8. 4. Manage the Router via the TP-Link Aginet App

The Aginet app runs on iOS and Android devices, such as smartphones and tablets.

1. Launch the Apple App Store or Google Play store and search "TP-Link Aginet" or simply scan the QR code to download and install the app.

2. Launch the Aginet app and log in with your TP-Link ID.

Note: If you don't have a TP-Link ID, create one first.

3. Connect your device to the router's wireless network.
4. Go back to the Aginet app, select the model of your router and log in with the password you set for the router.
5. Manage your router as needed.

Note: If you need to remotely access your router from your smart devices, you need to:

- Log in with your TP-Link ID. If you don't have one, refer to Register a TP-Link ID.
- Make sure your smartphone or tablet can access the internet with cellular data or a Wi-Fi network.

Chapter 9

USB Settings

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

The router supports USB external flash drives and hard drives.

It contains the following sections:

9. 1. Access the USB Storage Device

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

Tips:

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

9. 1. 1. Access the USB Device Locally

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

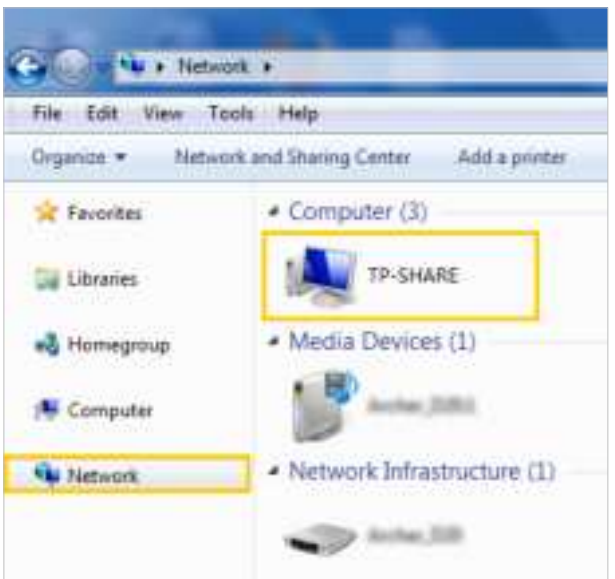
Windows computer

- **Method 1:**

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

Note:

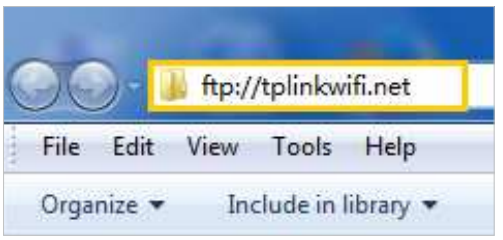
Operations in different systems are similar. Here we take Windows 7 as an example.



<table>
<tr><td>Windows computer</td><td>

- **Method 2:**

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



</td></tr>
<tr><td>Mac</td><td>

1) Select Go > Connect to Server.

2) Type the server address smb://tplinkwifi.net.

3) Click Connect.

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

</td></tr>
<tr><td>Tablet</td><td>Use a third-party app for network files management.</td></tr>
</table>

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

9. 1. 2. Access the USB Device Remotely

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

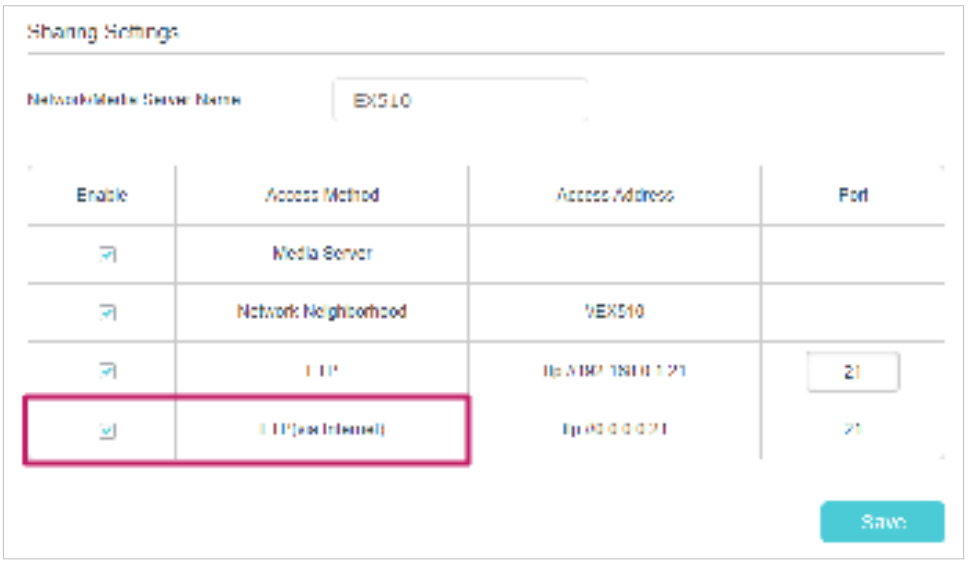
- Share photos and other large files with your friends without logging in to (and paying for) a photo-sharing site or email system.
- Get a safe backup for the materials for a presentation.
- Remove the files on your camera's memory card from time to time during the journey.

Note:

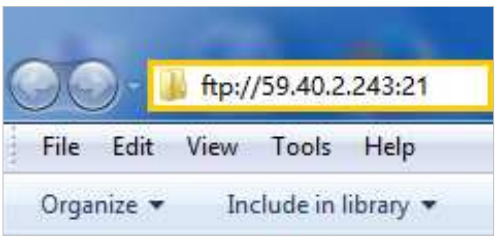
If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), you cannot use this feature because private addresses are not routed on the internet.

Follow the steps below to configure remote access settings.

1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > USB Sharing > Sharing Access > Sharing Settings.
3. Tick the FTP checkbox, and then click Save.



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

Computer	1) Open the Windows Explorer (or go to Computer, only for Windows users) or open a web browser. 2) Type the server address in the address bar: Type in ftp://<WAN IP address of the router>:<port number> (such as ftp://59.40.2.243:21). If you have specified the domain name of the router, you can also type in ftp://<domain name>:<port number> (such as ftp://MyDomainName:21)  3) Press Enter on the keyboard. 4) Access with the username and password you set in To Set Up Authentication for Data Security. Tips: You can also access the USB disk via a third-party app for network files management, which can resume broken file transfers.
Tablet	Use a third-party app for network files management.

Tips:

Click Set Up a Dynamic DNS Service Account to learn how to set up a domain name for you router.

9. 1. 3. Customize the Access Settings

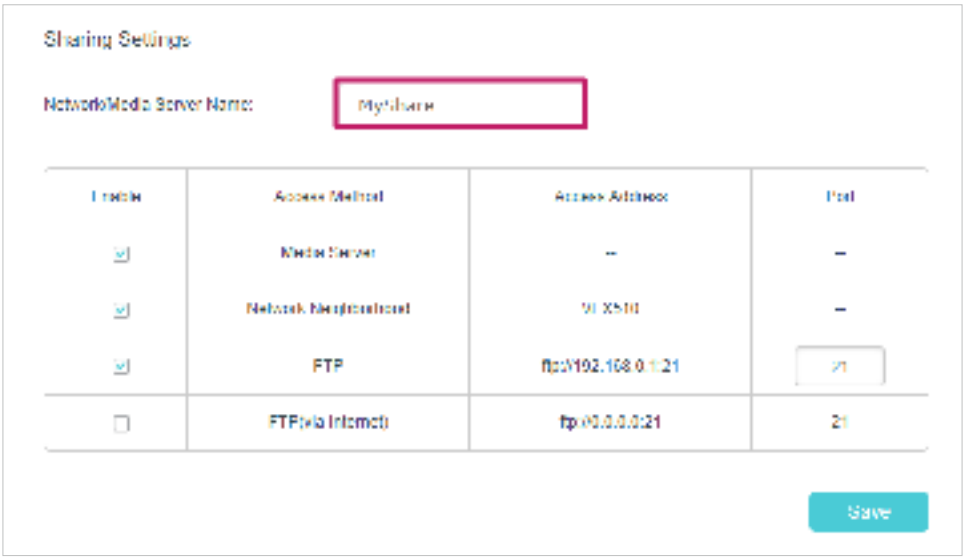
By default, all the network clients can access all folders on your USB disk. You can customize your sharing settings by setting a sharing account, sharing specific contents and setting a new sharing address on the router's web management page.

1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > USB Sharing > Sharing Access > Sharing Settings.

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

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

1. In the Sharing Settings session, make sure Media Server is ticked, and enter a Network/Media Server Name as you like, such as MyShare, then click Save.

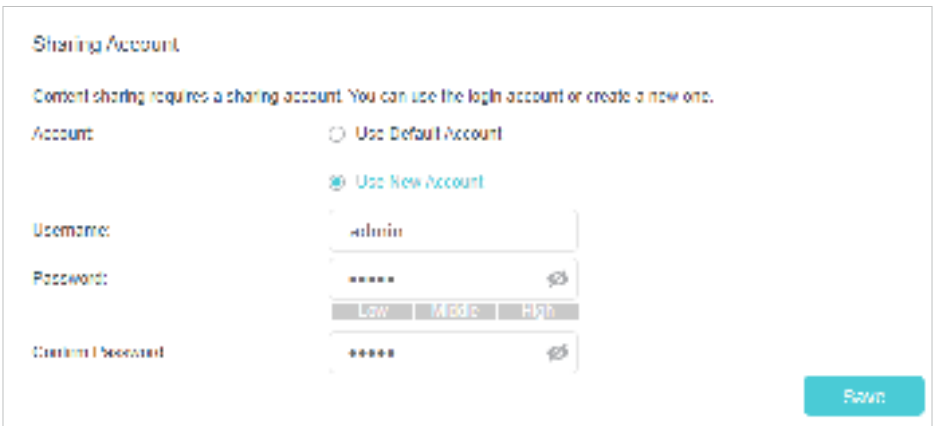


2. Now you can access the USB storage device by visiting \\MyShare (for Windows) or smb://MyShare (for Mac).

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

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

1. In the Sharing Account section, enable Use New Account.



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

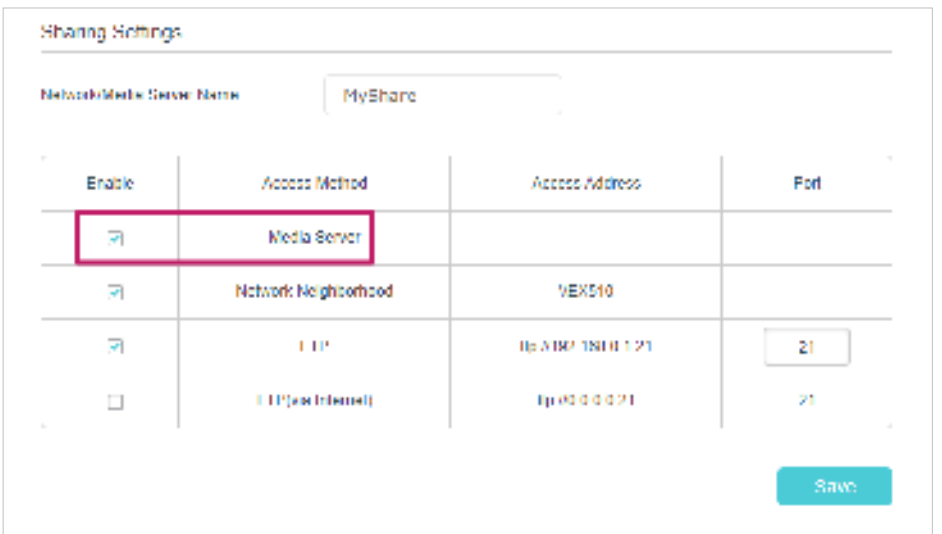
Note:

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

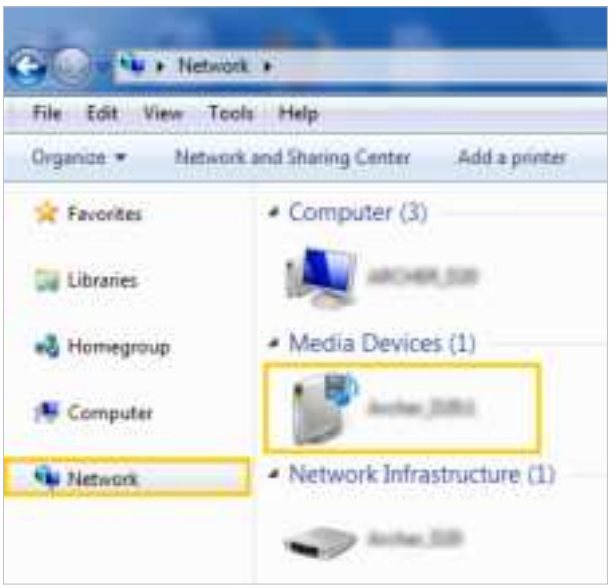
9. 2. Media Sharing

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

1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > USB Sharing > Sharing Access > Sharing Settings.
3. Enable Media Server.



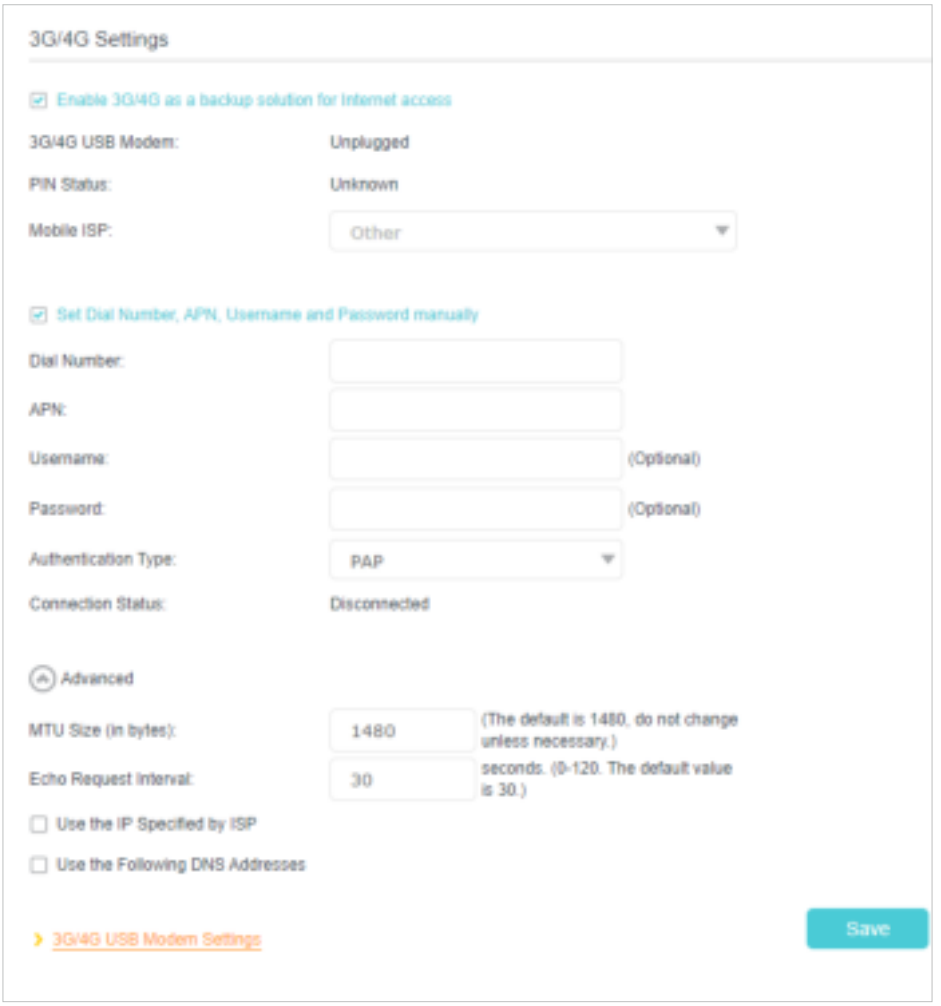
4. When your USB storage device is inserted into the router, your DLNA-supported devices (such as your computer and pad) connected to the router can detect and play the media files on the USB storage devices.
5. Refer to the following table for detailed instructions.

Windows Computer	• Go to Computer > Network, then click the Media Server Name (Model number-share by default) in the Media Devices section. **Note:** Here we take Windows 7 as an example. 
Tablet	• Use a third-party DLNA-supported player.

9. 3. 3G/4G Settings

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

1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > USB Sharing > 3G/4G Settings.



3. Tick the checkbox to enable 3G/4G as a backup solution for Internet access.

4. Tick the checkbox to set the Dial Number, APN, Username and Password manually.

Note: The following Advanced settings will only display if you enable 3G/4G as the backup solution for Internet access.

5. Click Save.

Chapter 10

EasyMesh with Seamless Roaming

This chapter introduces the TP-Link EasyMesh feature.

It contains the following sections:

TP-Link EasyMesh Controller and TP-Link EasyMesh Agent work together to form one unified Wi-Fi network. Walk through your home and stay connected with the fastest possible speeds thanks to EasyMesh's seamless coverage.

Unified Wi-Fi Network

Controller and agents share the same wireless settings, including network name, password, access control settings and more.

Seamless Roaming

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

Easy Setup and Management

Set up a EasyMesh network with a push of WPS buttons. Manage all network devices on the Aginet app or at your router's web management page.

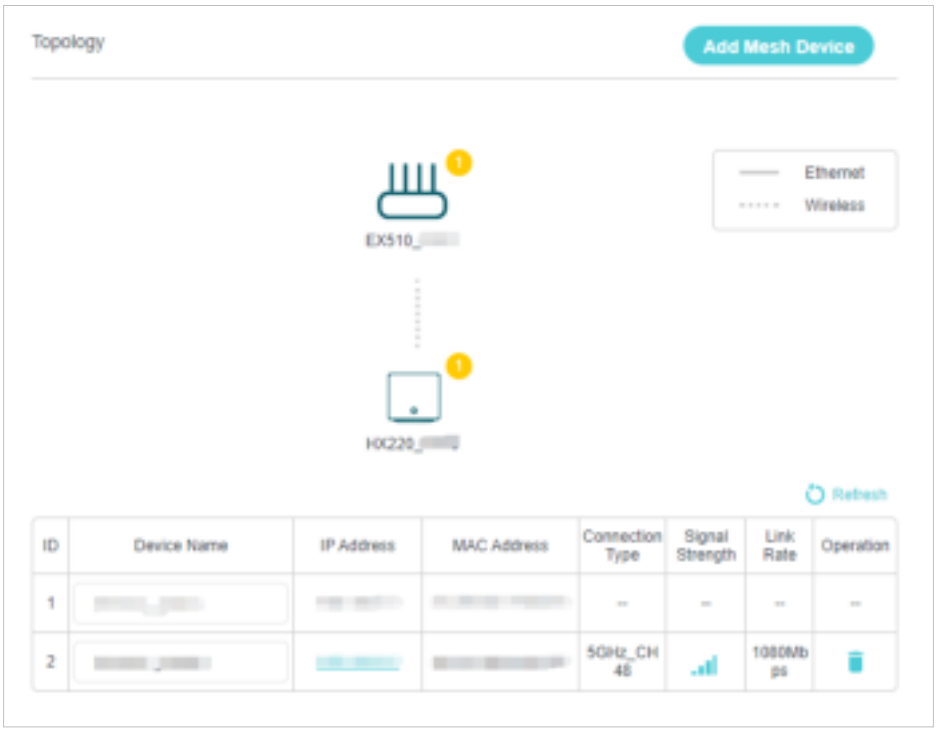
10. 1. Set Up a EasyMesh Network

1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with your TP-Link ID or the password you set for the router.
1. Go to Basic > Mesh or Advanced > Wireless > Mesh, and enable EasyMesh.

2. Connect a EasyMesh agent to this controller by following the setup instructions in the agent's manual. The agent will be listed on the controller's Mesh page.

   Note: To check full list of TP-Link EasyMesh devices, visit https://www.tp-link.com.

3. If you have set up the agent to join the EasyMesh network, it will be listed on the controller's EasyMesh page.



   Otherwise, you need to find it in the Add Mesh Device list and click Add to add it to the EasyMesh network.

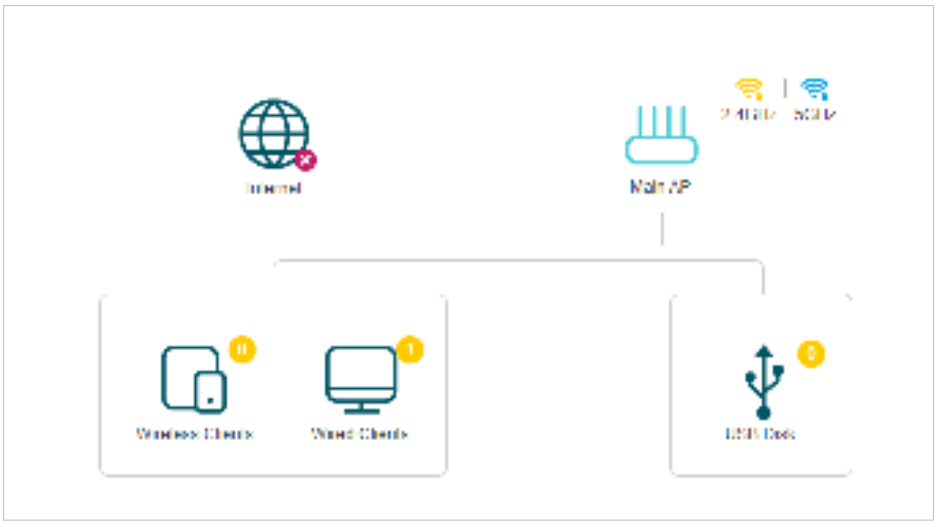
Done! Now your controller and agents successfully form a EasyMesh network!

10. 2. Manage Devices in the EasyMesh Network

In a EasyMesh network, you can manage all mesh devices and connected clients on your router's web page.

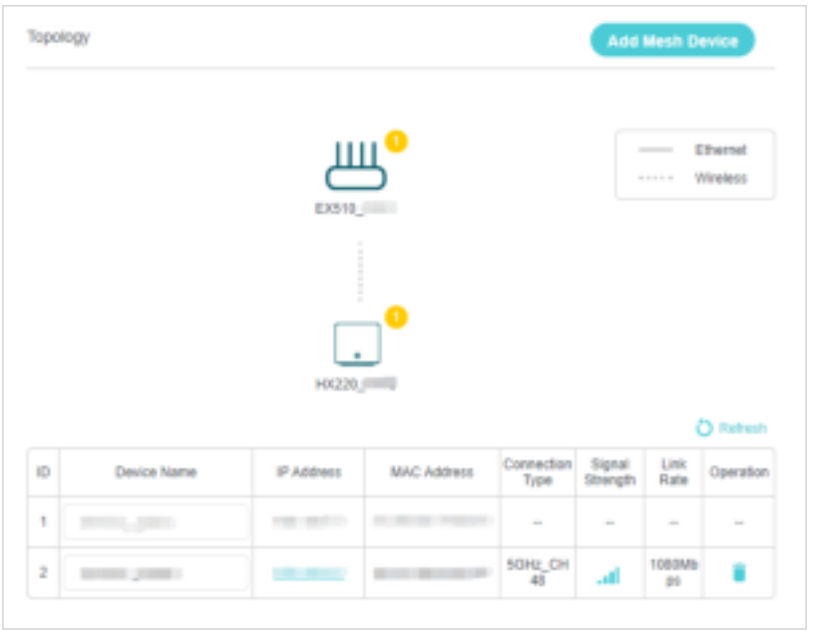
- **To view mesh devices and connected clients in the network:**

1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with your TP-Link ID or the password you set for the router.
2. Go to Basic > Network Map.
3. Click to view all mesh devices, and click to view all connected clients.



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

1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with your TP-Link ID or the password you set for the router.
2. Go to Basic > Network Map.



3. Click the Mesh device's IP Address to redirect to the web management page of this device and view detailed information.

4. Manage the EasyMesh device as needed. You can:
   - Change device information.
   - Delete this device from the EasyMesh network.

Chapter 11

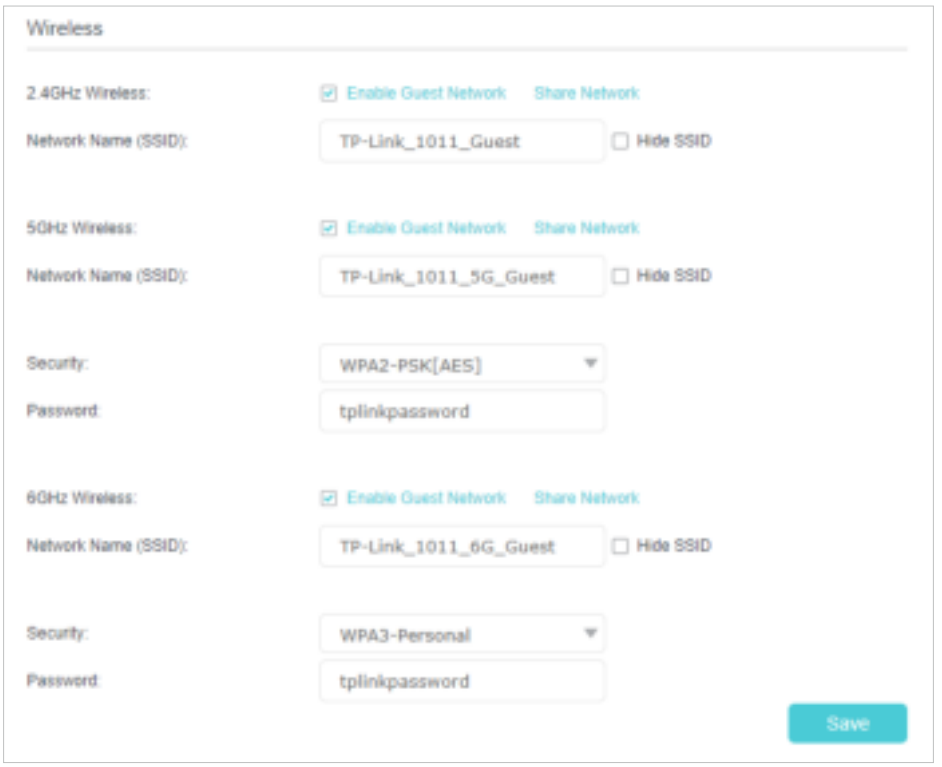
Guest Network

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

It contains the following sections:

11. 1. Create a Network for Guests

1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > Guest Network. Locate the Wireless section.
3. Create a guest network as needed.
   1) Tick the Enable checkbox for the 2.4GHz or 5GHz wireless network.
   2) Customize the SSID. Don't select Hide SSID unless you want your guests to manually input the SSID for guest network access.
   3) Select the Security type and customize your own password. If No security is selected, no password is needed to access your guest network.



4. Click Save. Now your guests can access your guest network using the SSID and password you set!

Tips:
To view guest network information, go to Network Map and locate the Guest Network section. You can turn on or off the guest network function conveniently.

11. 2. Customize Guest Network Options

1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with your TP-Link ID or the password you set for the router.

2. Go to Advanced > Guest Network. Locate the Settings section.

3. Customize guest network options according to your needs.

- Allow guests to see each other

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

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

Chapter 12

NAT Forwarding

The router's NAT (Network Address Translation) feature makes devices on the LAN use the same public IP address to communicate with devices on the internet, which protects the local network by hiding IP addresses of the devices. However, it also brings about the problem that an external host cannot initiatively communicate with a specified device on the local network.

With the forwarding feature the router can penetrate the isolation of NAT and allows devices on the internet to initiatively communicate with devices on the local network, thus realizing some special functions.

The TP-Link router supports four forwarding rules. If two or more rules are set, the priority of implementation from high to low is Port Forwarding, Port Triggering, UPNP and DMZ.

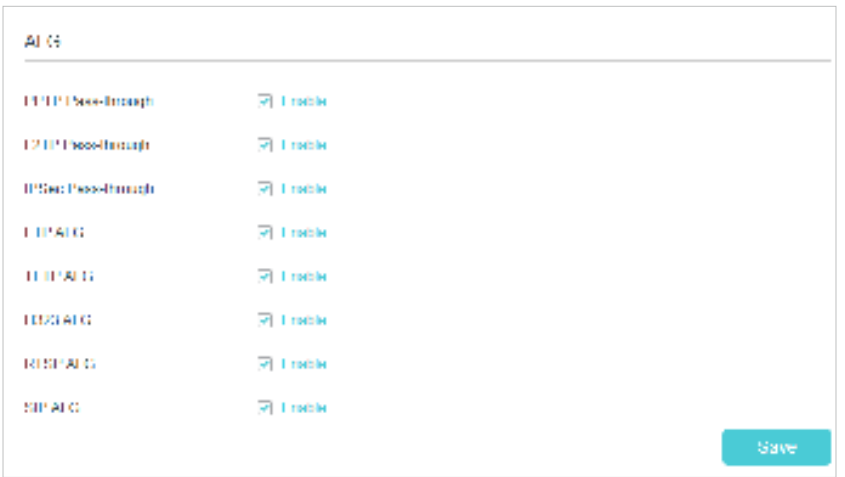
It contains the following sections:

12. 1. ALG

ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc. It is recommended to keep the default settings.

You may need to disable SIP ALG when you are using voice and video applications to create and accept a call through the router, since some voice and video communication applications do not work well with SIP ALG.

Visit http://tplinkwifi.net or http://192.168.0.1, and log in with your TP-Link ID or the password you set for the router. Go to Advanced > Security > ALG.



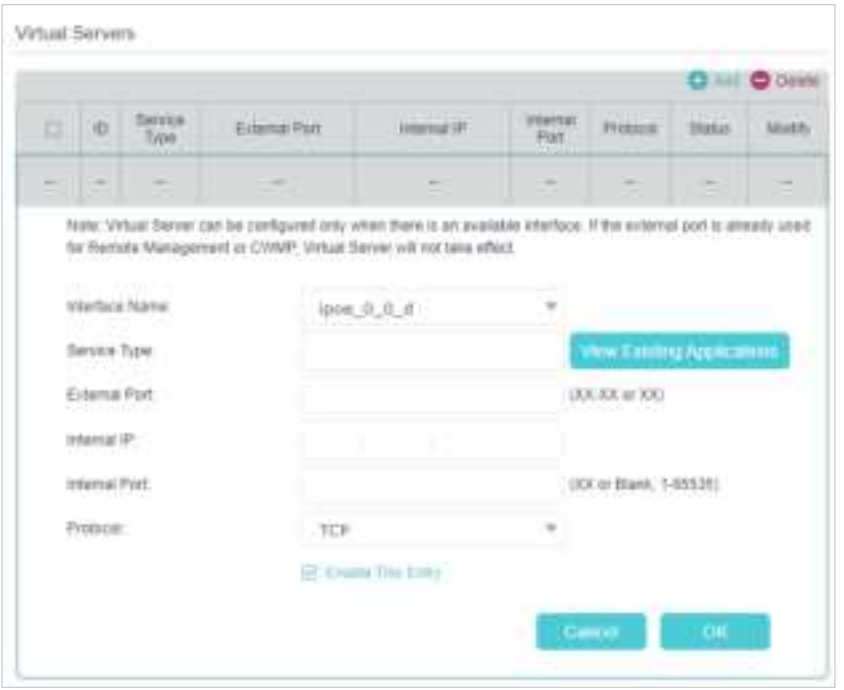
12. 2. Set Up Public Services on The Local Network by Virtual Servers

Virtual Servers are used to set up public services on the local network. A virtual server is defined as an external port, and all requests from the Internet to this external port will be redirected to a designated computer, which must be configured with a static or reserved IP address. When you build up a server on the local network and want to share it on the Internet, Virtual Servers can realize the service and provide it to the Internet users.

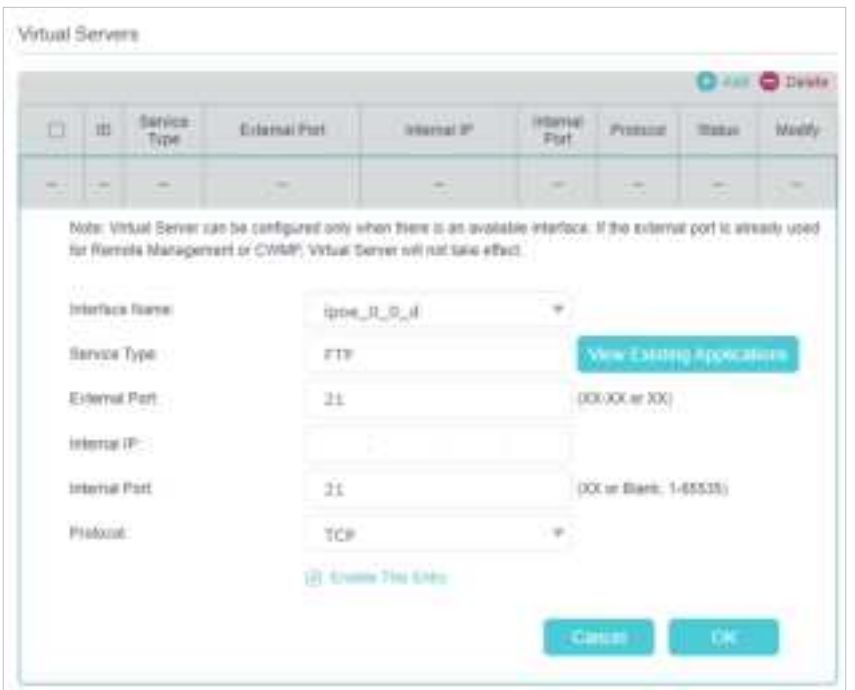
The table displays the relevant parameters of the virtual server.

To set up a Virtual Server rule:

1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > NAT Forwarding > Virtual Servers and click Add.
3. Select an interface name from the drop-down list.



4. Click View Existing Applications to select a service from the list to automatically populate the appropriate port number in the External Port and Internal Port fields. If the service is not listed, enter the External Port number (e.g. 21) or a range of ports (e.g. 21-25). Leave the Internal Port blank if it is the same as the External Port or enter a specific port number (e.g. 21) if the External Port is a single port. The following picture takes application FTP as an example.



5. Enter the IP address of the computer running the service application in the Internal IP field.
6. Select a protocol for the service application: TCP, UDP, or All from the Protocol drop-down list.
7. Select Enable This Entry.
8. Click OK.

Tips:

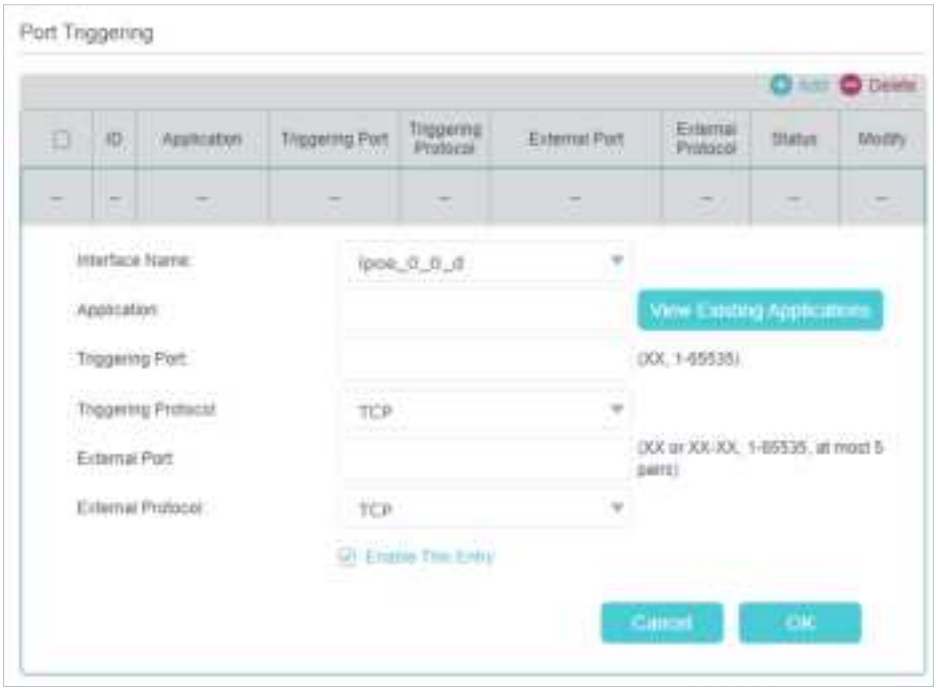
- If you want to disable this entry, click the Bulb icon.
- It is recommended to keep the default settings of Internal Port and Protocol if you are not clear about which port or protocol to use.
- If the local host device is hosting more than one type of available services, you need to create a rule for each service. Please note that the External Port should NOT be overlapped.

12. 3. Open Ports Dynamically by Port Triggering

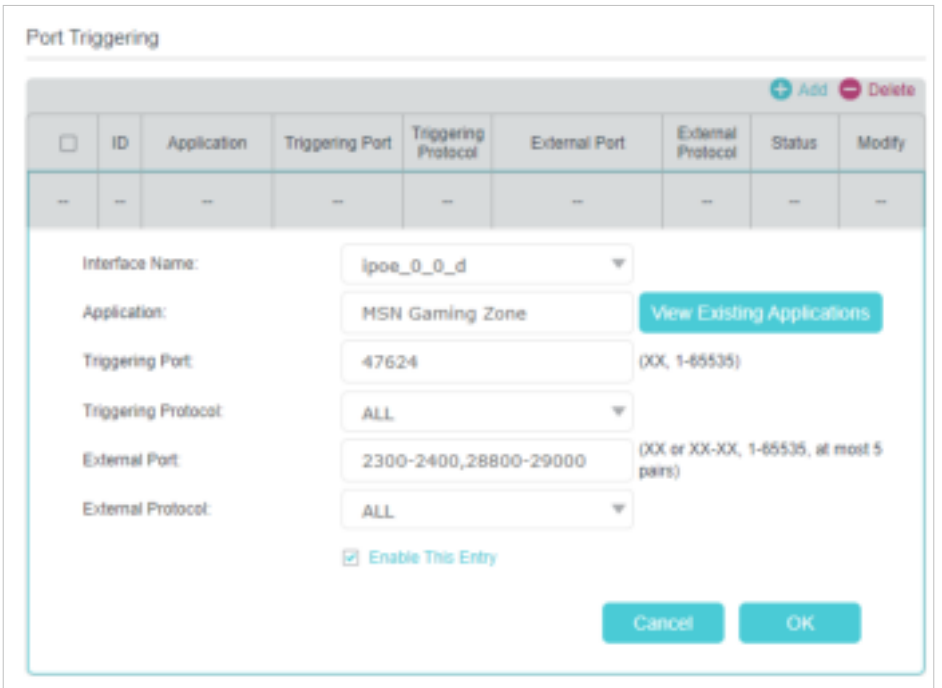
Port Triggering can specify a triggering port and its corresponding external ports. When a host on the local network initiates a connection to the triggering port, all the external ports will be opened for subsequent connections. The router can record the IP address of the host. When the data from the 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 or http://192.168.0.1, 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 Existing Applications, 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 OK.

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.

12. 4. 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.
1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > NAT Forwarding > DMZ and tick to enable DMZ.
2. Enter the PC's IP address 192.168.0.100 manually in the DMZ Host IP Address field.

3. 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.

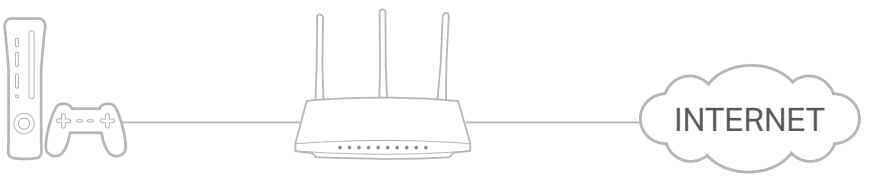
12. 5. Make Xbox Online Games Run Smoothly by UPnP

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).

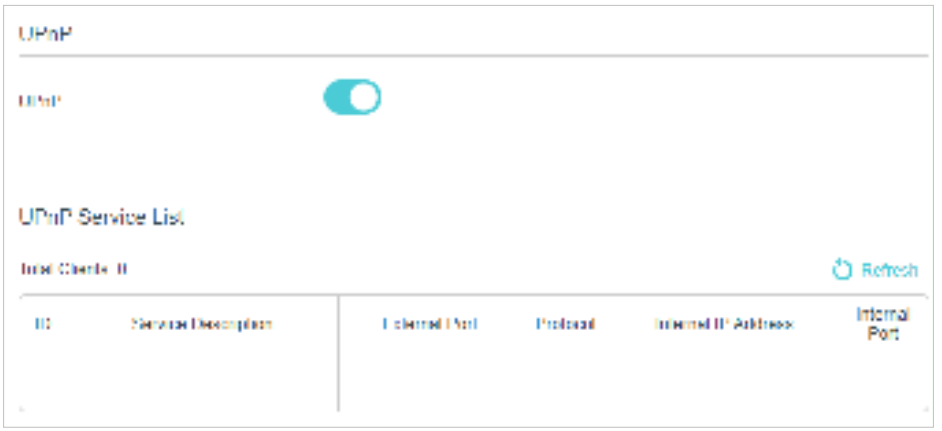
For example, when you connect your Xbox to the router which has connected to the internet to play online games, UPnP will send request to the router to open the corresponding ports allowing the following data penetrating the NAT to transmit. Therefore, you can play Xbox online games without a hitch.



If necessary, you can follow the steps to change the status of UPnP.

1. Visit http://tplinkwifi.net or http://192.168.0.1, 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 13

Parental Controls

This function allows you to block inappropriate, explicit and malicious websites, and control access to specified websites at specified time.

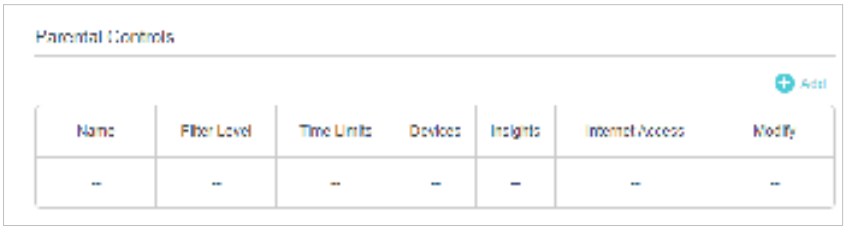
I want to:

Control what types of websites my children or other home network users can visit and the time of day they are allowed to access the internet.

For example, I want to allow my children's devices (e.g. a computer or a tablet) to access only www.tp-link.com and Wikipedia.org from 18:00 (6 PM) to 22:00 (10 PM) on the weekdays and not other time.

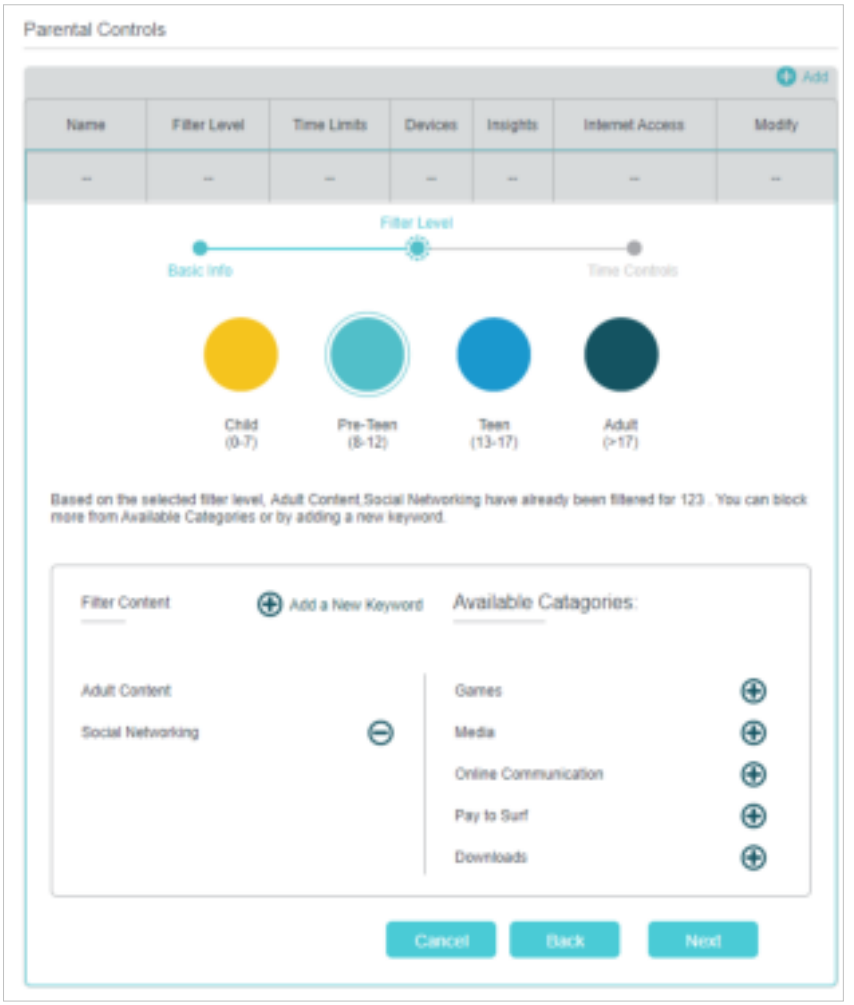
How can I do that?

1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with the password you set for the router.
2. Go to Basic > Parental Controls or Advanced > Parental Controls.



3. Click Add, and then enter the Name manually. Click Add and specify the devices belonging to the family member. Click Next.

4. Select a filter level based on the age of the family member. Blocked content will then be displayed in the Filter Content list. Click Next.



5. (Optional) Delete items from the Filter Content list, add items from the Available Categories list, or click Add a New Keyword to add a filter keyword (for example, "Facebook") or URL.

6. Enable Time Limits for Mon to Fri and Sat & Sun, then set the daily internet time allowed. Enable BedTime on School Nights (Sunday to Thursday) and Weekend (Friday and Saturday), then set the time period during devices in the profile cannot access the internet.

7. Click Save.

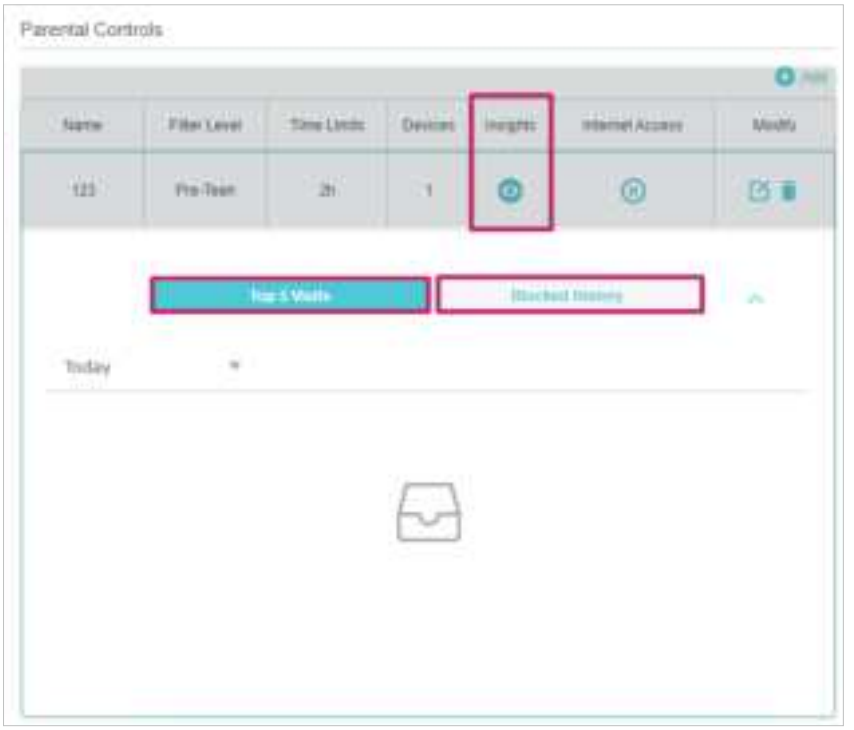
Done!

Now you can control your children's internet access as needed.

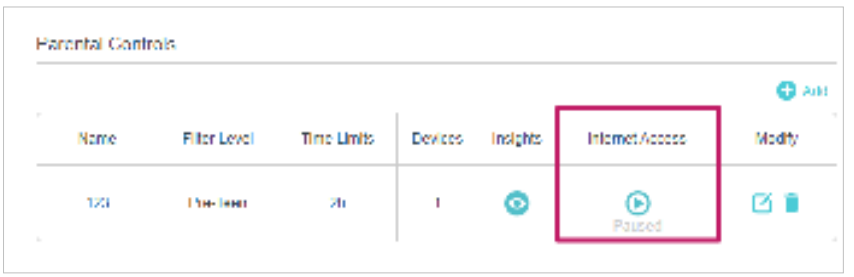
Tips:

- To monitor internet usage of a family member:

1. Find the profile of the family member, then click the **Insights** icon.
2. On the **Top 5 Visits** page, select a day of the last 7 days to check the time spent online and top visited websites. You can block the websites if needed.
3. On the **Blocked History** page, select a day of the last 7 days to check the blocked website history. You can **unblock websites** if needed, and click Unblocked Websites to view them.



- To pause or resume internet access of a family member:
  Find the profile of the family member, then click the **Pause/Play** icon.



Chapter 14

Quality of Service

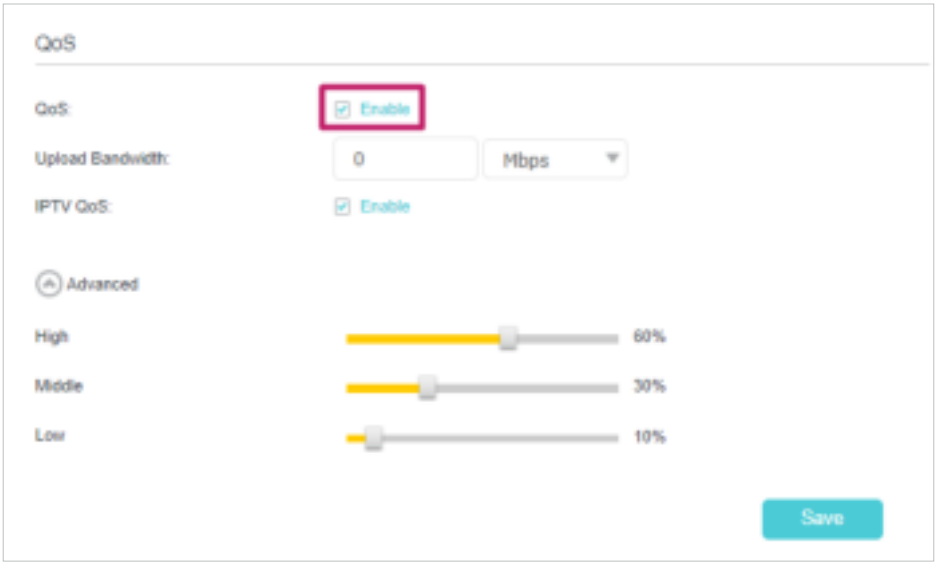
This function allows you to specify the priority of traffic and minimizes the impact of network congestion.

The router allows you to configure the quality of service (QoS) for optimal throughput and performance when handling differentiated wireless traffic, such as Voiceover-IP (VoIP), other types of audio, video, streaming media, and traditional IP data.

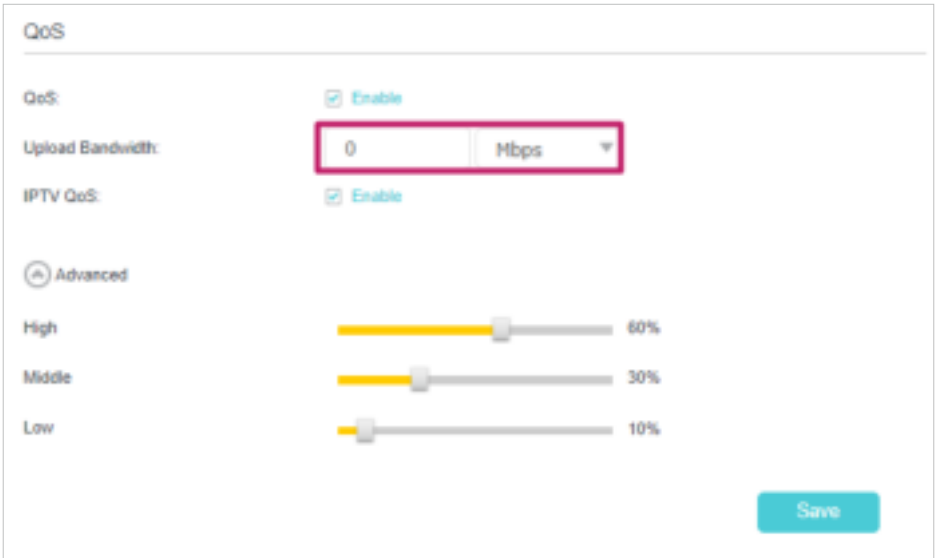
To configure QoS on the routers, you should set parameters on the transmission queues for different types of wireless traffic. In normal use, we recommend that you keep the default values for the routers.

To set up QoS for the network:

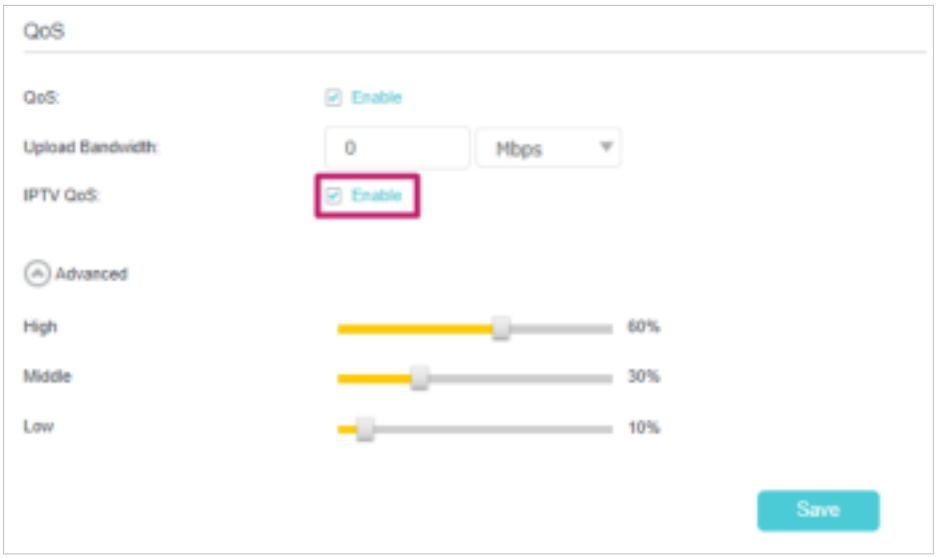
1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with the password you set for the router.
2. Go to Advanced > QoS.
3. Enable QoS.



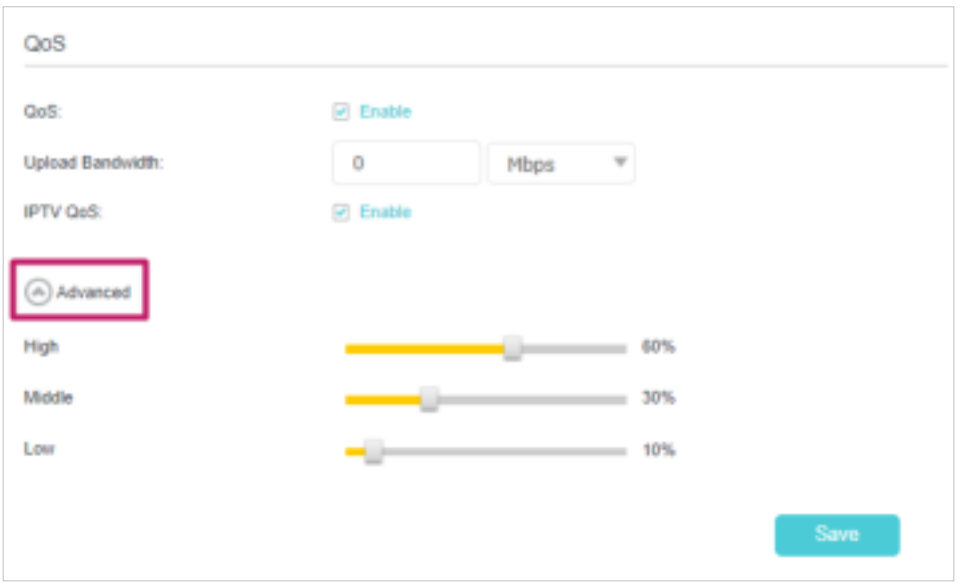
4. Enter the upload and download bandwidths provided by your ISP.



5. (Optional) Enable IPTV QoS, then set the priority and reserved bandwidth of IPTV traffic.



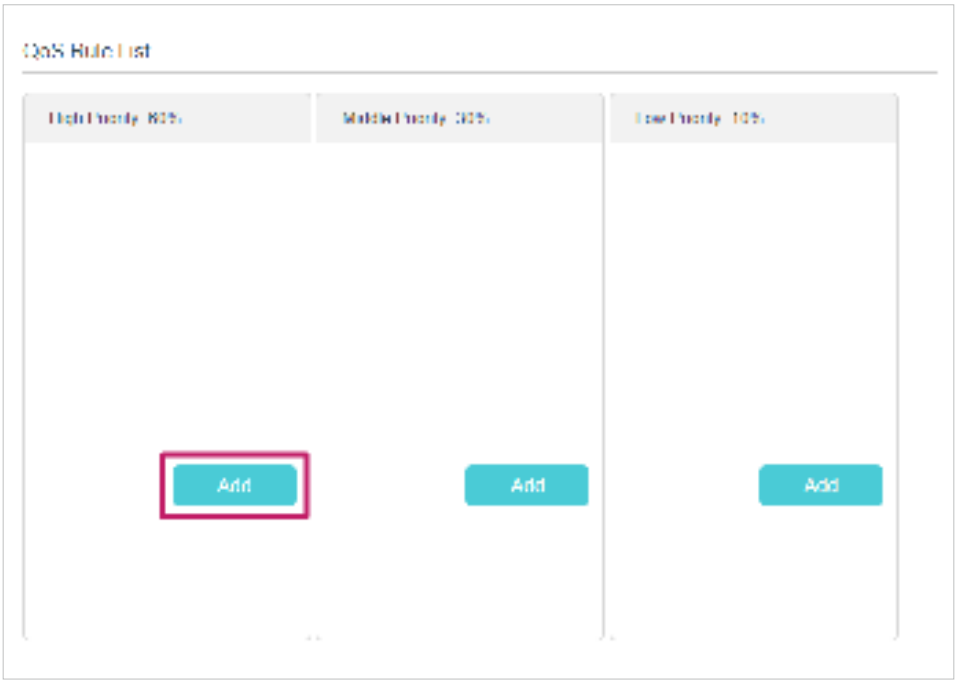
6. (Optional) Click Advanced and arrange the sliders to set the bandwidth percentage of each priority.



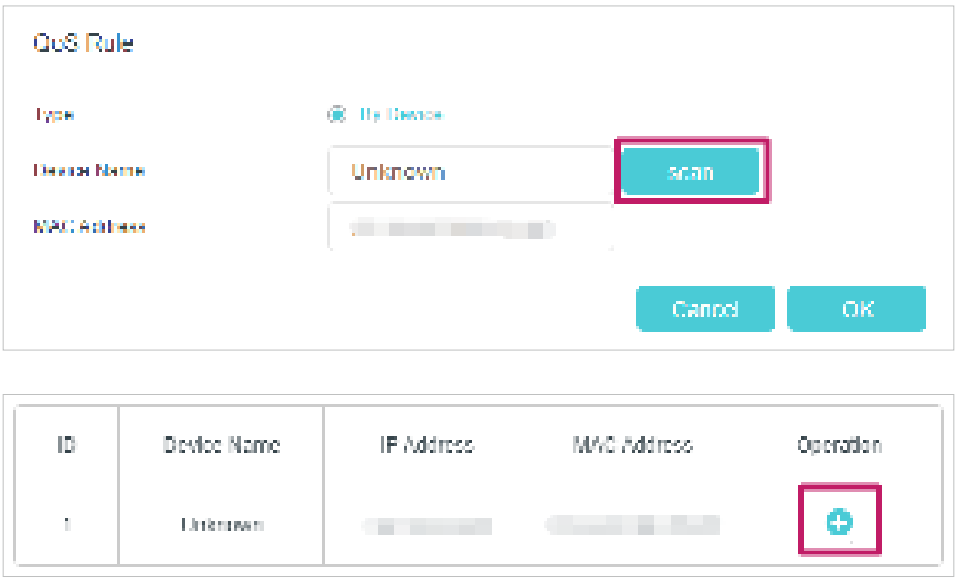
7. Click Save to make the settings effective.

To set up QoS for a specific device:

1. Visit http://tplinkwifi.net or http://192.168.88.1, and log in with the password you set for the router.
2. Go to Advanced > QoS.
3. In the QoS Rule List table, choose a priority section and click Add.



4. In the QoS Rule window, click scan and click to choose a device, then click OK to add it to the rule.



Chapter 15

Network Security

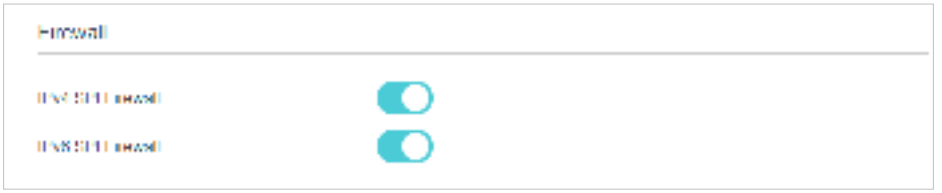
This chapter guides you on how to protect your home network from unauthorized users by implementing network security functions. You can block or allow specific client devices to access your wireless network using MAC Filtering, or using Access Control for wired and wireless networks, or you can prevent ARP spoofing and ARP attacks by using IP & MAC Binding.

This chapter contains the following sections:

15. 1. Firewall & DoS Protection

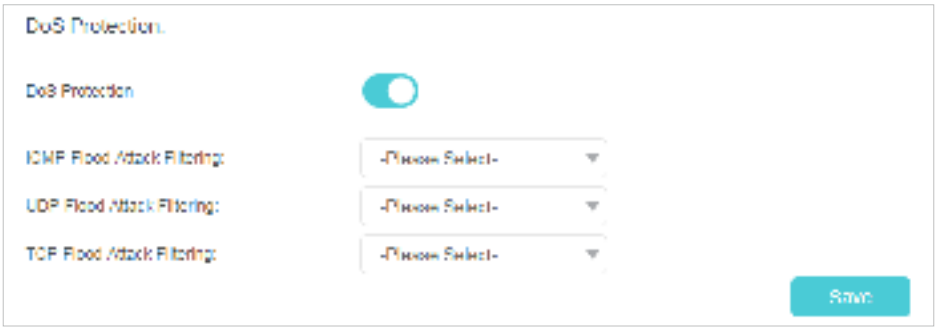
The SPI (Stateful Packet Inspection) Firewall and DoS (Denial of Service) Protection protect the router from cyber attacks.

The SPI Firewall can prevent cyber attacks and validate the traffic that is passing through the router based on the protocol. This function is enabled by default, and it is recommended to keep the default settings.



DoS Protection can protect your home network against DoS attacks from flooding your network with server requests. Follow the steps below to configure DoS Protection.

1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with the password you set for the router.
2. Go to Advanced > Security > Firewall & DoS Protection.



3. Enable DoS Protection.
4. Set the protection level (Low, Middle or High) for ICMP-Flood Attack Filtering, UDP-Flood Attack Filtering and TCP-Flood Attack Filtering.
   - ICMP-Flood Attack Filtering - Enable to prevent the ICMP (Internet Control Message Protocol) flood attack.
   - UDP-Flood Attack Filtering - Enable to prevent the UDP (User Datagram Protocol) flood attack.
   - TCP-Flood Attack Filtering - Enable to prevent the TCP (Transmission Control Protocol) flood attack.
5. Click Save.

Tips:

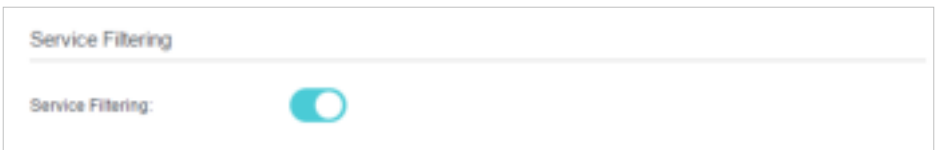
1. The level of protection is based on the number of traffic packets. You can specify the level under DoS Protection Level Settings.

2. The protection will be triggered immediately when the number of packets exceeds the preset threshold value, and the vicious host will be displayed in the Blocked DoS Host List.

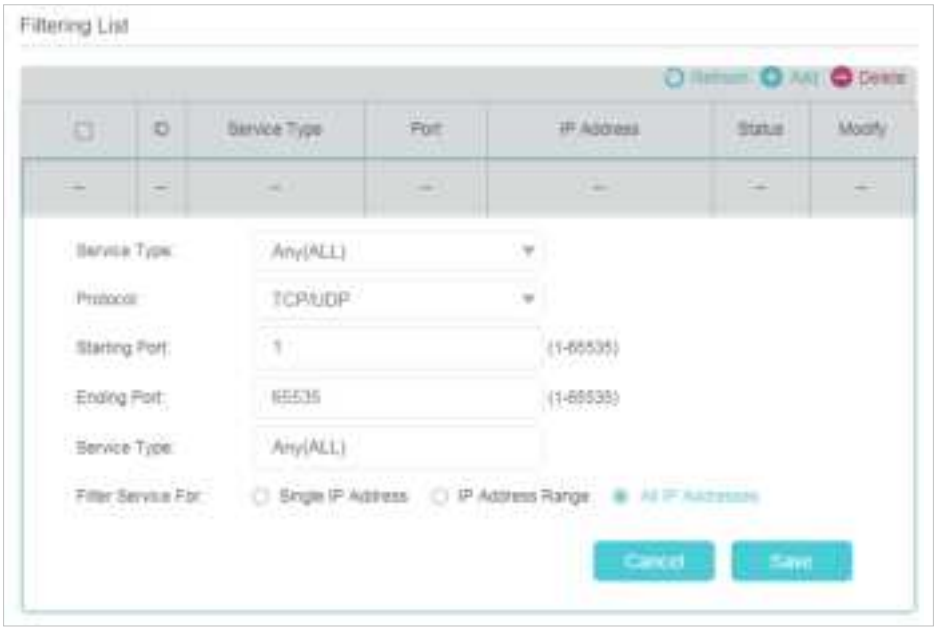
15. 2. Service Filtering

With Service Filtering, you can prevent certain users from accessing the specified service, and even block internet access completely.

1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with the password you set for the router.
2. Go to Advanced > Security > Service Filtering, and enable Service Filtering.



3. Click Add.



4. Select a Service Type from the drop-down list and the following four fields will be automatically filled in. Select Custom when your desired service type is not listed, and enter the information manually.
5. Specify the IP address(es) that this filtering rule will apply to.
6. Click Save to make the settings effective.

Note: If you want to disable an entry, click the icon.

15. 3. Access Control

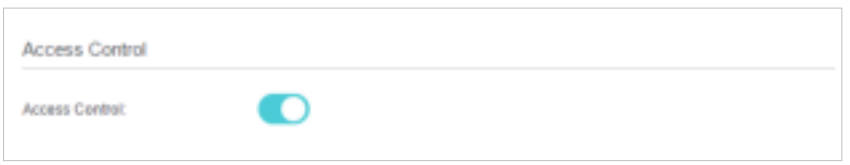
Access Control is used to block or allow specific client devices to access your network (via wired or wireless) based on a list of blocked devices (Blacklist) or a list of allowed devices (Whitelist).

I want to:

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

How can I do that?

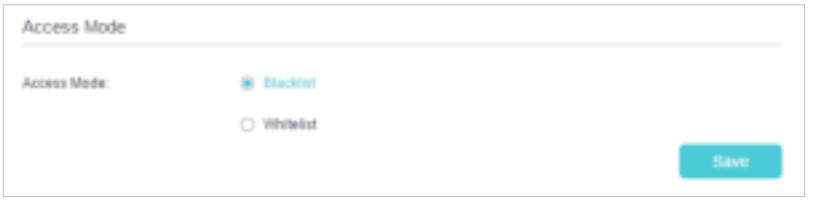
1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with the password you set for the router.
2. Go to Advanced > Security > Access Control and enable Access Control.



3. Select the access mode to either block (recommended) or allow the device(s) to access your network.

To block specific device(s):

1) Select Blacklist and click Save.

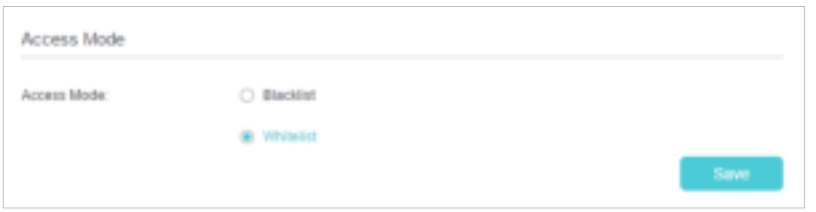


2) Select the device(s) to be blocked in the Online Devices table (or click the Add under the Devices in Blacklist and enter the Device Name and MAC Address manually).

3) Click Block above the Online Devices table. The selected devices will be added to Devices in Blacklist automatically.

To allow specific device(s):

1) Select Whitelist and click Save.



2) Click Add in the Devices in Whitelist section.

3) Enter the Device Name and MAC Address. (You can copy and paste the information from Online Devices table if the device is connected to your network.)

4) Click Save.

Done! Now you can block or allow specific client devices to access your network (via wired or wireless) by Blacklist or Whitelist.

15. 4. IP & MAC Binding

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

I want to: Prevent ARP spoofing and ARP attacks.

How can I do that?

1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with the password you set for the router.
2. Go to Advanced > Security > IP & MAC Binding, and enable IP & MAC Binding.

3. Bind your device(s) according to your needs.

   To bind the connected device(s):

   1) Select the device(s) to be bound in the ARP List.

   2) Click Bind to add to the Binding List.

   To bind the unconnected device:

   1) Click Add in the Binding List section.

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

   3) Select the Enable This Entry check box to enable the entry and click Save.

Done!

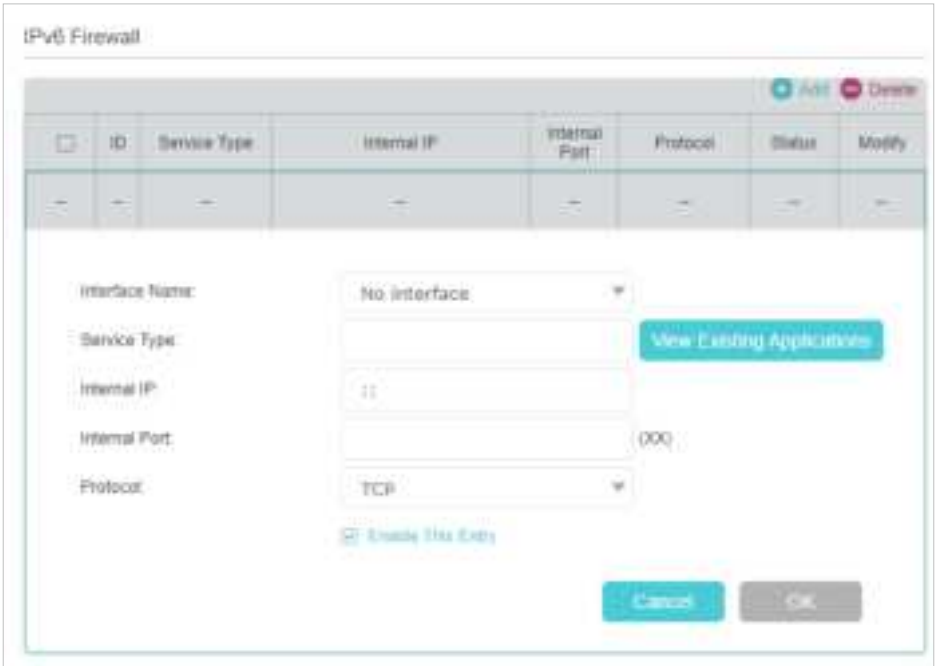
Enjoy the internet without worrying about ARP spoofing and ARP attacks.

15. 5. IPv6 Firewall

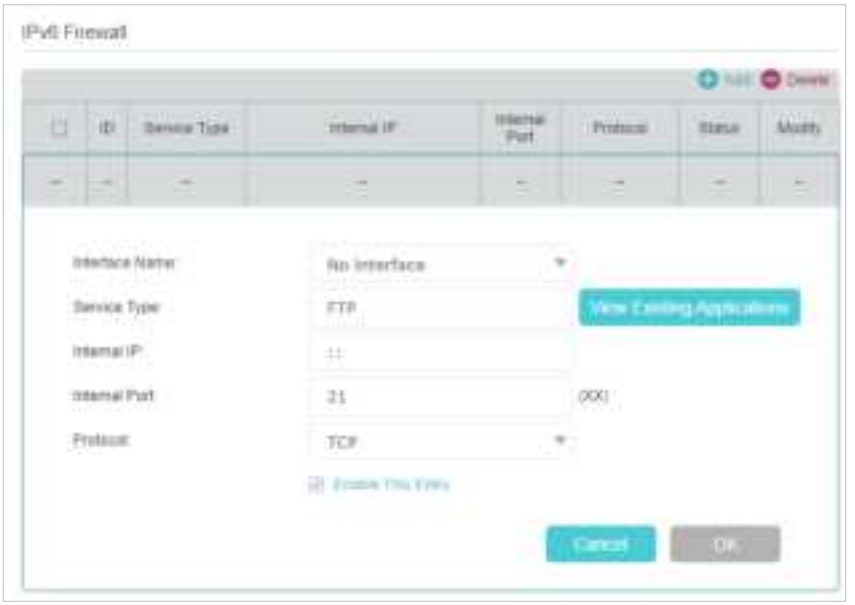
IPv6 Firewall protects your IPv6 network by preveting access from the internet. However, when you are hosting a service, such as a file sharing server in your local network, you can choose to allow access to the server from the internet by adding entries on this page. This feature is available only when you've set up an IPv6 connection.

1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with the password you set for the router.
2. Go to Advanced > Security > IPv6 Firewall.

3. Click Add.



4. Select an interface name from the drop-down list. Interface names are names of the internet connections you have set up.
5. Click View Existing Applications to select a service from the list to automatically populate the Port field with an propriate port number. It is recommended to keep the default Port if you are unsure about which one to use. If the service is not listed, manually enter the Service Type and the Port number (e.g., 21 or 21-25). The following picture takes application FTP as an example.



6. Select the local host device running the service. Enter its global IPv6 address in the Global IPv6 Address field.
7. Select a protocol for the service from the drop-down list.
8. Select Enable This Entry.
9. Click OK.

Tips:

- If you want to disable this entry, click the Bulb icon.
- If the local host device hosts more than one type of available service, you need to create a rule for each service. Please note that ports should NOT be used by multiple services.

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.

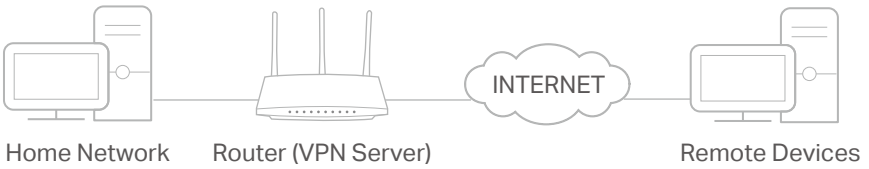
VPN Client allows devices in your home network to access remote VPN servers, without the need to install VPN software on each device.

This chapter contains the following sections:

16. 1. Use OpenVPN to Access Your Home Network

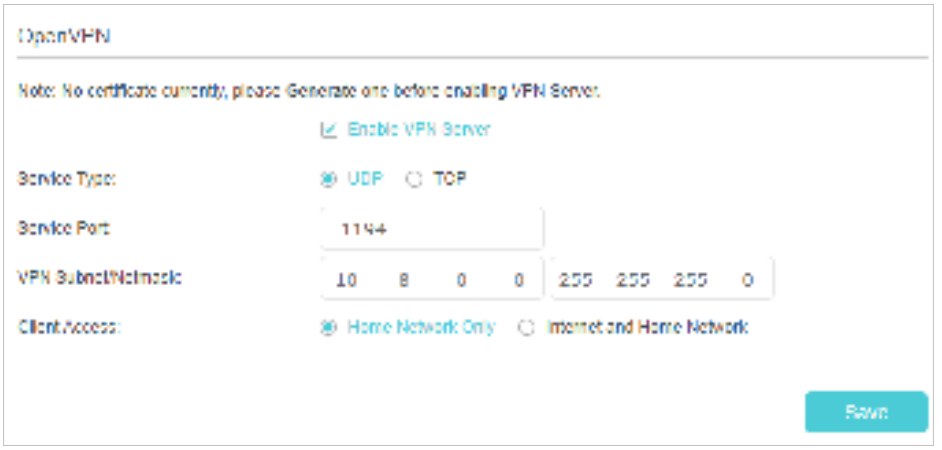
OpenVPN Server is used to create an OpenVPN connection for remote devices to access your home network.

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 or http://192.168.0.1, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > VPN > OpenVPN, and tick the box of Enable VPN Server.



Note:

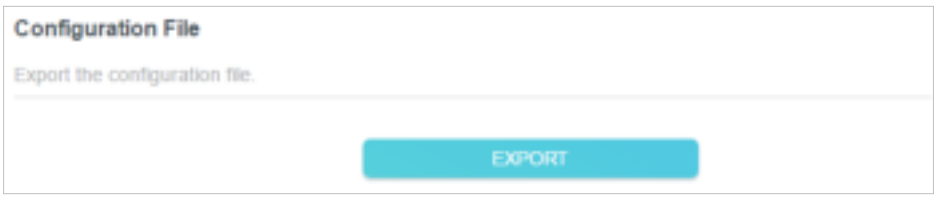
- Before you enable VPN Server, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router's WAN port and synchronize your System Time with internet.
- The first time you configure the OpenVPN Server, you may need to generate a certificate before you enable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

3. Select the Service Type (communication protocol) for OpenVPN Server: UDP, TCP.
4. Enter a VPN Service Port to which a VPN device connects, and the port number should be between 1024 and 65535.
5. In the VPN Subnet/Netmask fields, enter the range of IP addresses that can be leased to the device by the OpenVPN server.
6. Select your Client Access type. Select Home Network Only if you only want the remote device to access your home network; select Internet and Home Network if you also want the remote device to access internet through the VPN Server.

7. Click SAVE.
8. Click GENERATE to get a new certificate.

Note: If you have already generated one, please skip this step, or click GENERATE to update the certificate.

9. Click EXPORT to save the OpenVPN configuration file which will be used by the remote device to access your router.



Step 2. Configure OpenVPN Connection on Your Remote Device

1. Visit http://openvpn.net/index.php/download/community-downloads.html to download the OpenVPN software, and install it on your device where you want to run the OpenVPN client utility.

Note: You need to install the OpenVPN client utility on each device that you plan to apply the VPN function to access your router. Mobile devices should download a third-party app from Google Play or Apple App Store.

2. After the installation, copy the file exported from your router to the OpenVPN client utility's "config" folder (for example, C:\Program Files\OpenVPN\config on Windows). The path depends on where the OpenVPN client utility is installed.
3. Run the OpenVPN client utility and connect it to OpenVPN Server.

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 or http://192.168.0.1, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > VPN > PPTP VPN, and tick the box of Enable VPN Server.

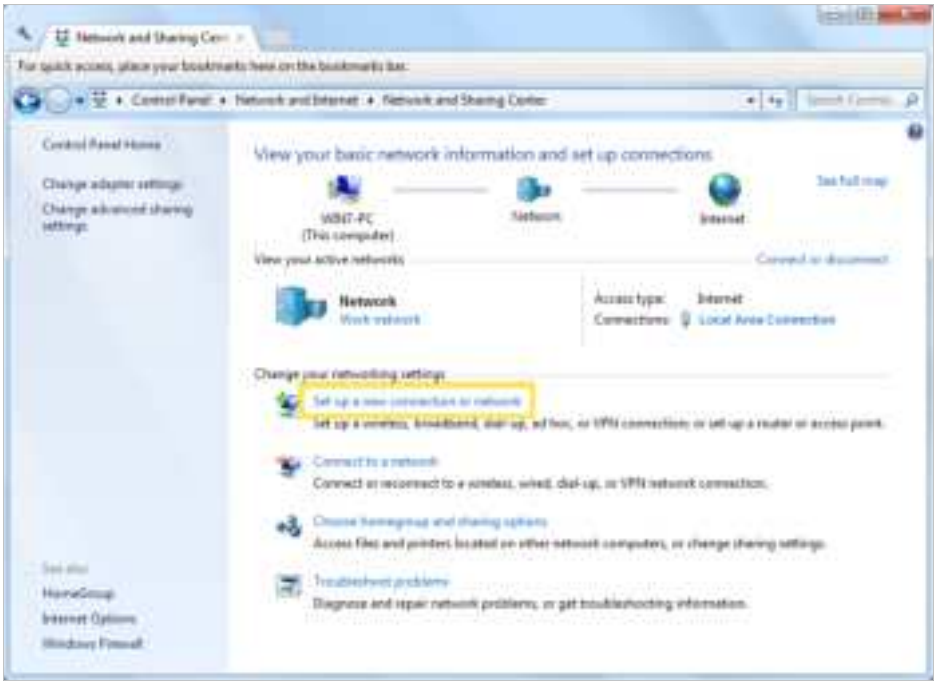
Note: Before you enable VPN Server, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router's WAN port and synchronize your System Time with internet.

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. Enter the Username and Password to authenticate clients to the PPTP VPN server.
5. Click SAVE.
6. On the client devices, create a PPTP VPN connection. The official supported platforms include Windows, Mac OSX, Linux, iOS, and Android.
7. Launch the PPTP VPN program, add a new connection and enter the domain name of the registered DDNS service or the static IP address that is assigned to the WAN port, to connect the client device to the PPTP VPN server.

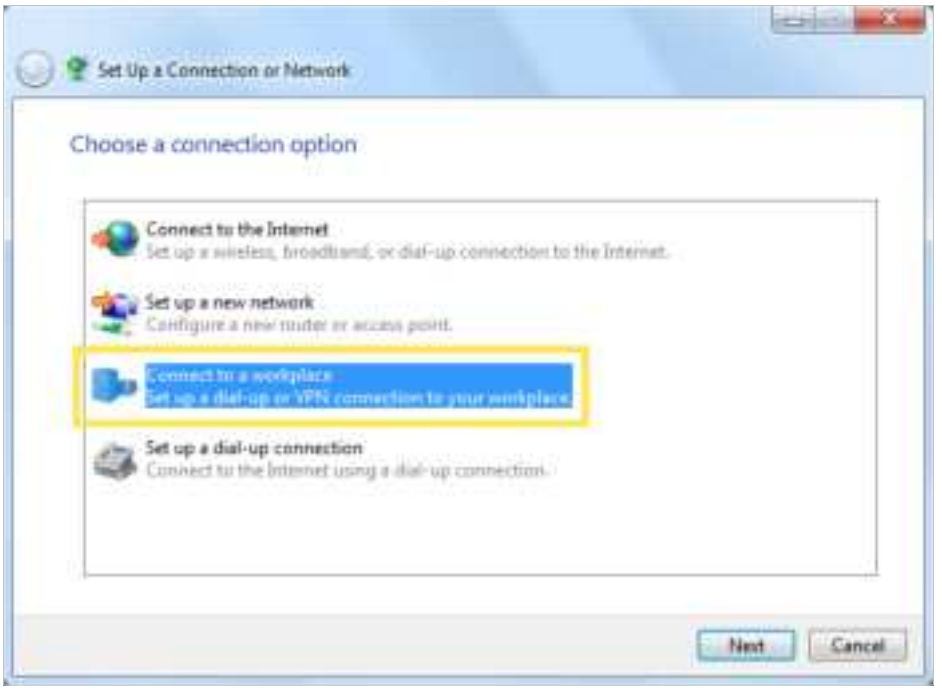
Step 2. Configure PPTP VPN Connection on Your Remote Device

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.

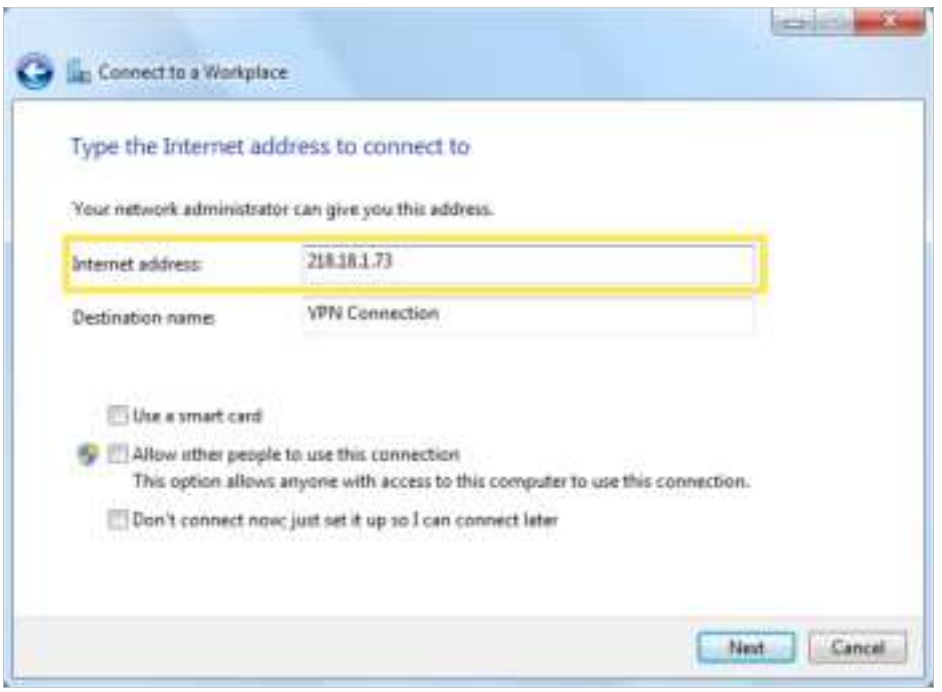


3. Select Connect to a workplace and click Next.



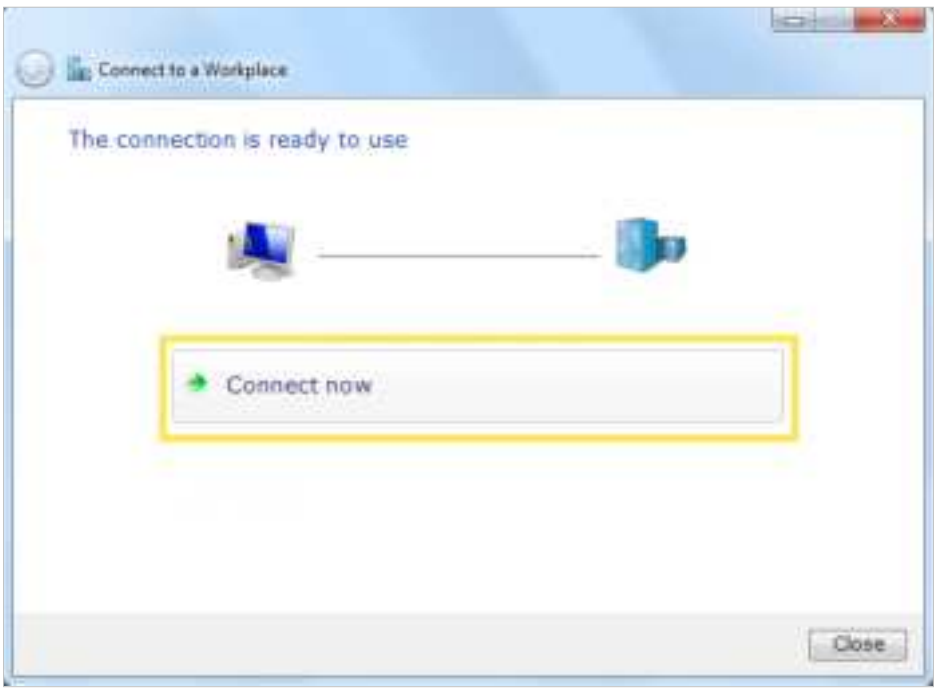
4. Select Use my Internet connection (VPN).

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.

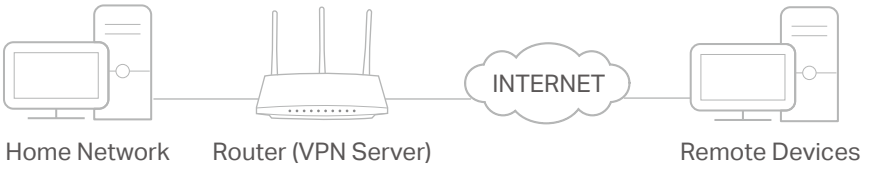
7. Click Connect Now when the VPN connection is ready to use.



16. 3. Use IPSec VPN to Access Your Home Network

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

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



Step 1. Set up IPSec VPN Server on Your Router

1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with your TP-Link ID or the password you set for the router.
2. Go to Advanced > VPN > IPSec VPN, and enable Dead Peer Detection.

Note:

- Firmware update may be required to support IPSec VPN Server.
- Before you enable Dead Peer Detection, 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. Click Add.
4. Configure the IPSec VPN server parameters.