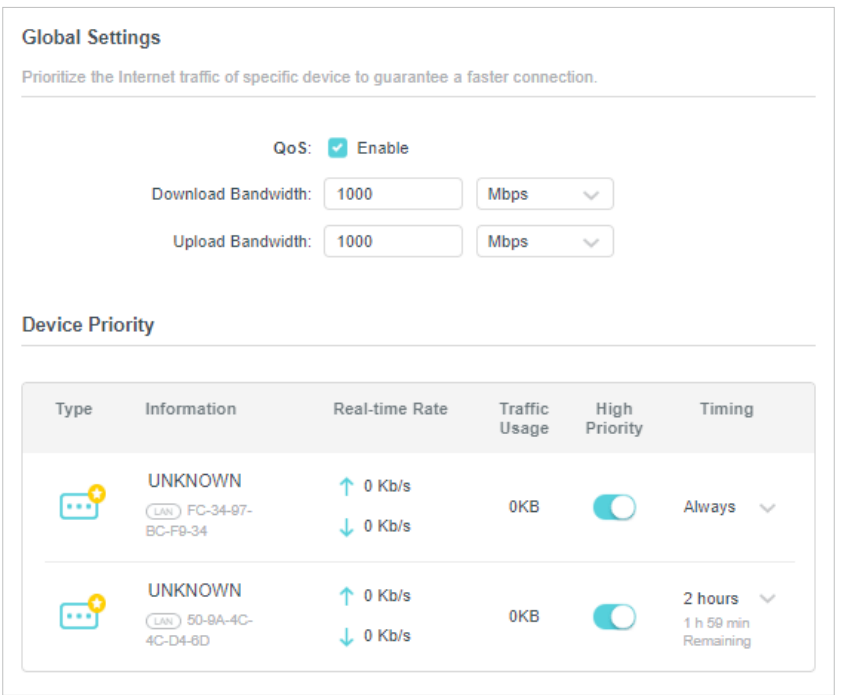


Note: You can go to Advanced > HomeShield > More Features for a detailed introduction and download Tether to enjoy full Homeshield Pro feature.

11. 3. QoS

QoS (Quality of Service) allows you to prioritize connection of specific devices for a set duration. Devices set as high priority will be allocated more bandwidth and so continue to run smoothly even when there is heavy traffic on the network.

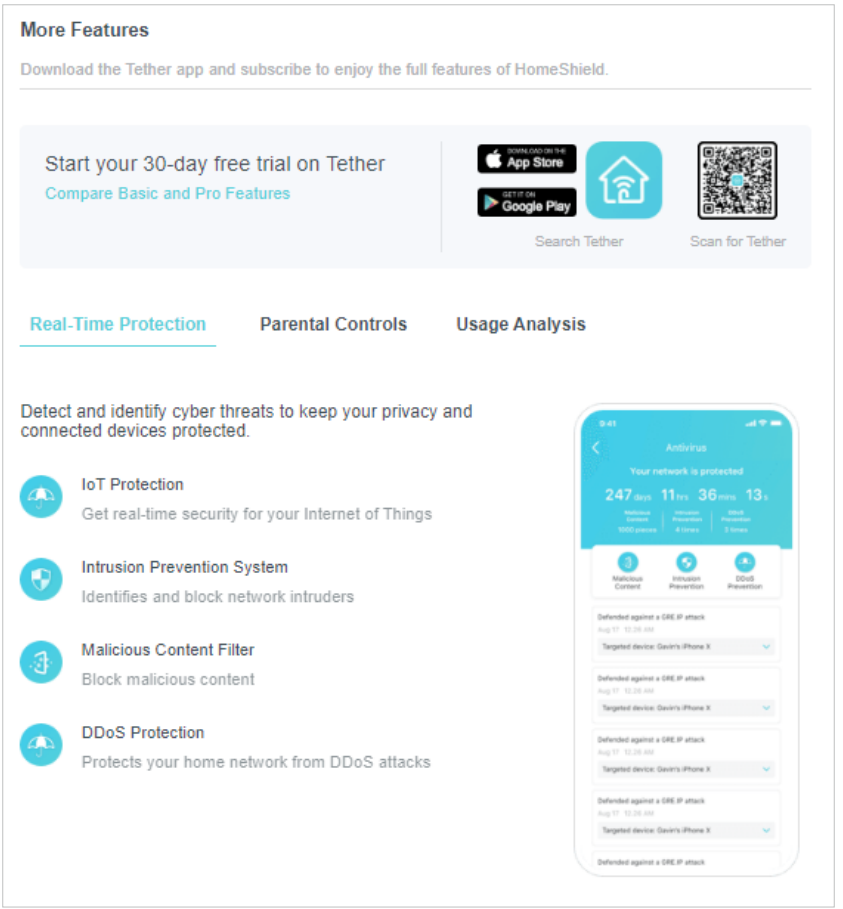
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > HomeShield > QoS.
3. Enable QoS to set the total bandwidth. Then click SAVE.
4. Enable High Priority for the desired device and set its effective time.



11. 4. More Features

Download the Tether app and subscribe to enjoy the full features of HomeShield.

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 > HomeShield > More Features.
3. Follow the web instructions to get full features of HomeShield.


More Features
Download the Tether app and subscribe to enjoy the full features of HomeShield.
Start your 30-day free trial on Tether
Compare Basic and Pro Features
App Store
Google Play
Search Tether
Scan for Tether
Real-Time Protection
Parental Controls
Usage Analysis
Detect and identify cyber threats to keep your privacy and connected devices protected.
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

Chapter 12

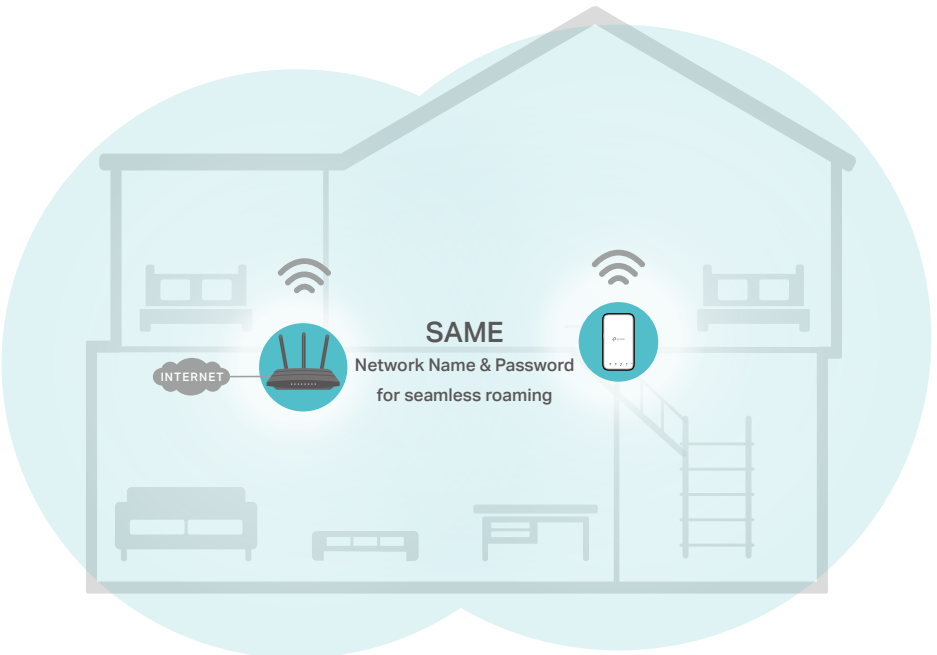
OneMesh with Seamless Roaming

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

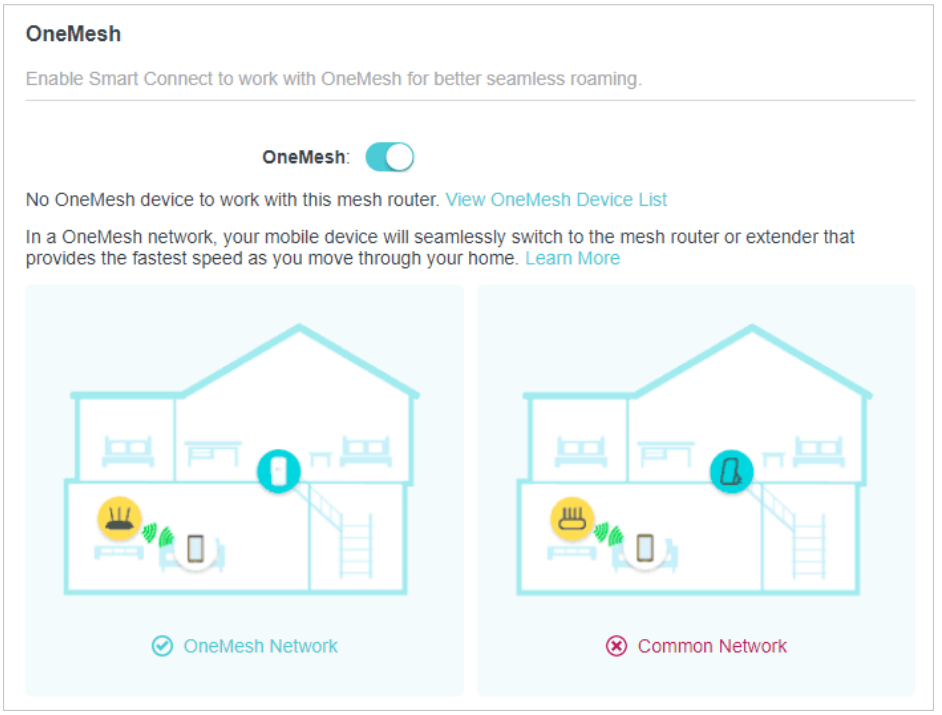
Devices automatically switch between your router and extenders as you move through your home for the fastest possible speeds.

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.

12. 1. Set Up a OneMesh Network

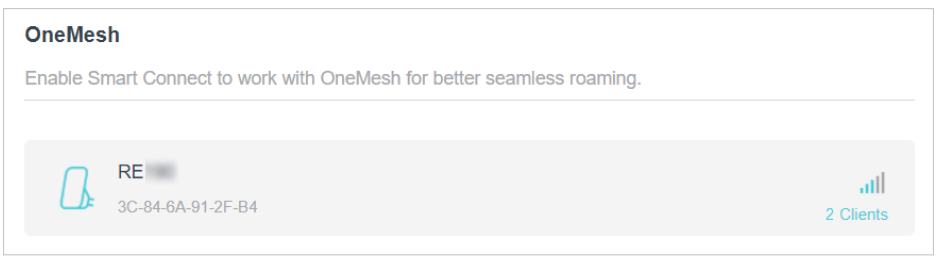
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > OneMesh.
3. Enable OneMesh.



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.

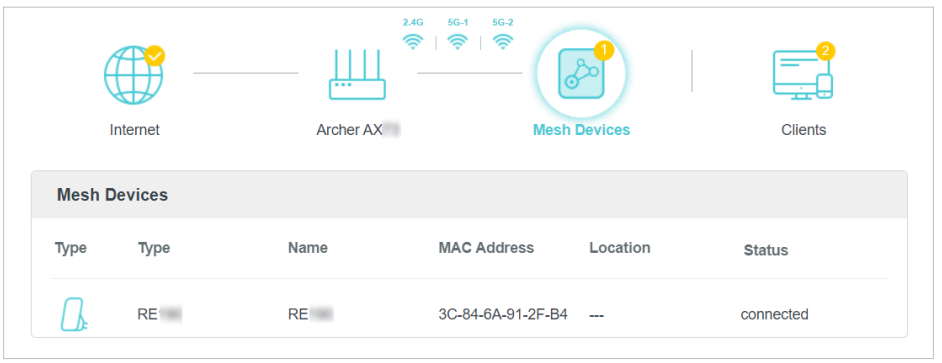
Done! Now your router and extender successfully form a OneMesh network!

12. 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.

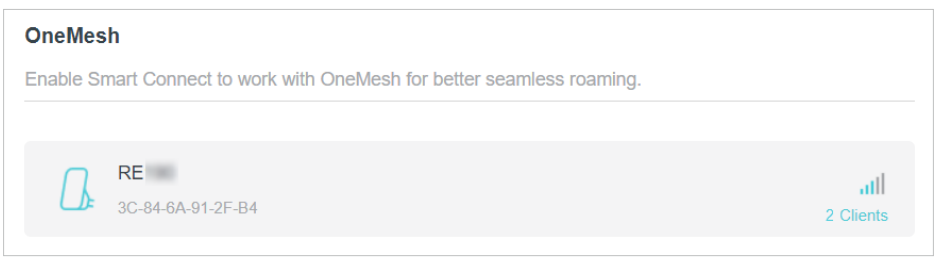
- **To view mesh devices and connected clients in the network:**

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.

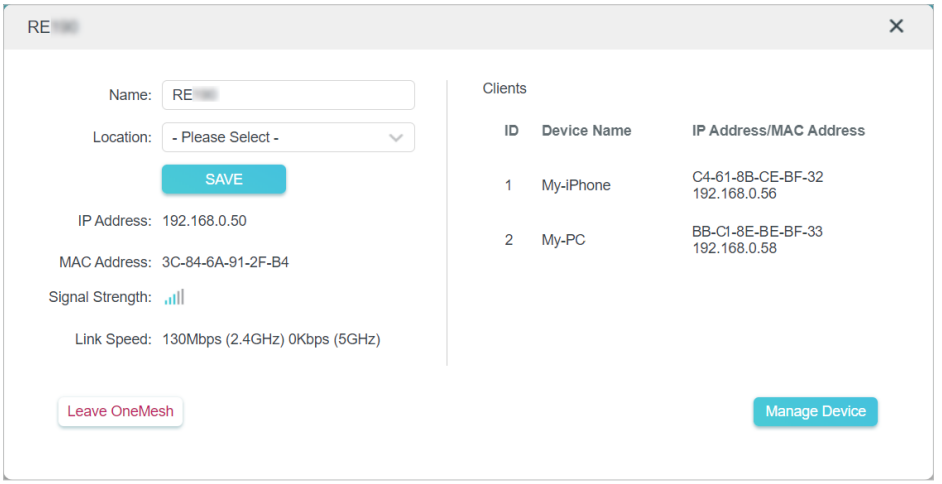


- **To manage a OneMesh device in the network:**

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.



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 13

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:

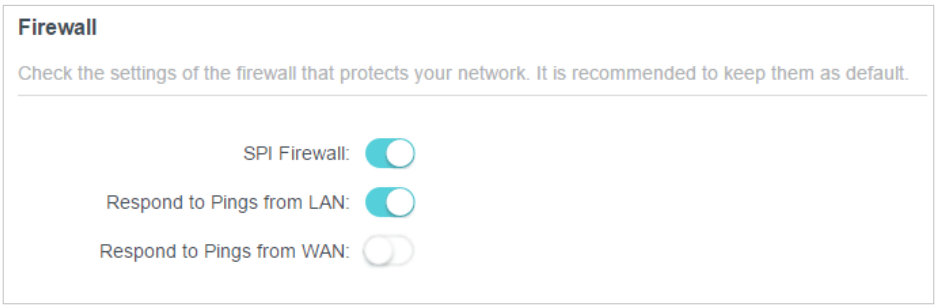
- Protect the Network from Cyber Attacks
- Access Control
- IP & MAC Binding
- ALG

*For a more comprehensive home network protection system, refer to the HomeShield chapter.

13. 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.



13. 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:

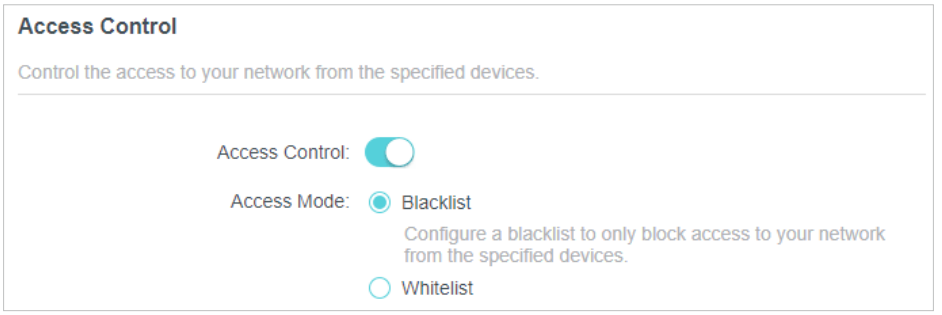
Block or allow specific client devices to access my network (via wired or wireless).

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.

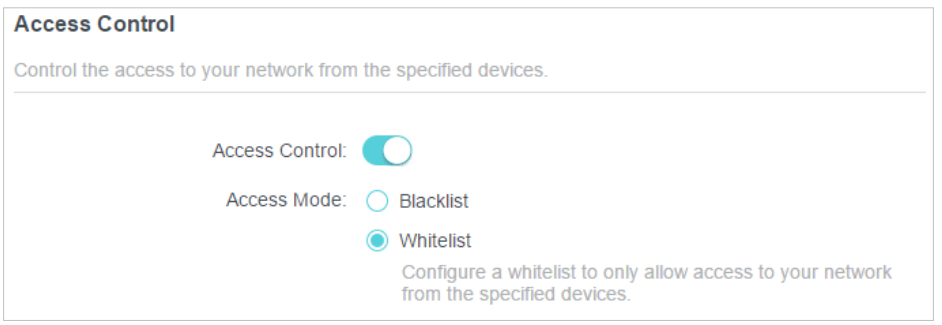


2) Click Add and select devices you want to be blocked and Click ADD.

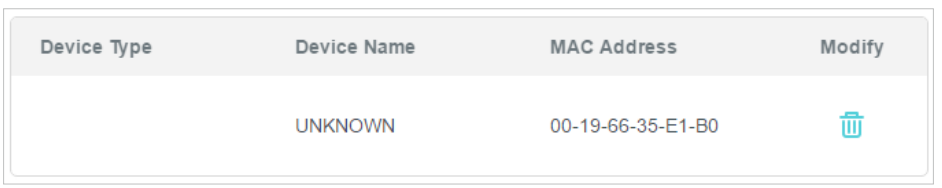
3) The Operation Succeeded message will appear on the screen, which means the selected devices have been successfully added to the blacklist.

To allow specific device(s):

1) Select Whitelist and click SAVE.



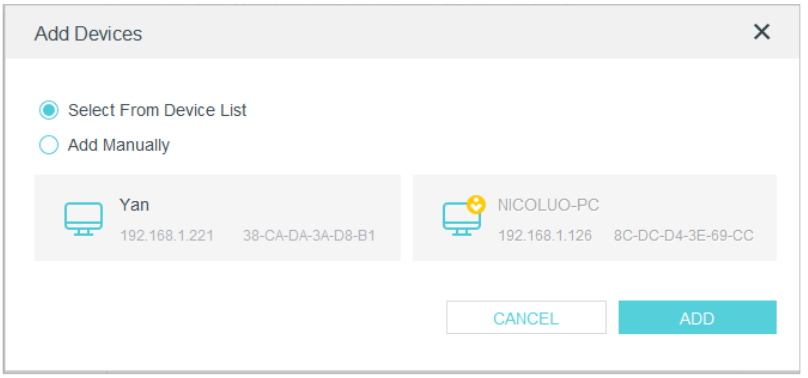
2) Your own device is in the whitelist by default and cannot be deleted. Click Add to add other devices to the whitelist.



- **Add connected devices**

1) Click Select From Device List.

2) Select the devices you want to be allowed and click ADD.

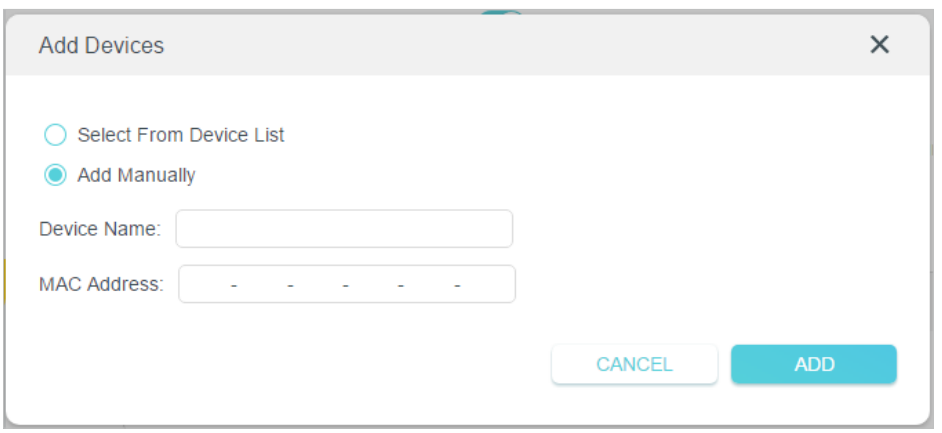


3) The Operation Succeeded message will appear on the screen, which means the selected devices have been successfully added to the whitelist.

- **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.

13. 3. IP & MAC Binding

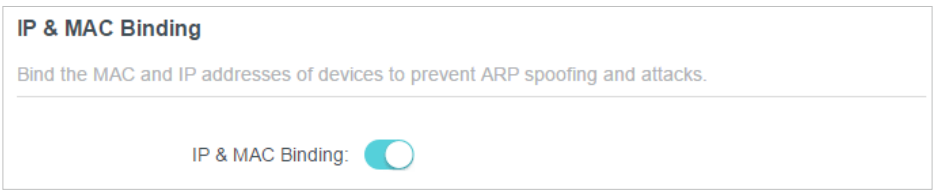
IP & MAC Binding, namely, ARP (Address Resolution Protocol) Binding, is used to bind network device's IP address to its MAC address. This will prevent ARP Spoofing and other ARP attacks by denying network access to an device with matching IP address in the Binding list, but unrecognized MAC address.

I want to:

Prevent ARP spoofing and ARP attacks.

How can I do that?

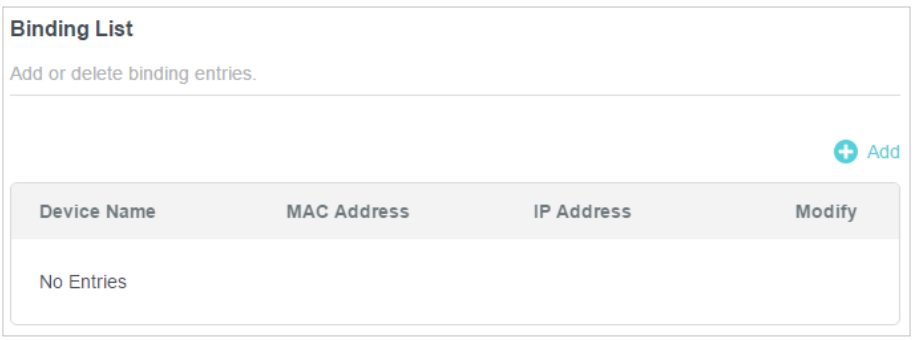
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > Security > IP & MAC Binding.
3. Enable IP & MAC Binding.



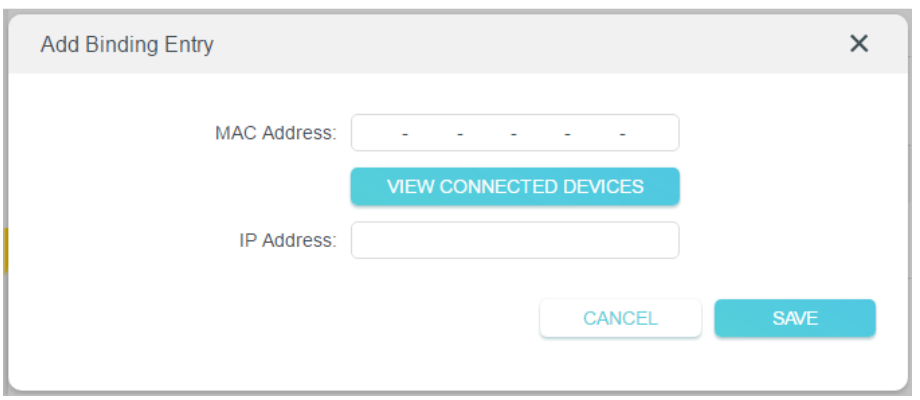
4. Bind your device(s) according to your need.

   To bind the connected device(s):

   1) Click Add in the Binding List section.



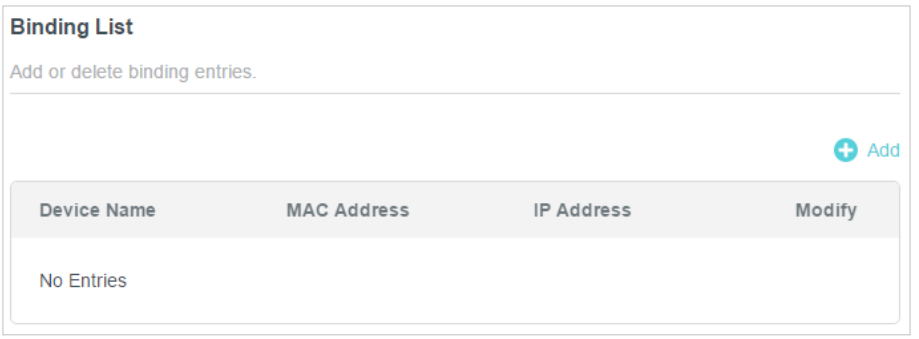
   2) Click VIEW CONNECTED DEVICES and select the device you want to bind. The MAC Address and IP Address fields will be automatically filled in.



   3) Click SAVE.

To bind the unconnected device:

1) Click Add in the Binding List section.



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

3) Click SAVE.

Done!

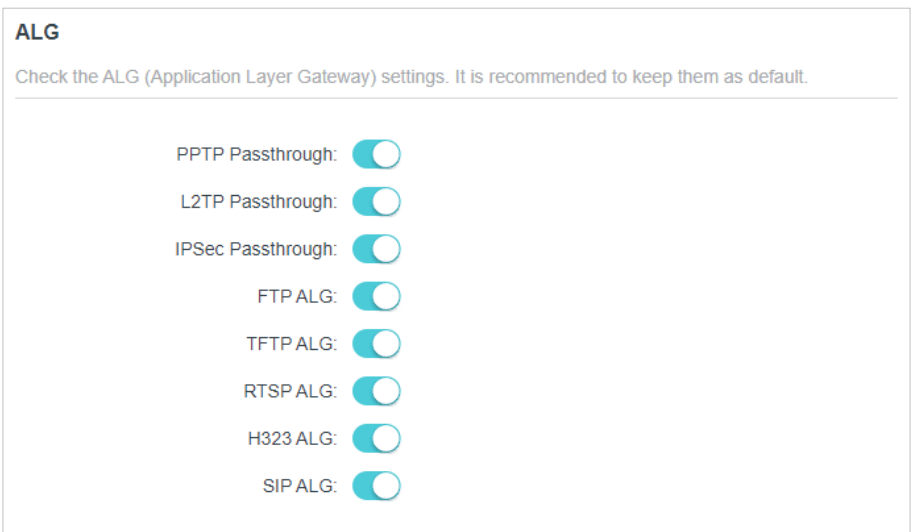
Now you don't need to worry about ARP spoofing and ARP attacks!

13. 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.



Chapter 14

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

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

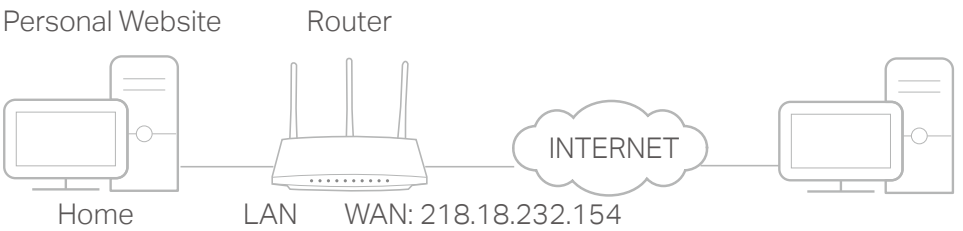
When you build up a server on the local network and want to share it on the internet, Port Forwarding can realize the service and provide it to internet users. At the same time Port Forwarding can keep the local network safe as other services are still invisible from the internet.

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:

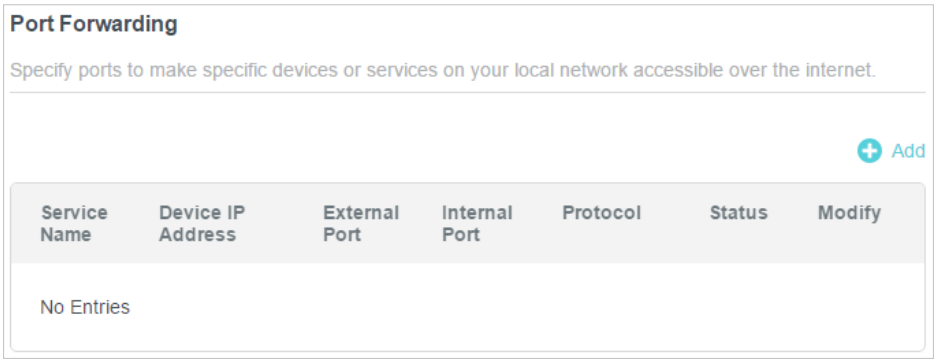
Share my personal website I've built in local network with my friends through the internet.

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.

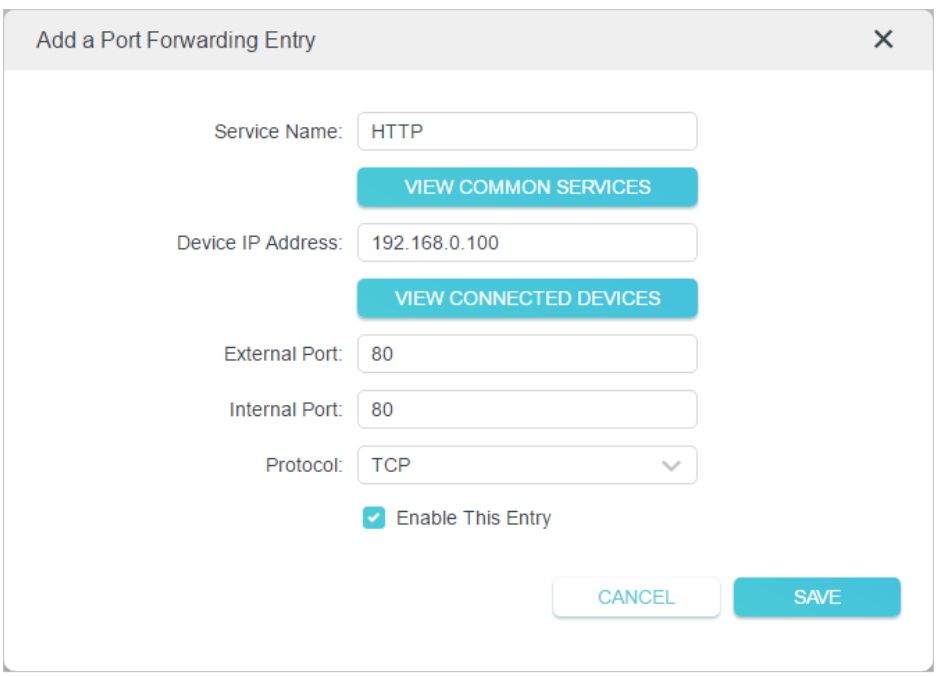


How can I do that?

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.



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.



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.

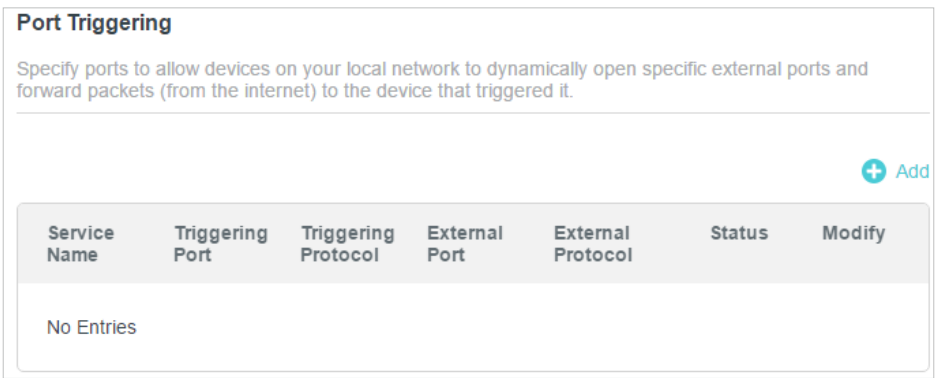
Tips:
- The WAN IP should be a public IP address. For the WAN IP is assigned dynamically by the ISP, it is recommended to apply and register a domain name for the WAN referring to Set Up a Dynamic DNS Service Account. Then users on the internet can use http:// domain name to visit the website.
- If you have changed the default External Port, you should use http:// WAN IP: External Port or http:// domain name: External Port to visit the website.

14. 2. Open Ports Dynamically by Port Triggering

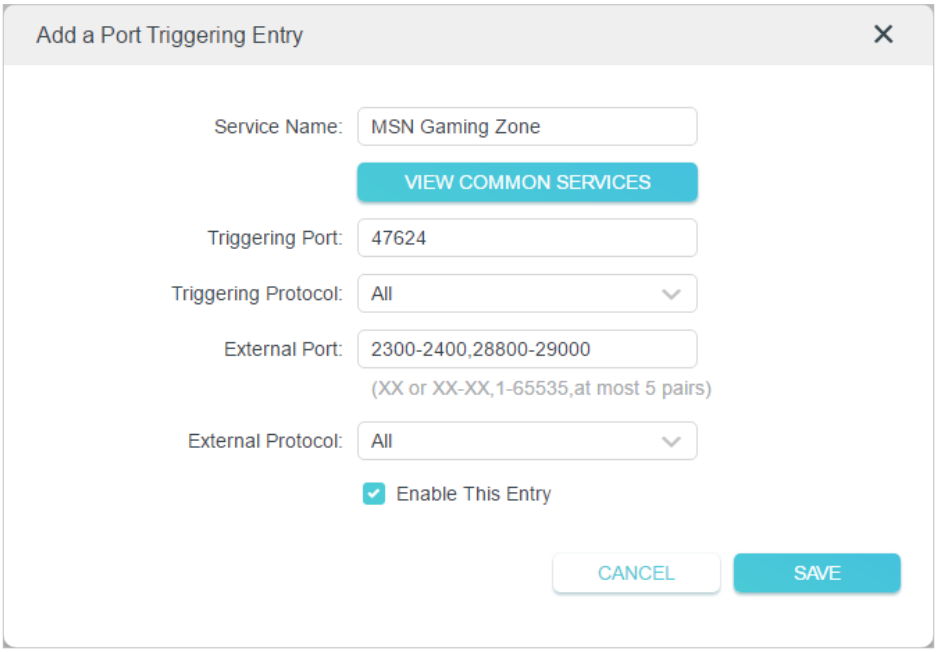
Port Triggering can specify a triggering port and its corresponding external ports. When a host on the local network initiates a connection to the triggering port, all the external ports will be opened for subsequent connections. The router can record the IP address of the host. When the data from the 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.



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.

14. 3. Make Applications Free from Port Restriction by DMZ

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

Note:

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

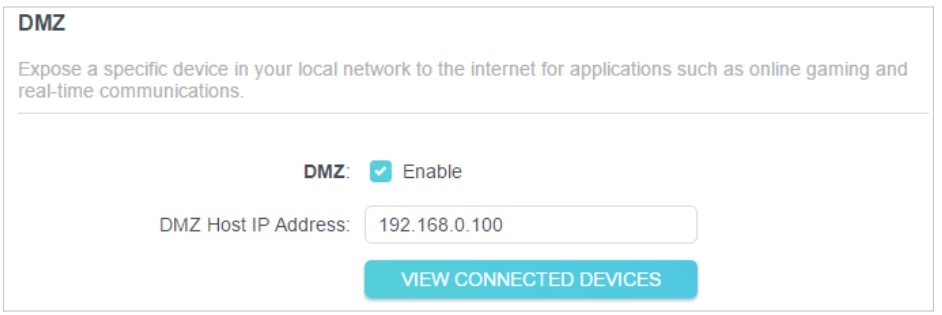
I want to:

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

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

How can I do that?

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



5. Click SAVE.

Done!

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

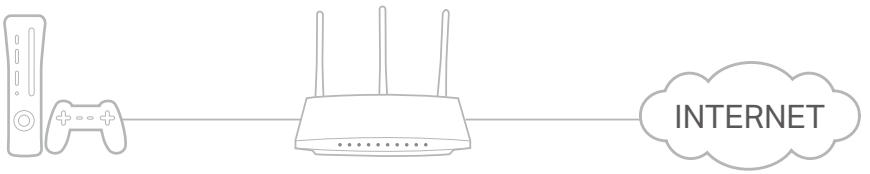
14. 4. Make Xbox Online Games Run Smoothly by UPnP

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).

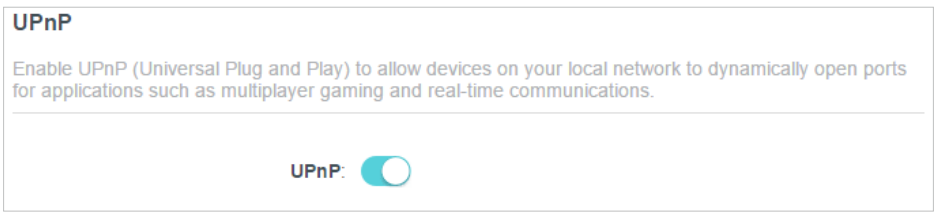
For example, when you connect your Xbox to the router which has connected to the internet to play online games, UPnP will send request to the router to open the

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 15

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.

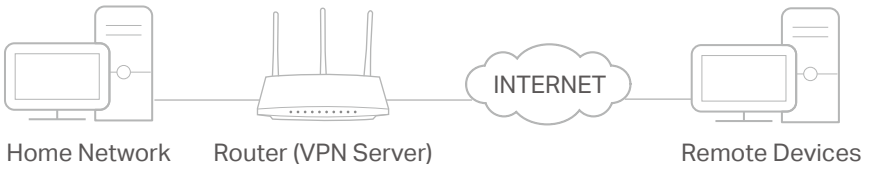
This chapter contains the following sections:

- 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

15. 1. Use OpenVPN to Access Your Home Network

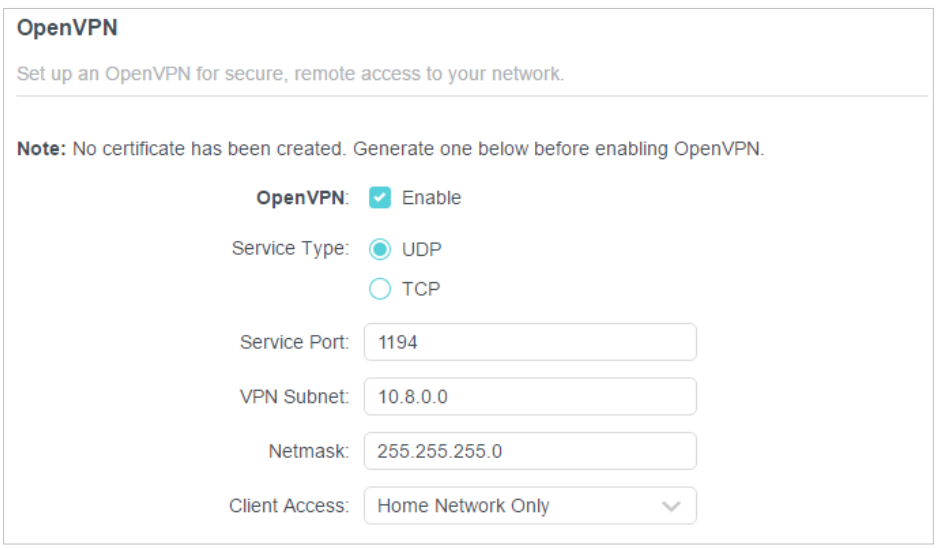
OpenVPN Server is used to create an OpenVPN connection for remote devices to access your home network.

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.

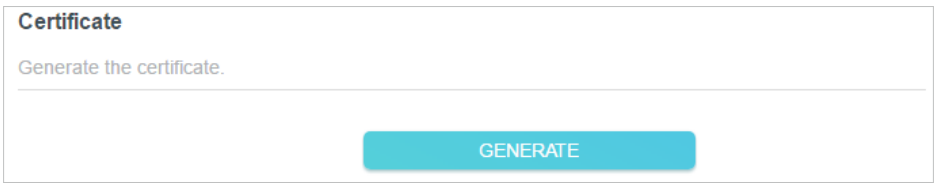


Note:

- 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.

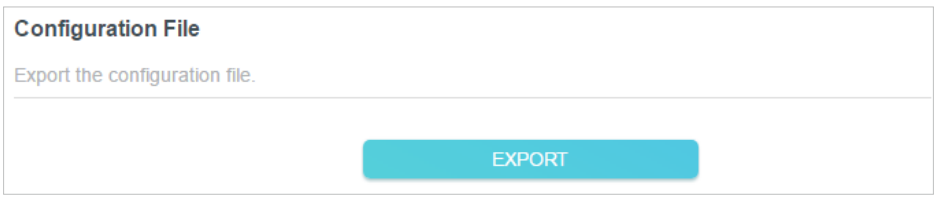
3. Select the Service Type (communication protocol) for OpenVPN Server: UDP, TCP.
4. Enter a VPN Service Port to which a VPN device connects, and the port number should be between 1024 and 65535.
5. In the VPN Subnet/Netmask fields, enter the range of IP addresses that can be leased to the device by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

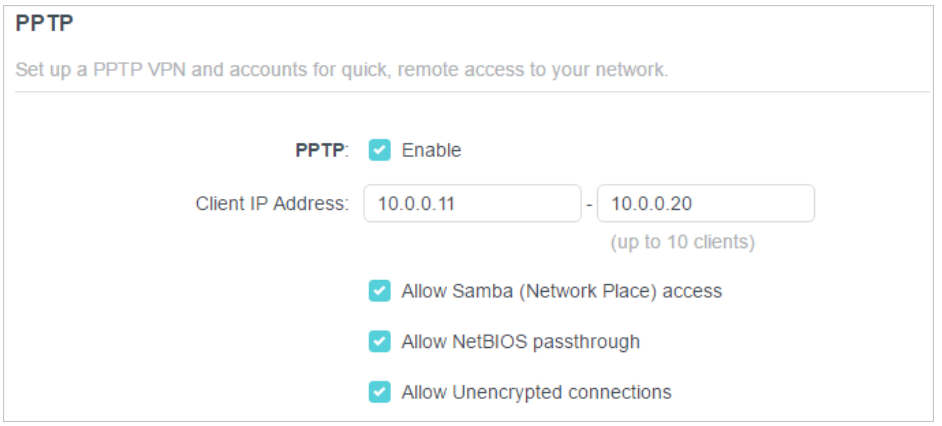
15. 2. Use PPTP VPN to Access Your Home Network

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.

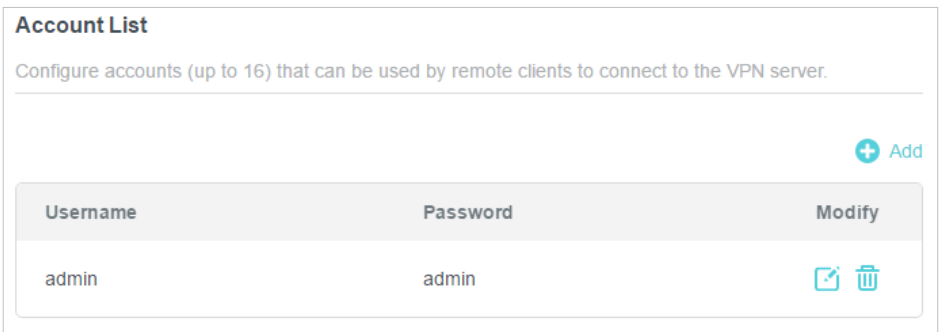
Step 1. Set up PPTP VPN Server on Your Router

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.

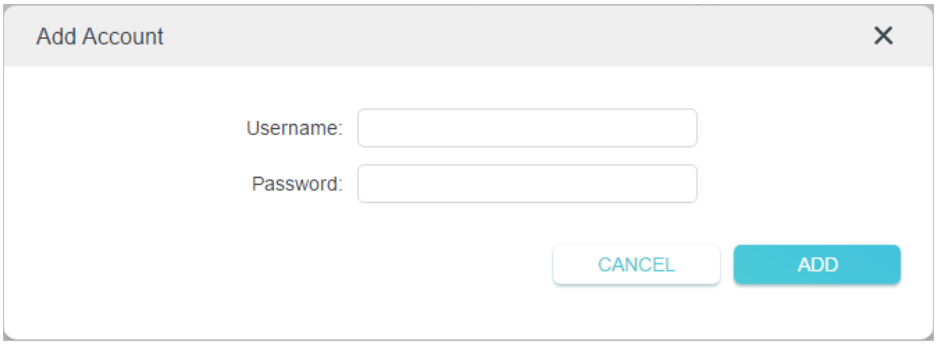


Note: Before you enable VPN Server, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router's WAN port and synchronize your System Time with internet.

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.

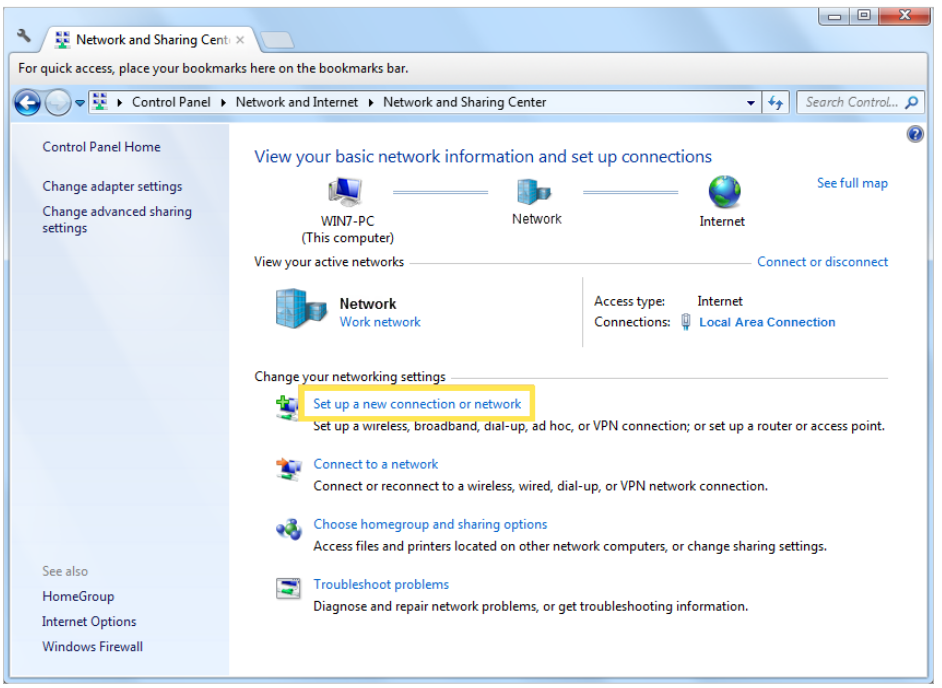


3) Click ADD.

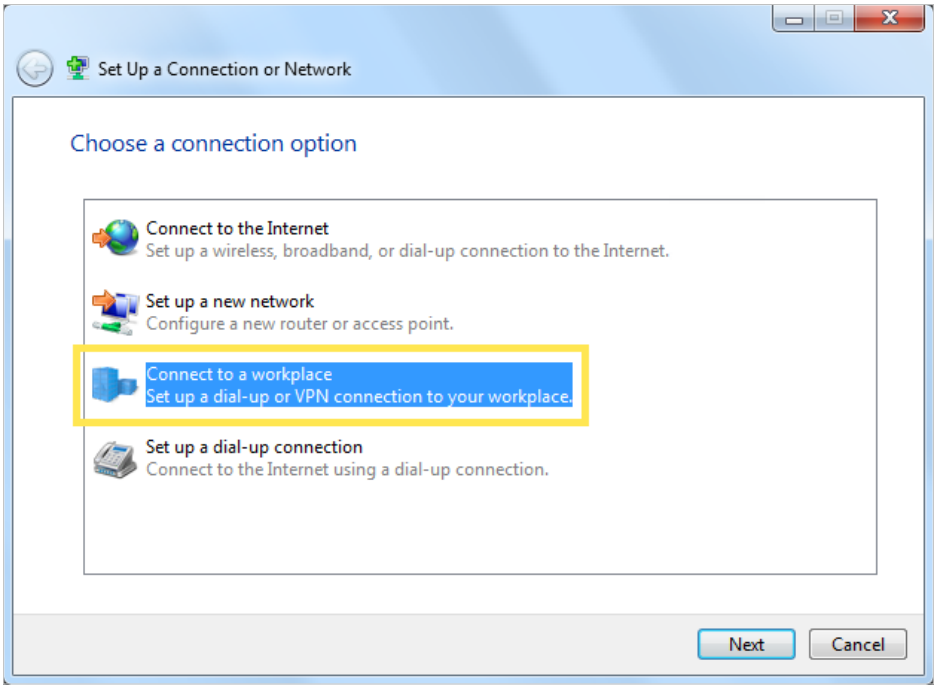
Step 2. Configure PPTP VPN Connection on Your Remote Device

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.

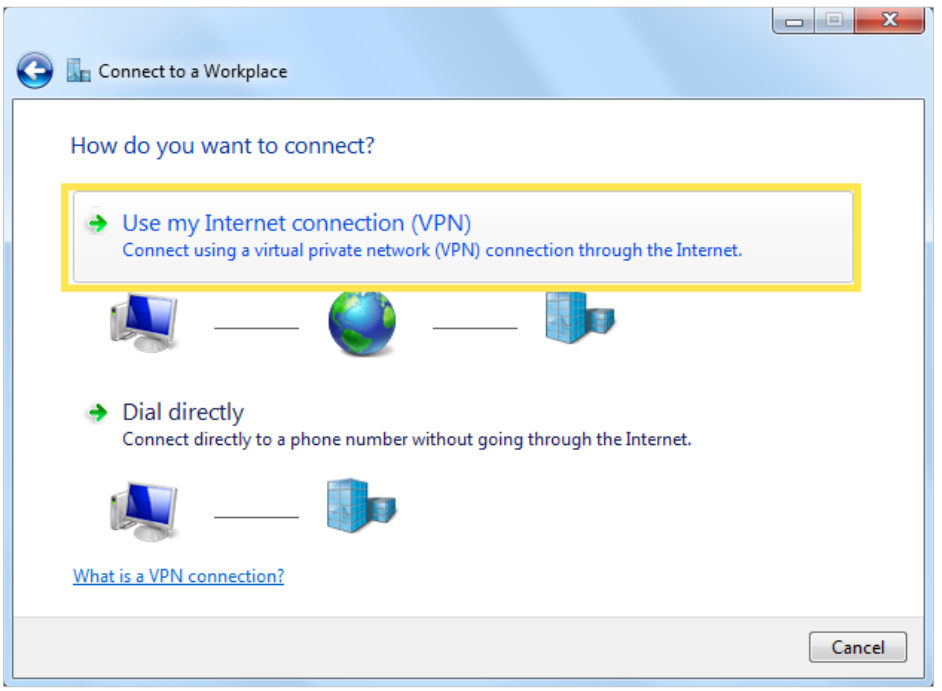
1. Go to Start > Control Panel > Network and Internet > Network and Sharing Center.
2. Select Set up a new connection or network.



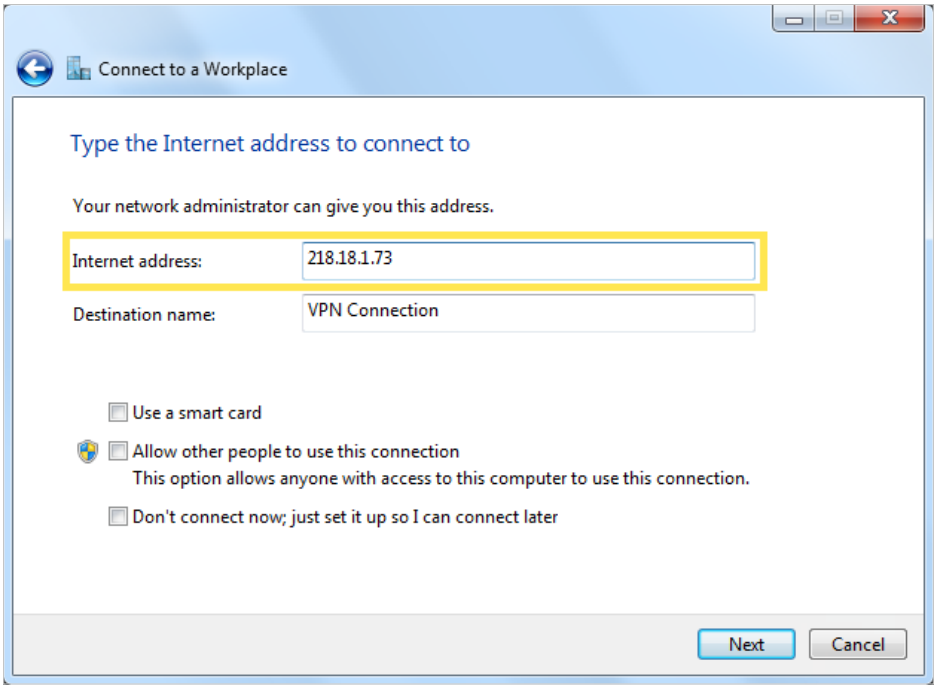
3. Select Connect to a workplace and click Next.



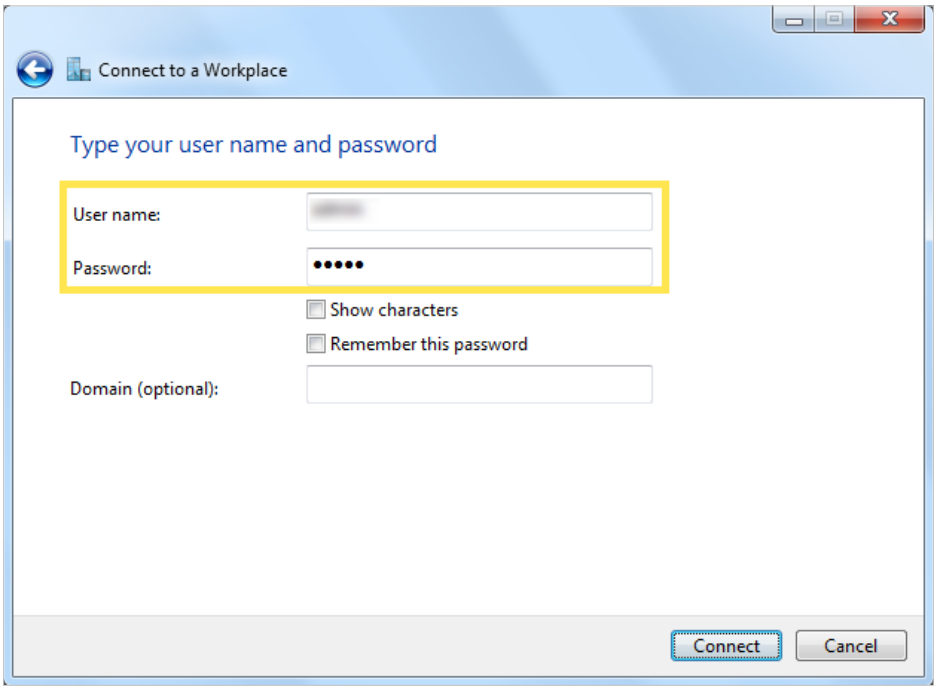
4. Select Use my Internet connection (VPN).



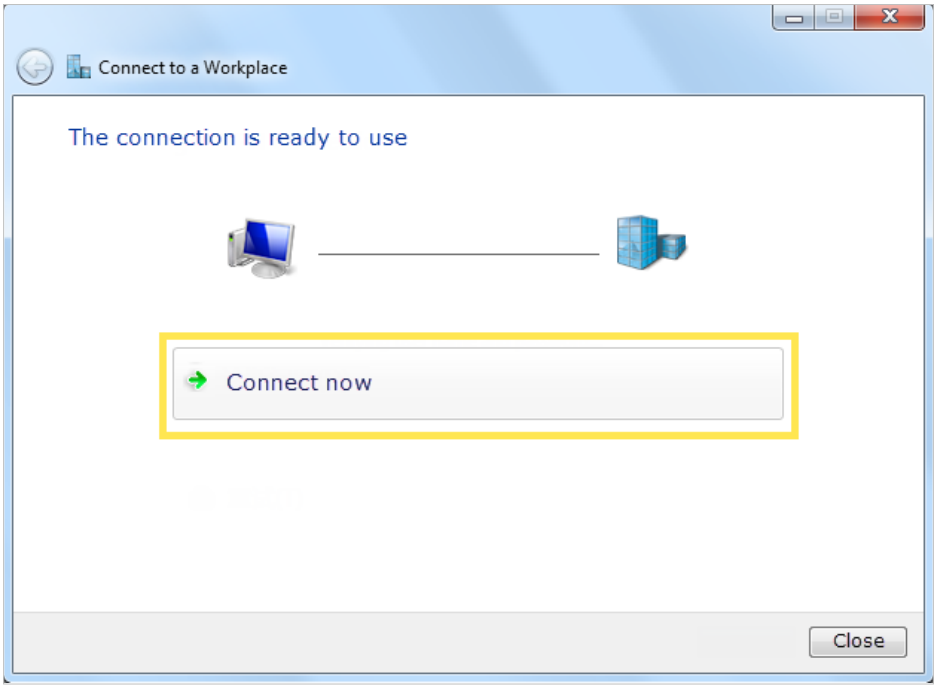
5. Enter the internet IP address of the router (for example: 218.18.1.73) in the Internet address field. Click Next.



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



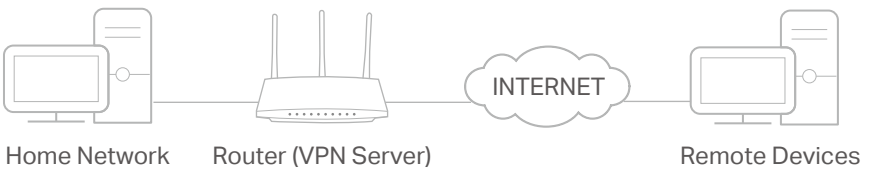
7. Click Connect Now when the VPN connection is ready to use.



15. 3. Use L2TP/IPSec VPN to Access Your Home Network

L2TP/IPSec VPN Server is used to create a L2TP/IPSec VPN connection for remote devices to access your home network.

To use the VPN feature, you need to set up L2TP/IPSec VPN Server on your router, and configure the L2TP/IPSec connection on remote devices. Please follow the steps below to set up the L2TP/IPSec VPN connection.

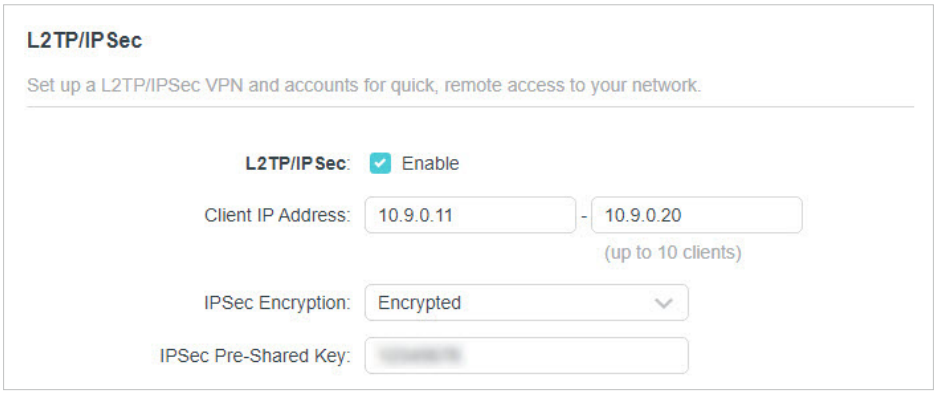


Step 1. Set up L2TP/IPSec VPN Server on Your Router

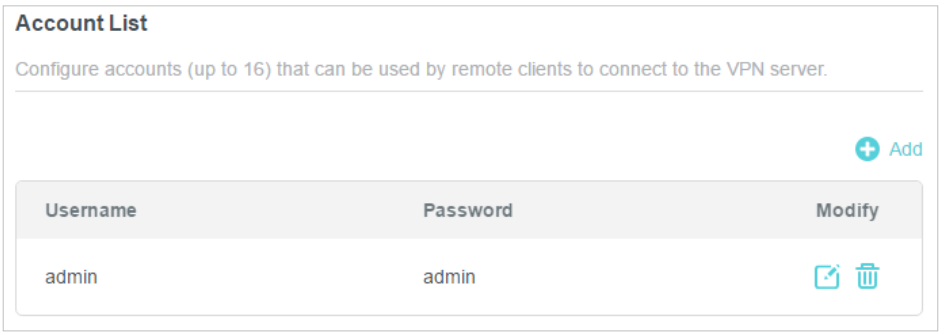
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > VPN Server > L2TP/IPSec, and enable L2TP/IPSec.

Note:

- Firmware update may be required to support L2TP/IPSec VPN Server.
- 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.

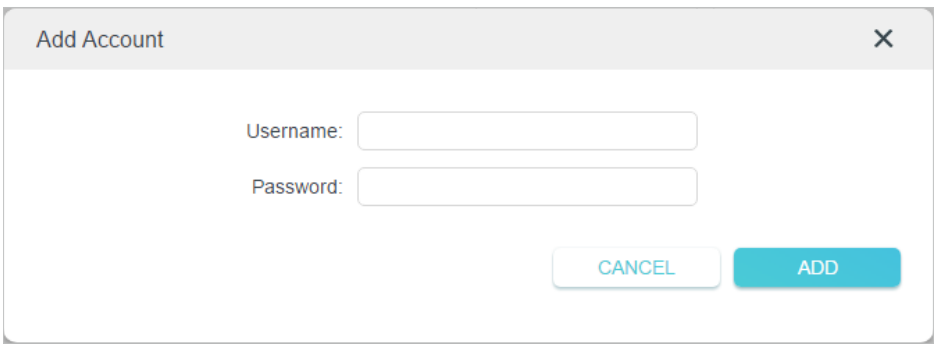


3. In the Client IP Address field, enter the range of IP addresses (up to 10) that can be leased to the devices by the L2TP/IPSec VPN server.
4. Keep IPSec Encryption as Encrypted and create an IPSec Pre-Shared Key.
5. Click SAVE.
6. Configure the L2TP/IPSec VPN connection account for the remote device. You can create up to 16 accounts.



4) Click Add.

5) Enter the Username and Password to authenticate devices to the L2TP/IPSec VPN Server.

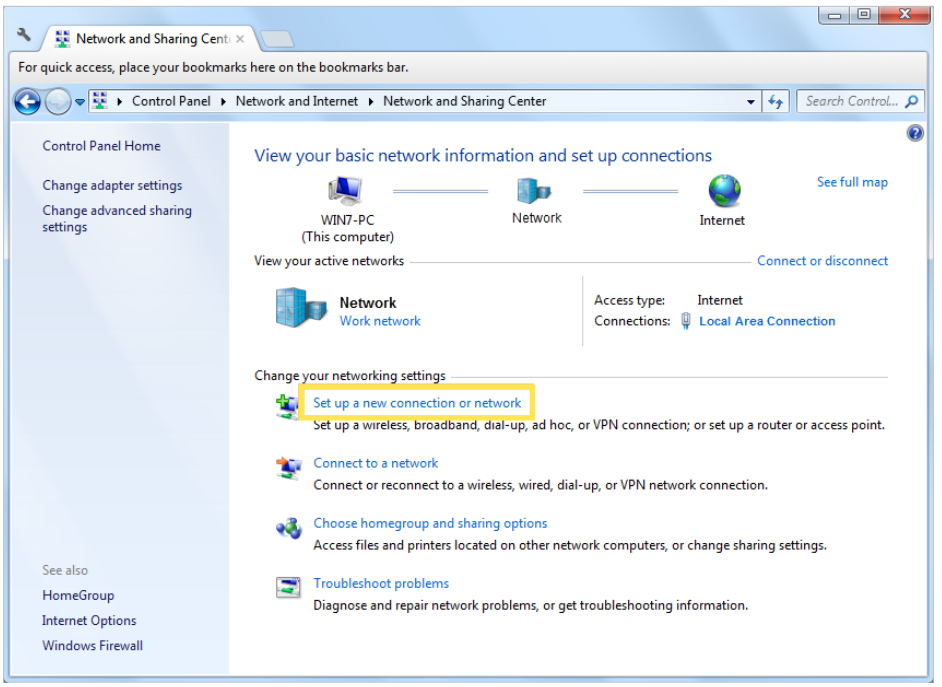


6) Click ADD.

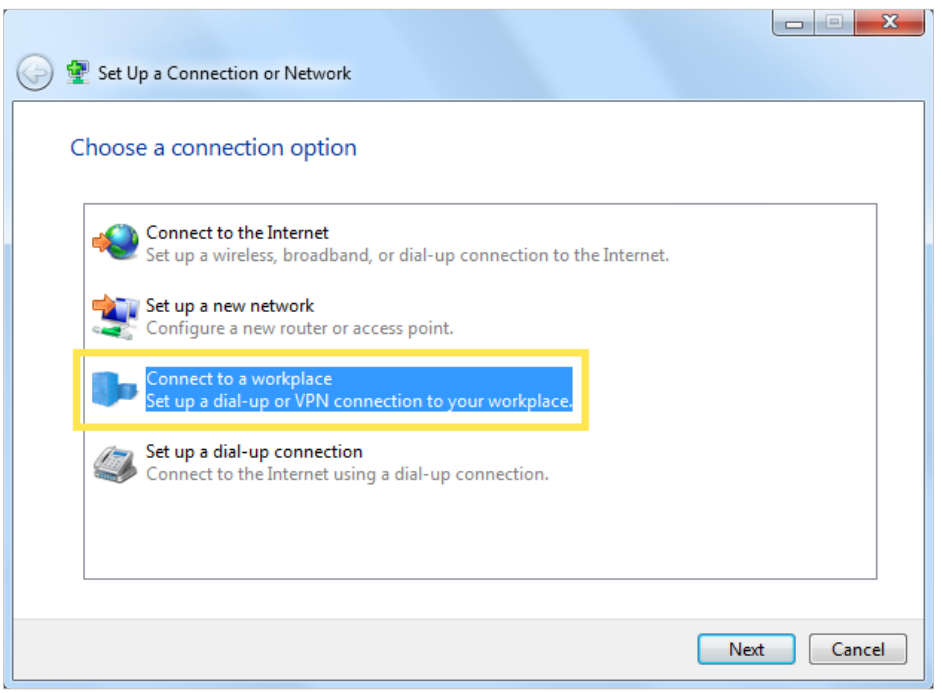
Step 2. Configure L2TP/IPSec VPN Connection on Your Remote Device

The remote device can use the Windows or Mac OS built-in L2TP/IPSec software or a third-party L2TP/IPSec software to connect to L2TP/IPSec Server. Here we use the Windows built-in L2TP/IPSec software as an example.

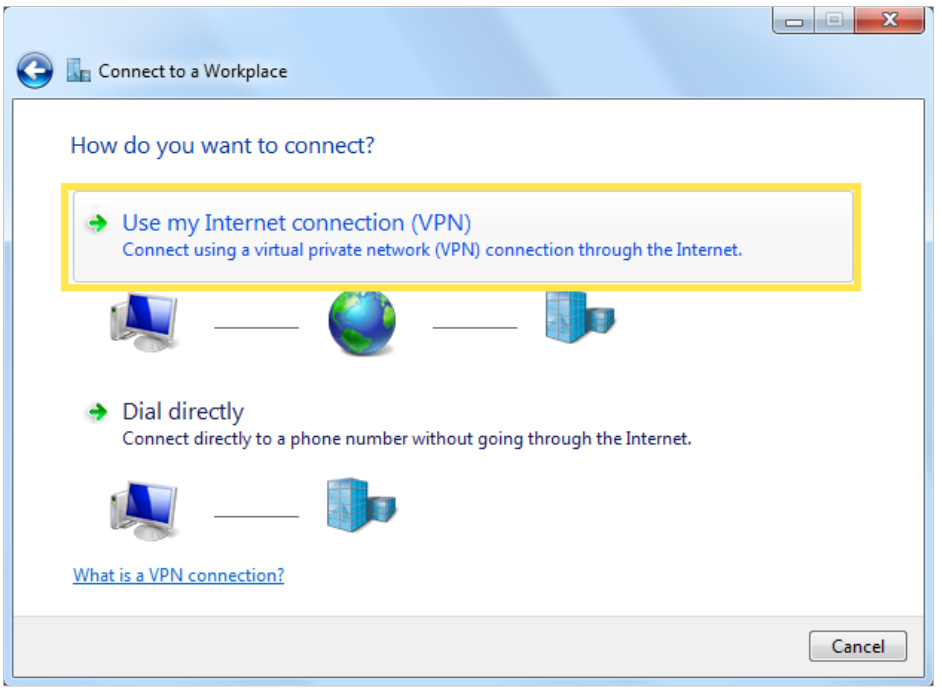
1. Go to Start > Control Panel > Network and Internet > Network and Sharing Center.
2. Select Set up a new connection or network.



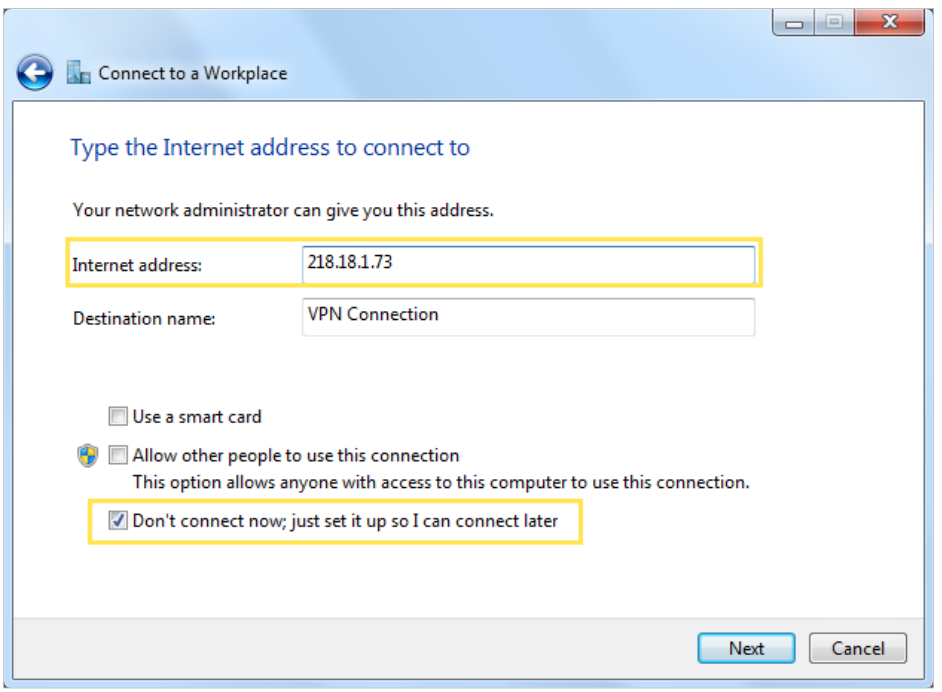
3. Select Connect to a workplace and click Next.



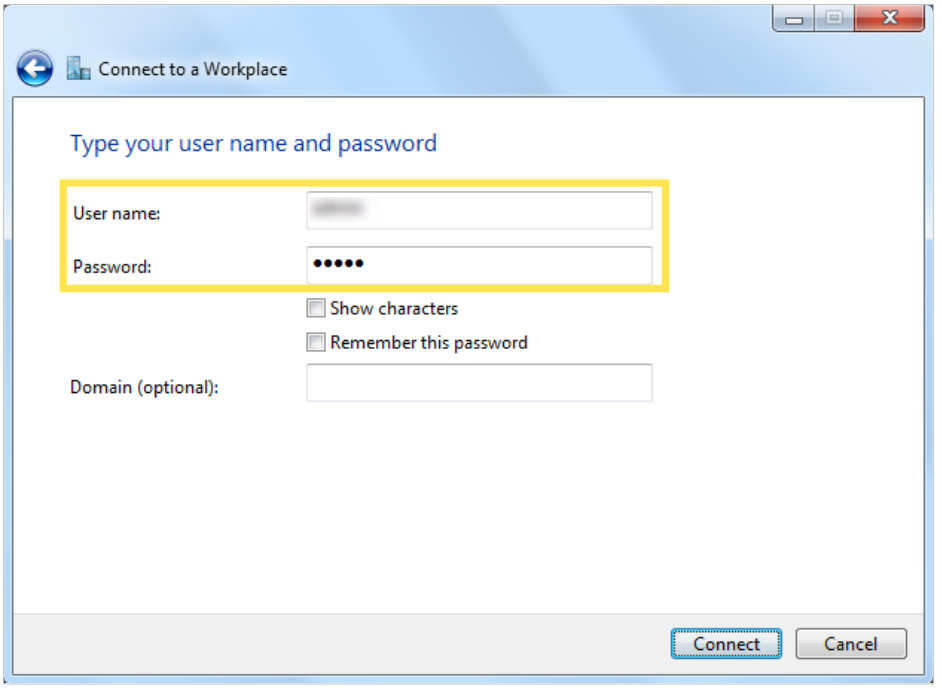
4. Select Use my Internet connection (VPN).



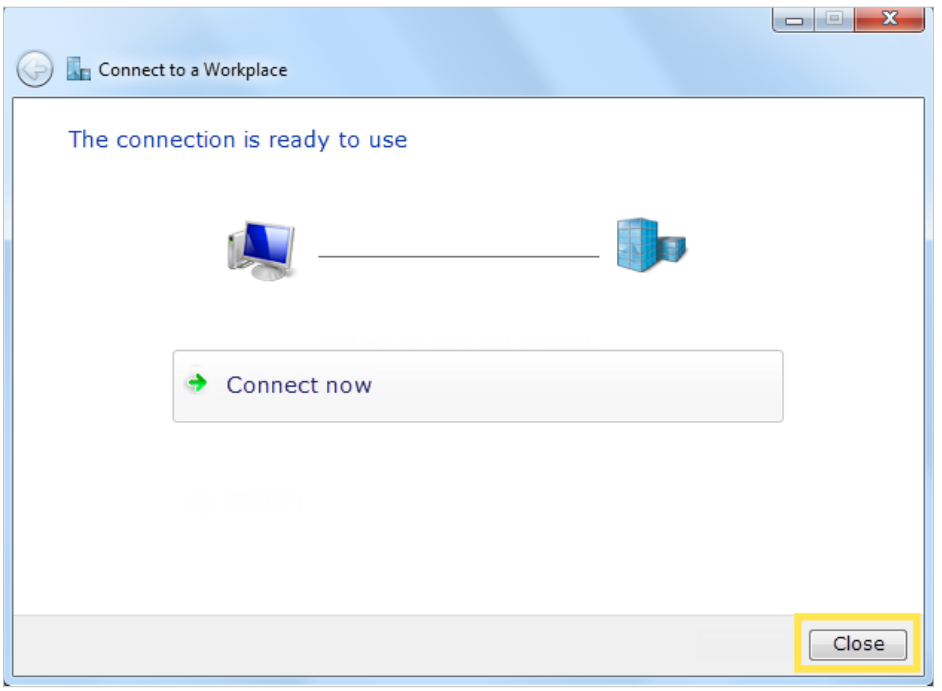
5. Enter the internet IP address of the router (for example: 218.18.1.73) in the Internet address field, and select the checkbox Don't connect now; just set it up so I can connect later. Click Next.



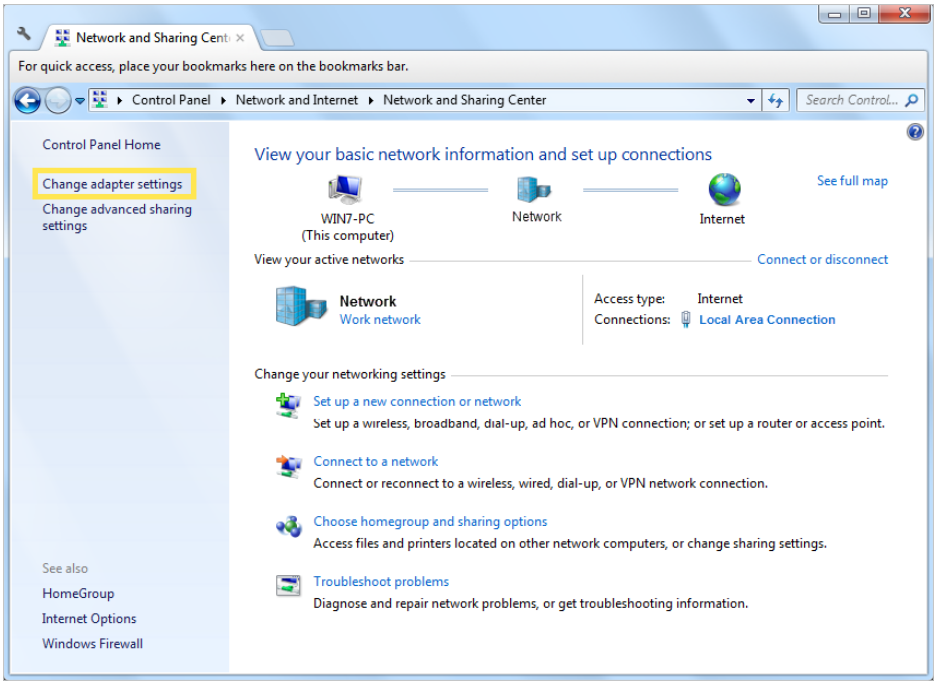
6. Enter the User name and Password you have set for the L2TP/IPSec VPN server on your router, and click Connect.



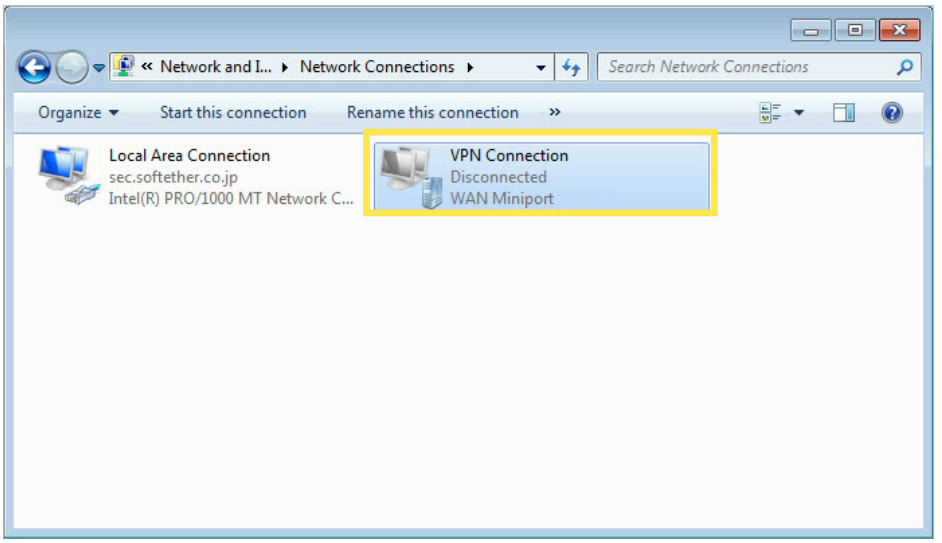
7. Click Close when the VPN connection is ready to use



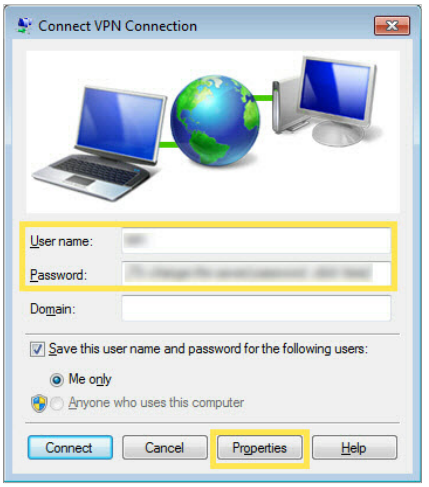
8. Go to Network and Sharing Center and click Change adapter settings.



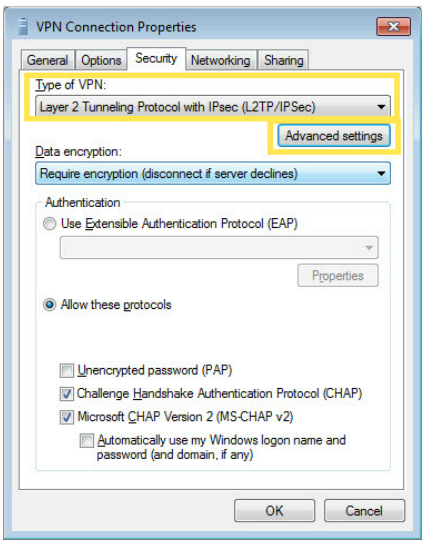
9. Find the VPN connection you created, then double-click it.



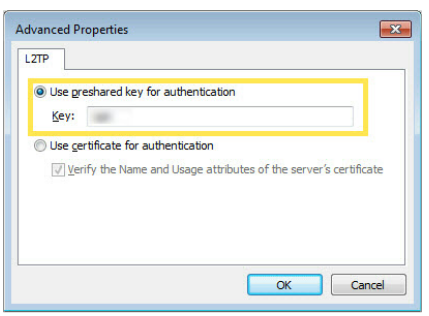
10. Enter the User name and Password you have set for the L2TP/IPSec VPN server on your router, and click Properties.



11. Switch to the Security tab, select Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec) and click Advanced settings.



12. Select Use preshared key for authentication and enter the IPSec Pre-Shared Key you have set for the L2TP/IPSec VPN server on your router. Then click OK.



Done! Click Connect to start VPN connection.