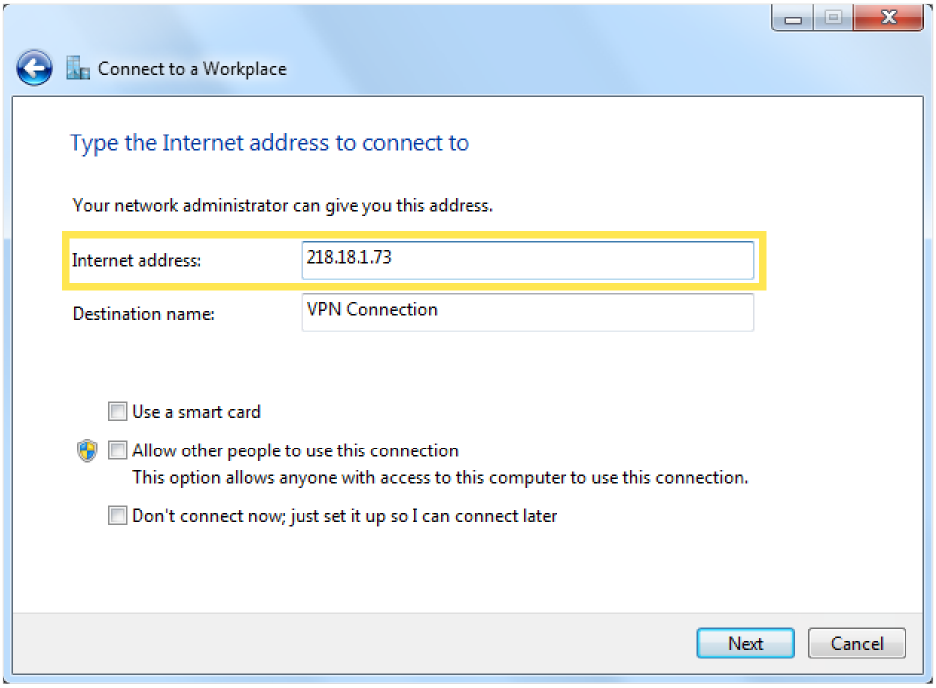


Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 218.18.1.73

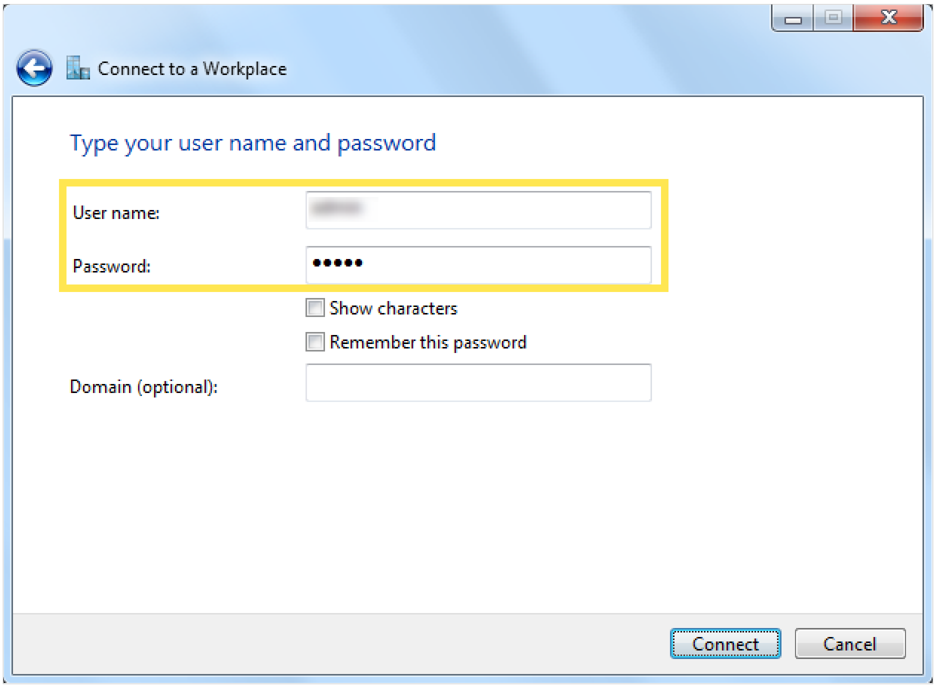
Destination name: VPN Connection

□ Use a smart card

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

□ Don't connect now; just set it up so I can connect later

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



Connect to a Workplace

Type your user name and password

User name: [redacted]

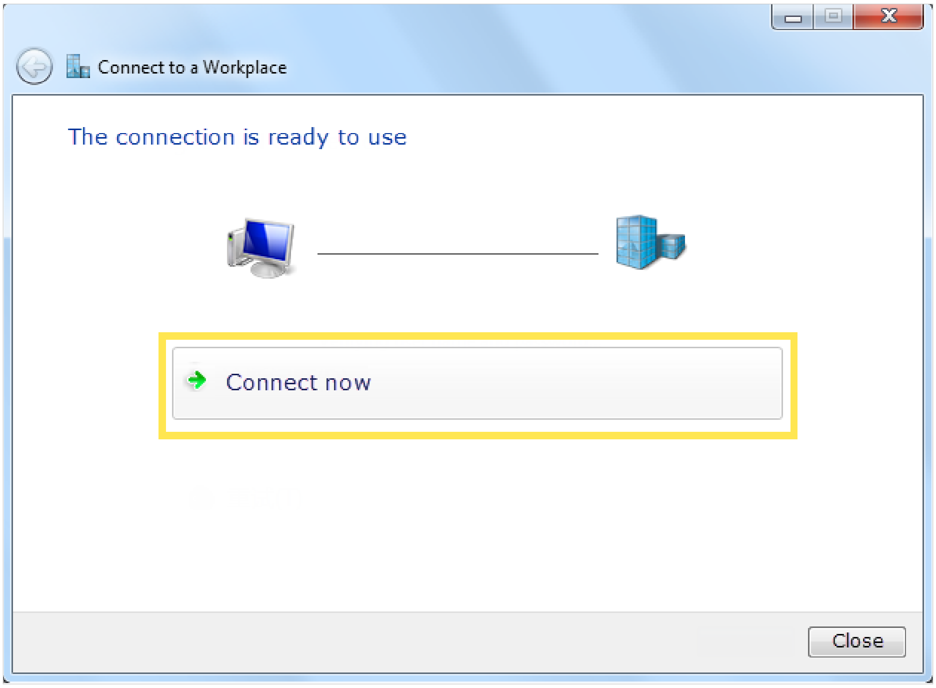
Password: •••••

□ Show characters

□ Remember this password

Domain (optional):

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

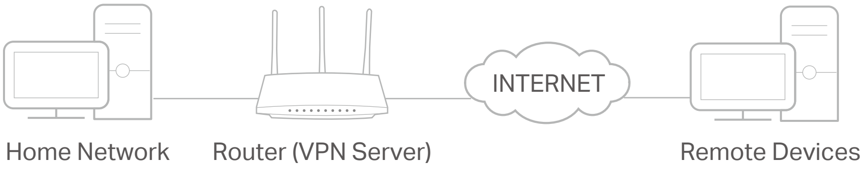


The connection is ready to use

14. 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.



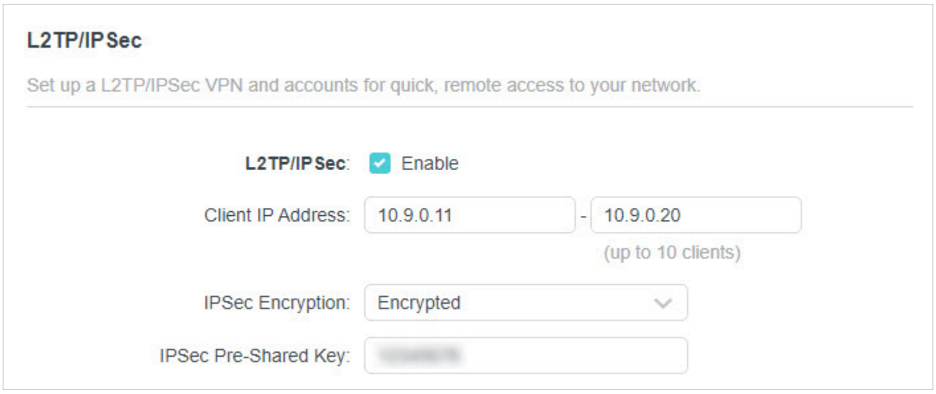
Step 1. Set up L2TP/IPSec VPN Server on Your Router

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.



L2TP/IPSec

Set up a L2TP/IPSec VPN and accounts for quick, remote access to your network.

L2TP/IPSec: ☑ Enable

Client IP Address: 10.9.0.11 - 10.9.0.20 (up to 10 clients)

IPSec Encryption: Encrypted

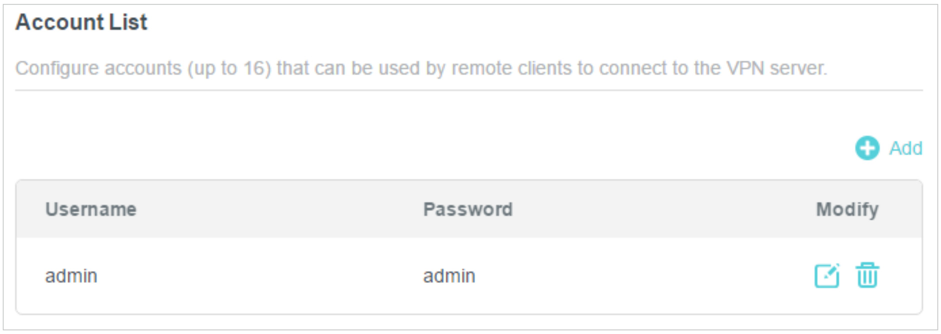
IPSec Pre-Shared Key:

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.



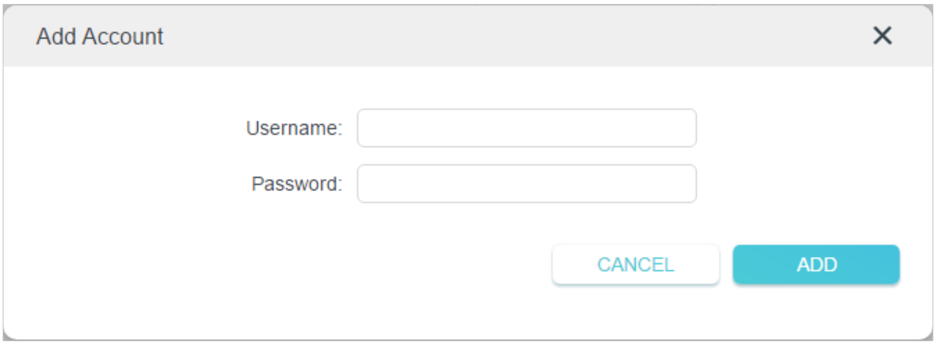
Account List

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

Username	Password	Modify
admin	admin	

4) Click Add.

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



Add Account

Username:

Password:

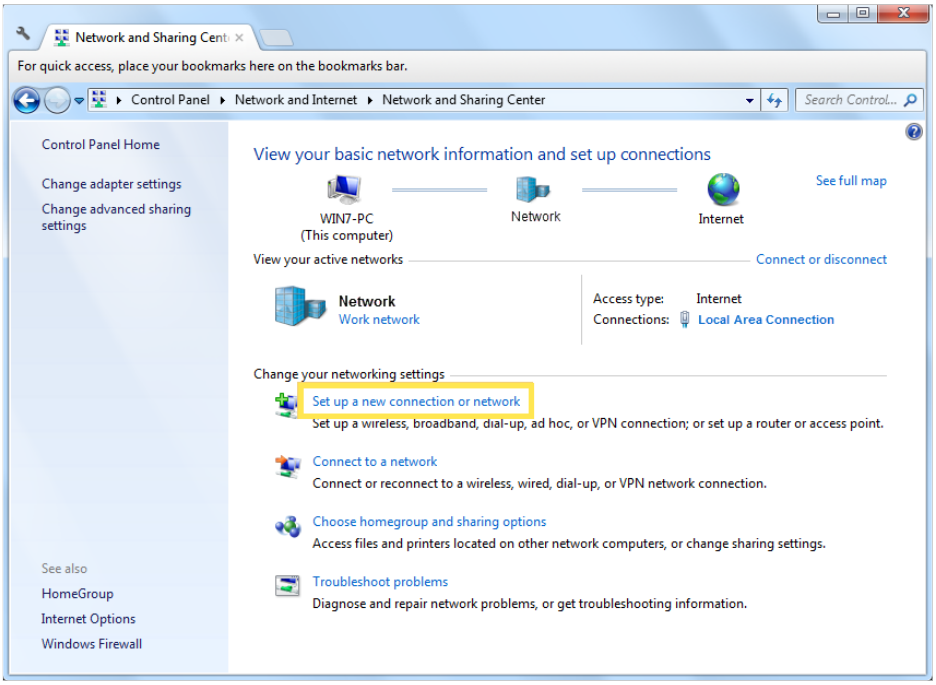
6) Click ADD.

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.



Network and Sharing Cent ×

For quick access, place your bookmarks here on the bookmarks bar.

Control Panel ▸ Network and Internet ▸ Network and Sharing Center

Search Control...

Control Panel Home

Change adapter settings

Change advanced sharing settings

View your basic network information and set up connections

See full map

WIN7-PC (This computer)

Network

Internet

View your active networks

Connect or disconnect

Network
Work network

Access type: Internet
Connections: Local Area Connection

Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

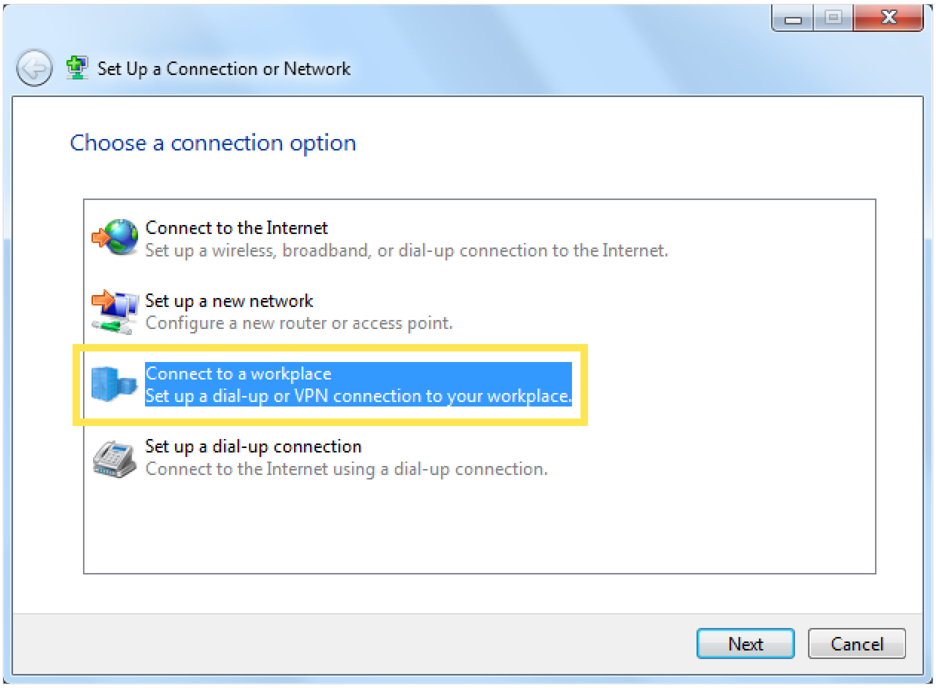
See also

HomeGroup

Internet Options

Windows Firewall

3. Select Connect to a workplace and click Next.



Set Up a Connection or Network

Choose a connection option

Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.

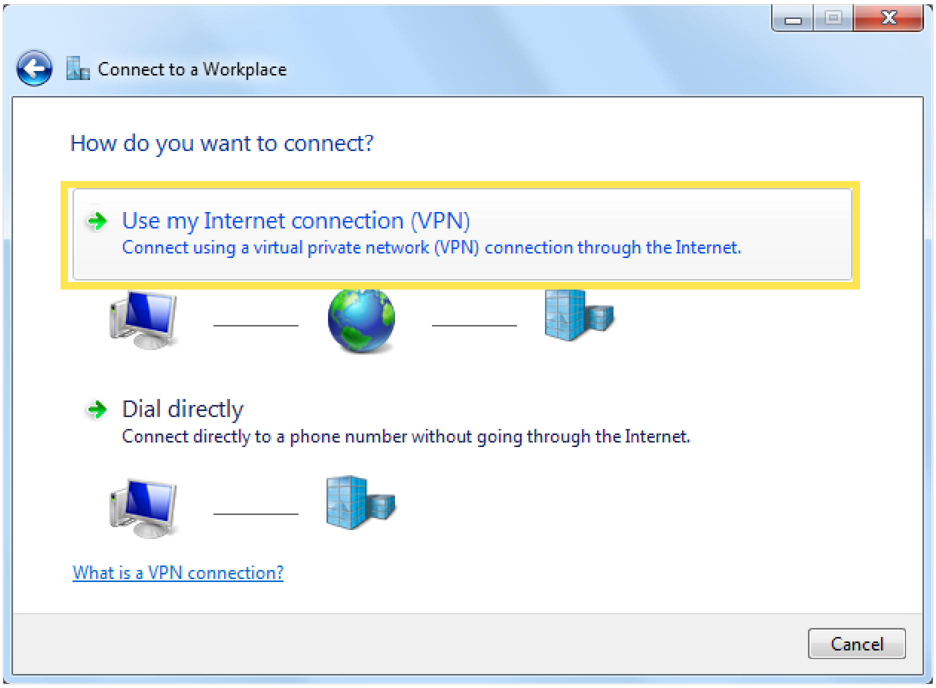
Set up a new network
Configure a new router or access point.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Set up a dial-up connection
Connect to the Internet using a dial-up connection.

Next Cancel

4. Select Use my Internet connection (VPN).



Connect to a Workplace

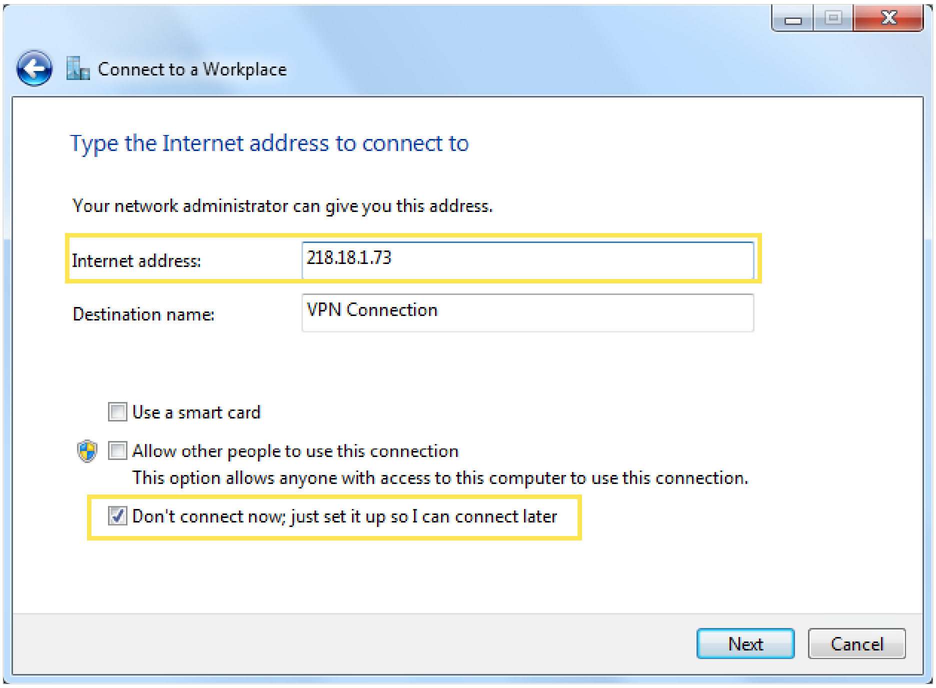
How do you want to connect?

→ Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

→ Dial directly
Connect directly to a phone number without going through the Internet.

What is a VPN connection?

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.



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 218.18.1.73

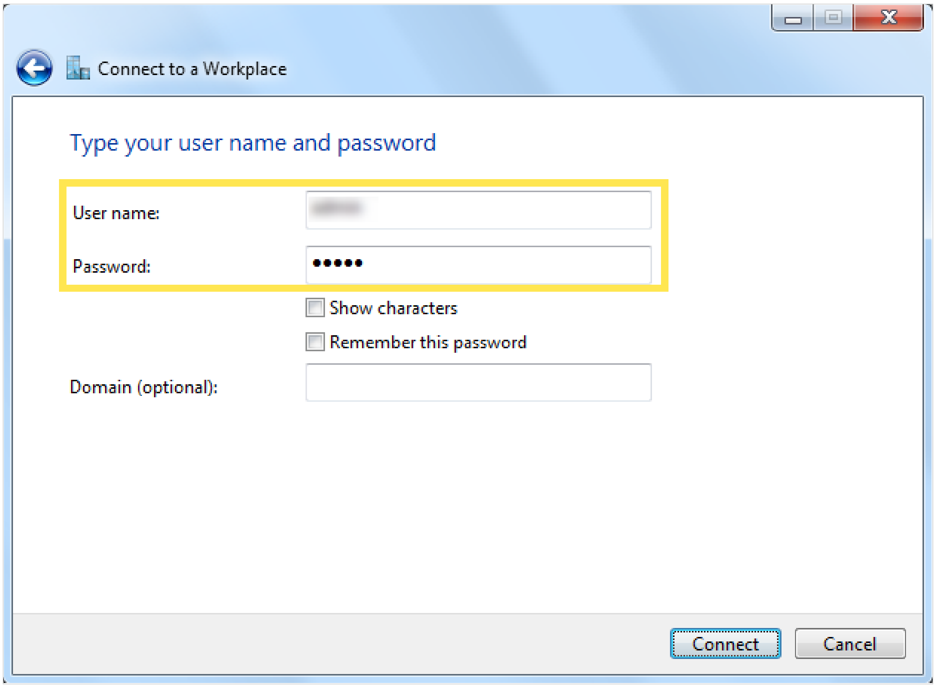
Destination name: VPN Connection

□ Use a smart card

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☑ Don't connect now; just set it up so I can connect later

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



Connect to a Workplace

Type your user name and password

User name: [redacted]

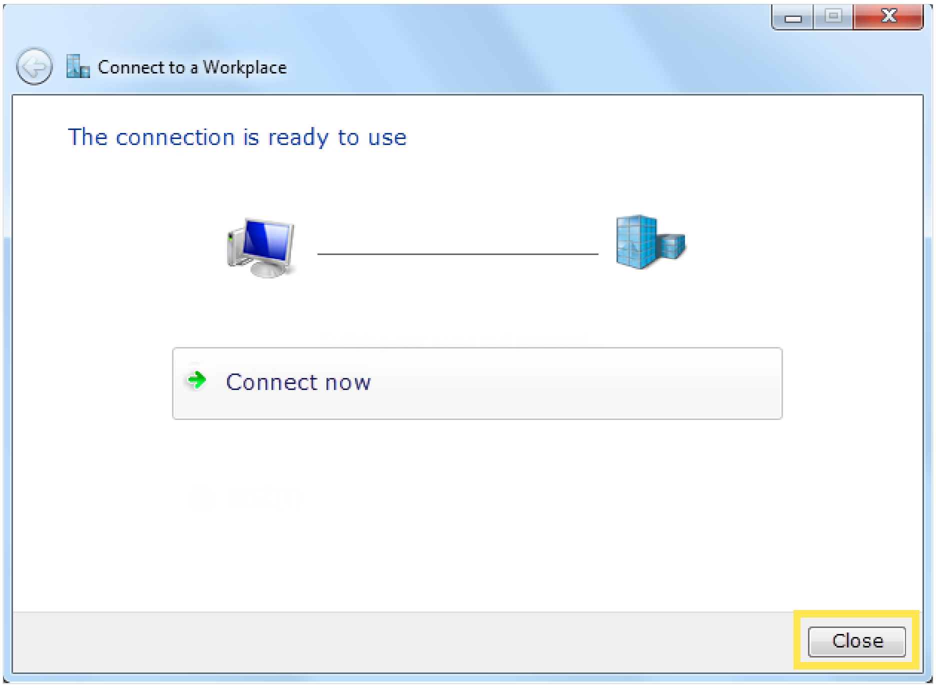
Password: •••••

□ Show characters

□ Remember this password

Domain (optional):

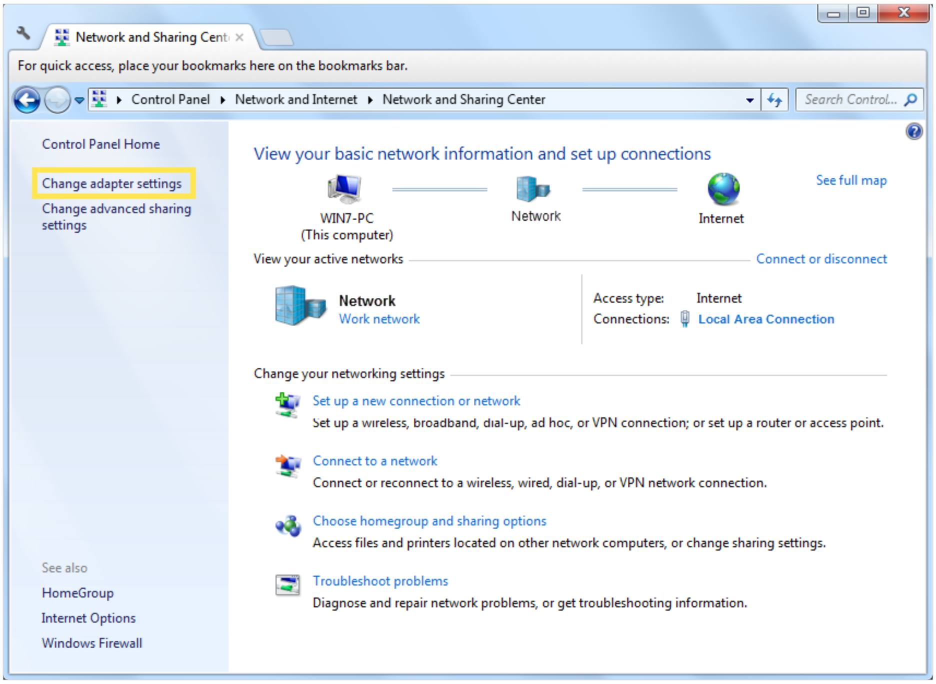
7. Click Close when the VPN connection is ready to use



Connect to a Workplace

The connection is ready to use

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



View your basic network information and set up connections

View your active networks

Network
Work network

Access type: Internet
Connections: Local Area Connection

Change your networking settings

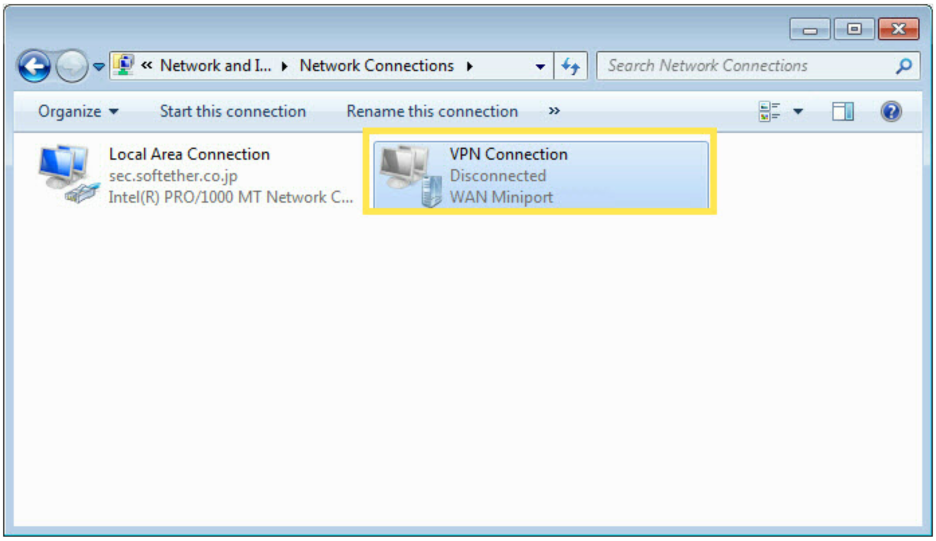
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

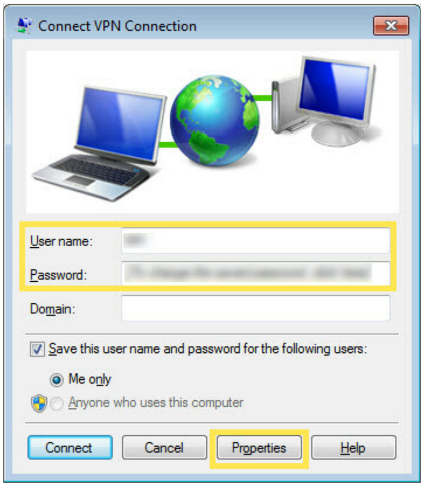
9. Find the VPN connection you created, then double-click it.


« Network and I... ▸ Network Connections ▸
Search Network Connections
Organize ▾
Start this connection
Rename this connection
»

Local Area Connection
sec.softether.co.jp
Intel(R) PRO/1000 MT Network C...

VPN Connection
Disconnected
WAN Miniport

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



Connect VPN Connection

User name: [redacted]

Password: [redacted]

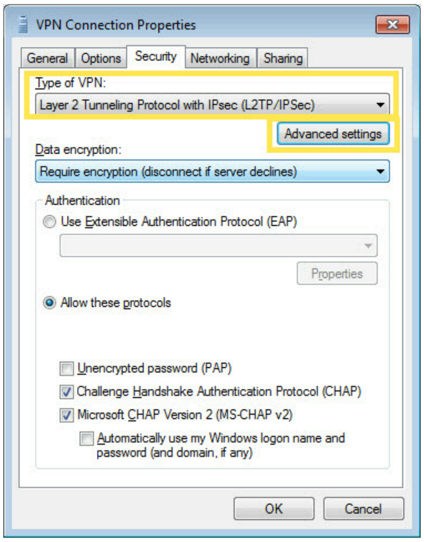
Domain:

☑ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

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



VPN Connection Properties

Type of VPN: Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)

Data encryption: Require encryption (disconnect if server declines)

Authentication

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

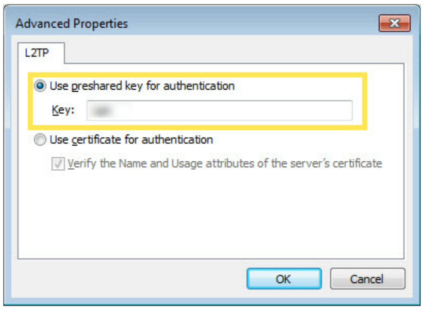
□ Unencrypted password (PAP)

☑ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)

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.



Advanced Properties

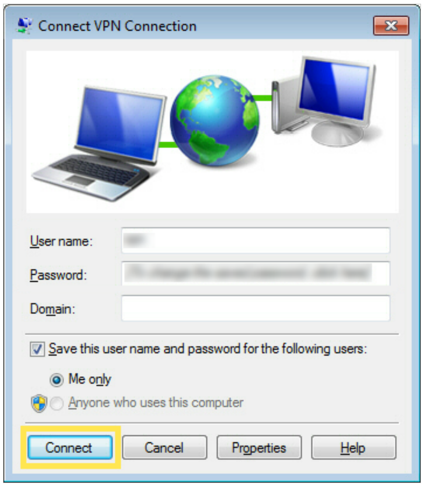
● Use preshared key for authentication

Key: [redacted]

○ Use certificate for authentication

☑ Verify the Name and Usage attributes of the server's certificate

Done! Click Connect to start VPN connection.



Connect VPN Connection

User name: [redacted]

Password: [redacted]

Domain:

☑ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

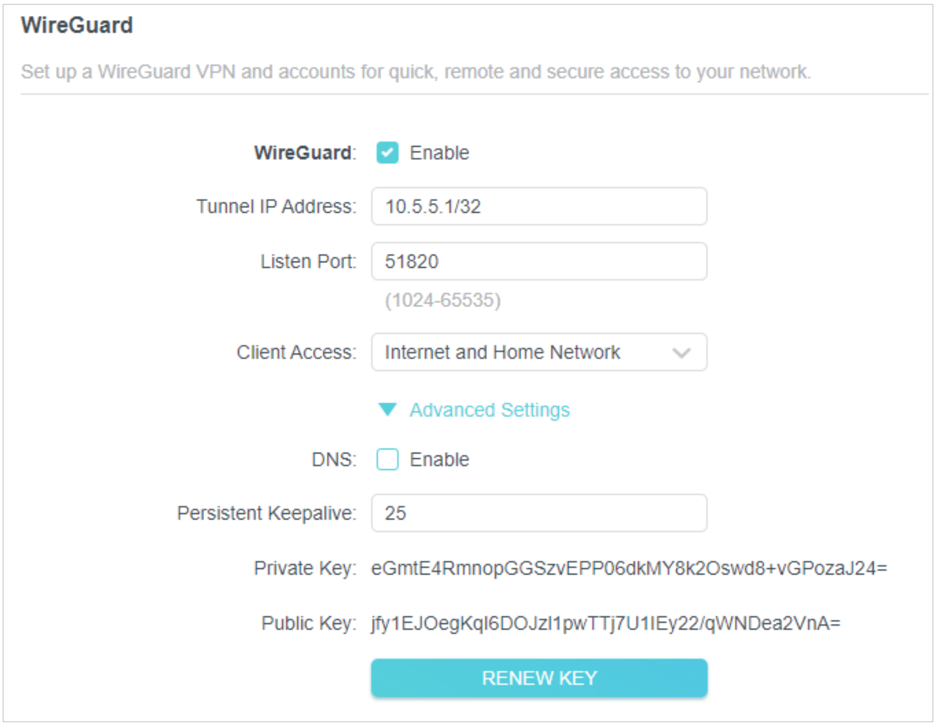
14. 4. Use WireGuard VPN to Access Your Home Network

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.



WireGuard

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

WireGuard: ☑ Enable

Tunnel IP Address: 10.5.5.1/32

Listen Port: 51820 (1024-65535)

Client Access: Internet and Home Network

▼ Advanced Settings

DNS: □ Enable

Persistent Keepalive: 25

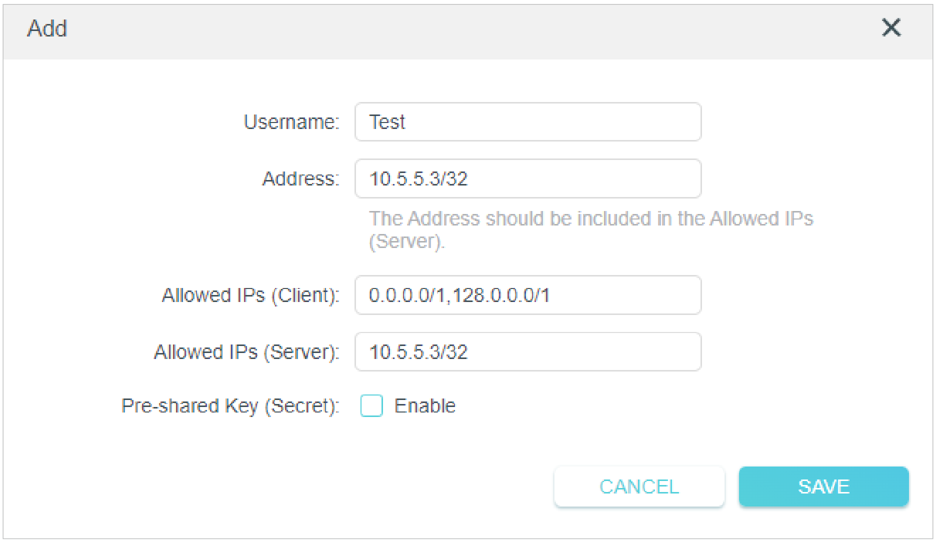
Private Key: eGmtE4RmnopGGSzvEPP06dkMY8k2Oswd8+vGPozaJ24=

Public Key: jfy1EJOegKql6DOJzl1pwTTj7U1lEy22/qWNDea2VnA=

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.



Add

Username: Test

Address: 10.5.5.3/32

The Address should be included in the Allowed IPs (Server).

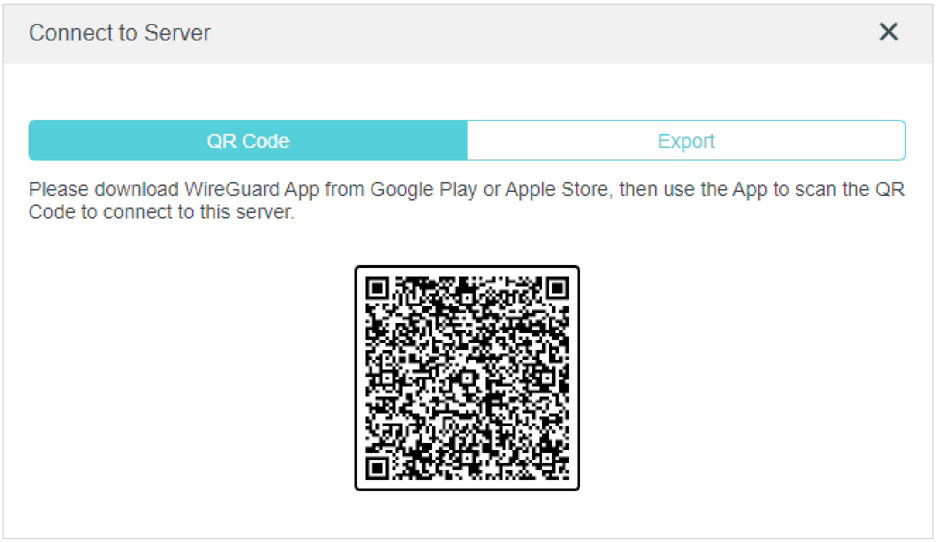
Allowed IPs (Client): 0.0.0.0/1,128.0.0.0/1

Allowed IPs (Server): 10.5.5.3/32

Pre-shared Key (Secret): □ Enable

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.

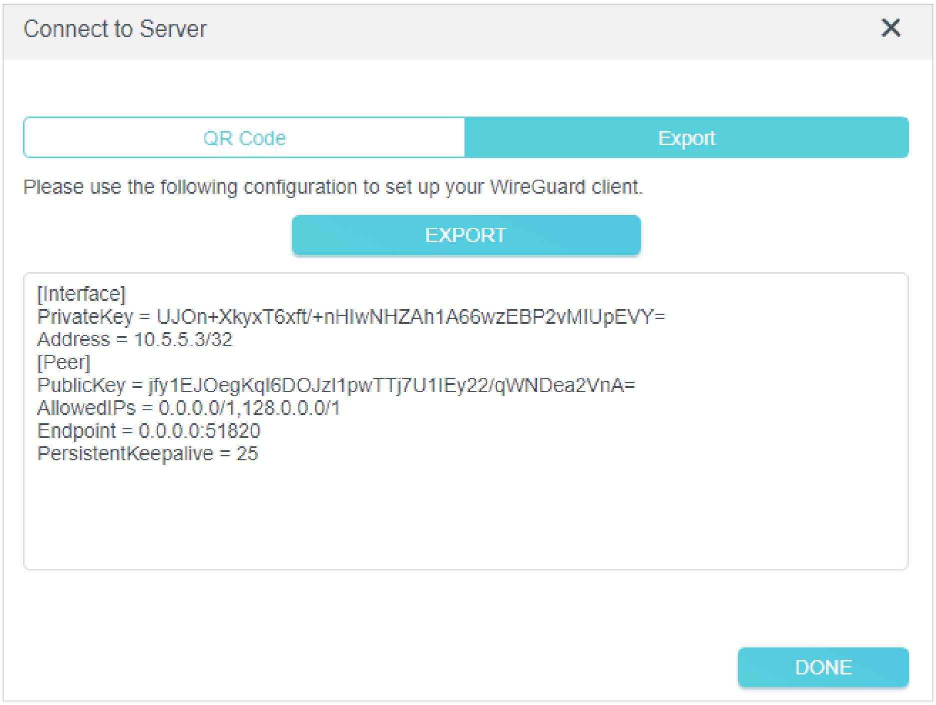


Connect to Server

Please download WireGuard App from Google Play or Apple Store, then use the App to scan the QR Code to connect to this 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.

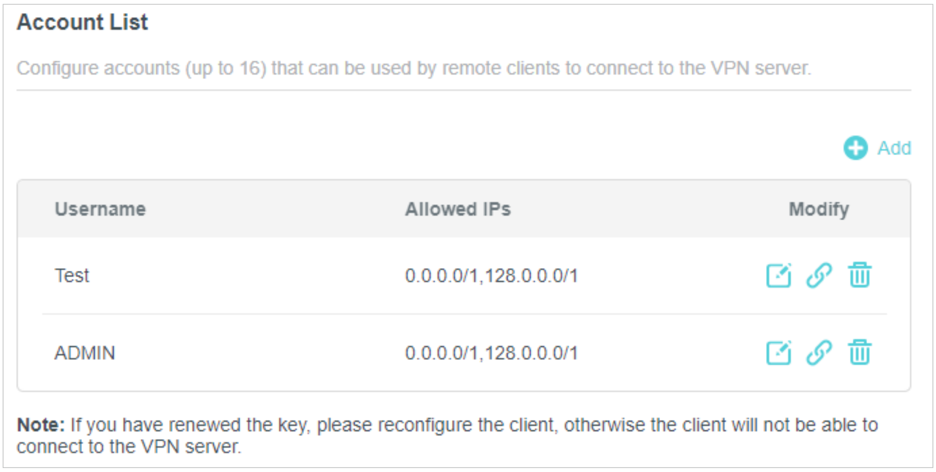


Connect to Server

Please use the following configuration to set up your WireGuard client.

```
[Interface]
PrivateKey = UJOn+XkyxT6xft/+nHIwNHZAh1A66wzEBP2vMIUpEVY=
Address = 10.5.5.3/32
[Peer]
PublicKey = jfy1EJOegKql6DOJzI1pwTTj7U1IEy22/qWNDea2VnA=
AllowedIPs = 0.0.0.0/1,128.0.0.0/1
Endpoint = 0.0.0.0:51820
PersistentKeepalive = 25
```

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



Account List

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

Add

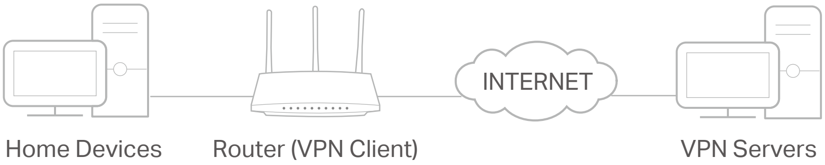
Username	Allowed IPs	Modify
Test	0.0.0.0/1,128.0.0.0/1	
ADMIN	0.0.0.0/1,128.0.0.0/1	

Note: If you have renewed the key, please reconfigure the client, otherwise the client will not be able to connect to the VPN server.

14. 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:

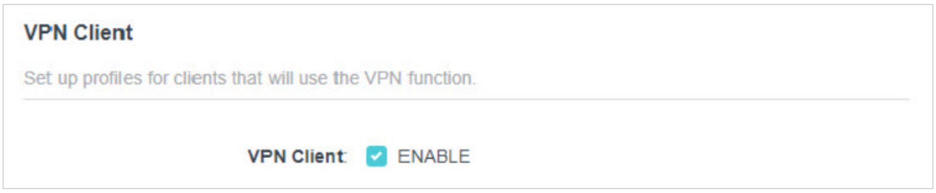


1. Visit http://tplinkwifi.net, and log in with your TP-Link ID or the password you set for the router.

2. Go to Advanced > VPN Client.

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

3. Enable VPN Client, then save the settings.



VPN Client

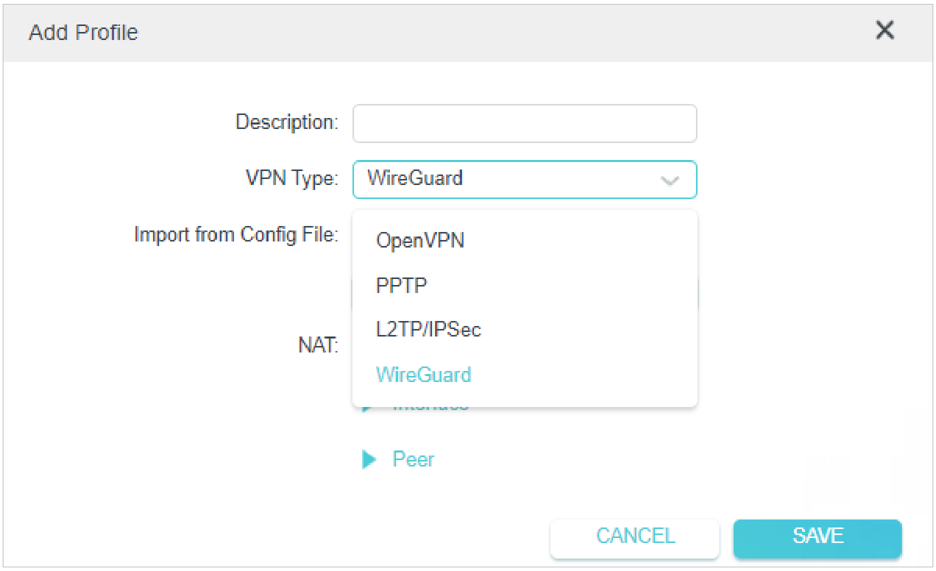
Set up profiles for clients that will use the VPN function.

VPN Client: ☑ ENABLE

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.



Add Profile

Description:

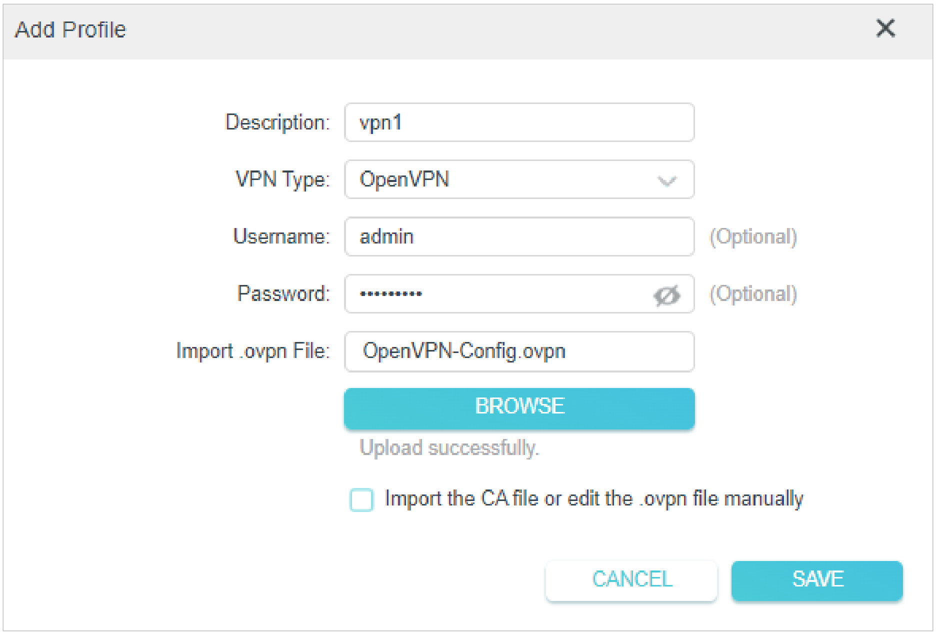
VPN Type: WireGuard

Import from Config File:

NAT:

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.



Add Profile

Description: vpn1

VPN Type: OpenVPN

Username: admin (Optional)

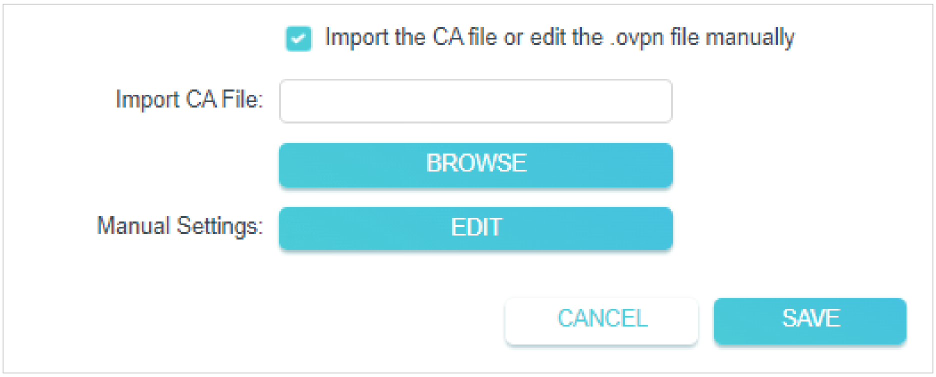
Password: ••••••••• (Optional)

Import .ovpn File: OpenVPN-Config.ovpn

Upload successfully.

□ Import the CA file or edit the .ovpn file manually

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.

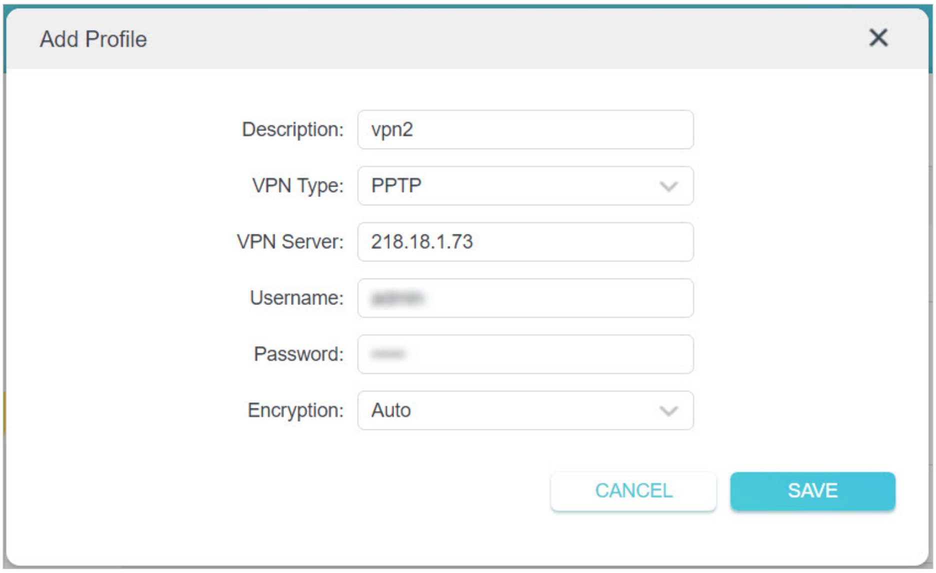


☑ Import the CA file or edit the .ovpn file manually

Import CA File:

Manual Settings:

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



Add Profile

Description: vpn2

VPN Type: PPTP

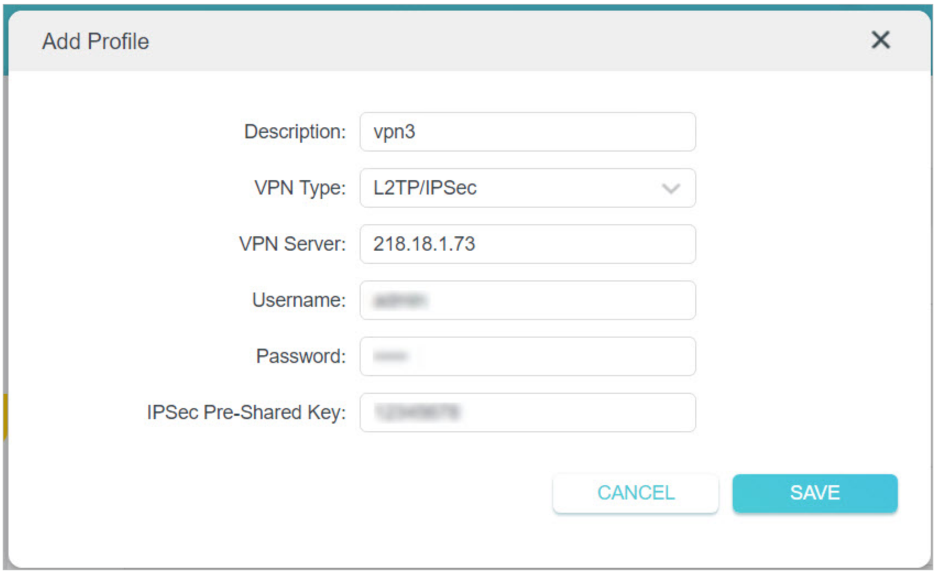
VPN Server: 218.18.1.73

Username: [redacted]

Password: [redacted]

Encryption: Auto

- 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.


Add Profile

Description: vpn3

VPN Type: L2TP/IPSec

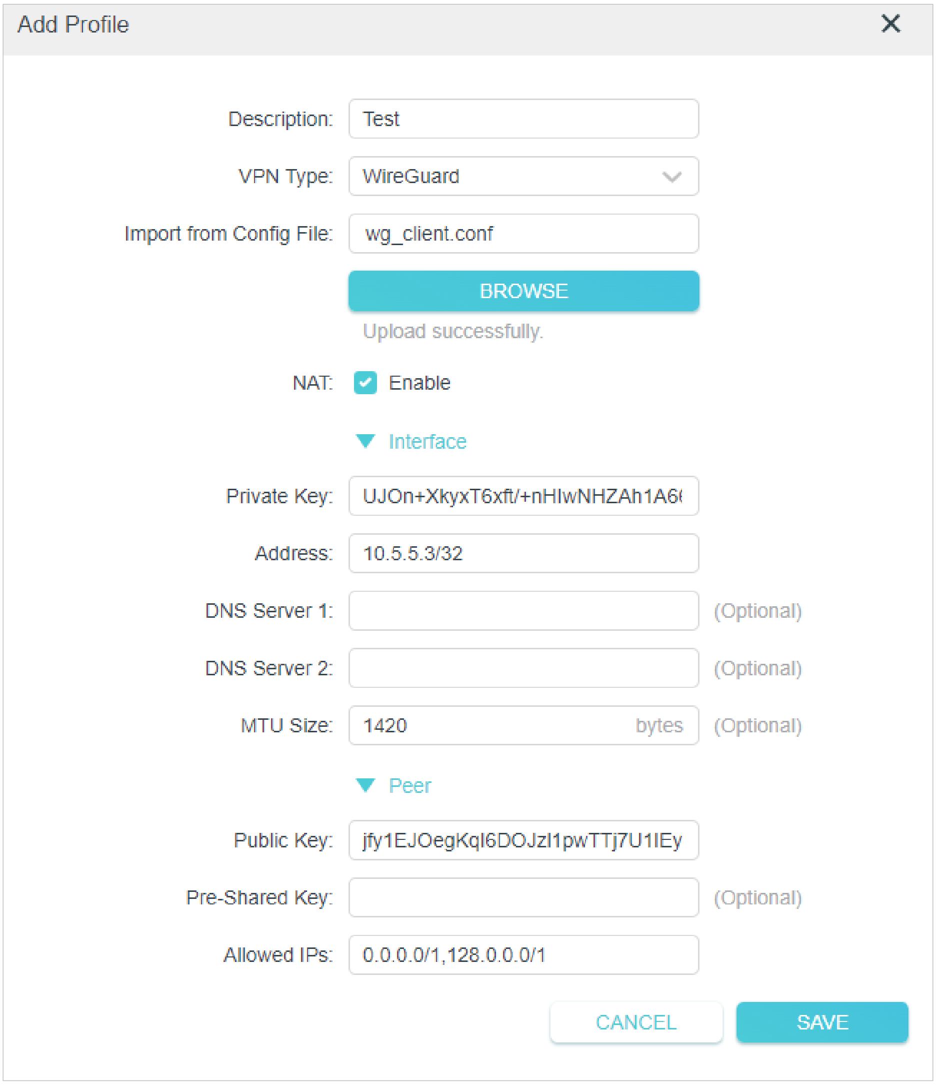
VPN Server: 218.18.1.73

Username: [redacted]

Password: [redacted]

IPSec Pre-Shared Key: [redacted]

- 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.



Add Profile ✕

Description: Test

VPN Type: WireGuard

Import from Config File: wg_client.conf

Upload successfully.

NAT: ☑ Enable

▼ Interface

Private Key: UJOn+XkyxT6xft/+nHIwNHZAh1A6

Address: 10.5.5.3/32

DNS Server 1: (Optional)

DNS Server 2: (Optional)

MTU Size: 1420 bytes (Optional)

▼ Peer

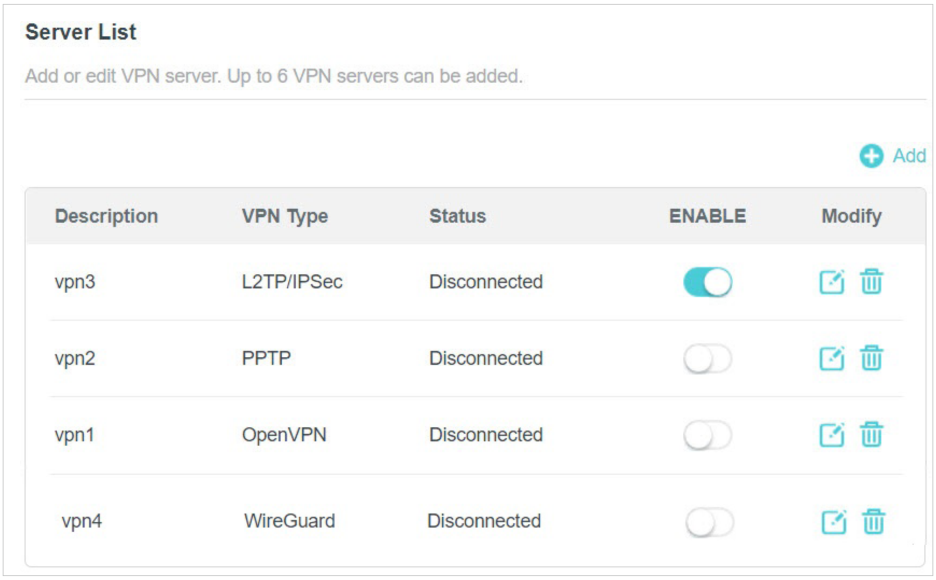
Public Key: jfy1EJOegKql6DOJzl1pwTTj7U1IEy

Pre-Shared Key: (Optional)

Allowed IPs: 0.0.0.0/1,128.0.0.0/1

4) Save the settings.

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



Server List

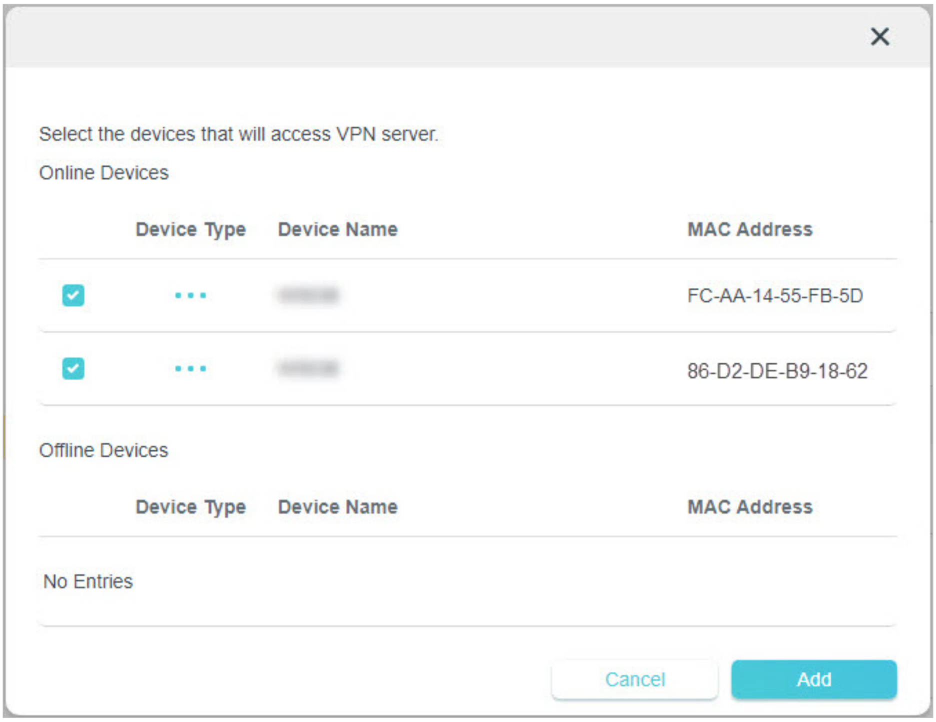
Add or edit VPN server. Up to 6 VPN servers can be added.

Description	VPN Type	Status	ENABLE	Modify
vpn3	L2TP/IPSec	Disconnected	●	
vpn2	PPTP	Disconnected	○	
vpn1	OpenVPN	Disconnected	○	
vpn4	WireGuard	Disconnected	○	

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.



Select the devices that will access VPN server.

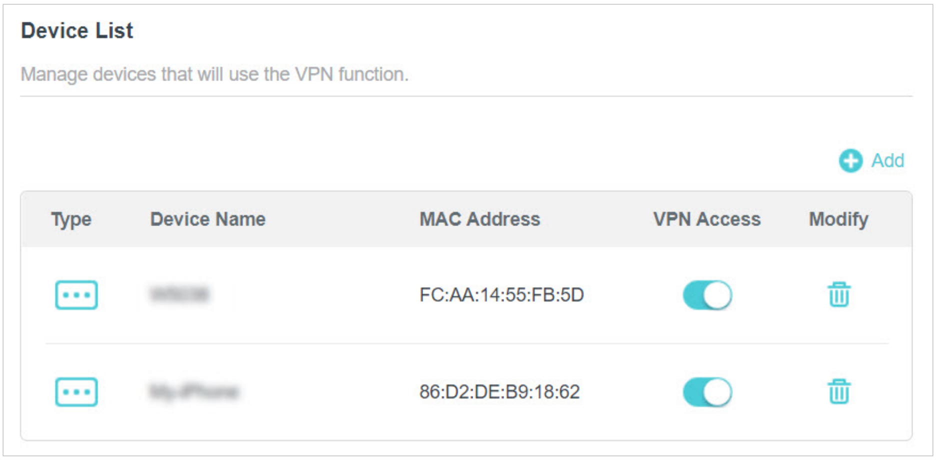
Online Devices

	Device Type	Device Name	MAC Address
☑	···	[redacted]	FC-AA-14-55-FB-5D
☑	···	[redacted]	86-D2-DE-B9-18-62

Offline Devices

Device Type	Device Name	MAC Address
No Entries		

6. Save the settings.



Device List

Manage devices that will use the VPN function.

Add

Type	Device Name	MAC Address	VPN Access	Modify
•••	[redacted]	FC:AA:14:55:FB:5D	●	🗑
•••	[redacted]	86:D2:DE:B9:18:62	●	🗑

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

Chapter 15

Customize Your Network Settings

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

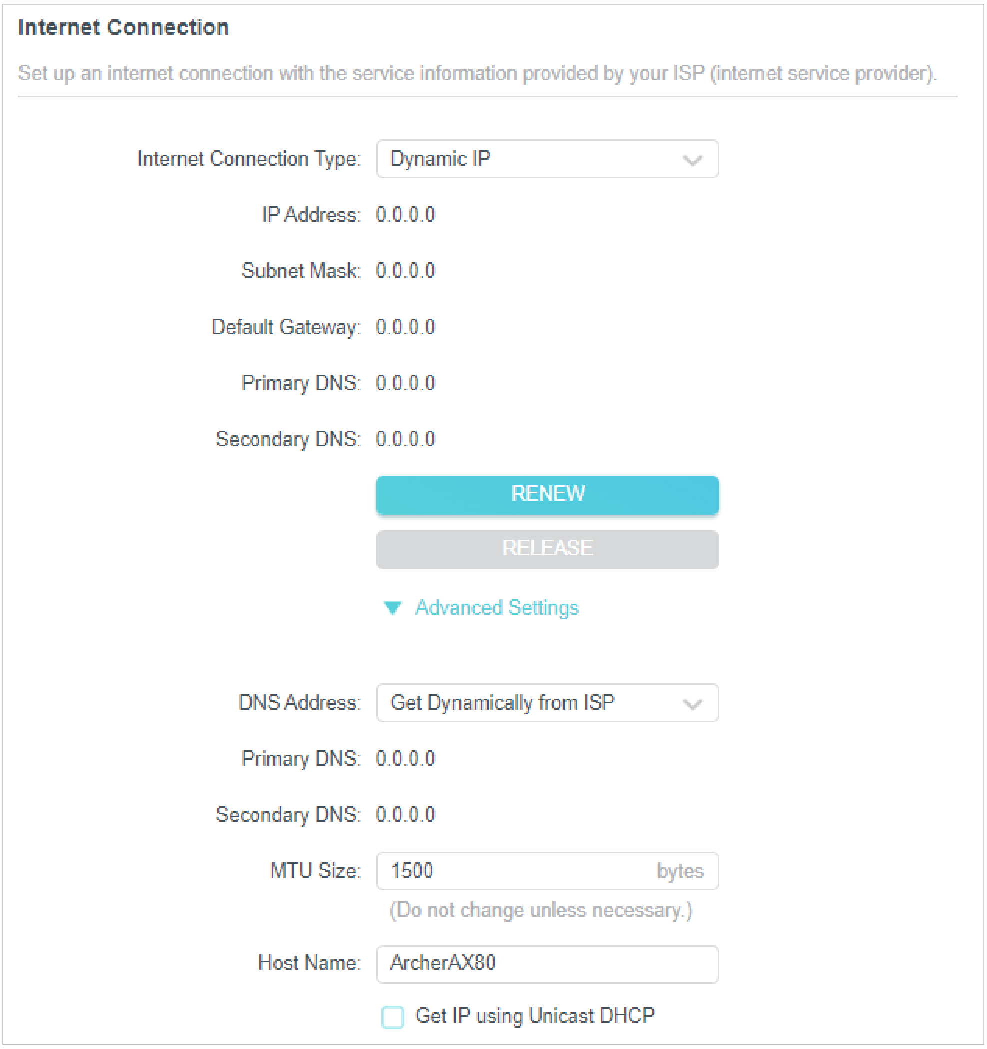
It contains the following sections:

15. 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 connection settings:**



Internet Connection

Set up an internet connection with the service information provided by your ISP (internet service provider).

Internet Connection Type: Dynamic IP

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0

DNS Address: Get Dynamically from ISP

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0

MTU Size: 1500 bytes

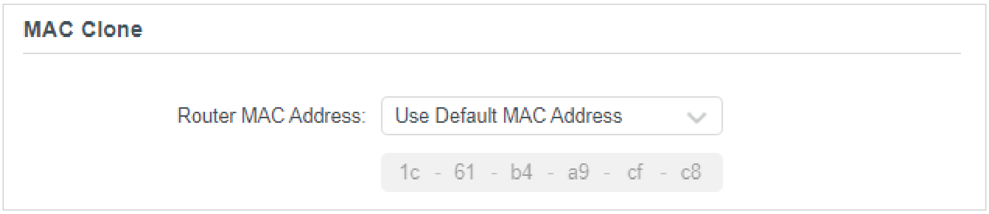
(Do not change unless necessary.)

Host Name: ArcherAX80

□ Get IP using Unicast DHCP

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:**



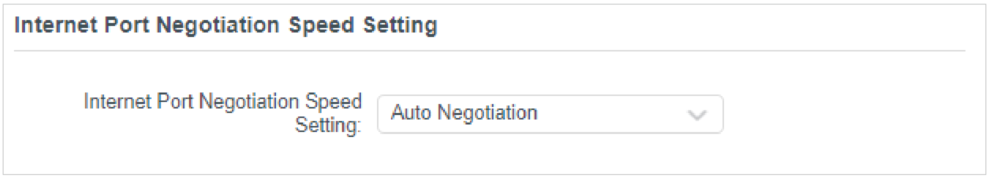
MAC Clone

Router MAC Address: Use Default MAC Address

1c - 61 - b4 - a9 - cf - c8

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

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



Internet Port Negotiation Speed Setting

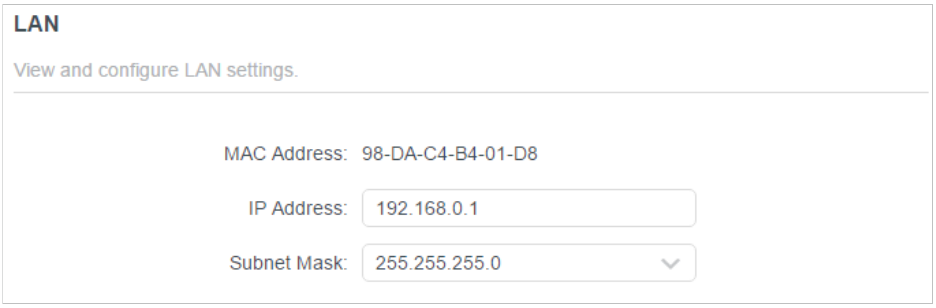
Internet Port Negotiation Speed Setting: Auto Negotiation

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

15. 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.



LAN

View and configure LAN settings.

MAC Address: 98-DA-C4-B4-01-D8

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

4. Click SAVE.

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

15. 3. Configure to Support IPTV Service

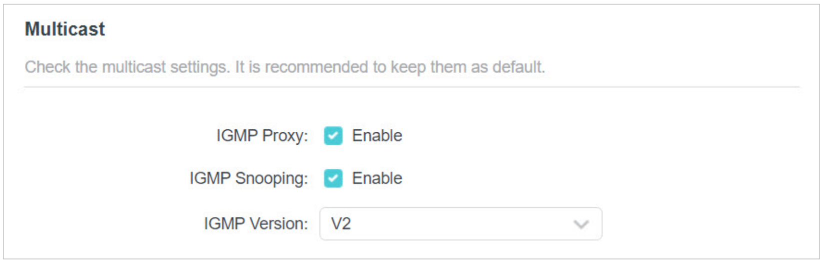
I want to:

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

How can I do that?

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

   1) Tick the IGMP Proxy and IGMP Snooping checkbox, then select the IGMP Version, either V2 or V3, as required by your ISP.

   Multicast

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

   IGMP Proxy: ☑ Enable

   IGMP Snooping: ☑ Enable

   IGMP Version: V2

   2) Click SAVE.

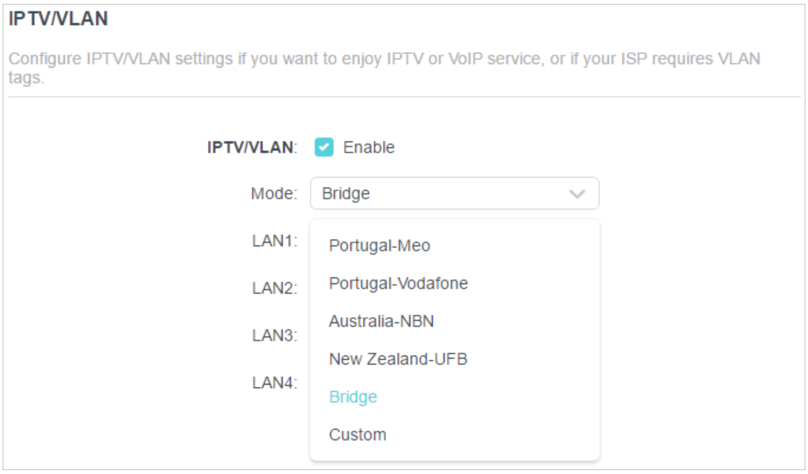
   3) After configuring IGMP proxy, IPTV can work behind your router now. You can connect your set-top box to any of the router's Ethernet port.

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

   1) Tick Enable IPTV/VLAN.

   2) Select the appropriate Mode according to your ISP.

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



IPTV/VLAN

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

IPTV/VLAN: ☑ Enable

Mode: Bridge

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!

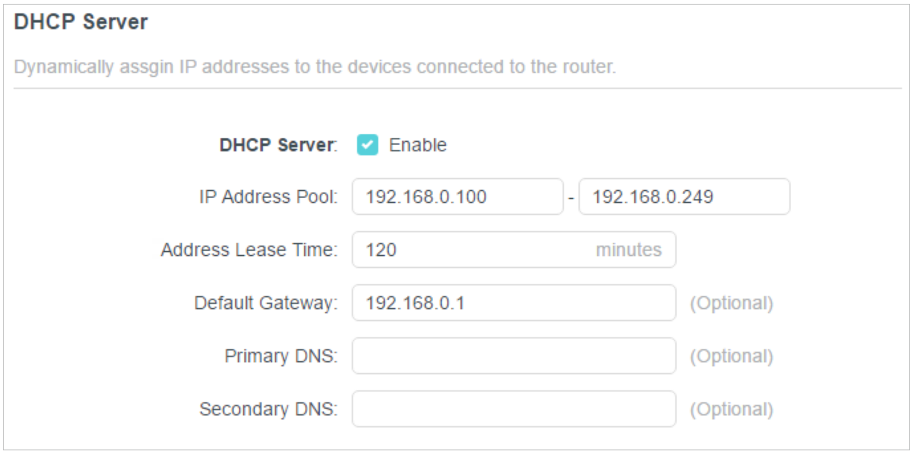
Your IPTV setup is done now! You may need to configure your set-top box before enjoying your TV.

15. 4. Specify DHCP Server Settings

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

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

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



DHCP Server

Dynamically assgin IP addresses to the devices connected to the router.

DHCP Server: ☑ Enable

IP Address Pool: 192.168.0.100 - 192.168.0.249

Address Lease Time: 120 minutes

Default Gateway: 192.168.0.1 (Optional)

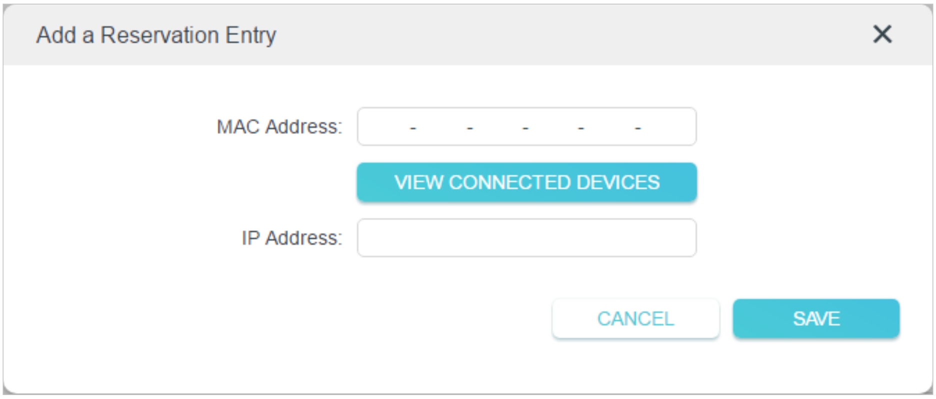
Primary DNS: (Optional)

Secondary DNS: (Optional)

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

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

1. Click Add in the Address Reservation section.



Add a Reservation Entry ✕

MAC Address: - - - - -

IP Address:

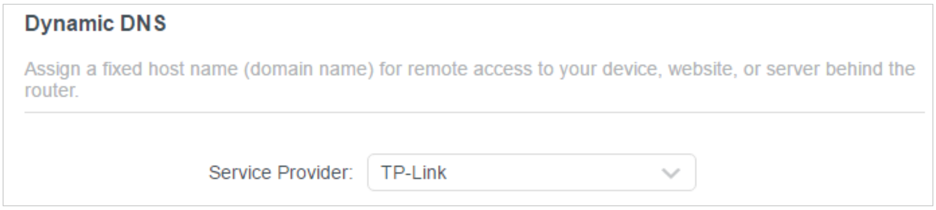
2. Click VIEW CONNECTED DEVICES and select the you device you want to reserve an IP for. Then the MAC Address will be automatically filled in. Or enter the MAC address of the client device manually.
3. Enter the IP address to reserve for the client device.
4. Click SAVE.

15. 5. Set Up a Dynamic DNS Service Account

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

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

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



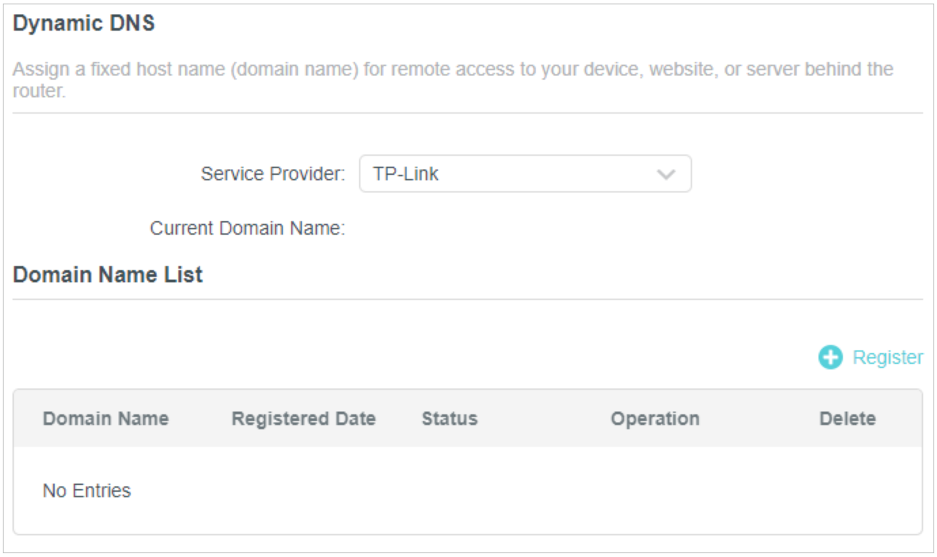
Dynamic DNS

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

Service Provider: TP-Link

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

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



Dynamic DNS

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

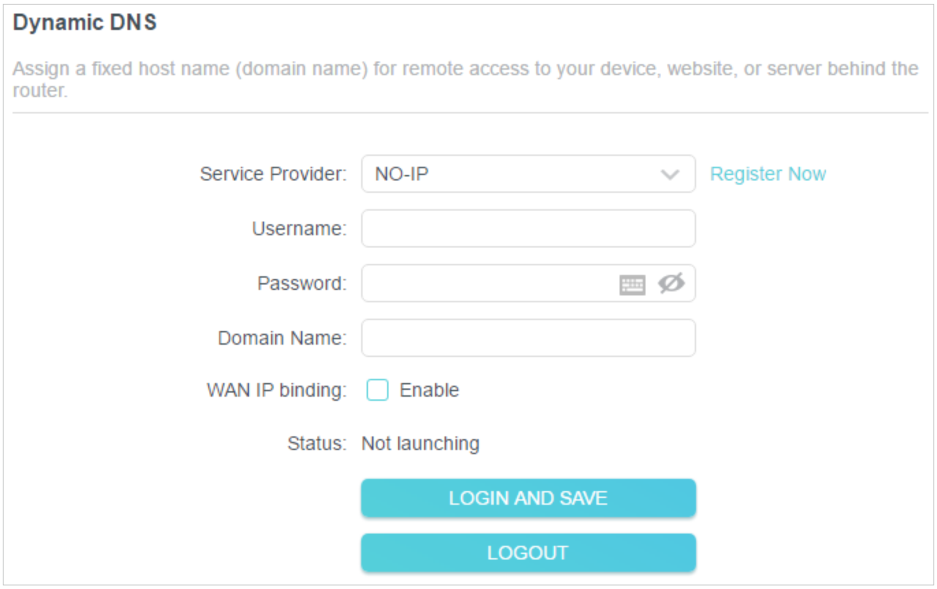
Service Provider: TP-Link

Current Domain Name:

Domain Name List

Domain Name	Registered Date	Status	Operation	Delete
No Entries				

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



Dynamic DNS

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

Service Provider: NO-IP

Username:

Password:

Domain Name:

WAN IP binding: □ Enable

Status: Not launching

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.

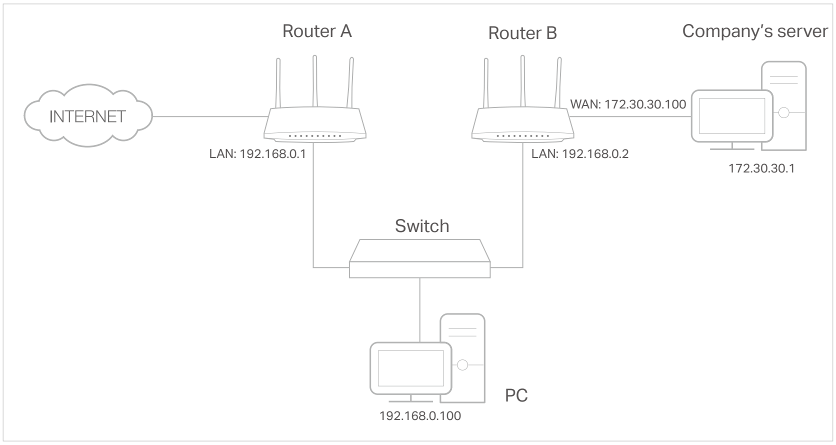
15. 6. Create Static Routes

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

I want to:

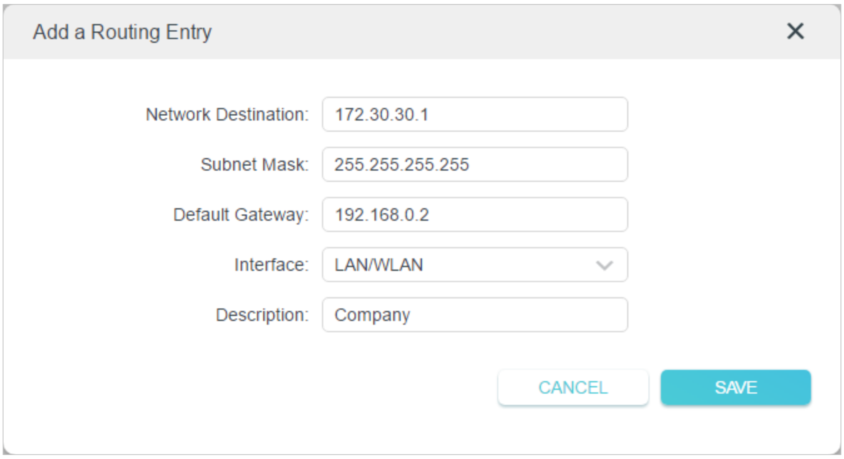
Visit multiple networks and servers at the same time.

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



How can I do that?

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



Add a Routing Entry

Network Destination: 172.30.30.1

Subnet Mask: 255.255.255.255

Default Gateway: 192.168.0.2

Interface: LAN/WLAN

Description: Company

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

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

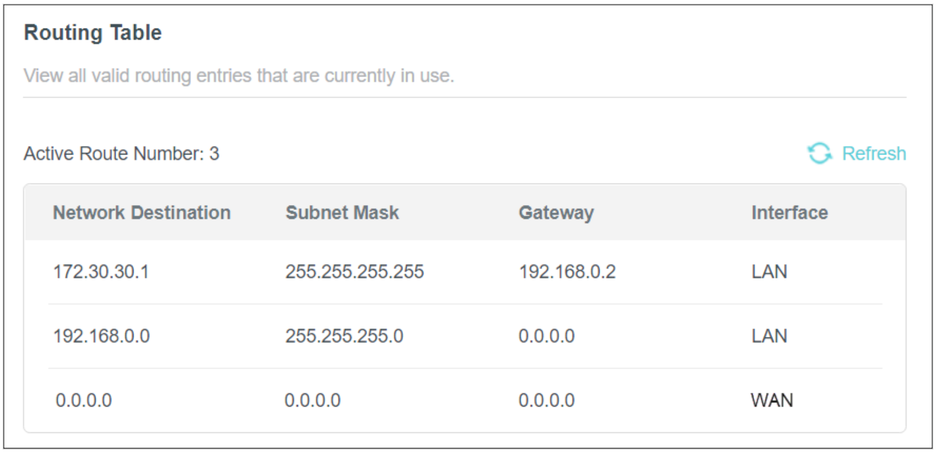
Default Gateway: The IP address of the gateway device to which the data packets will be sent. This IP address must be on the same subnet with the router's IP which sends out data. In the example, the data packets will be sent to the LAN port of Router B and then to the Server, so the default gateway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

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

Description: Enter a description for this static routing entry.

5. Click SAVE.

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



Routing Table

View all valid routing entries that are currently in use.

Active Route Number: 3

Network Destination	Subnet Mask	Gateway	Interface
172.30.30.1	255.255.255.255	192.168.0.2	LAN
192.168.0.0	255.255.255.0	0.0.0.0	LAN
0.0.0.0	0.0.0.0	0.0.0.0	WAN

Done!

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

Chapter 16

Manage the Router

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

It contains the following sections:

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

16. 1. Update the Firmware

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

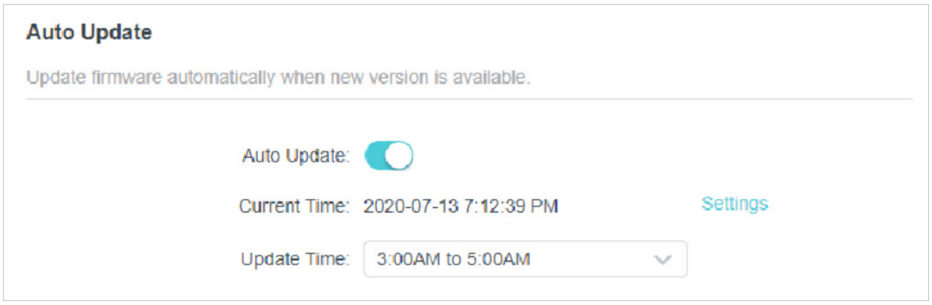
We will inform you through the web management page if there's any new firmware available for your router. Also, the latest firmware will be released at the TP-Link official website www.tp-link.com, and you can download it from the Support page for free.

Note:

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

16. 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.



Auto Update

Update firmware automatically when new version is available.

Auto Update: ●

Current Time: 2020-07-13 7:12:39 PM

Update Time: 3:00AM to 5:00AM

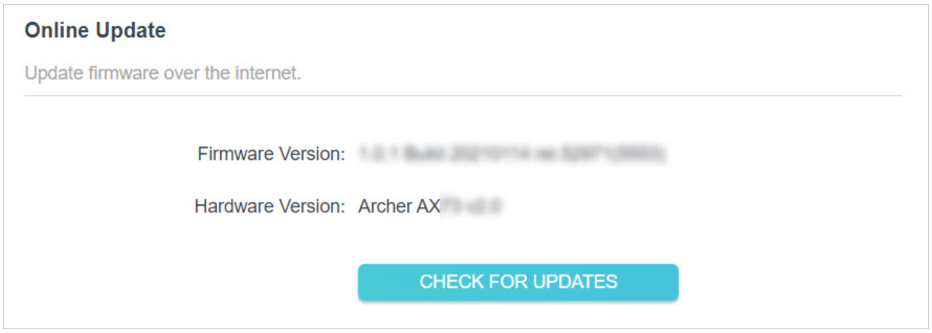
4. Specify the Update Time and save the settings.

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

16. 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.



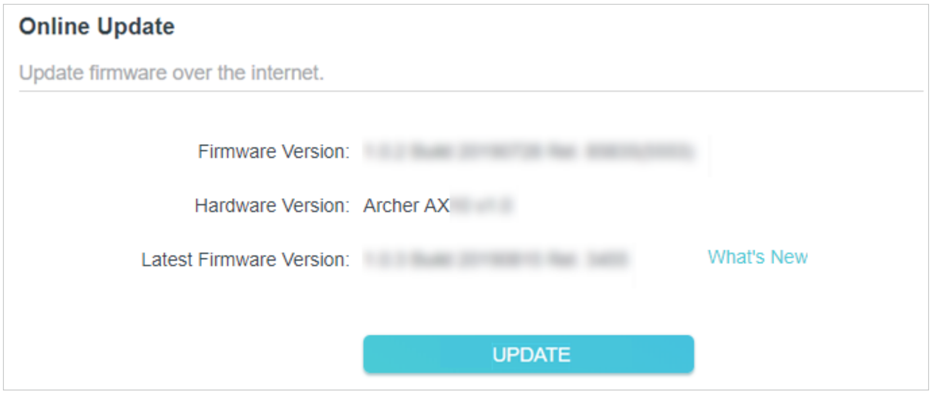
Online Update

Update firmware over the internet.

Firmware Version: [redacted]

Hardware Version: Archer AX[redacted]

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



Online Update

Update firmware over the internet.

Firmware Version: [redacted]

Hardware Version: Archer AX[redacted]

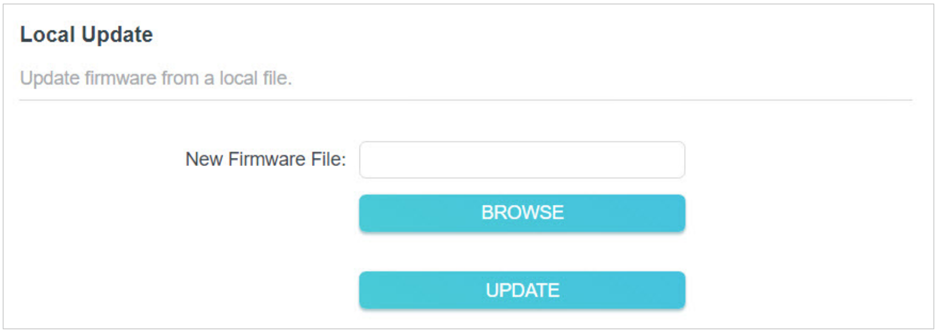
Latest Firmware Version: [redacted]

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.

16. 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.



Local Update

Update firmware from a local file.

New Firmware File: