

Bound Accounts				
+ Bind - Unbind				
☐	ID	Email	Binding Date	Role
☐	1	thangpvn_123@tp-link.com	2023-01-01	Admin
☒	2	thangpvn_123@tp-link.com	2023-01-01	User

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

Note: If you need to remotely access your mesh device 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

EasyMesh with Seamless Roaming

This chapter introduces the TP-Link EasyMesh feature.

It contains the following sections:

- [Set Up a EasyMesh Network](#)
- [Manage Devices in the EasyMesh Network](#)

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.

What's EasyMesh?

EasyMesh implements a standards-based approach, combining easy-to-use, self-adapting Wi-Fi with a flexible design, easy setup, and enhanced network intelligence. In an Mesh network, your mobile device will seamlessly switch between the main Router/Gateway(Controller) and Agents, provides the optimal Wi-Fi connection as you move through your home.



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 mesh device's web management page.

9. 1. Set Up a EasyMesh Network

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
1. Go to **Basic > Mesh** or **Advanced > Wireless > Mesh**.

EasyMesh

Connect EasyMesh devices to create a mesh network for seamless Wi-Fi coverage and centralized management.

Note: WPA3-Personal and WPA2-Enterprise are unavailable since EasyMesh doesn't support these security types.

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.

Topology

Add Mesh Device

1

EX510_

.....

1

HX220_

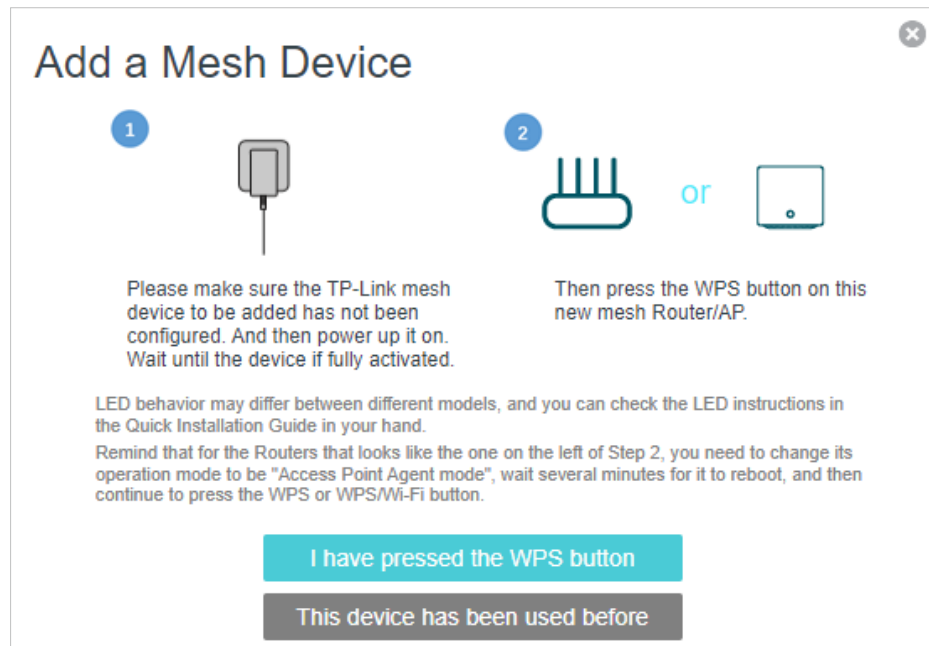
Ethernet

Wireless

Refresh

ID	Device Name	IP Address	MAC Address	Connection Type	Signal Strength	Link Rate	Operation
1				--	--	--	--
2				5GHz_CH 48		1080Mbps	

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



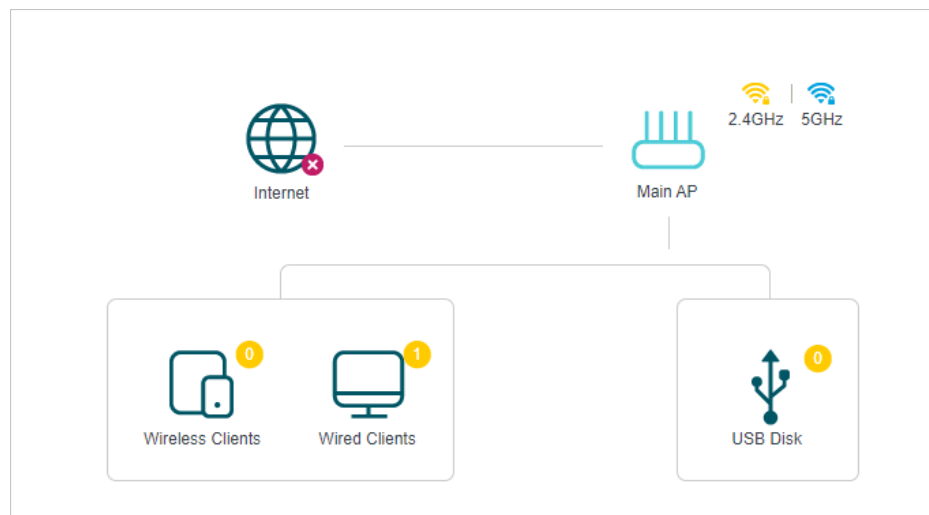
Done! Now your controller and agents successfully form a EasyMesh network!

9.2. Manage Devices in the EasyMesh Network

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

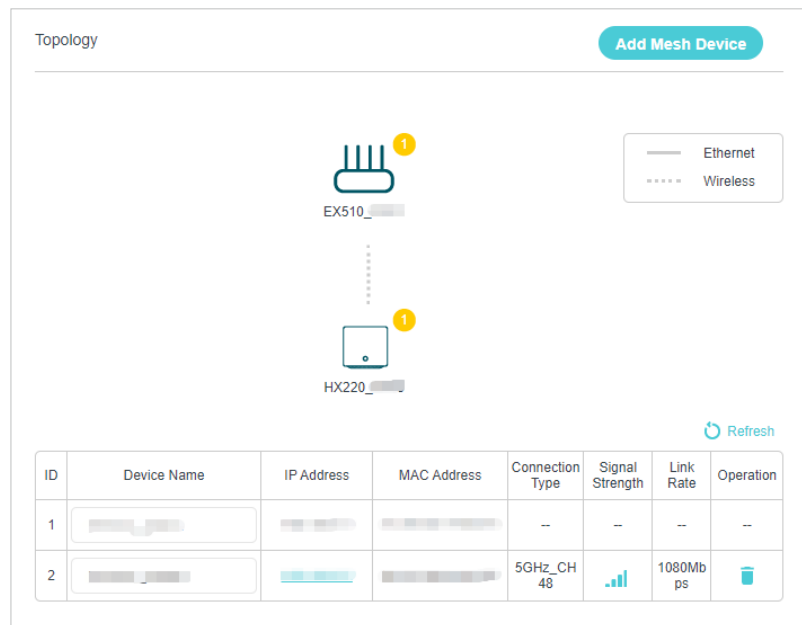
- To view mesh devices and connected clients in the network:**

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
2. Go to **Basic > Network Map**.
3. Click  to view all mesh devices, and click   to view all connected clients.

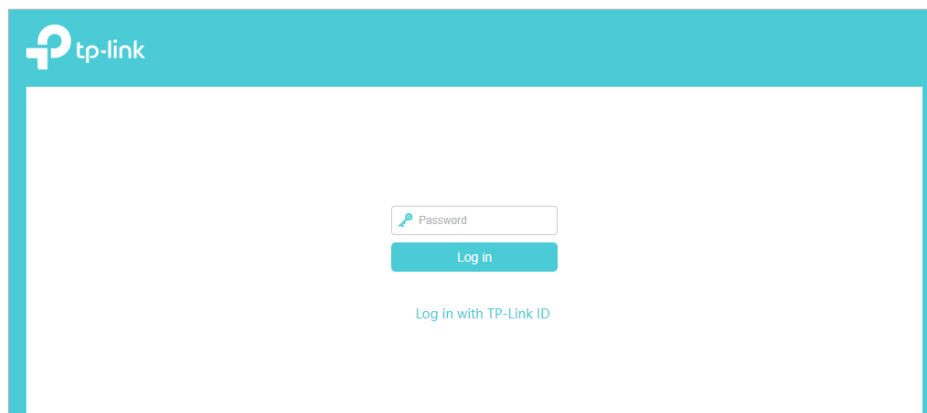


- **To manage a EasyMesh device in the network:**

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
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 10

Guest Network

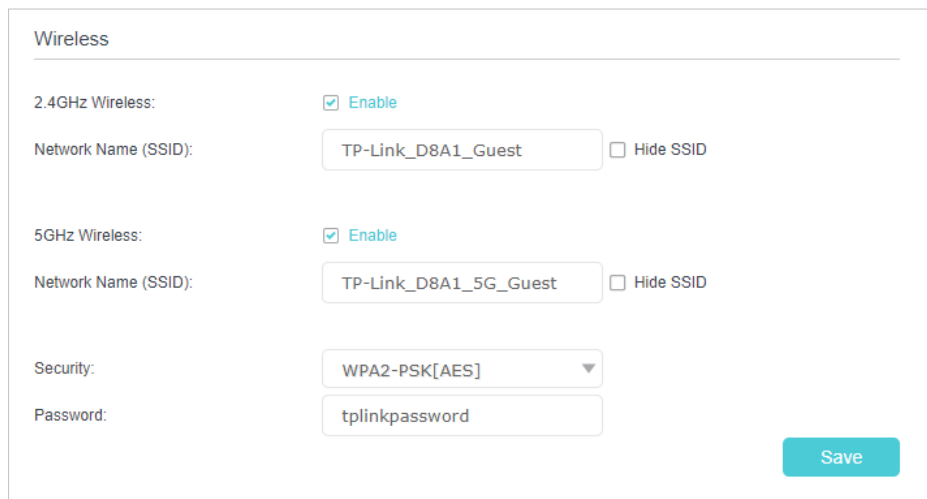
This function allows you to provide Wi-Fi access for guests without disclosing your main network. When you have guests in your house, apartment, or workplace, you can create a guest network for them. In addition, you can customize guest network options to ensure network security and privacy.

It contains the following sections:

- [Create a Network for Guests](#)
- [Customize Guest Network Options](#)

10.1. Create a Network for Guests

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
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.



The screenshot shows the 'Wireless' configuration page for a TP-Link guest network. It has two sections for 2.4GHz and 5GHz wireless networks. Both sections have an 'Enable' checkbox checked. The 2.4GHz section has a 'Network Name (SSID)' field with 'TP-Link_D8A1_Guest' and a 'Hide SSID' checkbox. The 5GHz section has a 'Network Name (SSID)' field with 'TP-Link_D8A1_5G_Guest' and a 'Hide SSID' checkbox. Below these is a 'Security' dropdown menu set to 'WPA2-PSK[AES]' and a 'Password' field with 'tplinkpassword'. A 'Save' button is at the bottom right.

Wireless	
2.4GHz Wireless:	☒ Enable
Network Name (SSID):	TP-Link_D8A1_Guest ☐ Hide SSID
5GHz Wireless:	☒ Enable
Network Name (SSID):	TP-Link_D8A1_5G_Guest ☐ Hide SSID
Security:	WPA2-PSK[AES]
Password:	tplinkpassword
Save	

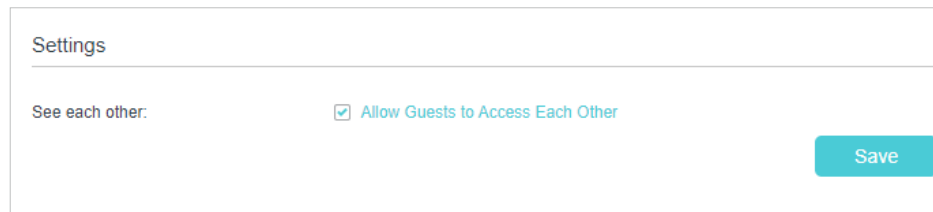
4. Click **Save**. Now your guests can access your guest network using the SSID and password you set!

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.

10.2. Customize Guest Network Options

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
2. Go to **Advanced** > **Guest Network**. Locate the **Settings** section.
3. Customize guest network options according to your needs.



Settings

See each other: ☒ Allow Guests to Access Each Other

Save

- [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 11

NAT Forwarding

The mesh device'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 mesh device 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 mesh device 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:

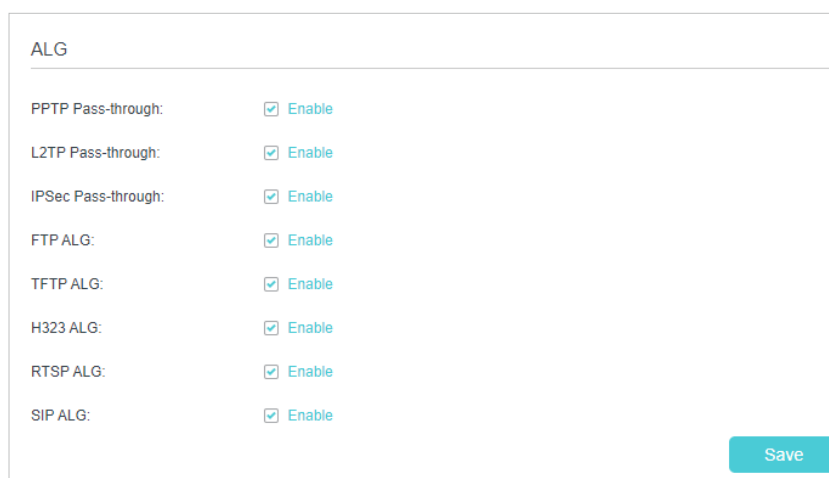
- [ALG](#)
- [Set Up Public Services on The Local Network by Virtual Servers](#)
- [Open Ports Dynamically by Port Triggering](#)
- [Make Applications Free from Port Restriction by DMZ](#)
- [Make Xbox Online Games Run Smoothly by UPnP](#)

11.1. 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 mesh device, since some voice and video communication applications do not work well with SIP ALG.

Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device. Go to **Advanced** > **Security** > **ALG**.



ALG	
PPTP Pass-through:	☒ Enable
L2TP Pass-through:	☒ Enable
IPSec Pass-through:	☒ Enable
FTP ALG:	☒ Enable
TFTP ALG:	☒ Enable
H323 ALG:	☒ Enable
RTSP ALG:	☒ Enable
SIP ALG:	☒ Enable

Save

11.2. 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://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
2. Go to **Advanced** > **NAT Forwarding** > **Virtual Servers** and click  **Add**.
3. Select an interface name from the drop-down list.

Virtual Servers

+ Add - Delete

☐	ID	Service Type	External Port	Internal IP	Internal Port	Protocol	Status	Modify
--	--	--	--	--	--	--	--	--

Note: Virtual Server can be configured only when there is an available interface. If the external port is already used for Remote Management or CWMP, Virtual Server will not take effect.

Interface Name:

Service Type: [View Existing Applications](#)

External Port: (XX-XX or XX)

Internal IP: . . .

Internal Port: (XX or Blank, 1-65535)

Protocol:

☒ Enable This Entry

[Cancel](#) [OK](#)

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.

Virtual Servers

+ Add - Delete

☐	ID	Service Type	External Port	Internal IP	Internal Port	Protocol	Status	Modify
--	--	--	--	--	--	--	--	--

Note: Virtual Server can be configured only when there is an available interface. If the external port is already used for Remote Management or CWMP, Virtual Server will not take effect.

Interface Name:

Service Type: [View Existing Applications](#)

External Port: (XX-XX or XX)

Internal IP: . . .

Internal Port: (XX or Blank, 1-65535)

Protocol:

☒ Enable This Entry

[Cancel](#) [OK](#)

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.

11.3. 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 mesh device can record the IP address of the host. When the data from the internet return to the external ports, the mesh device 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://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
2. Go to **Advanced > NAT Forwarding > Port Triggering** and click  **Add**.

Port Triggering

☐	ID	Application	Triggering Port	Triggering Protocol	External Port	External Protocol	Status	Modify
--	--	--	--	--	--	--	--	--

Interface Name:

Application: [View Existing Applications](#)

Triggering Port:

Triggering Protocol:

External Port: (XX or XX-XX, 1-65535, at most 5 pairs)

External Protocol:

☒ [Enable This Entry](#)

[Cancel](#) [OK](#)

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.

Port Triggering

+ Add
- Delete

☐	ID	Application	Triggering Port	Triggering Protocol	External Port	External Protocol	Status	Modify
--	--	--	--	--	--	--	--	--

Interface Name: ipoe_0_0_d ▼

Application: MSN Gaming Zone View Existing Applications

Triggering Port: 47624 (XX, 1-65535)

Triggering Protocol: ALL ▼

External Port: 2300-2400,28800-29000 (XX or XX-XX, 1-65535, at most 5 pairs)

External Protocol: ALL ▼

☒ Enable This Entry

Cancel
OK

4. Click **OK**.

Port Triggering								
 Add  Delete								
☐	ID	Application	Triggering Port	Triggering Protocol	External Port	External Protocol	Status	Modify
☐	1	MSN Gaming Zone	47624	TCP or UDP	2300-2400, 28800-29000	TCP or UDP		 

 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.

11.4. 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 192.168.88.100.
2. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
1. Go to [Advanced](#) > [NAT Forwarding](#) > [DMZ](#) and tick to enable DMZ.
3. Enter the PC's IP address 192.168.88.100 manually in the [DMZ Host IP Address](#) field.

DMZ

DMZ: ☒ Enable

DMZ Host IP Address:

Save

2. 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.

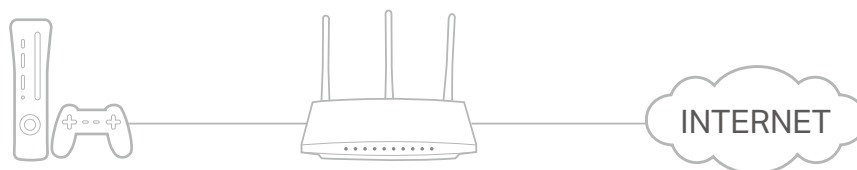
11.5. Make Xbox Online Games Run Smoothly by UPnP

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 mesh device.
- 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 mesh device which has connected to the internet to play online games, UPnP will send request to the mesh device 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://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.

2. Go to [Advanced](#) > [NAT Forwarding](#) > [UPnP](#) and toggle on or off according to your needs.

UPnP

UPnP: ☒

UPnP Service List

Total Clients: 0 [Refresh](#)

ID	Service Description	External Port	Protocol	Internal IP Address	Internal Port
--	--	--	--	--	--

Chapter 12

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:

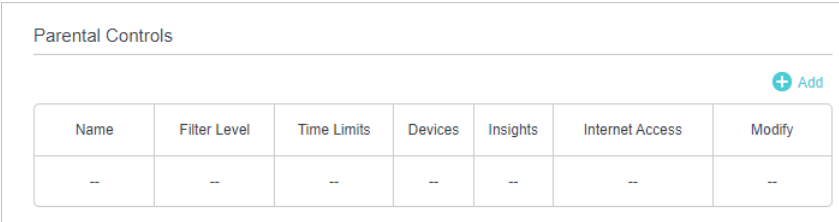
Control what types of websites my children or other home network users can visit and the time of day they are allowed to access the internet.

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.

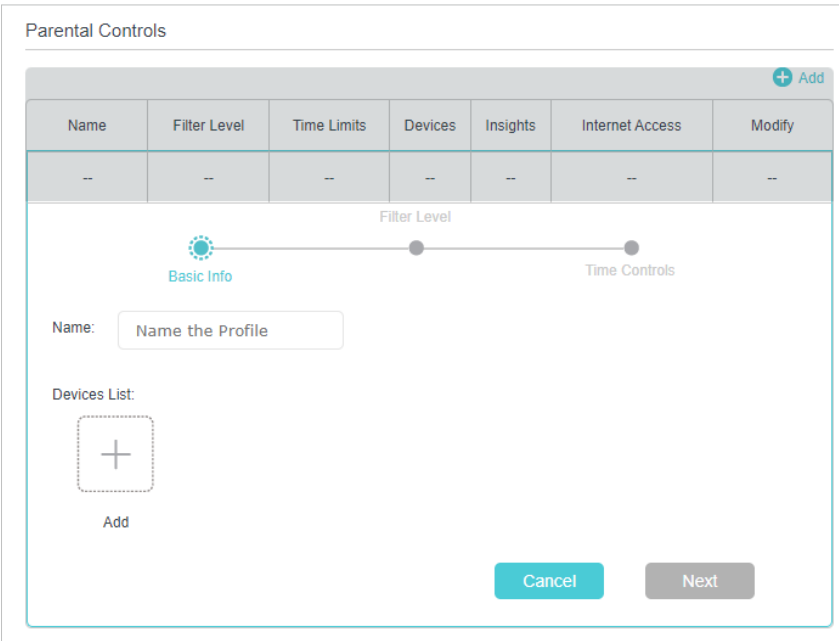
How can I do that?

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.

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](#).

Parental Controls

+ Add

Name	Filter Level	Time Limits	Devices	Insights	Internet Access	Modify
--	--	--	--	--	--	--

Basic Info

Filter Level

Time Controls

Child (0-7)

Pre-Teen (8-12)

Teen (13-17)

Adult (>17)

Based on the selected filter level, Adult Content, Social Networking have already been filtered for 123. You can block more from Available Categories or by adding a new keyword.

Filter Content

+ Add a New Keyword

Available Categories:

Adult Content

Social Networking

Games

Media

Online Communication

Pay to Surf

Downloads

Cancel
Back
Next

- (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.
- 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.

Parental Controls

+ Add

Name	Filter Level	Time Limits	Devices	Insights	Internet Access	Modify
--	--	--	--	--	--	--

Filter Level

Basic Info

Time Controls

Weekdays

☒ Mon ☒ Tues ☒ Wed ☒ Thur ☒ Fri ☐ Sat ☐ Sun

Time Limits

Set daily time limits for the total time spent online.

Weekdays

☒ Enable

2h

30min

8h

Weekends

☒ Enable

2h

30min

8h

Bed Time

Set a time period while this profile cannot access the internet.

Weekdays

☒ Enable

From

10 : 00 PM

To

06 : 00 AM

Weekends

☒ Enable

From

10 : 00 PM

To

06 : 00 AM

Cancel

Back

Save

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.

Parental Controls

+ Add

Name	Filter Level	Time Limits	Devices	Insights	Internet Access	Modify
123	Pre-Teen	2h	1			

Top 5 Visits

Blocked History

Today

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

Parental Controls

+ Add

Name	Filter Level	Time Limits	Devices	Insights	Internet Access	Modify
123	Pre-Teen	2h	1		 Paused	

Chapter 13

Quality of Service

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

The mesh device 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 mesh devices, 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 mesh devices.

To set up QoS for the network:

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [QoS](#).
3. Enable [QoS](#).

The screenshot shows the QoS configuration page. The 'QoS' section is expanded, and the 'QoS' checkbox is checked and highlighted with a red box. Below it, 'Upload Bandwidth' and 'Download Bandwidth' are both set to 0 Mb/s. The 'IPTV QoS' checkbox is unchecked. The 'Advanced' section is also expanded, showing three sliders for 'High', 'Middle', and 'Low' traffic prioritization. The 'High' slider is at 60%, 'Middle' is at 30%, and 'Low' is at 10%. A 'Save' button is located at the bottom right of the page.

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

The screenshot shows the 'QoS' configuration page. At the top, the title 'QoS' is displayed. Below it, the 'QoS:' section has a checked 'Enable' checkbox. Underneath, 'Upload Bandwidth:' and 'Download Bandwidth:' are both set to '0' with a unit dropdown menu showing 'Mb...'. The 'IPTV QoS:' section has an unchecked 'Enable' checkbox. Below this is an 'Advanced' section with a plus icon. Three sliders are visible: 'High:' at 60%, 'Middle:' at 30%, and 'Low:' at 10%. A 'Save' button is at the bottom right.

QoS

QoS: ☒ Enable

Upload Bandwidth: 0 Mb... ▼

Download Bandwidth: 0 Mb... ▼

IPTV QoS: ☐ Enable

⬆ Advanced

High: 60%

Middle: 30%

Low: 10%

Save

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

This screenshot is identical to the previous one, but with the 'IPTV QoS:' checkbox now checked and highlighted with a red box. The 'Advanced' section remains collapsed.

QoS

QoS: ☒ Enable

Upload Bandwidth: 0 Mb... ▼

Download Bandwidth: 0 Mb... ▼

IPTV QoS: ☒ Enable

⬆ Advanced

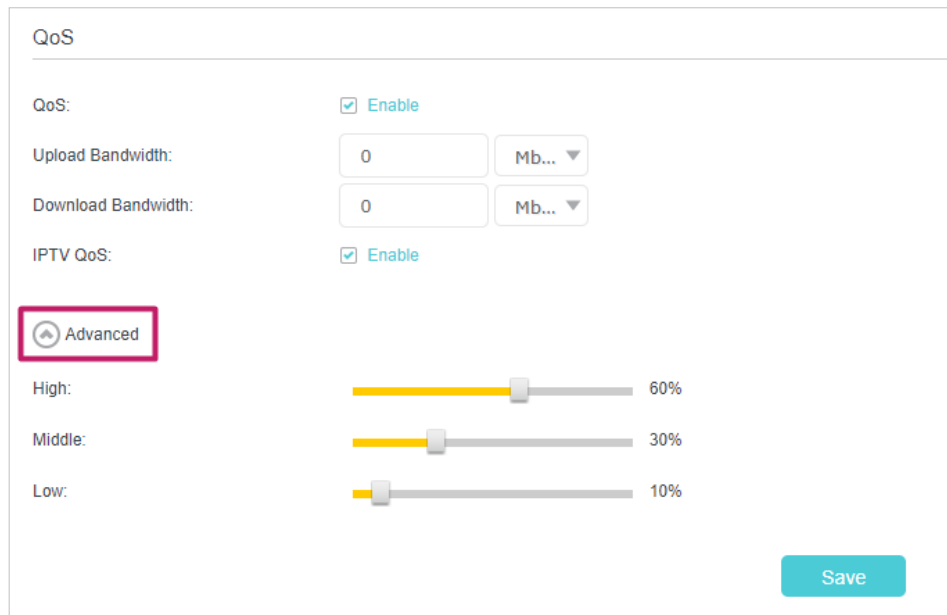
High: 60%

Middle: 30%

Low: 10%

Save

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



QoS

QoS: ☒ Enable

Upload Bandwidth: Mb... ▼

Download Bandwidth: Mb... ▼

IPTV QoS: ☒ Enable

Advanced

High: 60%

Middle: 30%

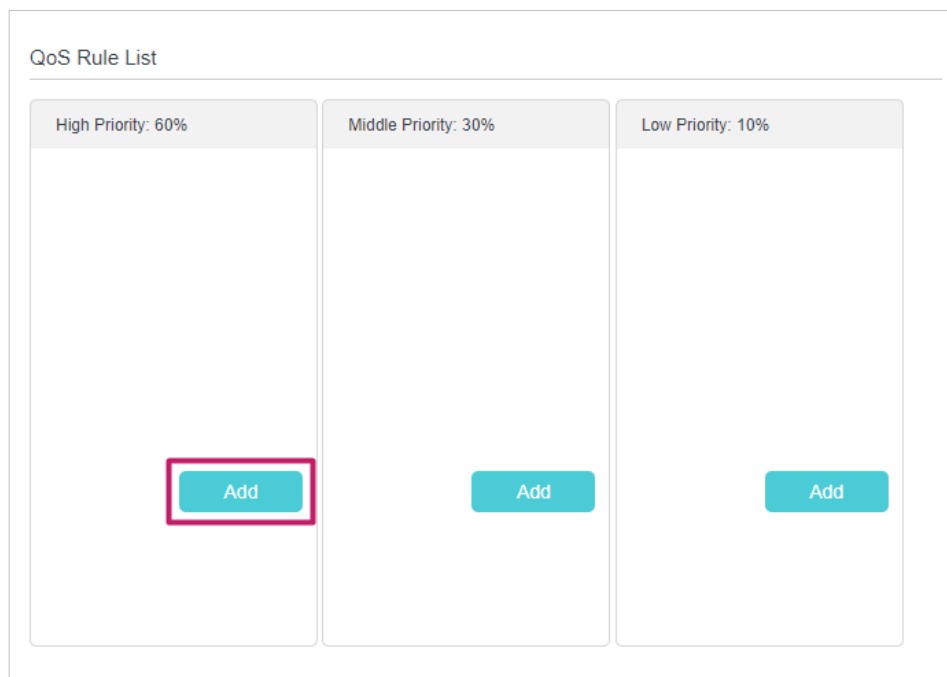
Low: 10%

Save

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 mesh device.
2. Go to [Advanced](#) > [QoS](#).
3. In the [QoS Rule List](#) table, choose a priority section and click [Add](#).



QoS Rule List

High Priority: 60%	Middle Priority: 30%	Low Priority: 10%
Add	Add	Add

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

QoS Rule

Type: ☒ By Device

Device Name:

Unknown

scan

MAC Address:

Cancel

OK

ID	Device Name	IP Address	MAC Address	Operation
1	Unknown			+

Chapter 14

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.

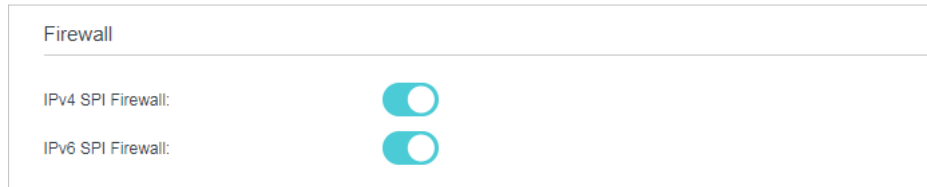
This chapter contains the following sections:

- [Firewall & DoS Protection](#)
- [Service Filtering](#)
- [Access Control](#)
- [IP & MAC Binding](#)
- [IPv6 Firewall](#)

14.1. Firewall & DoS Protection

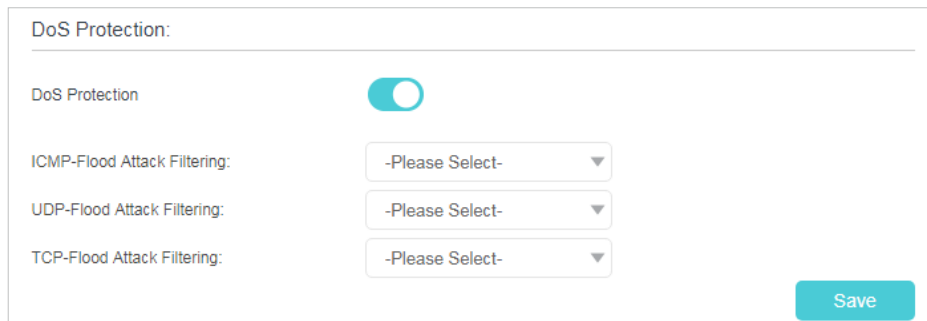
The SPI (Stateful Packet Inspection) Firewall and DoS (Denial of Service) Protection protect the mesh device from cyber attacks.

The SPI Firewall can prevent cyber attacks and validate the traffic that is passing through the mesh device 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://192.168.88.1>, and log in with the password you set for the mesh device.
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](#).

Dos Protection Level Settings

ICMP-Flood Protection Level:	Low:	1200	(5-3600) packets/sec
	Middle:	2400	(5-3600) packets/sec
	High:	3600	(5-3600) packets/sec
UDP-Flood Protection Level:	Low:	1200	(5-3600) packets/sec
	Middle:	2400	(5-3600) packets/sec
	High:	3600	(5-3600) packets/sec
TCP-SYN-Flood Protection Level:	Low:	1200	(5-3600) packets/sec
	Middle:	2400	(5-3600) packets/sec
	High:	3600	(5-3600) packets/sec

Save

- 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](#).

Blocked DoS Host List

Host Number: 0 Refresh Delete

☐	ID	IP Address	MAC Address
--	--	--	--

14.2. Service Filtering

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

- Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with the password you set for the mesh device.
- Go to [Advanced](#) > [Security](#) > [Service Filtering](#), and enable [Service Filtering](#).

Service Filtering

Service Filtering: ☒

- Click [Add](#).

Filtering List

Refresh + Add - Delete

☐	ID	Service Type	Port	IP Address	Status	Modify
--	--	--	--	--	--	--

Service Type:

Protocol:

Starting Port: (1-65535)

Ending Port: (1-65535)

Service Type:

Filter Service For: ☐ Single IP Address ☐ IP Address Range ☒ All IP Addresses

Cancel Save

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.

14.3. 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://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to **Advanced > Security > Access Control** and enable **Access Control**.

Access Control

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**.

Access Mode

Access Mode:

☒ **Blacklist**
☐ Whitelist

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.

Devices in Blacklist

[+ Add](#)
[- Delete](#)

☐	ID	Device Name	MAC Address	Modify
--	--	--	--	--

Online Devices

[Refresh](#)
[Block](#)

☐	ID	Device Name	IP Address	MAC Address	Connection Type
☐	1	DESKTOP-XXXXXX	192.168.0.100	8C:8C:4B:1D:8D:4B	Wired

To allow specific device(s):

- 1) Select **Whitelist** and click **Save**.

Access Mode

Access Mode:

☐ Blacklist
 ☒ **Whitelist**

Save

- 2) Click **Add** in the **Devices in Whitelist** section.

The screenshot shows a web interface titled "Devices in Whitelist". At the top right, there are "Add" (green plus icon) and "Delete" (red minus icon) buttons. Below this is a table with the following columns: a checkbox, "ID", "Device Name", "MAC Address", and "Modify". The table body is currently empty. Below the table, there are two input fields: "Device Name:" and "MAC Address:". The "MAC Address" field has a placeholder showing five dashes separated by spaces. At the bottom right, there are "Cancel" and "Save" buttons.

- 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](#).

14. 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://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [Security](#) > [IP & MAC Binding](#), and enable [IP & MAC Binding](#).

IP & MAC Binding

IP & MAC Binding: ☒

Binding List

[+ Add](#) [- Delete](#)

☐	ID	MAC Address	IP Address	Status	Enable	Modify
☐	--	--	--	--	--	--

ARP List

[Refresh](#) [Bind](#)

☐	ID	MAC Address	IP Address	Bound	Modify
☐	1	84-16-F9-03-E2-D3	192.168.0.100	Unloaded	

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.

Binding List

[+ Add](#) [- Delete](#)

☐	ID	MAC Address	IP Address	Status	Enable	Modify
☐	--	--	--	--	--	--

MAC Address:

IP Address:

☒ [Enable This Entry](#)

[Cancel](#) [OK](#)

- 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](#).

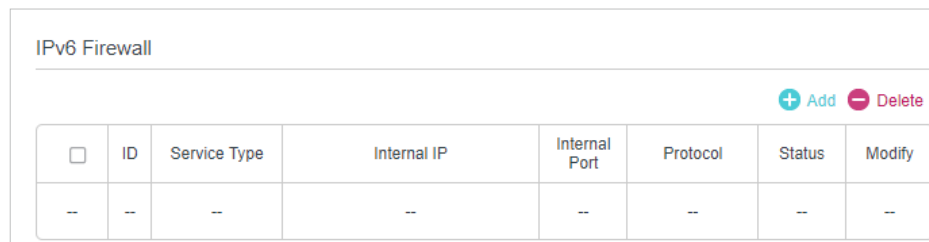
Done!

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

14.5. IPv6 Firewall

IPv6 Firewall protects your IPv6 network by preventing 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://192.168.88.1>, and log in with the password you set for the mesh device.
2. Go to [Advanced](#) > [Security](#) > [IPv6 Firewall](#).

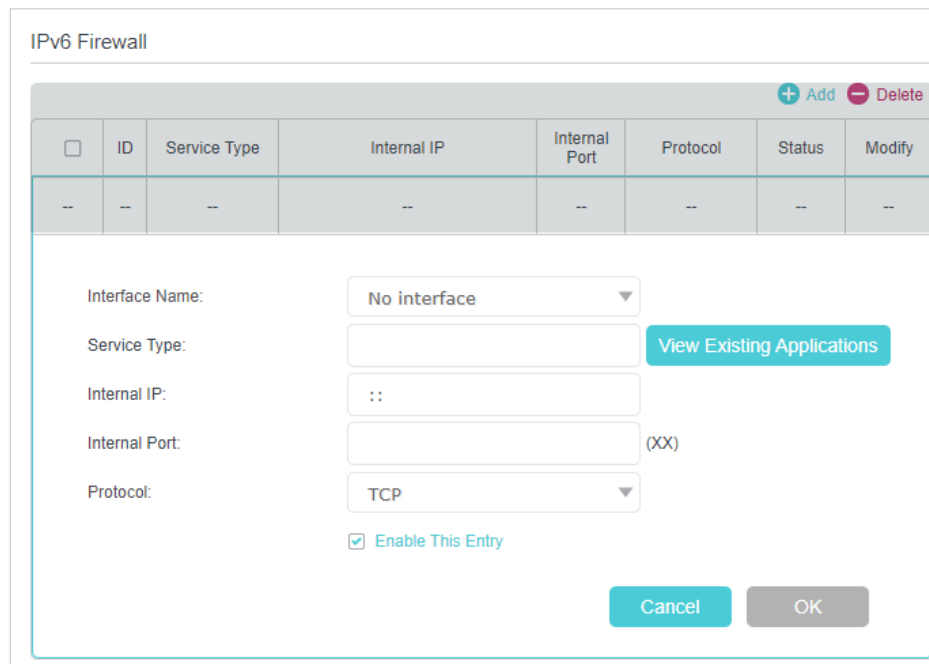


IPv6 Firewall

[+ Add](#) [- Delete](#)

☐	ID	Service Type	Internal IP	Internal Port	Protocol	Status	Modify
--	--	--	--	--	--	--	--

3. Click [Add](#).



IPv6 Firewall

[+ Add](#) [- Delete](#)

☐	ID	Service Type	Internal IP	Internal Port	Protocol	Status	Modify
--	--	--	--	--	--	--	--

Interface Name:

Service Type: [View Existing Applications](#)

Internal IP:

Internal Port: (XX)

Protocol:

☒ [Enable This Entry](#)

[Cancel](#) [OK](#)

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 appropriate 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.

IPv6 Firewall

+ Add - Delete

☐	ID	Service Type	Internal IP	Internal Port	Protocol	Status	Modify
--	--	--	--	--	--	--	--

Interface Name:

Service Type: [View Existing Applications](#)

Internal IP:

Internal Port: (XX)

Protocol:

☒ Enable This Entry

[Cancel](#) [OK](#)

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 15

VPN Server&Client

The mesh device 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 mesh device 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.

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

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

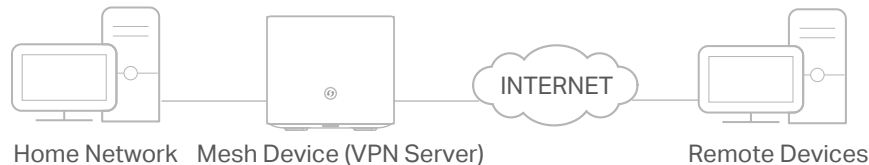
This chapter contains the following sections:

- [Use OpenVPN to Access Your Home Network](#)
- [Use PPTP VPN to Access Your Home Network](#)
- [Use IPSec VPN to Access Your Home Network](#)
- [VPN Connections](#)

15.1. Use OpenVPN to Access Your Home Network

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

To use the VPN feature, you need to enable OpenVPN Server on your mesh device, 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 Mesh Device

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
2. Go to **Advanced > VPN > OpenVPN**, and tick the box of **Enable VPN Server**.

OpenVPN

Note: No certificate currently, please **Generate** one before enabling VPN Server.

☒ **Enable VPN Server**

Service Type: ☒ **UDP** ☐ **TCP**

Service Port:

VPN Subnet/Netmask:

Client Access: ☒ **Home Network Only** ☐ **Internet and Home Network**

Save

Note:

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

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

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

Certificate
Generate the certificate.

GENERATE

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

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

Configuration File
Export the configuration file.

EXPORT

Step 2. Configure OpenVPN Connection on Your Remote Device

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

■ **Note:** You need to install the **OpenVPN** client utility on each device that you plan to apply the VPN function to access your mesh device. 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 mesh device to the OpenVPN client utility's "config" folder (for example, **C:\Program Files\OpenVPN\config** on Windows). The path depends on where the OpenVPN client utility is installed.
3. Run the OpenVPN client utility and connect it to OpenVPN Server.

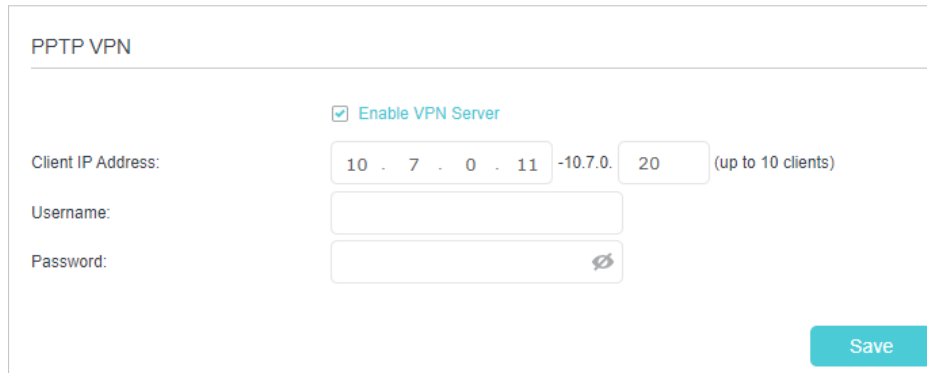
15.2. Use PPTP VPN to Access Your Home Network

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

To use the VPN feature, you need to set up PPTP VPN Server on your mesh device, 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 Mesh Device

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
2. Go to **Advanced > VPN > PPTP VPN**, and tick the box of **Enable VPN Server**.



PPTP VPN

☒ Enable VPN Server

Client IP Address: 10 . 7 . 0 . 11 -10.7.0. 20 (up to 10 clients)

Username:

Password: 

Save

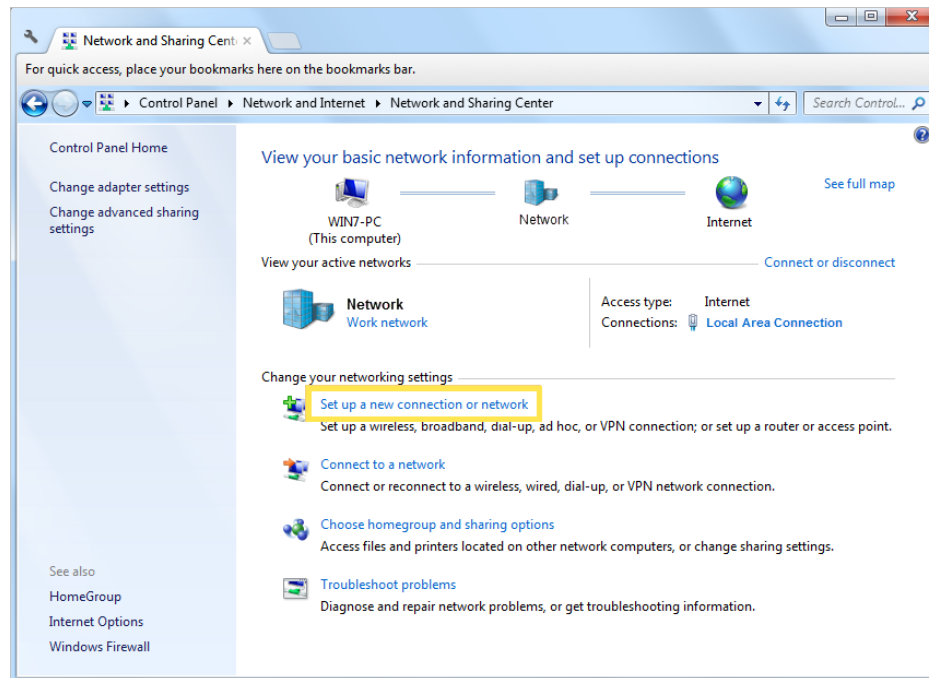
Note: Before you enable [VPN Server](#), we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for mesh device's WAN port and synchronize your [System Time](#) with internet.

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.

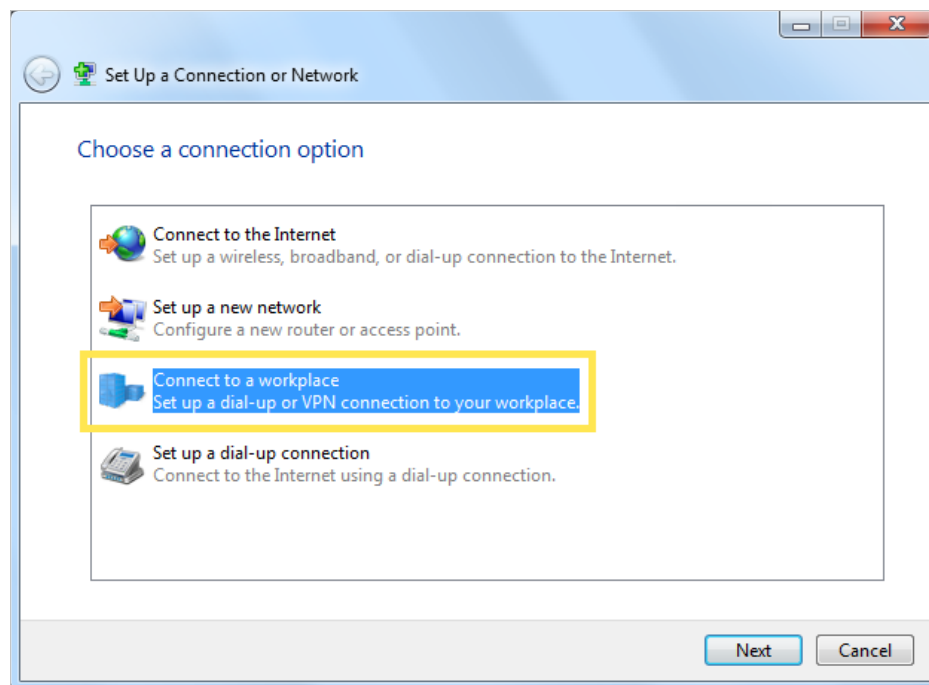
Step 2. Configure PPTP VPN Connection on Your Remote Device

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.

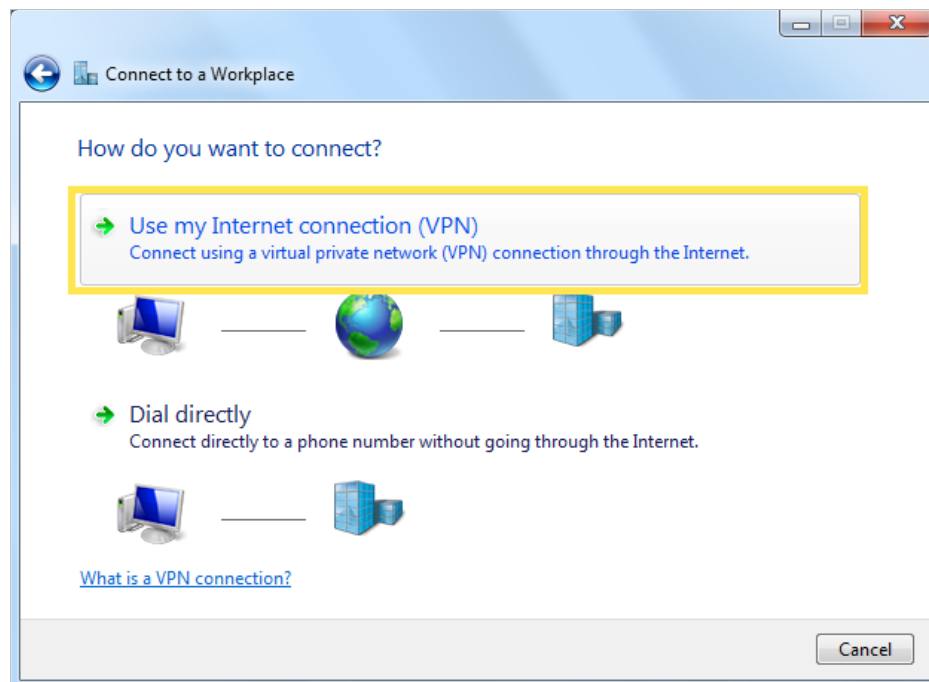
1. Go to [Start > Control Panel > Network and Internet > Network and Sharing Center](#).
2. Select [Set up a new connection or network](#).



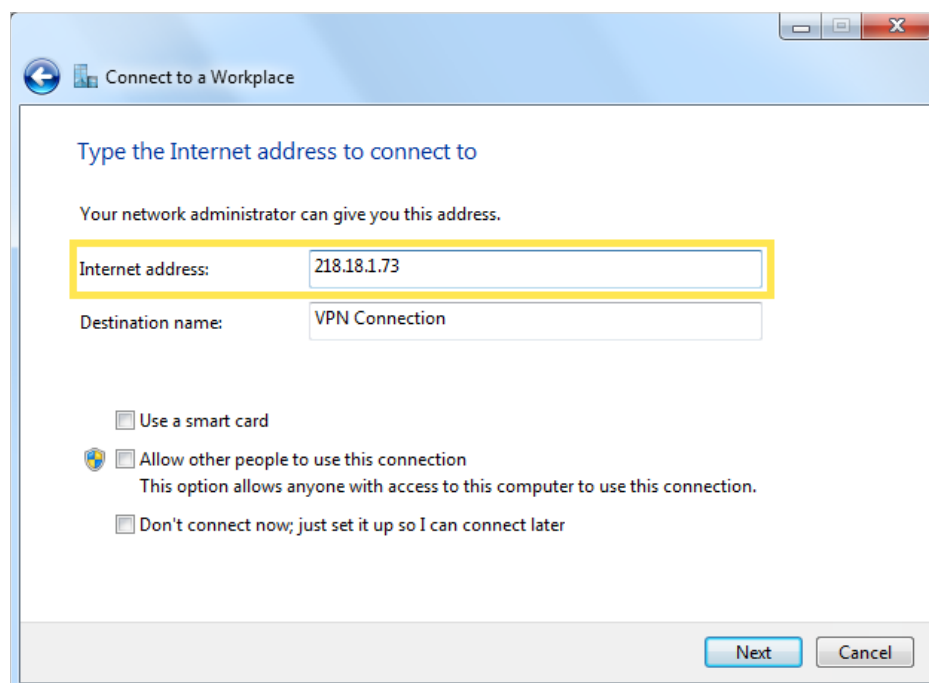
3. Select **Connect to a workplace** and click **Next**.



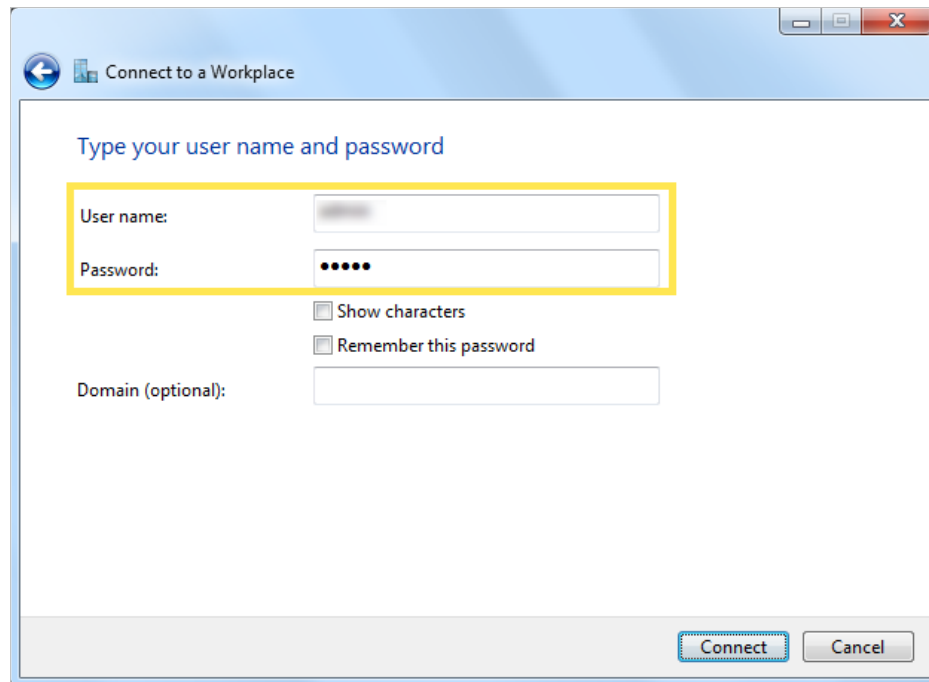
4. Select **Use my Internet connection (VPN)**.



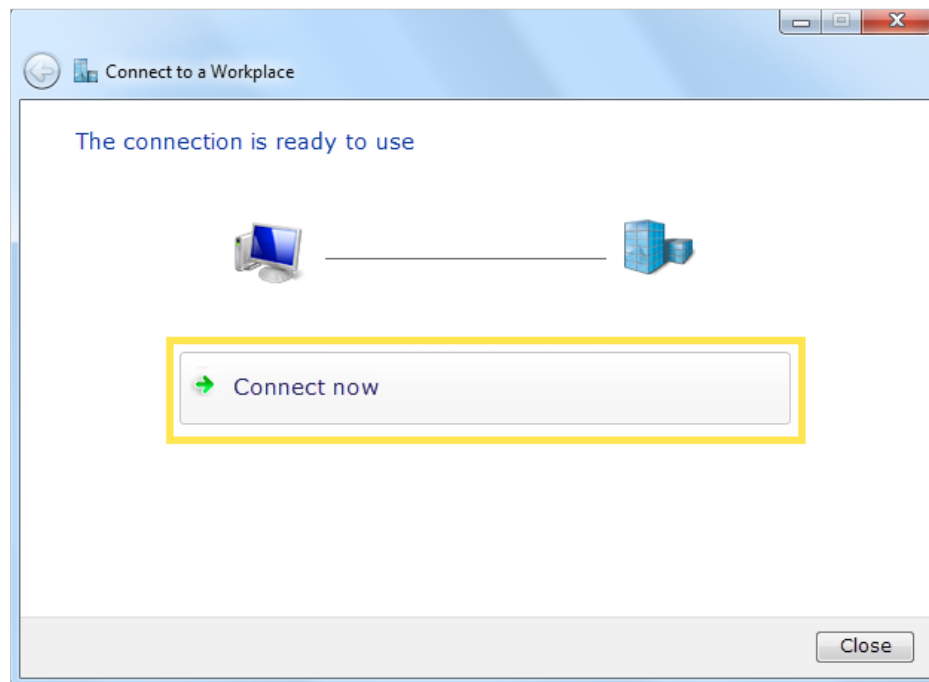
5. Enter the internet IP address of the mesh device (for example: 218.18.1.73) in the Internet address field. Click Next.



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



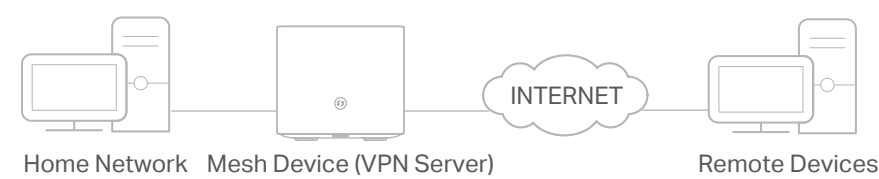
7. Click [Connect Now](#) when the VPN connection is ready to use.



15.3. 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 mesh device, and configure the IPSec 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 Mesh Device

1. Visit <http://tplinkwifi.net> or <http://192.168.88.1>, and log in with your TP-Link ID or the password you set for the mesh device.
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 mesh device’s WAN port and synchronize your [System Time](#) with internet.

IPSec VPN

Dead Peer Detection: 

 Add  Delete

☐	Connection Name	Remote Gateway	Local Address	Remote Address	Status	Enable	Modify
☐	--	--	--	--	--	--	--

3. Click [Add](#).
4. Configure the IPSec VPN server parameters.

Dead Peer Detection:
☒

+ Add
- Delete

☐	Connection Name	Remote Gateway	Local Address	Remote Address	Status	Enable	Modify
--	--	--	--	--	--	--	--

IPSec Connection Name:
Name

Remote IPSec Gateway (URL):
0.0.0.0

Tunnel access from local IP addresses:
Subnet Address

IP Address for VPN:
0 . 0 . 0 . 0

Subnet Mask:
255 . 255 . 255 . 0

Tunnel access from remote IP addresses:
Subnet Address

IP Address for VPN:
0 . 0 . 0 . 0

Subnet Mask:
255 . 255 . 255 . 0

Key Exchange Method:
Auto (IKE)

Authentication Method:
Pre-Shared Key

Pre-Shared Key:
psk_key

Perfect Forward Secrecy:
Enable

⌵ Advanced

Cancel
OK

- Configure the advanced settings according to the following explanation. We recommend that you keep the default settings. If you want to change these settings, make sure that both VPN server endpoints use the same Encryption Algorithm, Integrity Algorithm, Diffie-Hellman Group and Key Lifetime in both phase1 and phase2.

The screenshot shows a configuration window titled "Advanced" with a sub-header "Advanced". It is divided into two sections: "Phase 1" and "Phase 2".

Phase 1 Settings:

- Mode: Main (dropdown)
- Local Identifier Type: Local Wan IP (dropdown)
- Local Identifier: (text input)
- Remote Identifier Type: Remote Wan IP (dropdown)
- Remote Identifier: (text input)
- Encryption Algorithm: 3DES (dropdown)
- Integrity Algorithm: MD5 (dropdown)
- Diffie-Hellman Group for Key Exchange: 1024bit (dropdown)
- Key Life Time(Seconds): 3600 (text input)

Phase 2 Settings:

- Encryption Algorithm: 3DES (dropdown)
- Integrity Algorithm: MD5 (dropdown)
- Diffie-Hellman Group for Key Exchange: 1024bit (dropdown)
- Key Life Time(Seconds): 3600 (text input)

At the bottom right, there are "Cancel" and "OK" buttons.

6. Click **OK**.

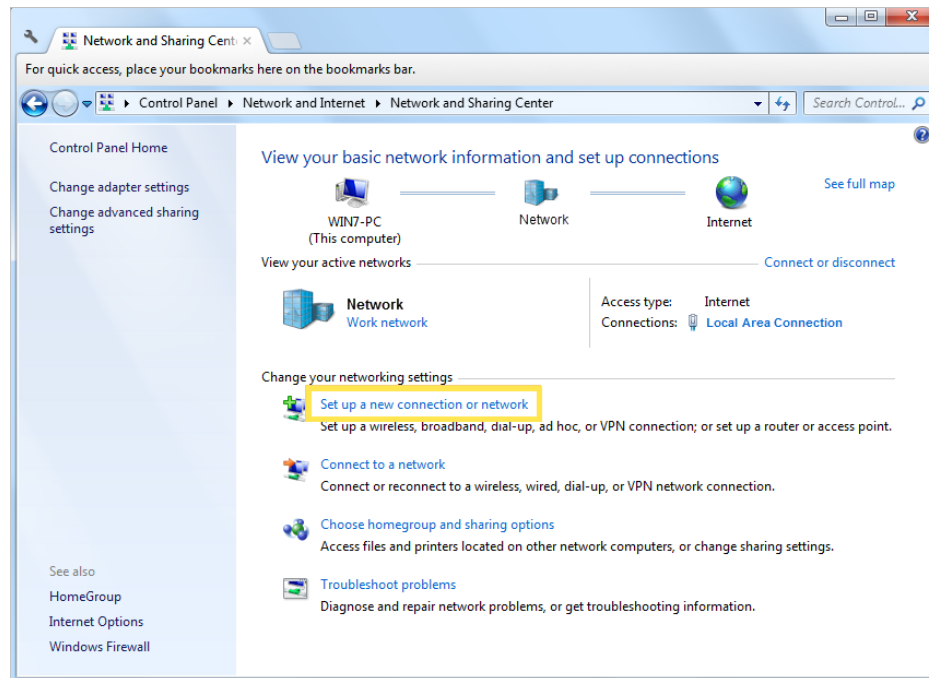
Note:

- For the comprehensive guide, please refer to the User Guide on the product's support page.

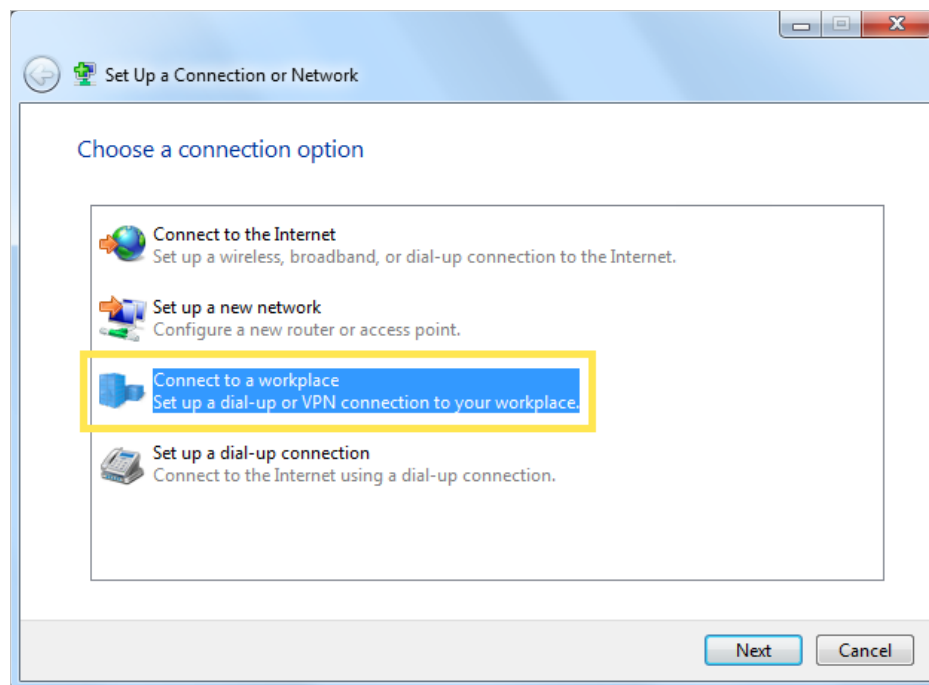
Step 2. Configure IPSec VPN Connection on Your Remote Device

The remote device can use the Windows or Mac OS built-in IPSec software or a third-party IPSec software to connect to IPSec Server. Here we use the [Windows built-in 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](#).



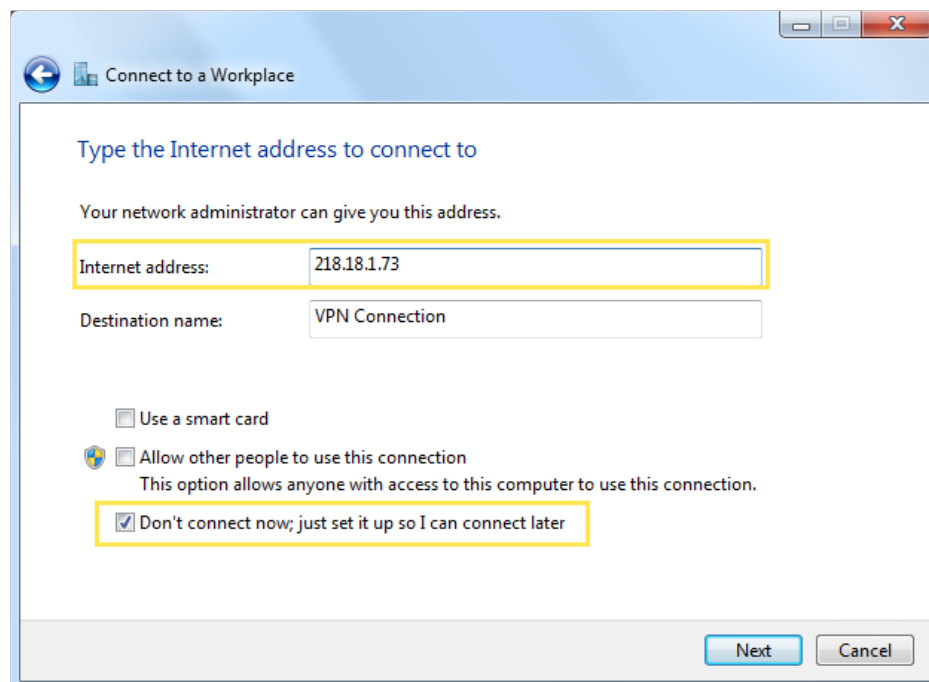
3. Select **Connect to a workplace** and click **Next**.



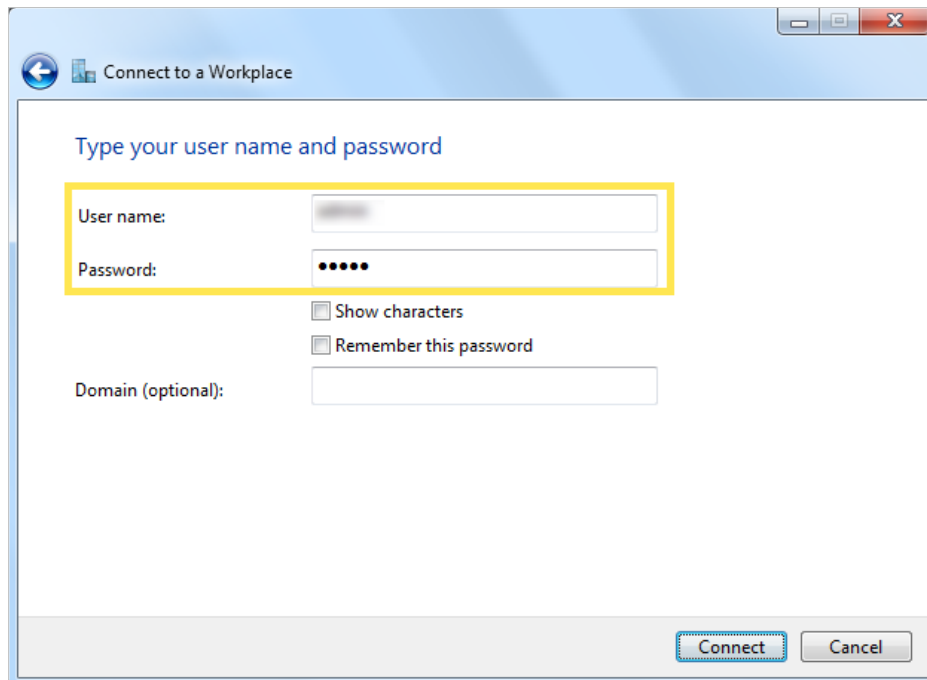
4. Select **Use my Internet connection (VPN)**.



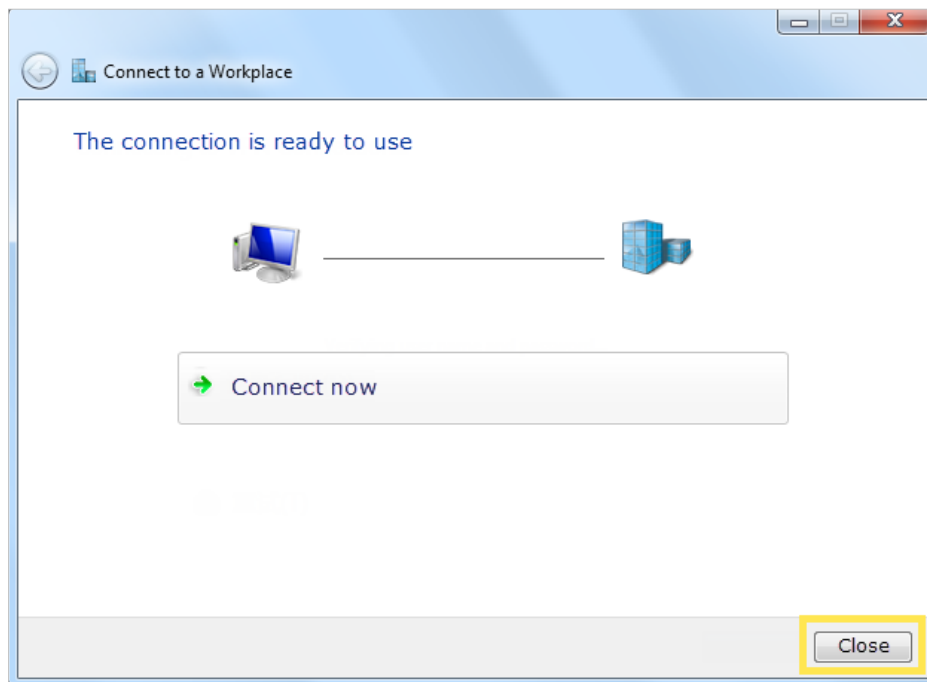
5. Enter the internet IP address of the mesh device (for example: 218.18.1.73) in the Internet address field, and select the checkbox **Don't connect now; just set it up so I can connect later**. Click **Next**.



6. Enter the **User name** and **Password** you have set for the IPSec VPN server on your mesh device, 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](#).