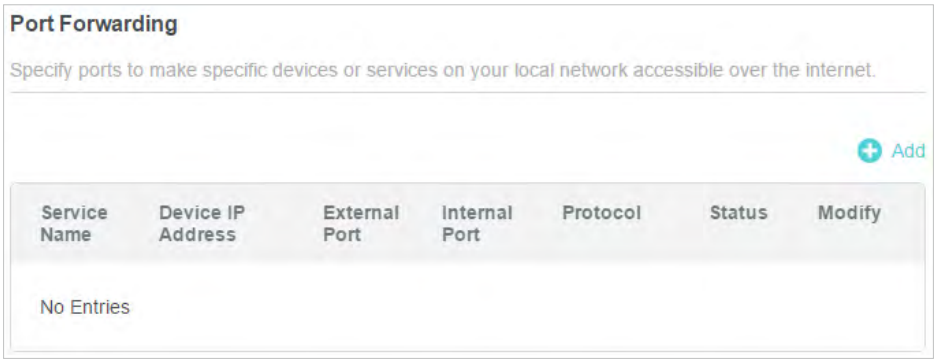
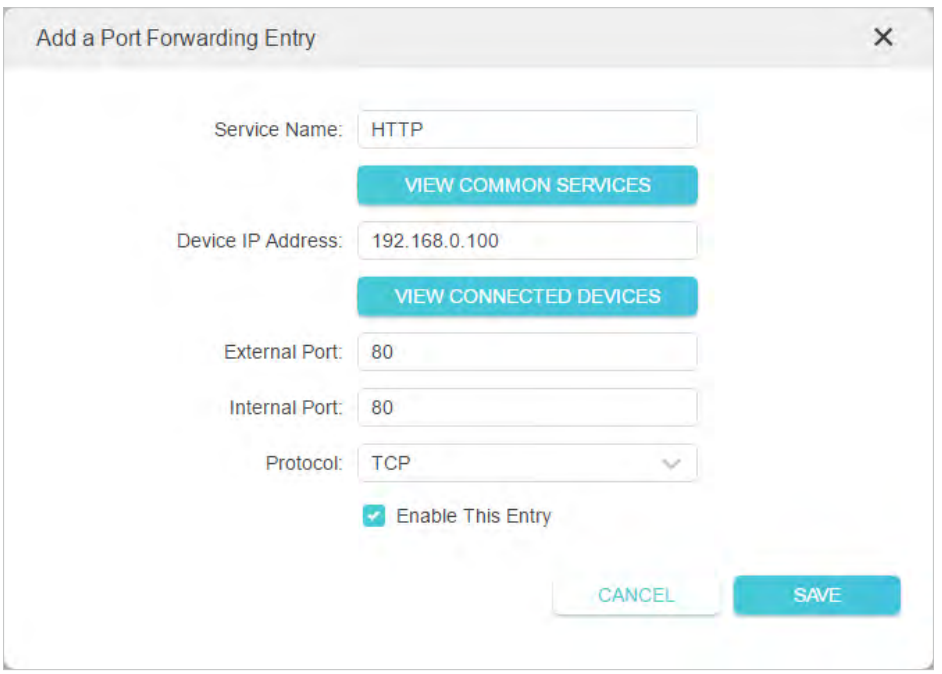


5. Click VIEW COMMON SERVICES and select HTTP. The External Port, Internal Port and Protocol will be automatically filled in.
6. Click VIEW CONNECTED DEVICES and select your home PC. The Device IP Address will be automatically filled in. Or enter the PC's IP address 192.168.0.100 manually in the Device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

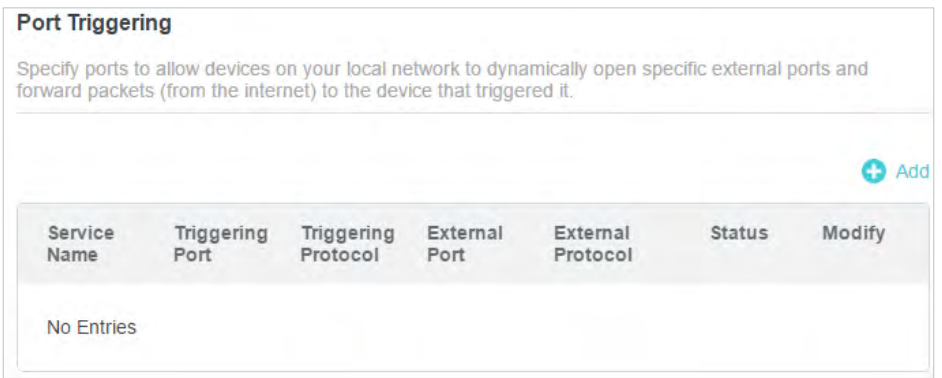
Tips:
- The WAN IP should be a public IP address. For the WAN IP is assigned dynamically by the ISP, it is recommended to apply and register a domain name for the WAN referring to Set Up a Dynamic DNS Service Account. Then users on the internet can use http:// domain name to visit the website.
- If you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

15. 2. Open Ports Dynamically by Port Triggering

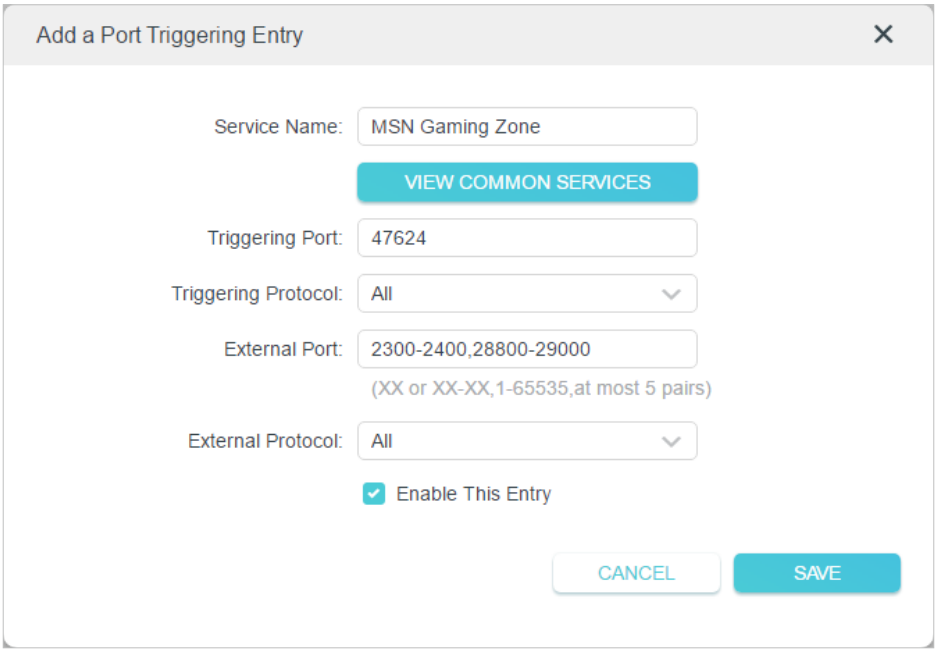
Port Triggering can specify a triggering port and its corresponding external ports. When a host on the local network initiates a connection to the triggering port, all the external ports will be opened for subsequent connections. The router can record the IP address of the host. When the data from the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

15. 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.

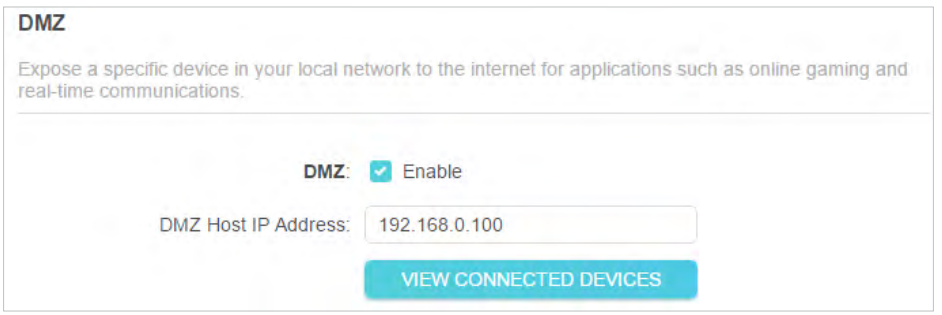
I want to:

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.

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

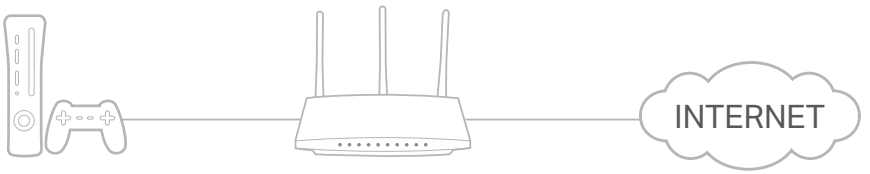
The UPnP (Universal Plug and Play) protocol allows applications or host devices to automatically find the front-end NAT device and send request to it to open the corresponding ports. With UPnP enabled, the applications or host devices on the local network and the internet can freely communicate with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

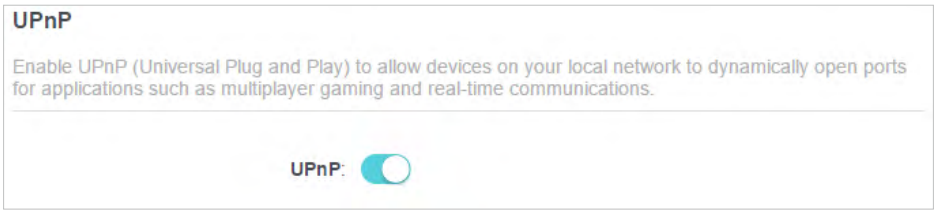
For example, when you connect your Xbox to the router which has connected to the internet to play online games, UPnP will send request to the router to open the

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 16

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.

WireGuard VPN is a secure, fast and modern VPN protocol. It is based on the UDP protocol and uses modern encryption algorithms to improve work efficiency.

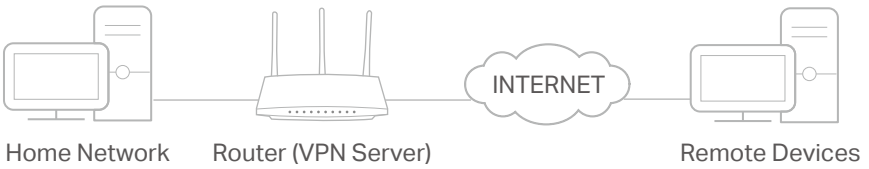
VPN Client allows devices in your home network to access remote VPN servers, without the need to install VPN software on each device.

This chapter contains the following sections:

16. 1. Use OpenVPN to Access Your Home Network

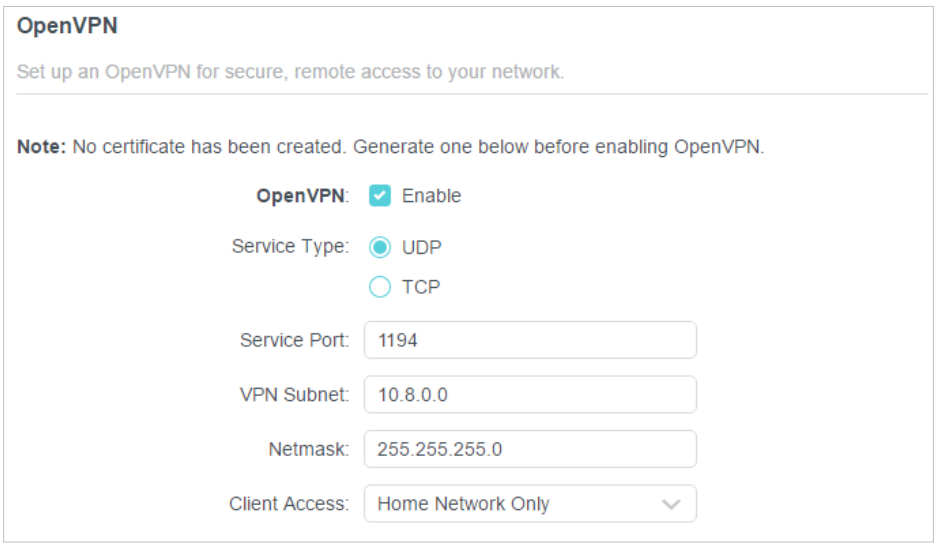
OpenVPN Server is used to create an OpenVPN connection for remote devices to access your home network.

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.

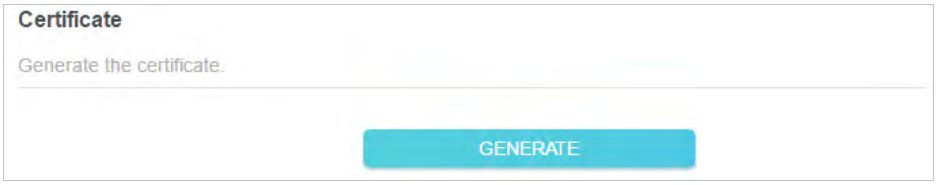


Note:

- 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.

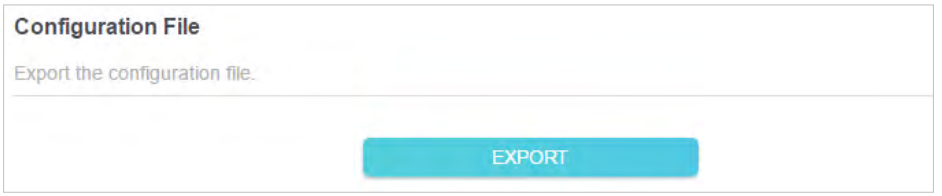
3. Select the Service Type (communication protocol) for OpenVPN Server: UDP, TCP.
4. Enter a VPN Service Port to which a VPN device connects, and the port number should be between 1024 and 65535.
5. In the VPN Subnet/Netmask fields, enter the range of IP addresses that can be leased to the device by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

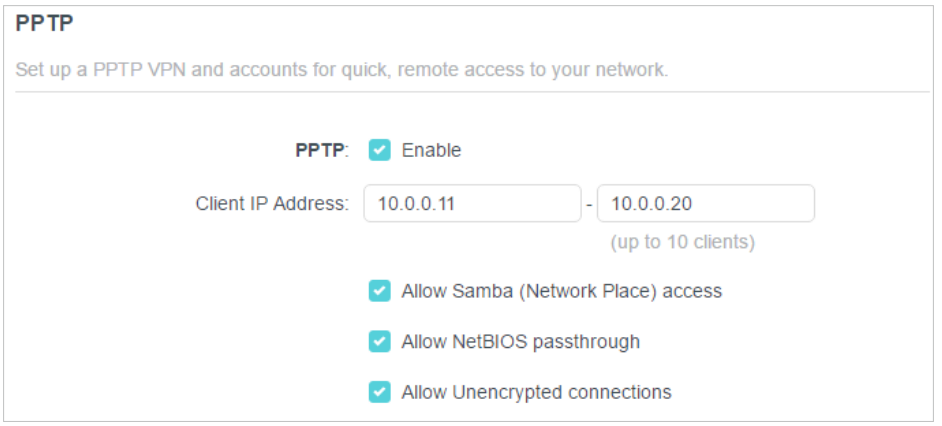
16. 2. Use PPTP VPN to Access Your Home Network

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.

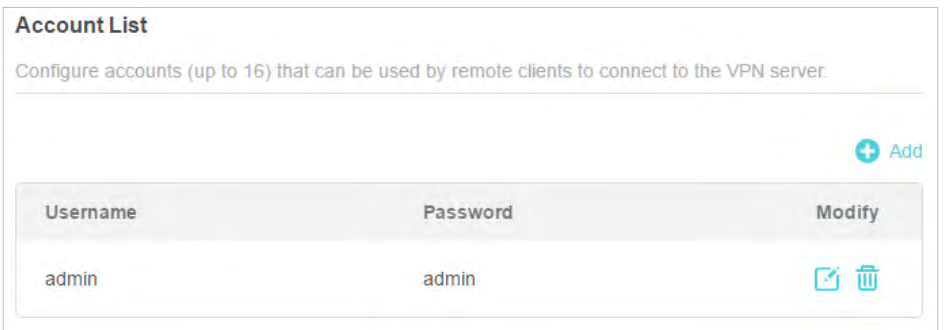
Step 1. Set up PPTP VPN Server on Your Router

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.

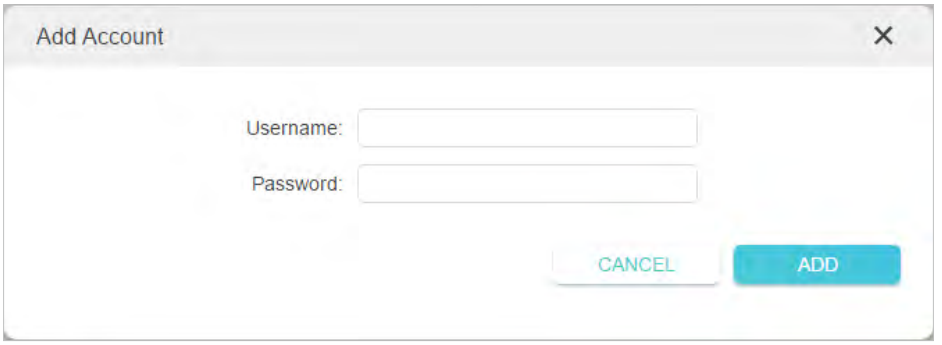


Note: Before you enable VPN Server, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router's WAN port and synchronize your System Time with internet.

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.

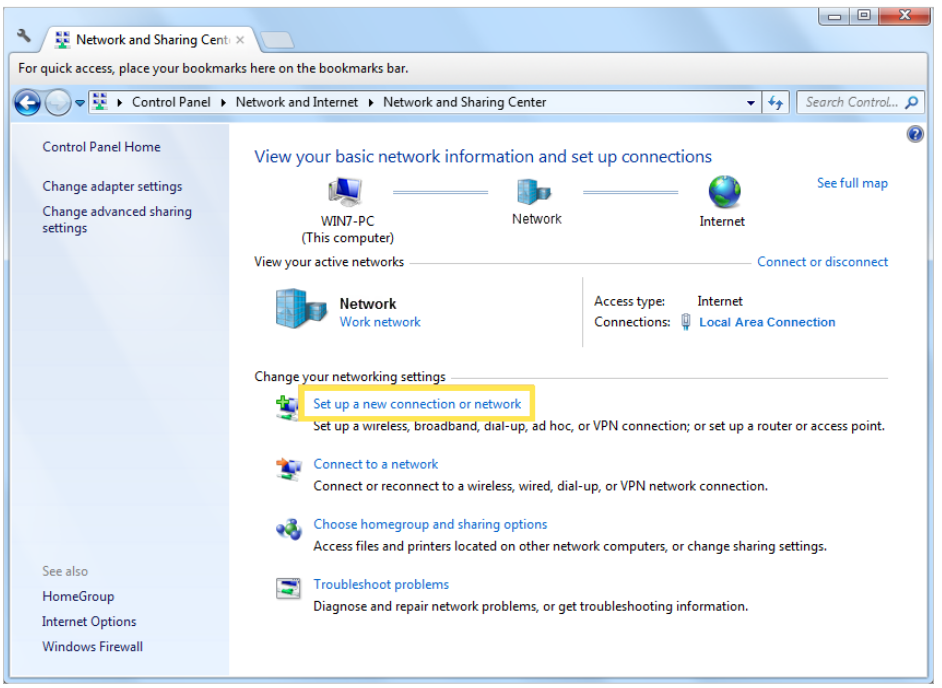


3) Click ADD.

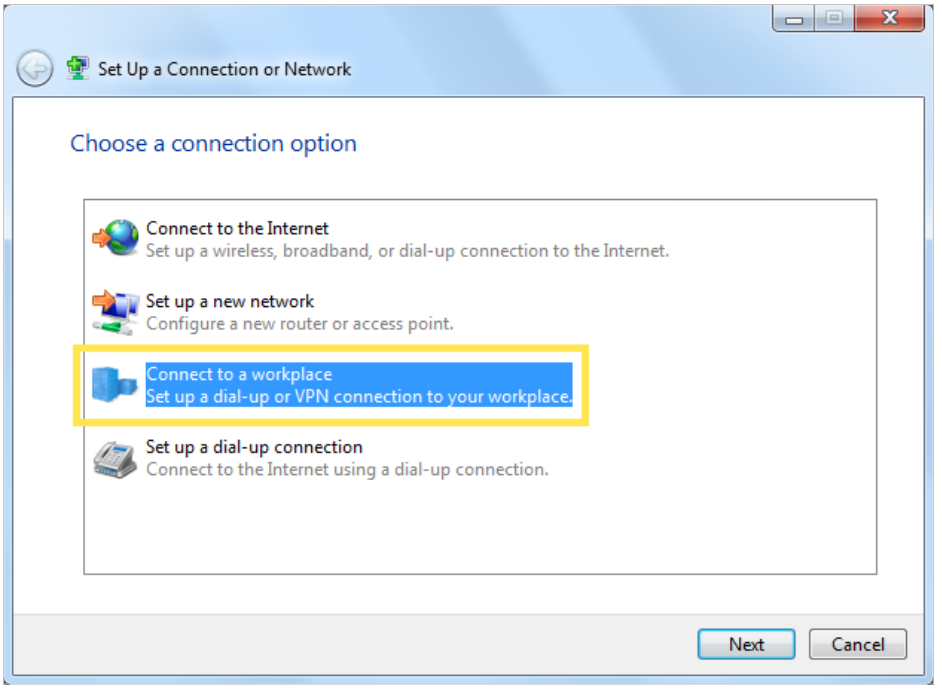
Step 2. Configure PPTP VPN Connection on Your Remote Device

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.

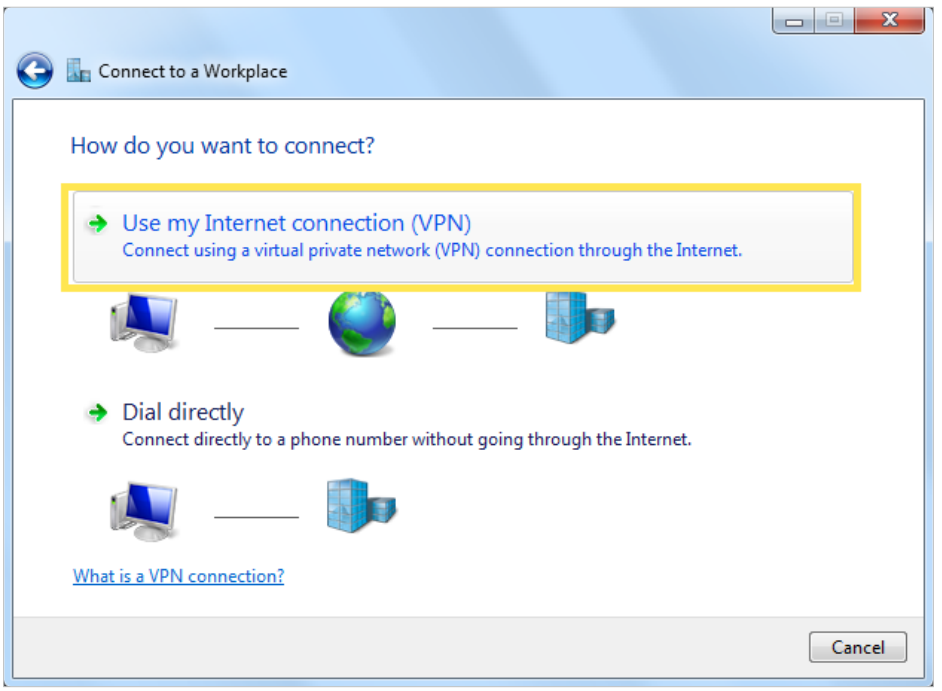
1. Go to Start > Control Panel > Network and Internet > Network and Sharing Center.
2. Select Set up a new connection or network.



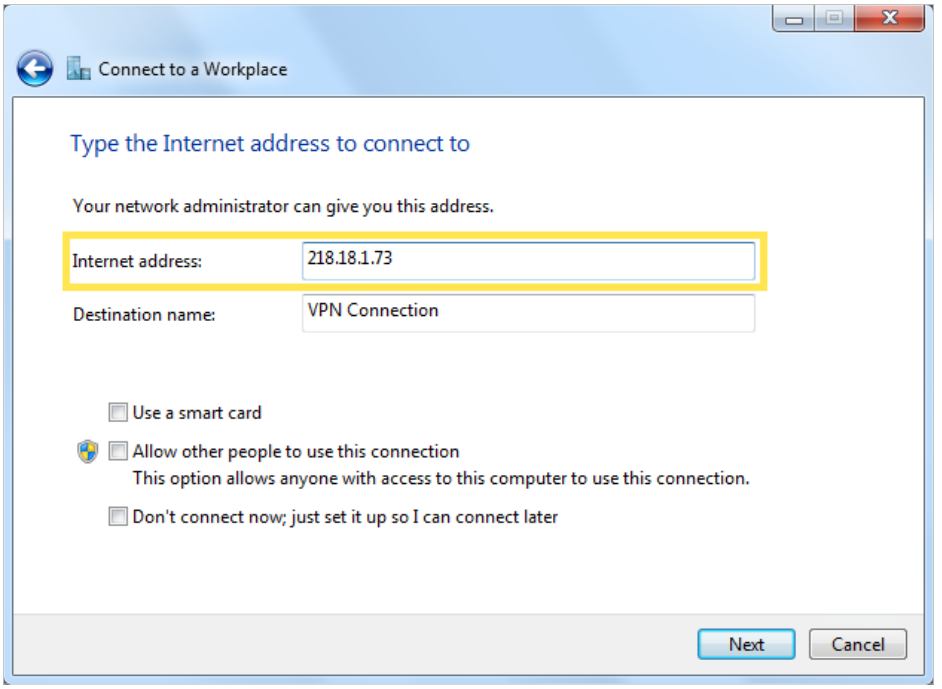
3. Select Connect to a workplace and click Next.



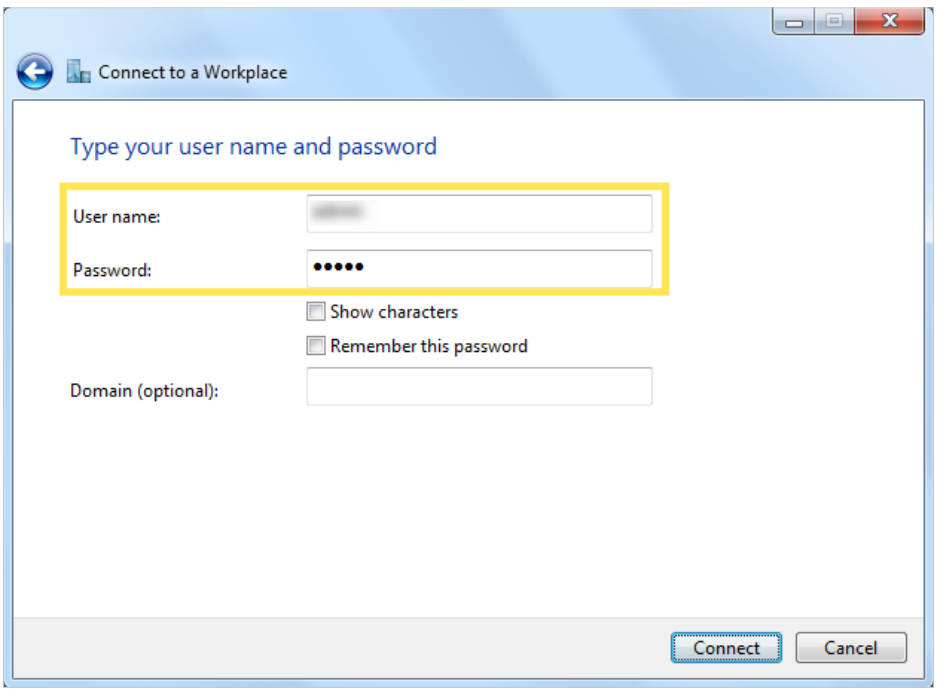
4. Select Use my Internet connection (VPN).



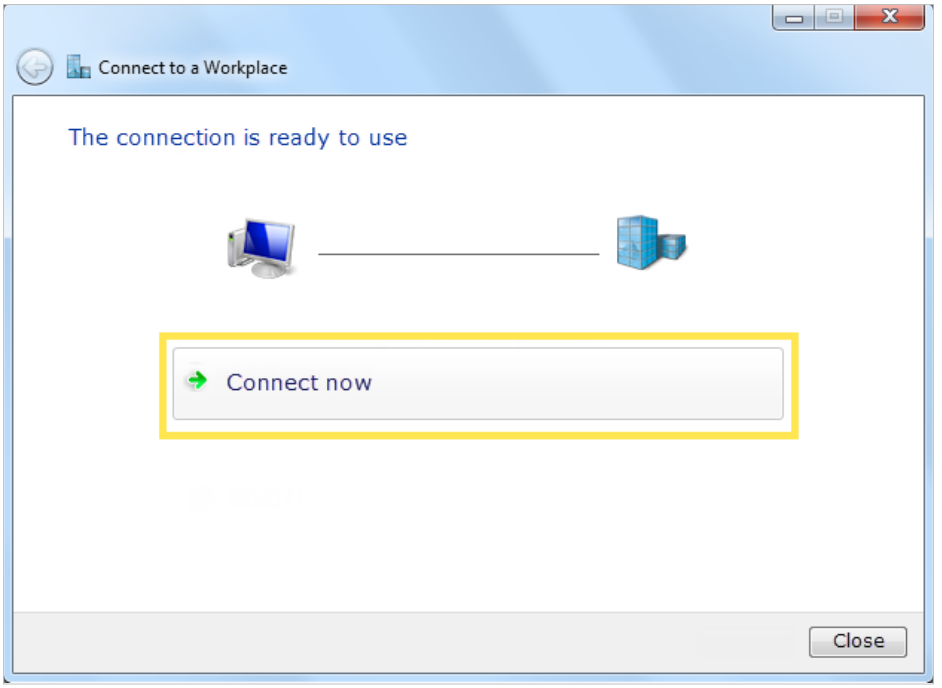
5. Enter the internet IP address of the router (for example: 218.18.1.73) in the Internet address field. Click Next.



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



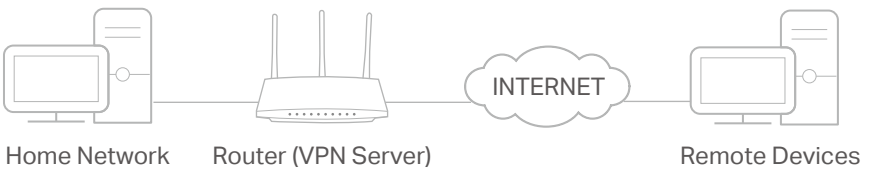
7. Click Connect Now when the VPN connection is ready to use.



16. 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.

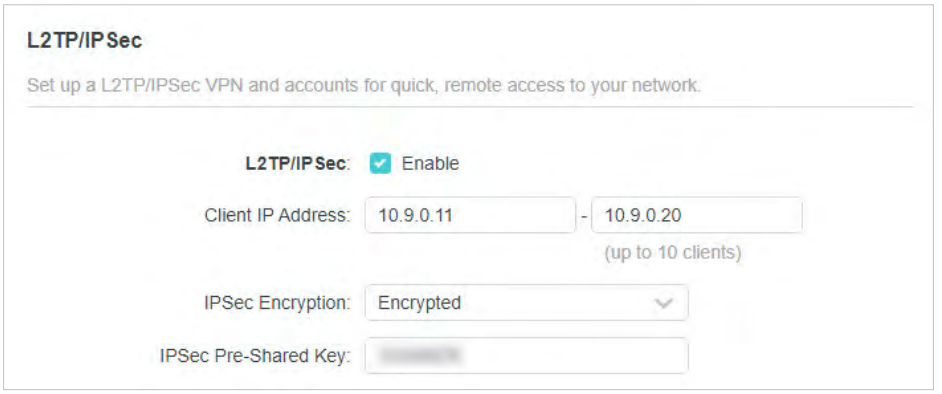


Step 1. Set up L2TP/IPSec VPN Server on Your Router

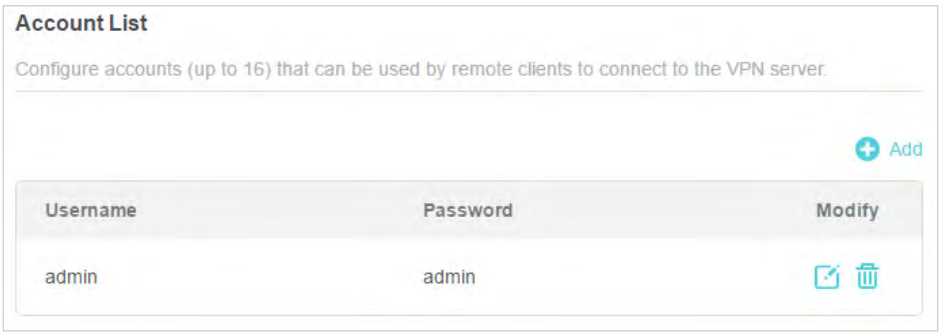
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > VPN Server > L2TP/IPSec, and enable L2TP/IPSec.

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.

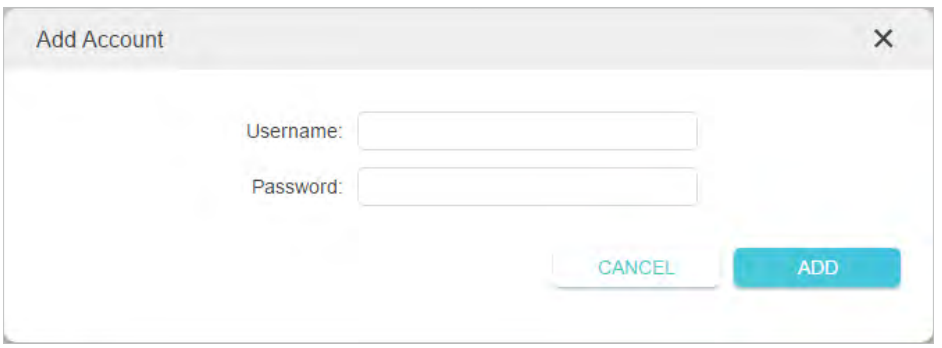


3. In the Client IP Address field, enter the range of IP addresses (up to 10) that can be leased to the devices by the L2TP/IPSec VPN server.
4. Keep IPSec Encryption as Encrypted and create an IPSec Pre-Shared Key.
5. Click SAVE.
6. Configure the L2TP/IPSec VPN connection account for the remote device.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

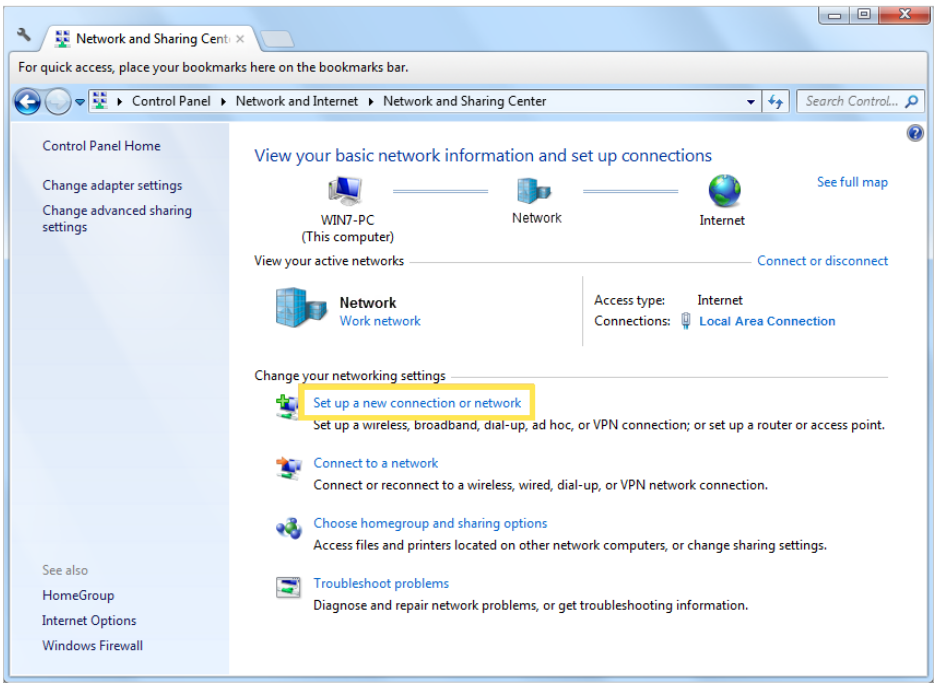


6) Click ADD.

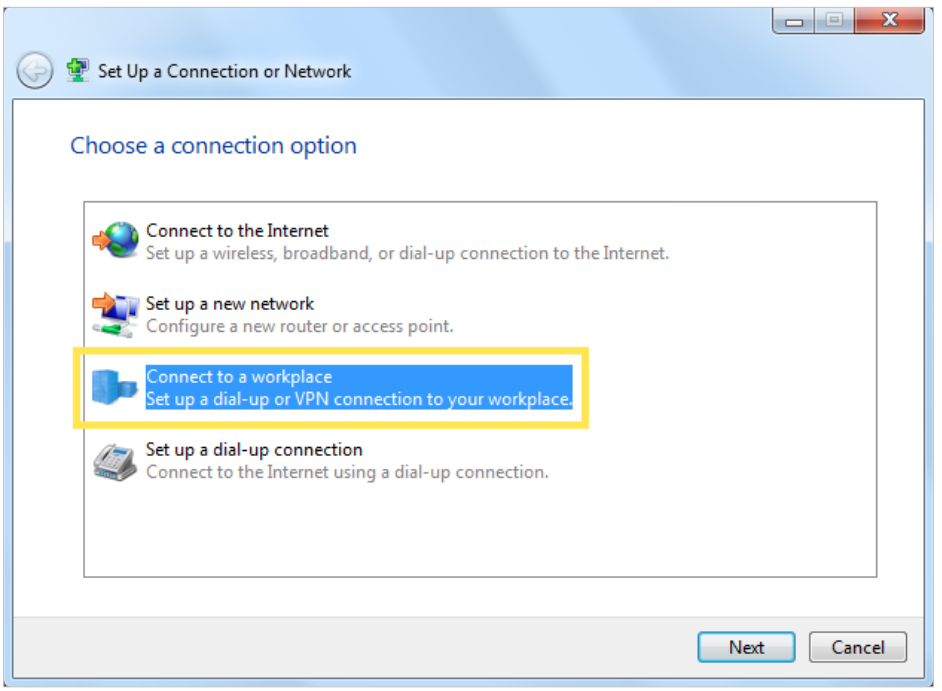
Step 2. Configure L2TP/IPSec VPN Connection on Your Remote Device

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.

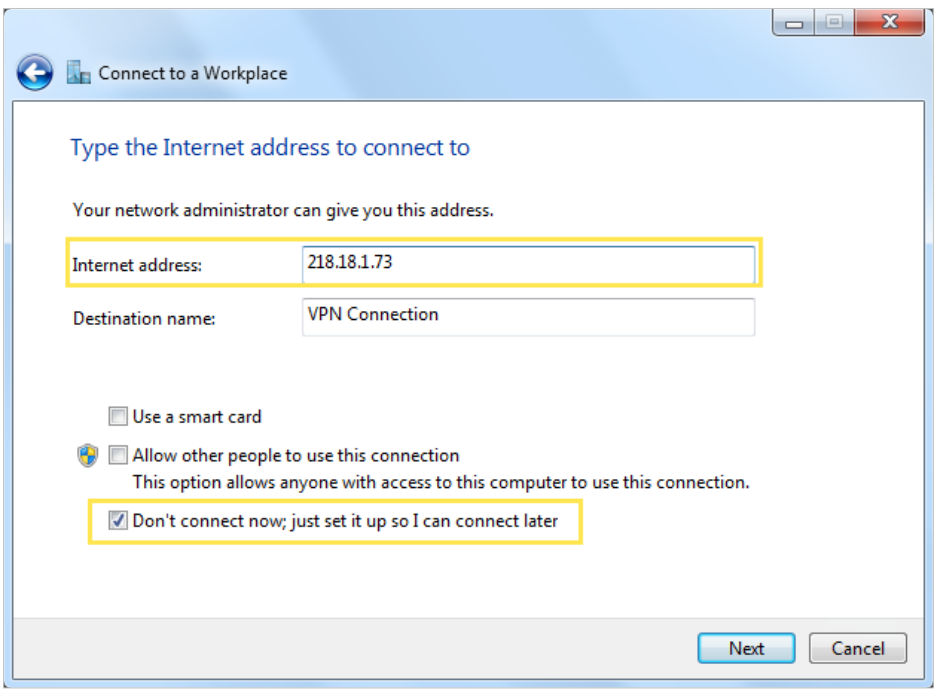


3. Select Connect to a workplace and click Next.

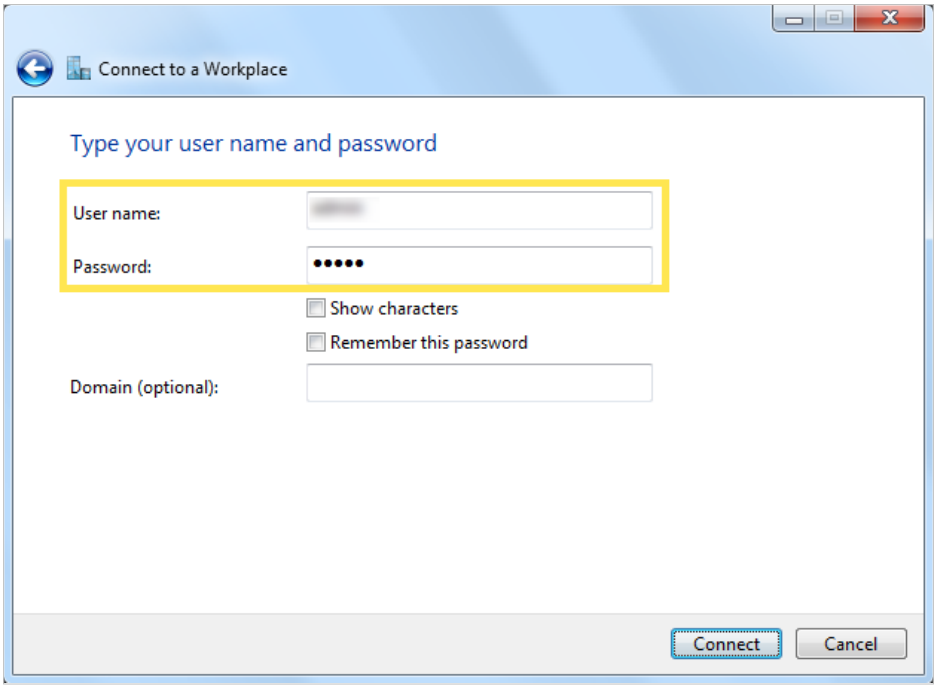


4. Select Use my Internet connection (VPN).

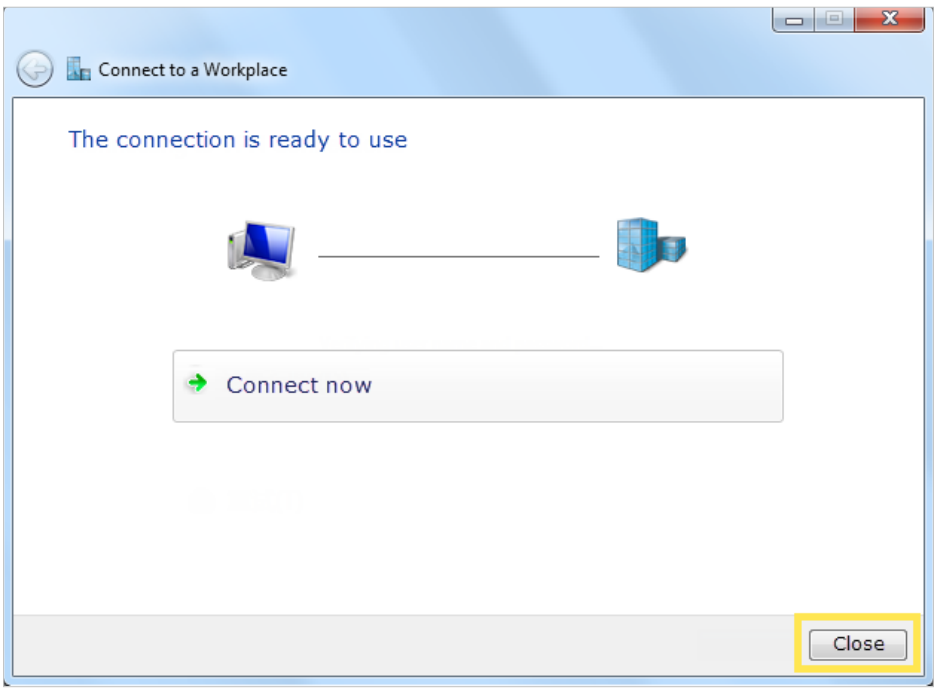
5. Enter the internet IP address of the router (for example: 218.18.1.73) in the Internet address field, and select the checkbox Don't connect now; just set it up so I can connect later. Click Next.



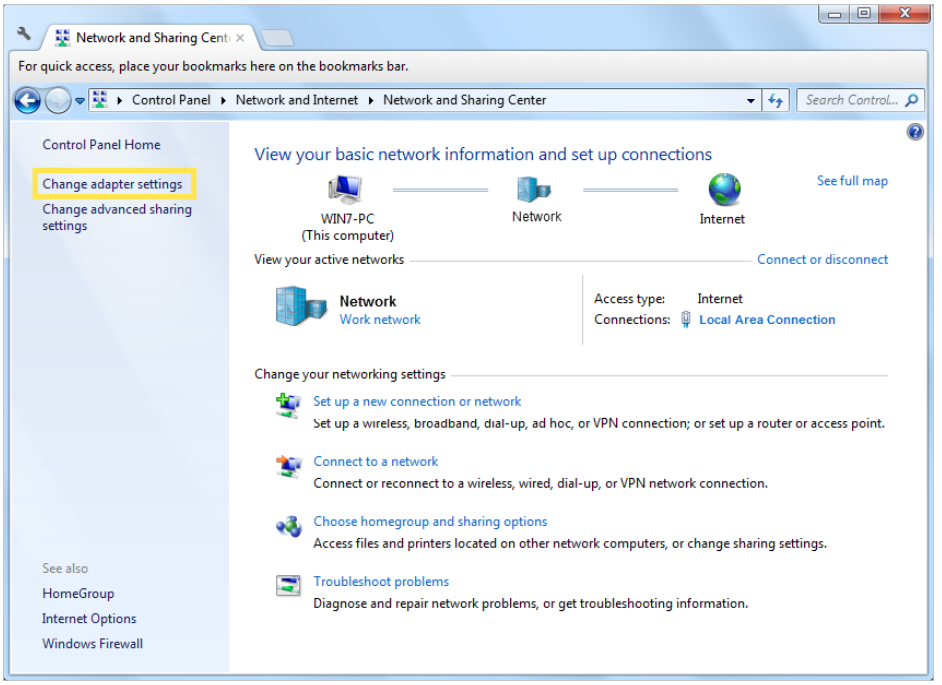
6. Enter the User name and Password you have set for the L2TP/IPSec VPN server on your router, and click Connect.



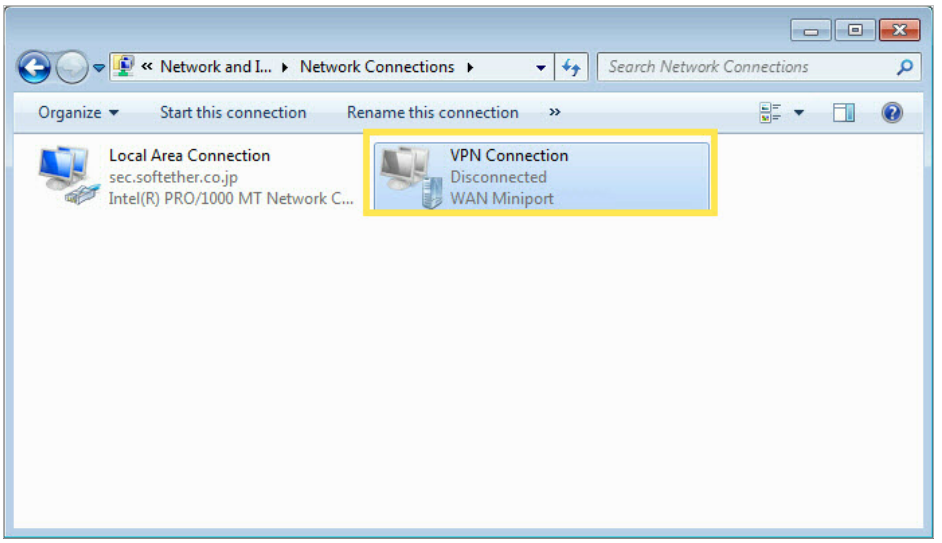
7. Click Close when the VPN connection is ready to use



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

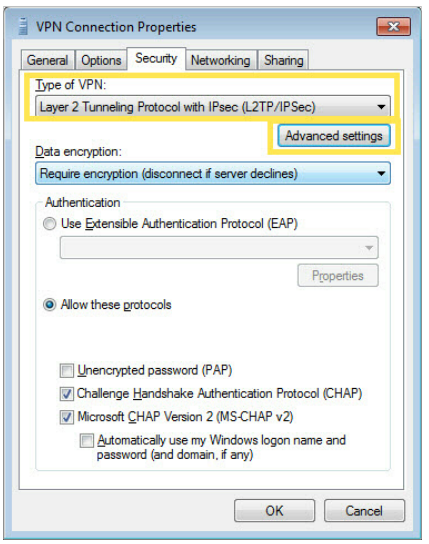


9. Find the VPN connection you created, then double-click it.

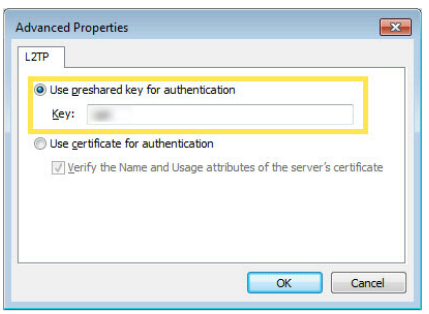


10. Enter the User name and Password you have set for the L2TP/IPSec VPN server on your router, and click Properties.

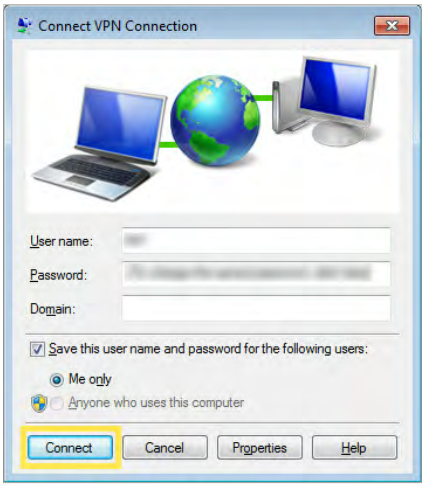
11. Switch to the Security tab, select Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec) and click Advanced settings.



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.

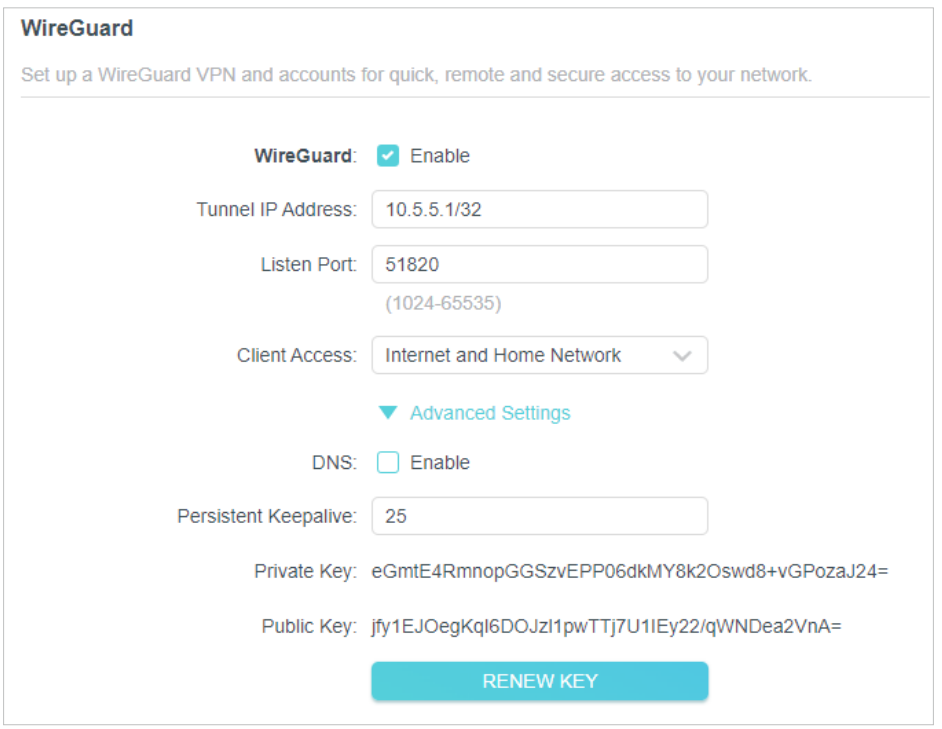


16. 4. Use WireGuard VPN to Access Your Home Network

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

Step 1. Set up WireGuard VPN Server on Your Router

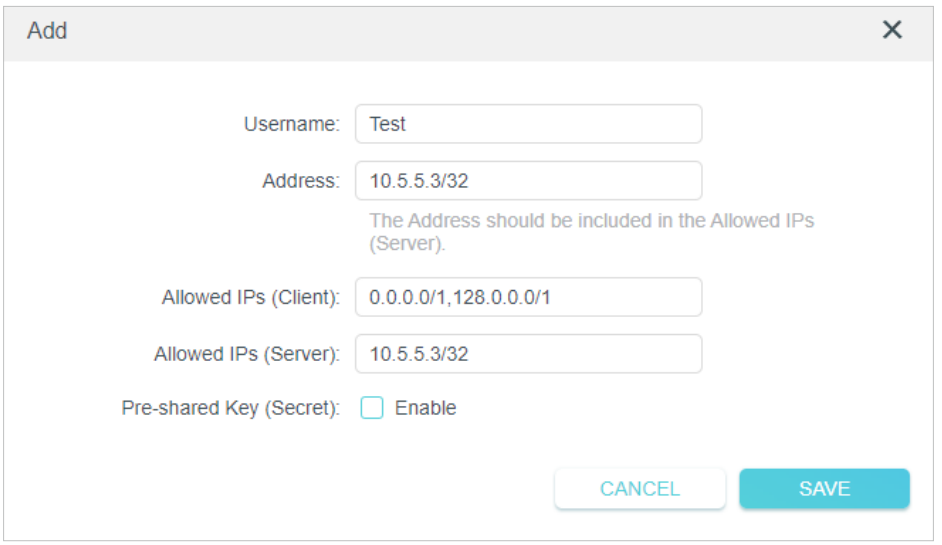
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > VPN Server > WireGuard, and tick the Enable box of WireGuard.



3. Set the tunnel IP address and listen port. Do NOT change it unless necessary.
4. 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.
5. (Optional) Click Advanced Settings to display more settings. If DNS is turned on, the router will become the DNS server of the VPN client that establishes a connection with it. Change the Persistent Keepalive time (25 seconds by default) to send out heartbeat regularly, you can also click RENEW KEY to update the private key and public key.

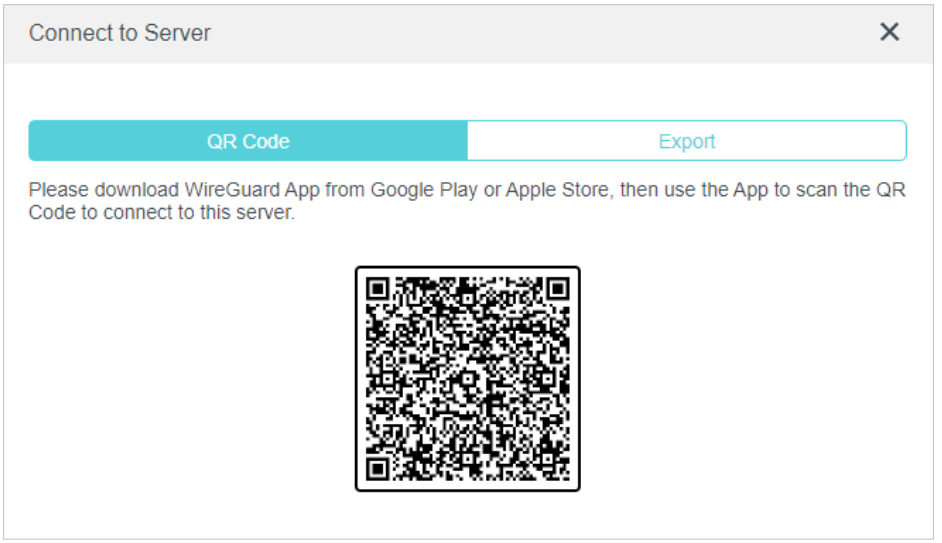
Step 2. Create accounts that can be used by remote clients to connect to the VPN server.

1. Locate the Account List section. Click Add to create an account.



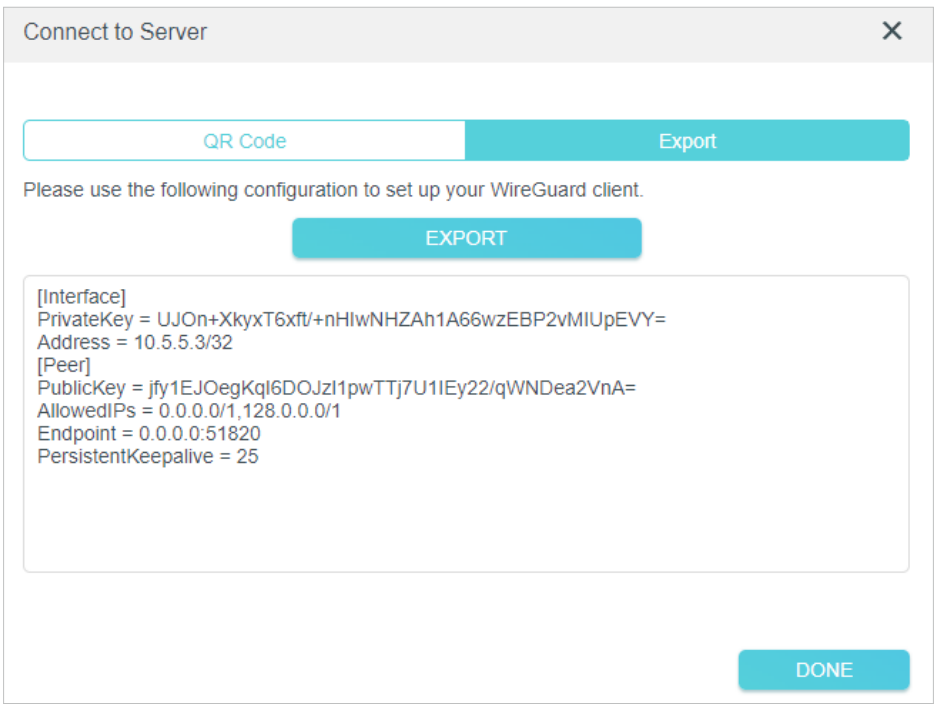
2. Give a name to this account.
3. Enter the address of the virtual interface assigned to this account. Do NOT change it unless necessary.
4. Traffic sent from the WireGard VPN client to the allowed IPs (client) will be transmitted through the tunnel. By default, all network traffic from clients will be transmitted through the tunnel. Do NOT change it unless necessary.
5. Traffic sent from the WireGard VPN server to the allowed IPs (server) will be transmitted through the tunnel. Do NOT change it unless necessary.
6. Enable or disable pre-shared key.
7. Click SAVE.

Note: One account can only be used by one WireGuard VPN client at the same time to connect to the WireGuard VPN server.

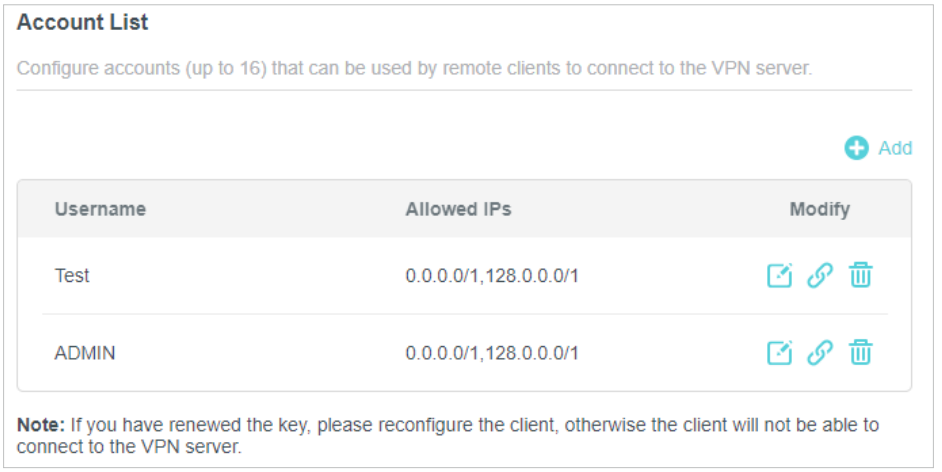


8. Connect to the WireGuard server.

- For mobile phones, download WireGuard App from Google Play or Apple Store, then use the App to scan the QR Code to connect to this server.
- For other devices (e.g. TP-Link WireGuard VPN client), Click EXPORT to save the WireGuard VPN configuration file which will be used by the remote device to access your router.



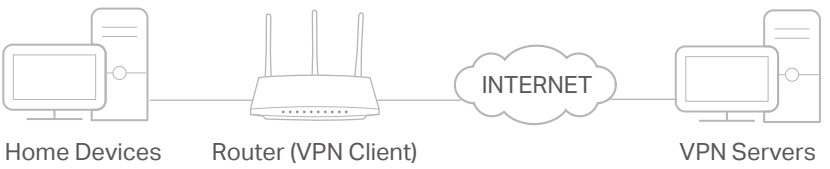
9. On the account list, you can click the button to modify the VPN server settings, connect to the server, or delete the account.



16. 5. Use VPN Client to Access a Remote VPN Server

VPN Client is used to create VPN connections for devices in your home network to access a remote VPN server.

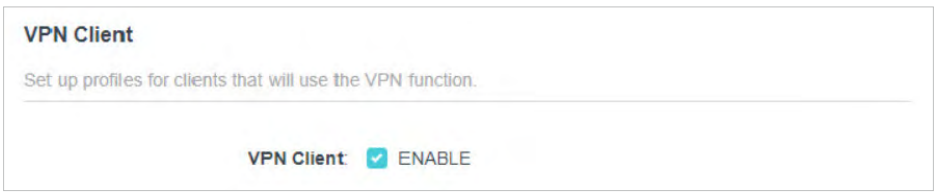
To use the VPN feature, simply configure a VPN connection and choose your desired devices on your router, then these devices can access the remote VPN server. Please follow the steps below:



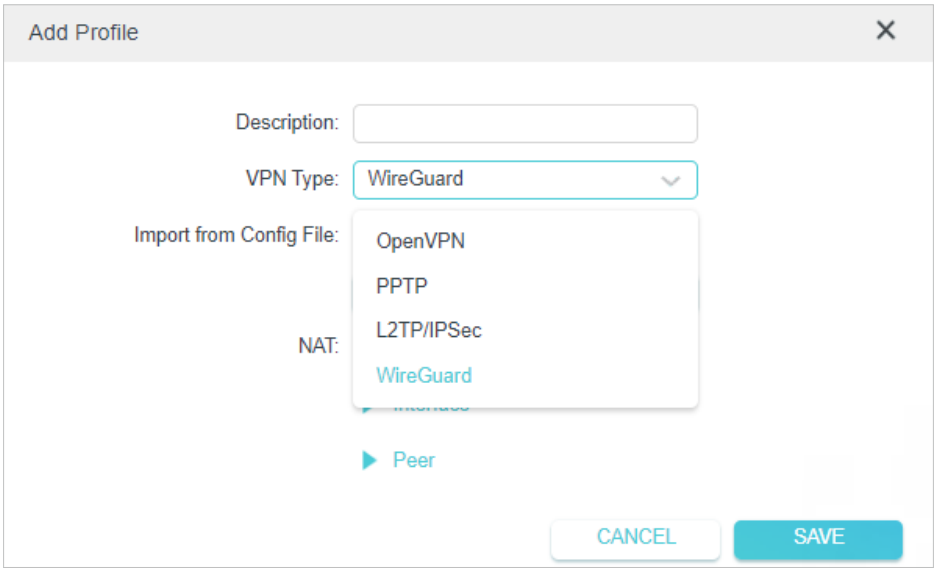
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > VPN Client.

Note: Firmware update may be required to support VPN Client.

3. Enable VPN Client, then save the settings.

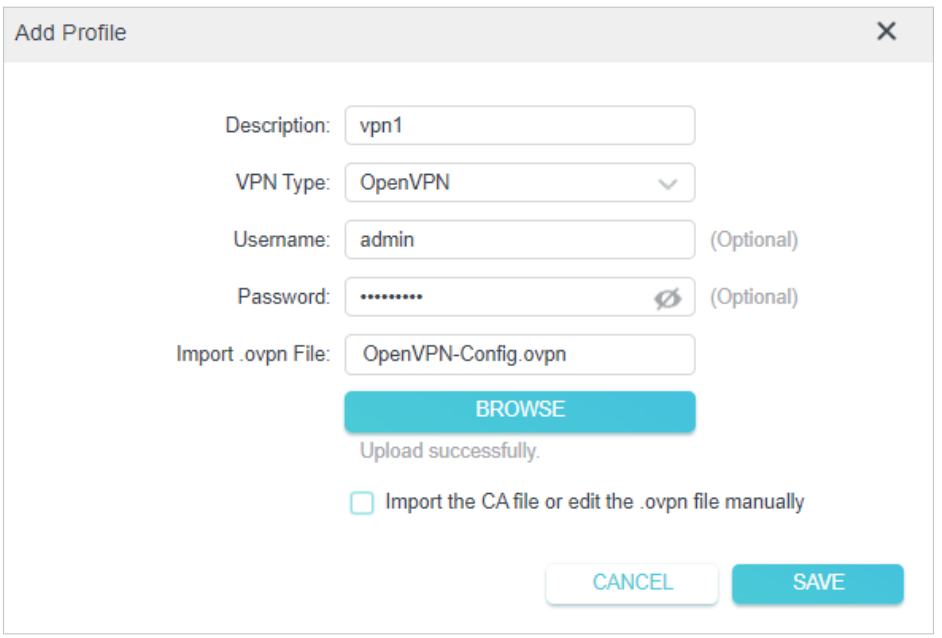


4. Add VPN servers, and enable the one you need.
   1) In the Server List section, click Add.
   2) Specify a description for the VPN, and choose the VPN type.

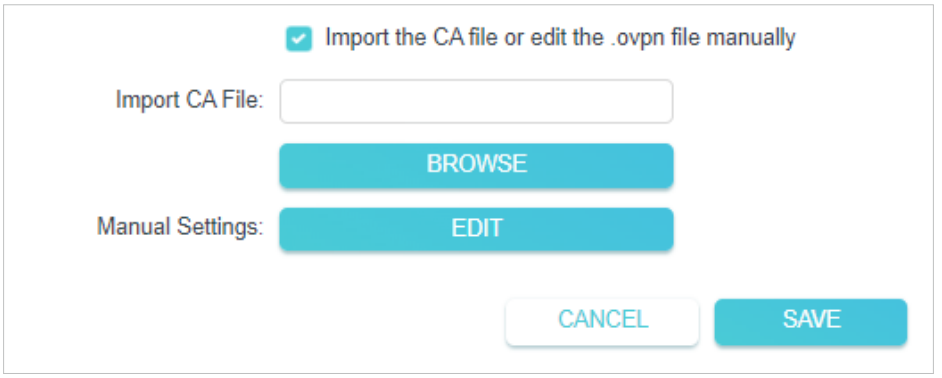


3) Enter the VPN information provided by your VPN provider.

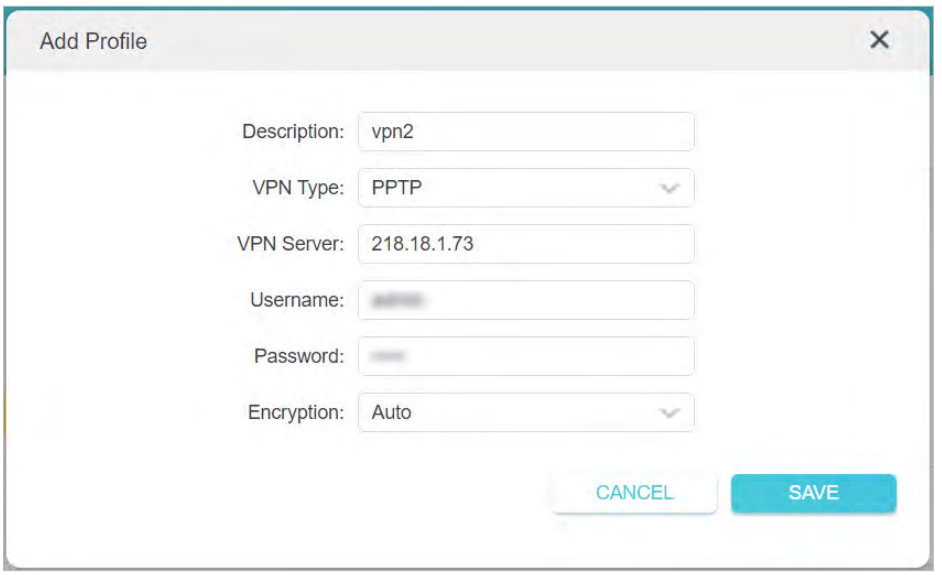
- OpenVPN: Enter the VPN username and password if required by your VPN provider, otherwise simply leave them empty. Then import the configuration file provided by your VPN provider.



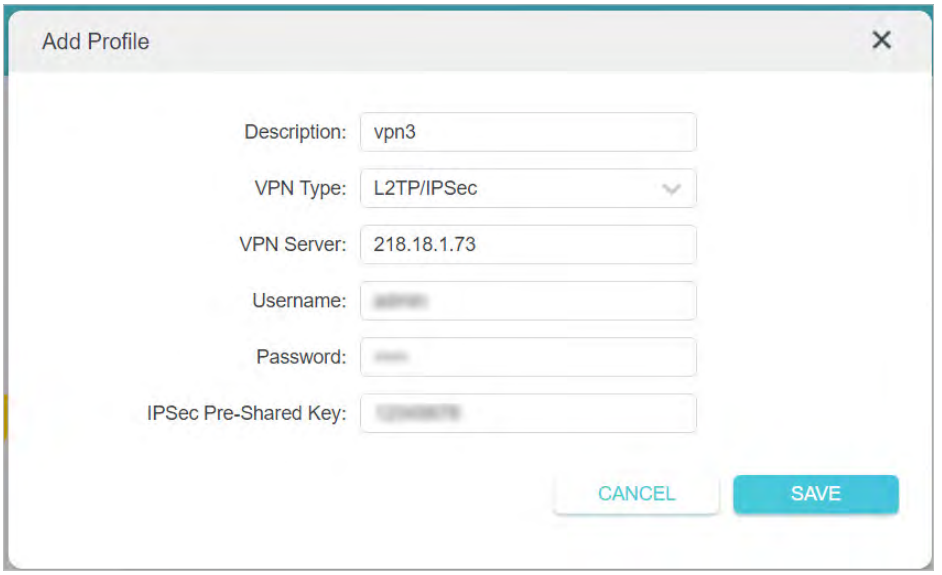
Note: You can also check the box of Import the CA file or edit the . ovpn file manually, then upload the CA file or manually configure the settings.



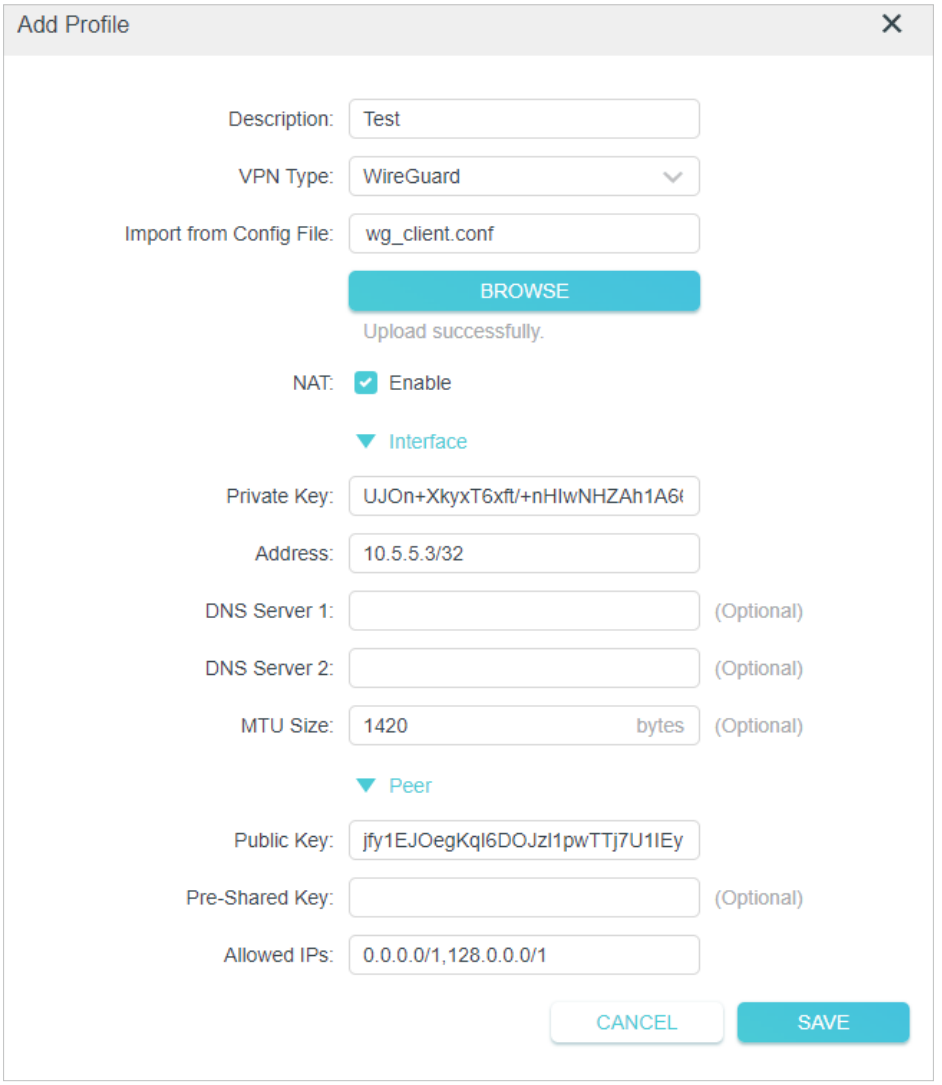
- PPTP: Enter the VPN server address (for example: 218.18.1.73) and the VPN username and password provided by your VPN provider.



- L2TP/IPSec VPN: Enter the VPN server address (for example: 218.18.1.73), VPN username and password, and IPSec pre-shared key provided by your VPN provider.

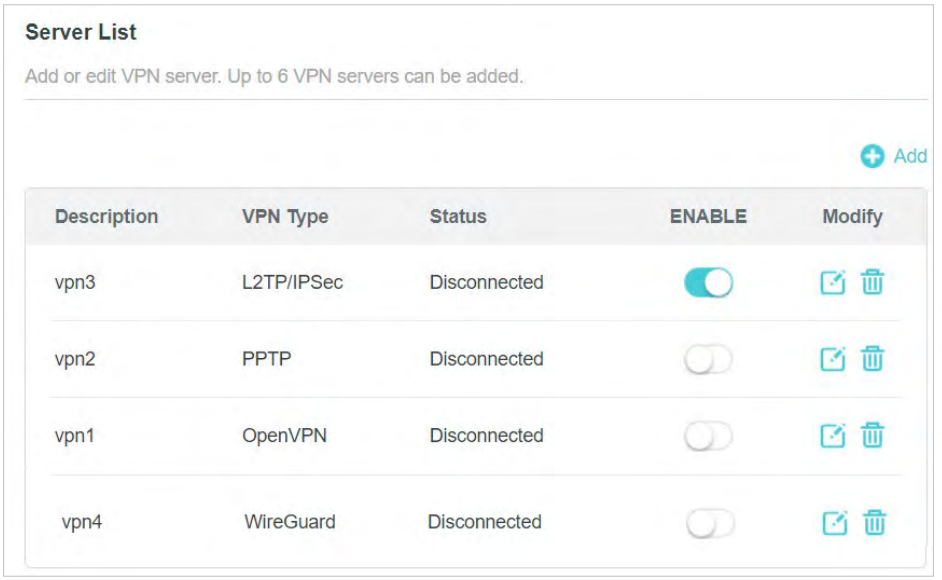


- WireGuard VPN: Give a description, and click BROWSE to import the WireGuard VPN server configuration. Then you will see the detailed parameters. Do NOT change the parameters unless necessary.



4) Save the settings.

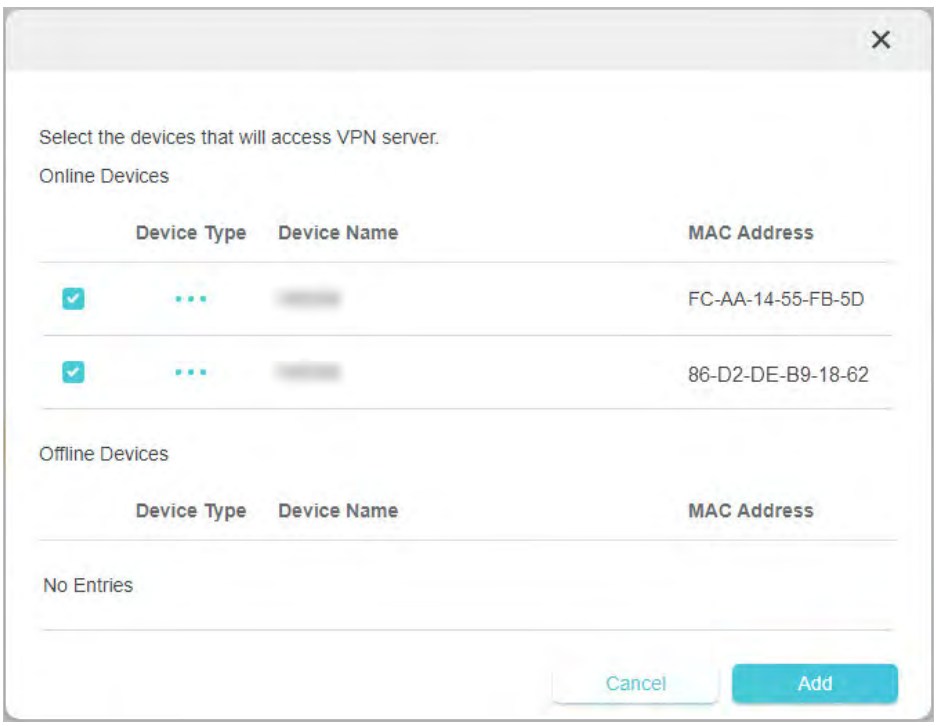
5) In the server list, enable the one you need.



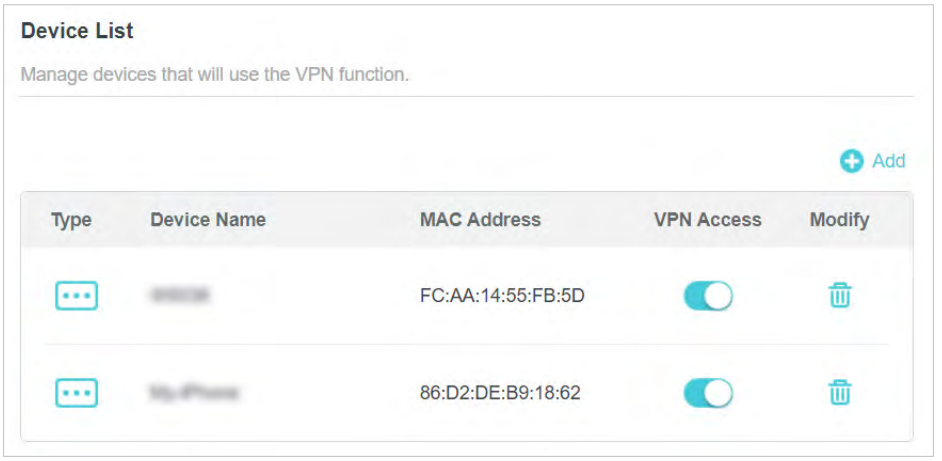
5. Add and manage the devices that will use the VPN function.

   1) In the Device List section, click Add.

   2) Choose and add the devices that will access the VPN server you have configured.



6. Save the settings.



Done! Now the devices you specified can access the VPN server you enabled.

Chapter 17

Customize Your Network Settings

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

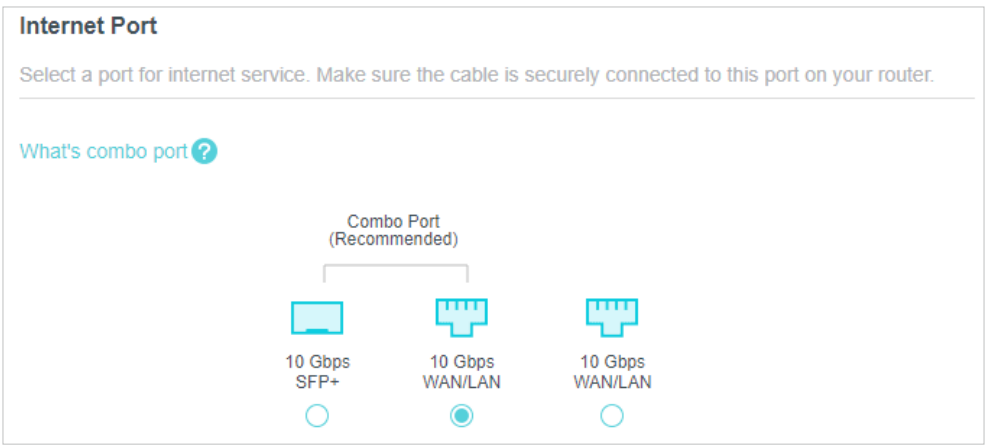
It contains the following sections:

17. 1. Change the Internet Settings

After setting up your internet, you can also easily change the internet settings if needed in the future.

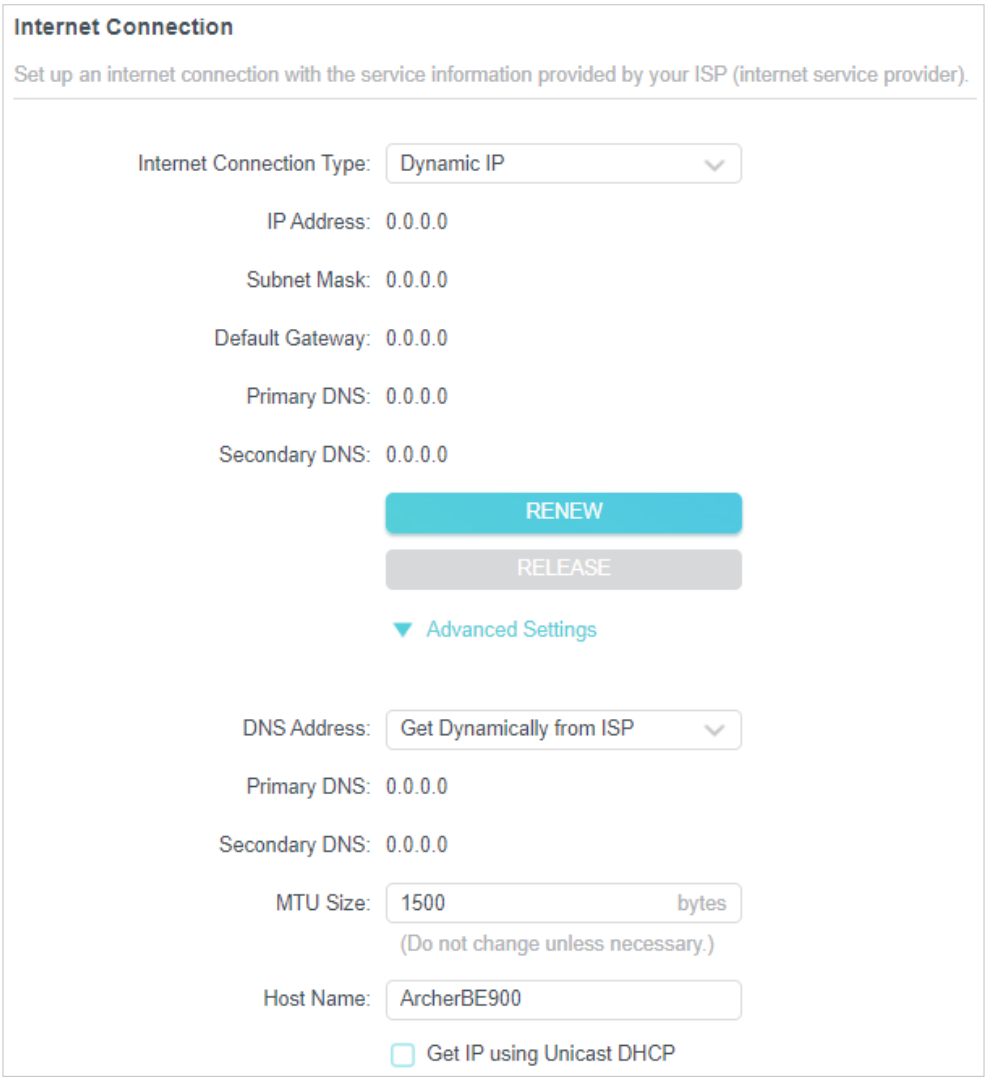
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > Network > Internet.

- **To change the internet port:**



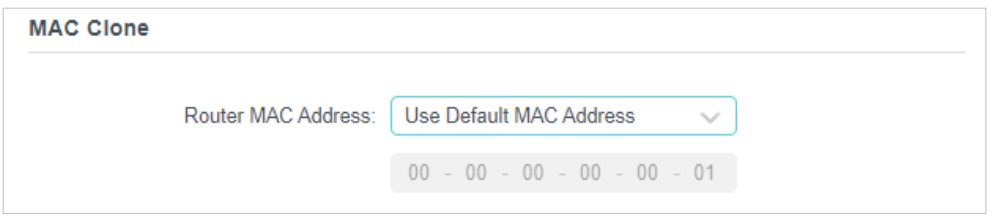
1. Select the desired internet port. Make sure the cable is securely connected to this port on your router.
2. Click SAVE.

- **To change the internet connection settings:**



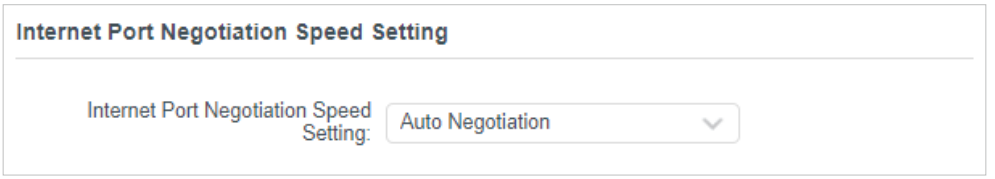
1. Select the internet connection type and configure the settings according to the information provided by your ISP.
2. Optional. Reveal the advanced settings and change the settings if needed. It's recommended to keep the default settings.
3. Click SAVE.

- **To change the MAC address of the router:**



You have three options, Use Default MAC Address, Clone Current Device MAC, Use Custom MAC Address.

- **To change the Internet Port Negotiation Speed Setting**

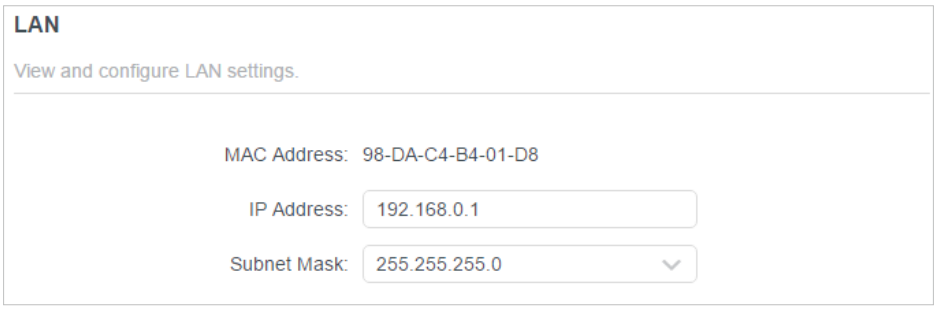


You can change the internet port speed mode. Auto Negotiation is recommended.

17. 2. Change the LAN Settings

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

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



4. Click SAVE.

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

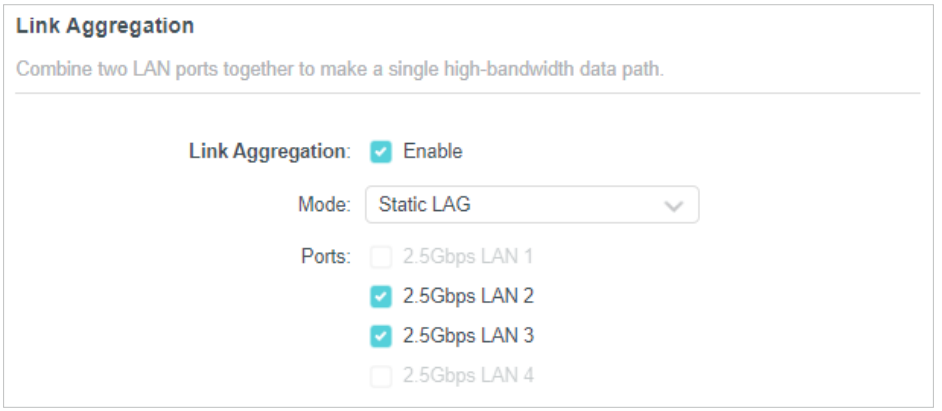
17. 3. Link Aggregation

The Link Aggregation feature combines two LAN ports together to make a single high-bandwidth data path, thus sustaining a higher-speed and more stable wired network.

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

3. Enable Link Aggregation.

Note: Link Aggregation and IPTV/VLAN cannot be enabled at the same time to avoid LAN port conflicts.



4. Select the Static LAG or LACP mode. It's recommended that you select the same link aggregation mode for both ends of the link.
5. Click SAVE. The LAN2 and LAN3 ports will be used for Link Aggregation.

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

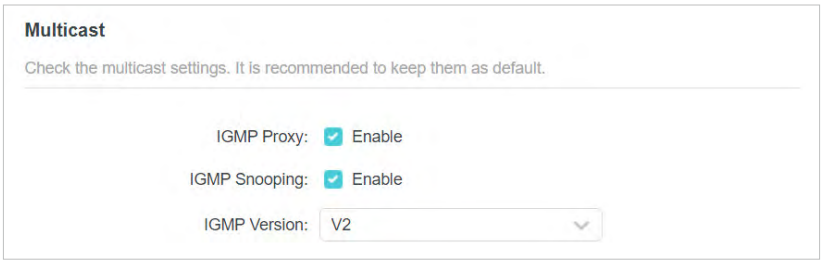
17. 4. Configure to Support IPTV Service

I want to:

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

How can I do that?

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



2) Click SAVE.

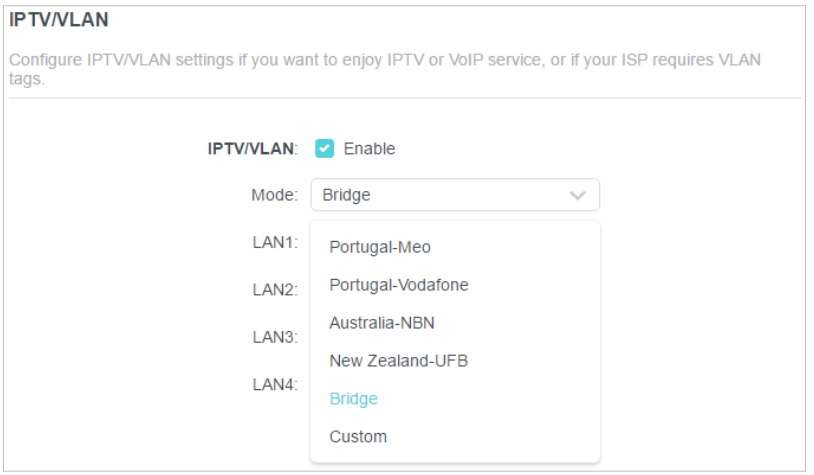
3) After configuring IGMP proxy, IPTV can work behind your router now. You can connect your set-top box to any of the router's Ethernet port.

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

1) Tick Enable IPTV/VLAN.

2) Select the appropriate Mode according to your ISP.

- Select Bridge if your ISP is not listed and no other parameters are required.
- Select Custom if your ISP is not listed but provides necessary parameters.



3) After you have selected a mode, the necessary parameters, including the LAN port for IPTV connection, are predetermined. If not, select the LAN type to determine which port is used to support IPTV service.

4) Click SAVE.

5) Connect the set-top box to the corresponding LAN port which is predetermined or you have specified in Step 3.

Done!

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

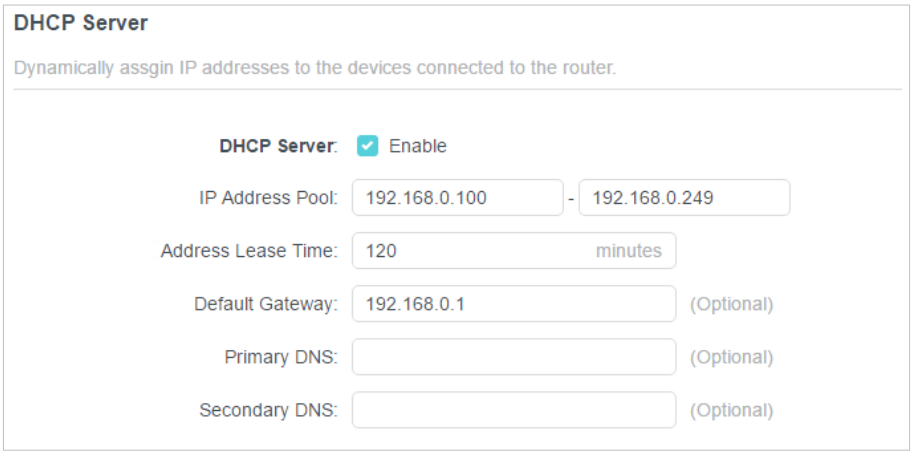
17. 5. Specify DHCP Server Settings

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

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

2. Go to Advanced > Network > DHCP Server.

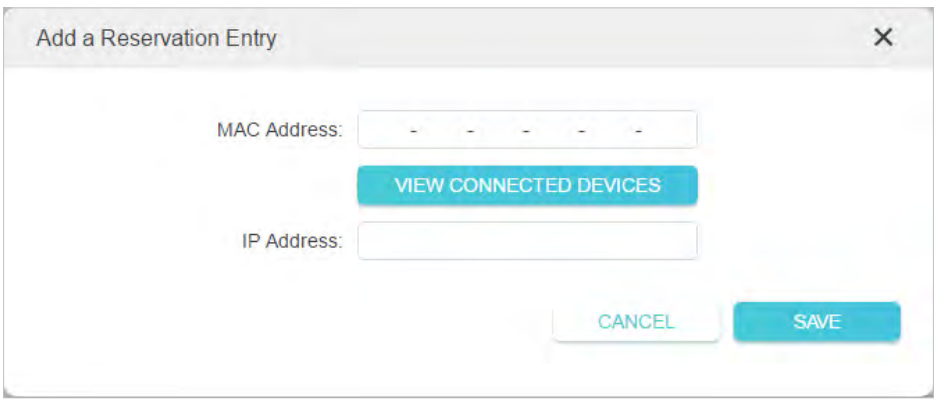
- **To specify the IP address that the router assigns:**



1. Tick the Enable checkbox.
2. Enter the starting and ending IP addresses in the IP Address Pool.
3. Enter other parameters if the ISP offers. The Default Gateway is automatically filled in and is the same as the LAN IP address of the router.
4. Click SAVE.

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

1. Click Add in the Address Reservation section.



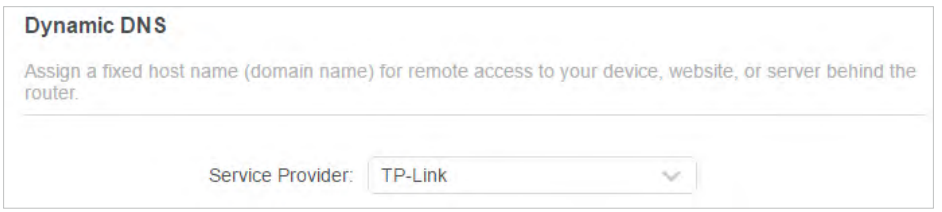
2. Click VIEW CONNECTED DEVICES and select the you device you want to reserve an IP for. Then the MAC Address will be automatically filled in. Or enter the MAC address of the client device manually.
3. Enter the IP address to reserve for the client device.
4. Click SAVE.

17. 6. Set Up a Dynamic DNS Service Account

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

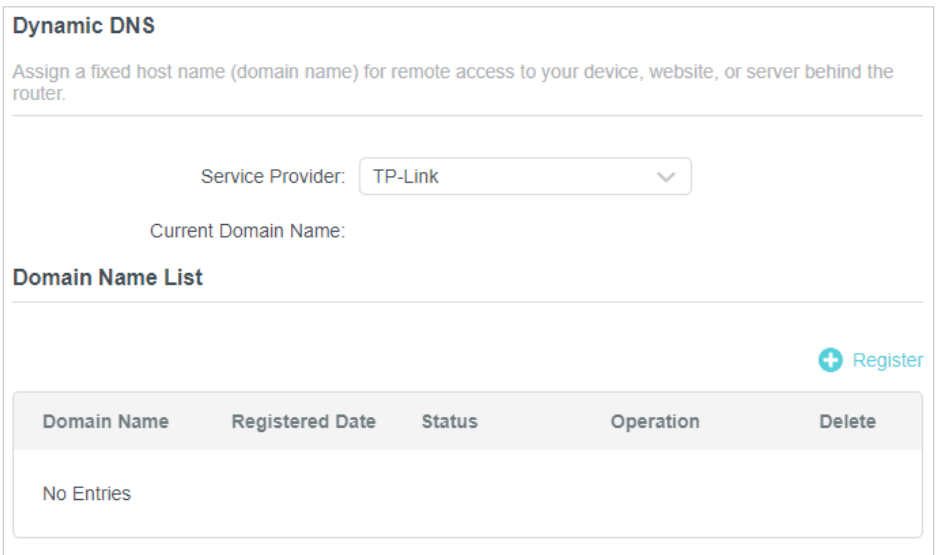
Note: DDNS does not work if the ISP assigns a private WAN IP address (such as 192.168.1.x) to the router.

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

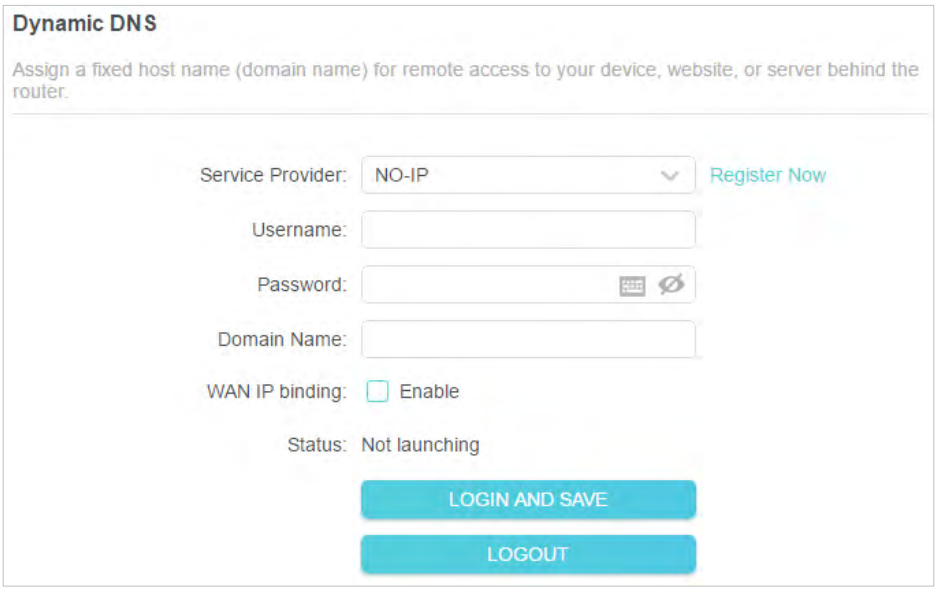


Note: To enjoy TP-Link's DDNS service, you have to log in with a TP-Link ID. If you have not logged in with one, click log in.

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



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



5. Click LOGIN AND SAVE.

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

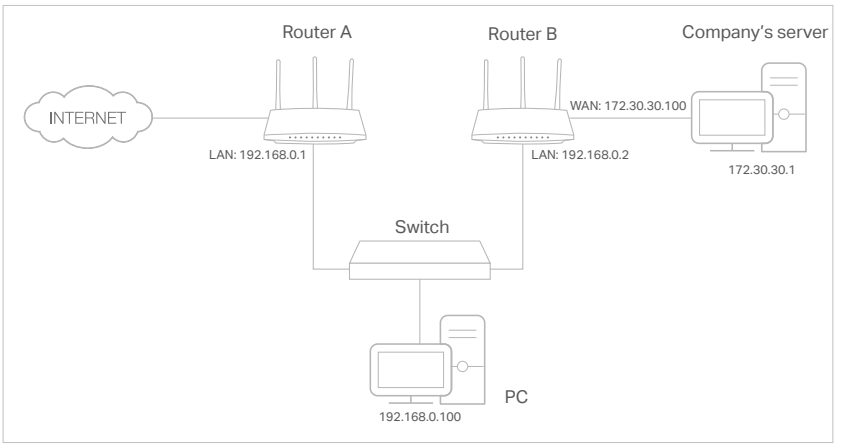
17. 7. Create Static Routes

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

I want to:

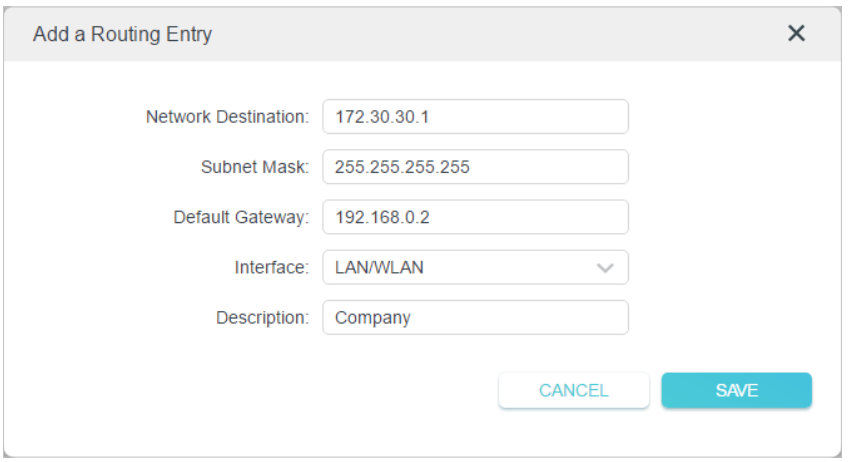
Visit multiple networks and servers at the same time.

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



How can I do that?

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



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

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

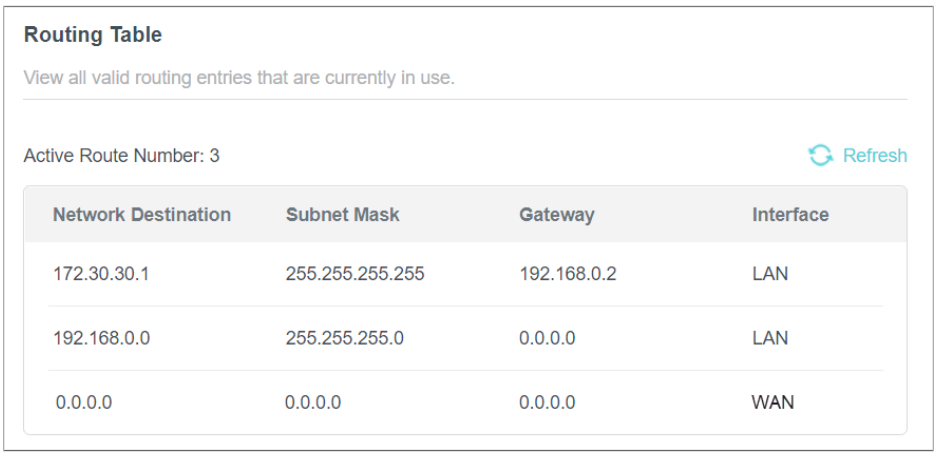
Default Gateway: The IP address of the gateway device to which the data packets

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

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

Description: Enter a description for this static routing entry.

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



Done!

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

Chapter 18

Manage the Router

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

It contains the following sections:

18. 1. Update the Firmware

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

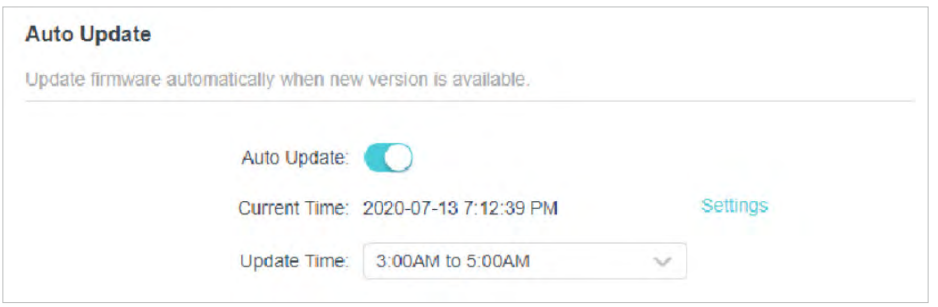
We will inform you through the web management page if there's any new firmware available for your router. Also, the latest firmware will be released at the TP-Link official website www.tp-link.com, and you can download it from the Support page for free.

Note:

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

18. 1. 1. Auto Update

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



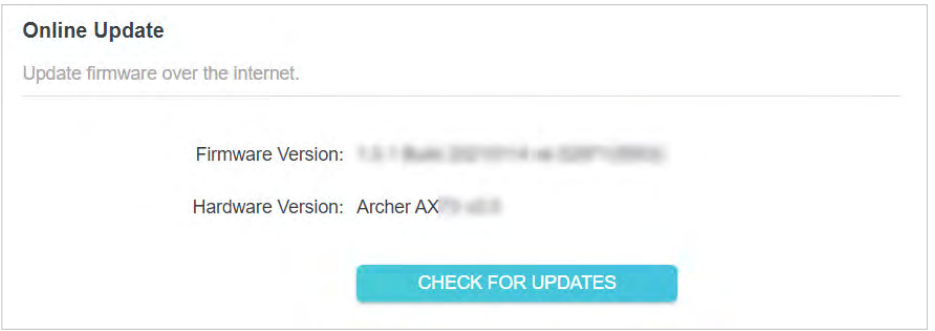
4. Specify the Update Time and save the settings.

The router will update firmware automatically at the specified time when new version is available.

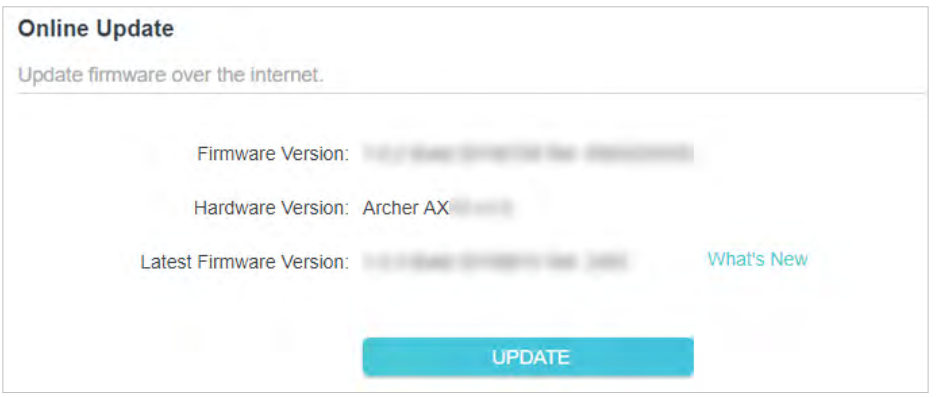
18. 1. 2. Online Update

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. When the latest firmware is available for your router, the update icon will display in the top-right corner of the page. Click the icon to go to the Firmware Update page.

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



3. Focus on the Online Update section, and click UPDATE if there is new firmware.

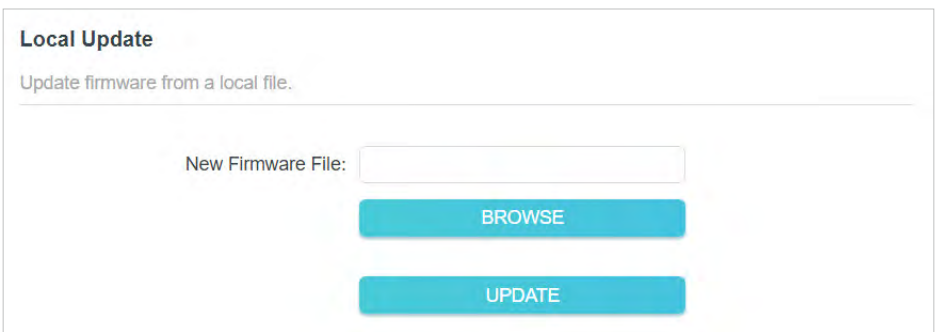


4. Wait a few minutes for the update and reboot to complete.

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

18. 1. 3. Local Update

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



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

Note: If you fail to update the firmware for the router, please contact our Technical Support.

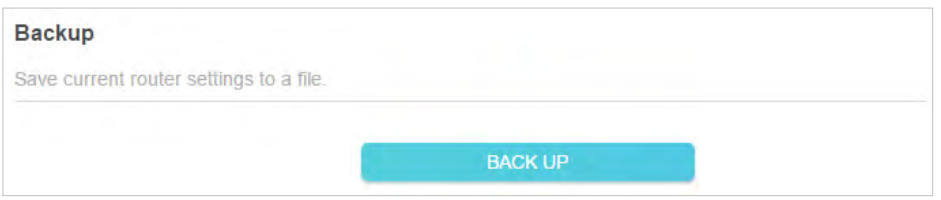
18. 2. Backup and Restore Configuration Settings

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

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

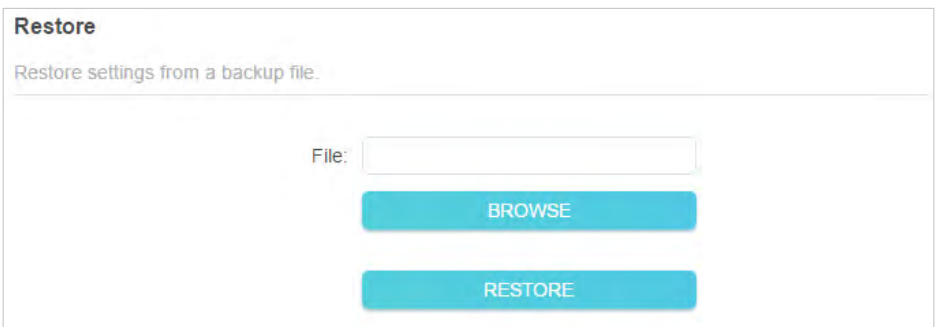
- **To backup configuration settings:**

Click BACK UP to save a copy of the current settings to your local computer. A '.bin' file of the current settings will be stored to your computer.



- **To restore configuration settings:**

1. Click BROWSE to locate the backup configuration file stored on your computer, and click RESTORE.

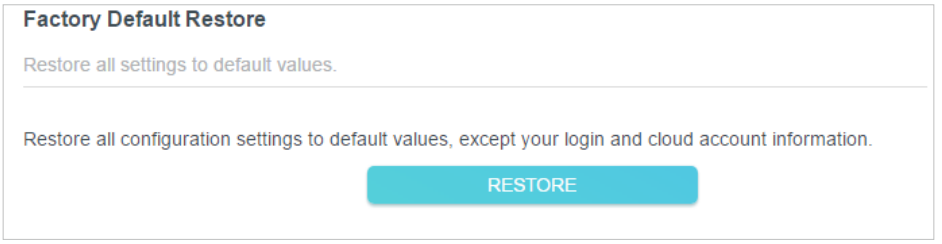


2. Wait a few minutes for the restoring and rebooting.

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

- **To reset the router except your login password and TP-Link ID:**

1. In the Factory Default Restore section, click RESTORE.



2. Wait a few minutes for the resetting and rebooting.

Note:

- During the resetting process, do not turn off the router.
- After reset, you can still use the current login password or the TP-Link ID to log in to the web management page.

- **To reset the router to factory default settings:**

1. Click FACTORY RESTORE to reset the router.

2. Wait a few minutes for the resetting and rebooting.

Note:

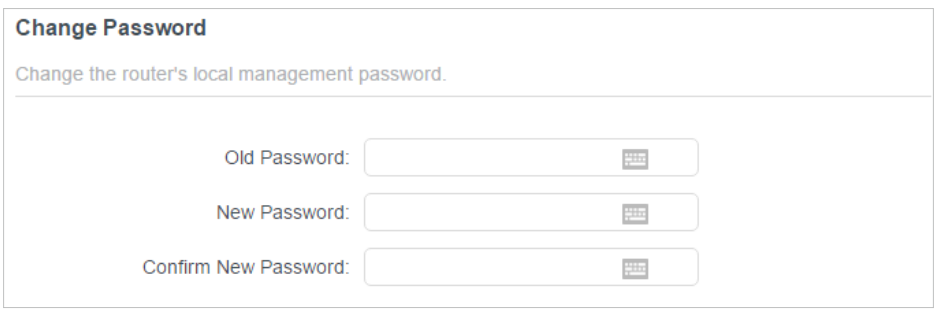
- During the resetting process, do not turn off or reset the router.
- We strongly recommend you backup the current configuration settings before resetting the router.

18. 3. Change the Login Password

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

Note: If you are using a TP-Link ID to log in to the web management page, the account management feature will be disabled. To manage the TP-Link ID, go to Advanced > TP-Link ID.

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > System > Administration and focus on the Change Password section.



3. Enter the old password, then a new password twice (both case-sensitive). Click SAVE.

4. Use the new password for future logins.

18. 4. Password Recovery

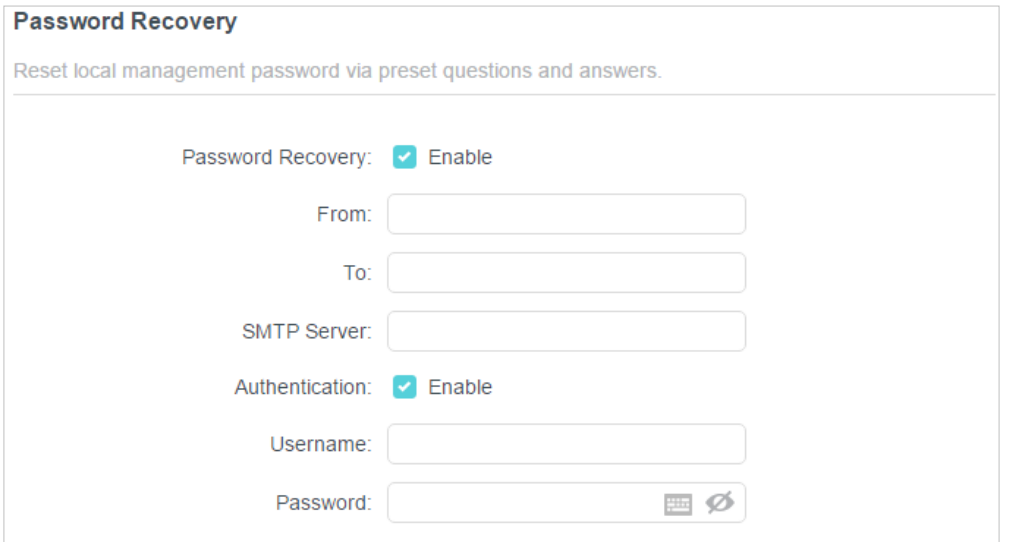
This feature allows you to recover the login password you set for you router in case you forget it.

Note: If you are using a TP-Link ID to log in to the web management page, the Password Recovery feature will be disabled. To manage the TP-Link ID, go to Advanced > TP-Link ID.

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > System > Administration and focus on the Password Recovery section.
3. Tick the Enable box of Password Recovery.
4. Specify a mailbox (From) for sending the recovery letter and enter its SMTP Server address. Specify a mailbox (To) for receiving the recovery letter. If the mailbox (From) to send the recovery letter requires encryption, Tick the Enable box of Authentication and enter its username and password.

Tips:

- SMTP server is available for users in most webmail systems. For example, the SMTP server address of Gmail is smtp.gmail.com.
- Generally, Authentication should be enabled if the login of the mailbox requires username and password.



5. Click SAVE.

To recover the login password, please visit http://tplinkwifi.net, click Forgot Password? on the login page and follow the instructions to set a new password.

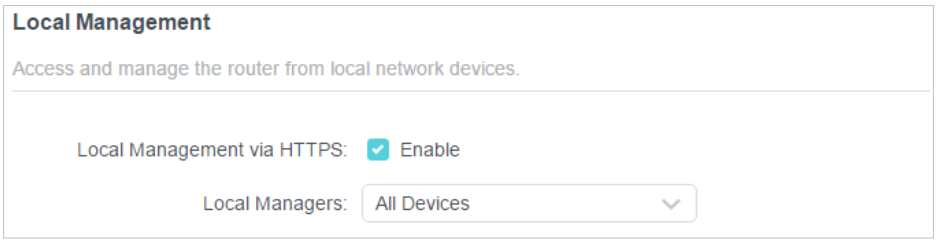
18. 5. Local Management

This feature allows you to limit the number of client devices on your LAN from accessing the router by using the MAC address-based authentication.

1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > System > Administration and complete the settings In Local Management section as needed.

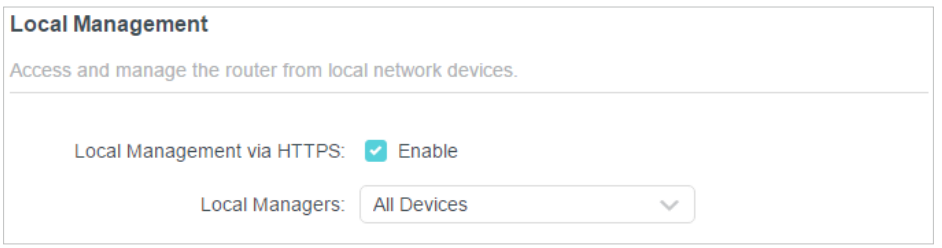
- **Access the router via HTTPS and HTTP:**

Tick the Enable box of Local Management via HTTPS to access the router via HTTPS and HTTP, or keep it disabled to access the router only via HTTP.



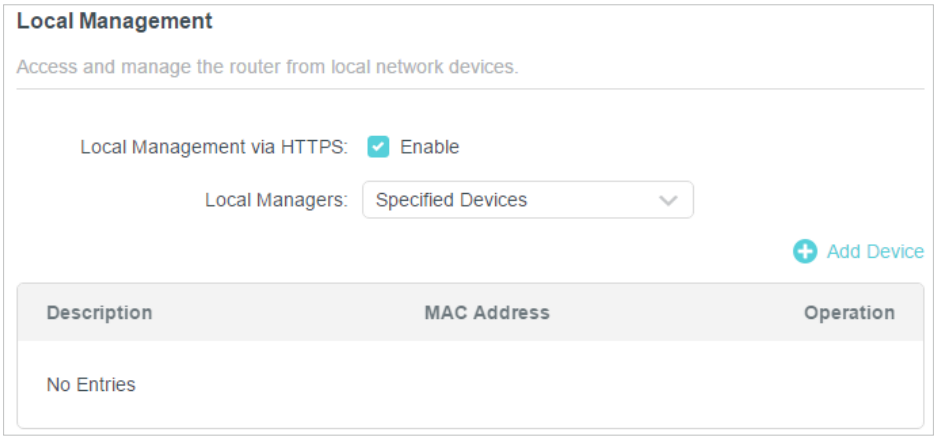
- **Allow all LAN connected devices to manage the router:**

Select All Devices for Local Managers.

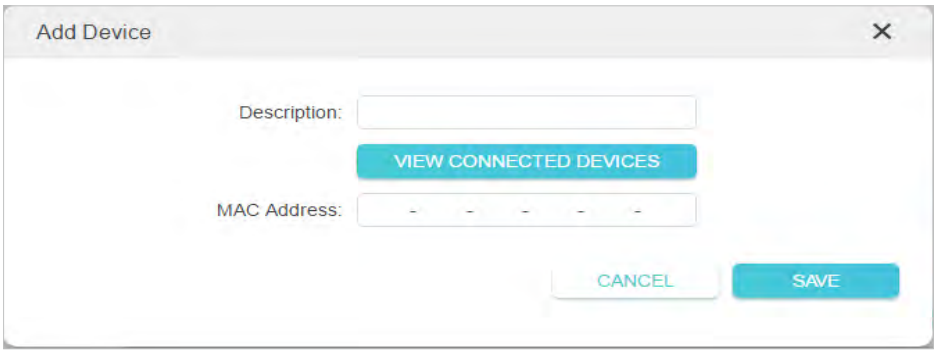


- **Allow specific devices to manage the router:**

1. Select All Devices for Local Managers and click SAVE.



2. Click Add Device.



3. Click VIEW CONNECTED DEVICES and select the device to manage the router from the Connected Devices list, or enter the MAC address of the device manually.
4. Specify a Description for this entry.
5. Click SAVE.

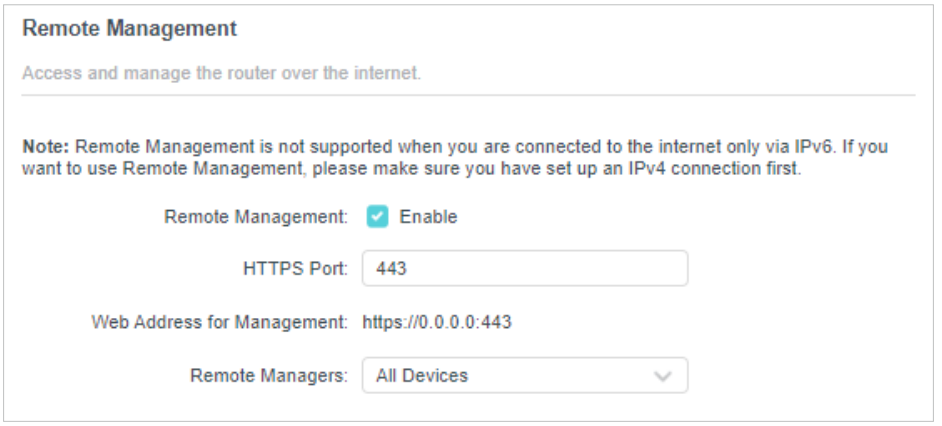
18. 6. Remote Management

This feature allows you to control remote devices' authority to manage the router.

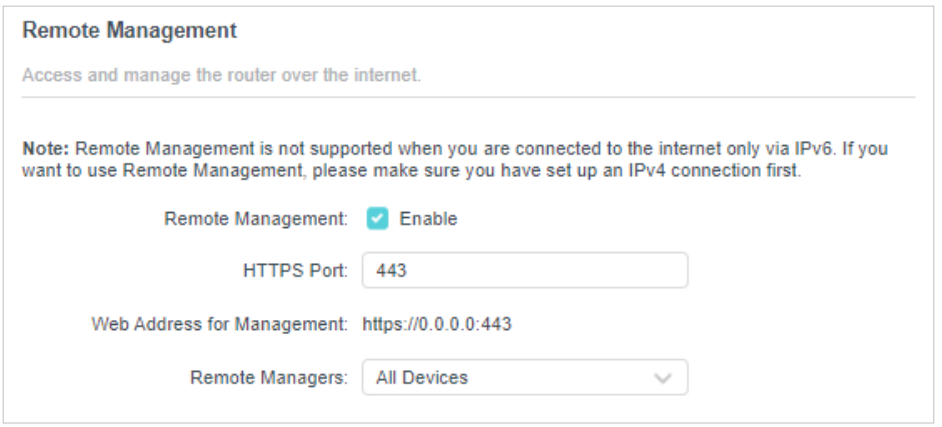
1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > System > Administration and complete the settings in Remote Management section as needed.

- **Forbid all devices to manage the router remotely:**

Do not tick the Enable checkbox of Remote Management.



- **Allow all devices to manage the router remotely:**



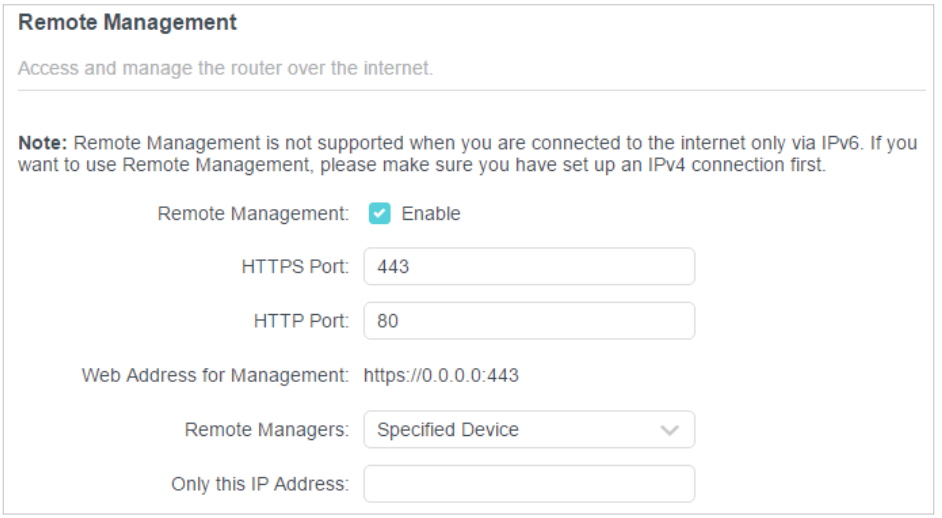
1. Tick the Enable checkbox of Remote Management.
2. Keep the HTTPS port as default settings (recommended) or enter a value between 1024 and 65535.
3. Select All Devices for Specified Devices.
4. Click SAVE.

Devices on the internet can log in to https://Router's WAN IP address:port number (such as https://113.116.60.229:1024) to manage the router.

Tips:

- You can find the WAN IP address of the router on Network Map > Internet.
- The router's WAN IP is usually a dynamic IP. Please refer to Set Up a Dynamic DNS Service Account if you want to log in to the router through a domain name.

- **Allow a specific device to manage the router remotely:**



1. Tick the Enable checkbox of Remote Management.
2. Keep the HTTPS and HTTP port as default settings (recommended) or enter a value between 1024 and 65535.
3. Select Specified Device for Remote Managers.
4. In the Only this IP Address field, enter the IP address of the remote device to manage the router.
5. Click SAVE.

Devices using this WAN IP can manage the router by logging in to http://Router's WAN IP:port number (such as http://113.116.60.229:1024).

Tips: The router's WAN IP is usually a dynamic IP. Please refer to Set Up a Dynamic DNS Service Account if you want to log in to the router through a domain name.

18. 7. System Log

When the router does not work normally, you can save the system log and send it to the technical support for troubleshooting.

- **To save the system log locally:**

1. Visit http://tplinkwifi.net, and log in your TP-Link ID or the password you set for the router.
2. Go to Advanced > System > System Log.
3. Choose the type and level of the system logs as needed.