



User Guide

Archer NX200/Archer NX210

Contents

About This Guide	1
 Chapter 1. Get to Know About Your Modem Router	 3
1. 1. Product Overview.....	4
1. 2. Appearance	4
1. 2. 1.Top Panel	4
1. 2. 2.The Back Panel.....	6
 Chapter 2. Connect the Hardware	 7
2. 1. Position Your Router	8
2. 2. Connect Your Router.....	8
 Chapter 3. Log In to Your Router.....	 11
 Chapter 4. Set Up Internet Connection	 13
4. 1. Use Quick Setup Wizard	14
4. 2. Quick Setup Via TP-Link Tether App.....	15
4. 3. Manually Set Up Your Internet Connection	16
4. 4. Test Internet Connectivity	19
4. 5. Set Up an IPv6 Internet Connection	20
4. 6. IPv6 Tunnel	25
4. 7. Create a Connection Profile.....	27
4. 8. Upgrade Your ISP Information.....	29
4. 9. PIN Management	30
4. 10. Data Settings	31
4. 11. USSD.....	32
 Chapter 5. SMS	 33
5. 1. View Messages.....	34
5. 2. Edit and Send a New Message	34
5. 3. View Sent Messages.....	35
5. 4. View Drafts	35
5. 5. SMS Settings	35
 Chapter 6. Customize Your Network Settings.....	 37
6. 1. Configure LAN Settings.....	38

6. 1. 1.	Change the LAN IP Address	38
6. 1. 2.	Use the Router as a DHCP Server.....	39
6. 1. 3.	Reserve LAN IP Addresses	40
6. 2.	Configure IPv6 LAN Settings.....	40
6. 2. 1.	Configure the RADVD Address Type.....	41
6. 2. 2.	Configure the DHCPv6 Server Address Type	41
6. 3.	Set Up a Dynamic DNS Service Account	42
6. 4.	Create Static Routes.....	43
6. 5.	RIP Settings	45
6. 6.	Specify Wireless Settings.....	46
6. 6. 1.	Change Basic Wireless Settings	46
6. 6. 2.	Advanced Wireless Settings.....	49
6. 6. 3.	View Wireless Information.....	52
6. 7.	Schedule Your Wireless Function	53
6. 8.	Use WPS for Wireless Connection	54

Chapter 7. TP-Link Cloud Service 57

7. 1.	Register a TP-Link ID.....	58
7. 2.	Change Your TP-Link ID Information.....	58
7. 3.	Manage the User TP-Link IDs	59
7. 3. 1.	Add TP-Link ID to Manage the Router.....	60
7. 3. 2.	Remove TP-Link ID(s) from Managing the Router.....	60
7. 4.	Manage the Router via the TP-Link Tether App	61

Chapter 8. EasyMesh with Seamless Roaming..... 62

8. 1.	Set Up a EasyMesh Network	63
8. 2.	Manage Devices in the EasyMesh Network.....	65

Chapter 9. Guest Network..... 67

9. 1.	Create a Network for Guests	68
9. 2.	Customize Guest Network Options.....	68

Chapter 10.NAT Forwarding..... 70

10. 1.	ALG	71
10. 2.	Set Up Public Services on The Local Network by Virtual Servers.....	71
10. 3.	Open Ports Dynamically by Port Triggering.....	73
10. 4.	Make Applications Free from Port Restriction by DMZ	75
10. 5.	Make Xbox Online Games Run Smoothly by UPnP	76

Chapter 11.Parental Controls	78
Chapter 12.Quality of Service	83
Chapter 13.Network Security	88
13. 1. Firewall & DoS Protection	89
13. 2. Service Filtering	90
13. 3. Access Control	91
13. 4. IP & MAC Binding	93
13. 5. IPv6 Firewall	95
Chapter 14.VPN Server&Client.....	97
14. 1. Use OpenVPN to Access Your Home Network.....	98
14. 2. Use PPTP VPN to Access Your Home Network	99
14. 3. Use IPSec VPN to Access Your Home Network	103
14. 4. VPN Connections.....	112
Chapter 15.Manage Your Router	113
15. 1. Set System Time	114
15. 2. Control the LED.....	115
15. 3. Test Internet Connectivity	115
15. 4. Update the Firmware.....	117
15. 5. Back Up and Restore Configuration Settings	118
15. 6. Reboot the Router	119
15. 7. Administration Management.....	120
15. 7. 1.Change the Login Password.....	120
15. 7. 2.Local Management	121
15. 7. 3.Remote Management	122
15. 7. 4.HTTP Referer Head Check	123
15. 7. 5.ICMP Ping	123
15. 7. 6.Session ID	124
15. 8. System Log.....	124
15. 9. Monitor the Internet Traffic Statistics.....	126
FAQ	127







About This Guide

This guide is a complement of Quick Installation Guide. The Quick Installation Guide instructs you on quick internet setup, and this guide provides details of each function and shows you the way to configure these functions appropriate to your needs.

Note: Features available in the router may vary by model and software version. Router availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual Router experience.

Conventions

In this guide the following conventions are used:

Convention	Description
<u>Underlined</u>	Underlined words or phrases are hyperlinks. You can click to redirect to a website or a specific section.
Teal	Contents to be emphasized and texts on the web page are in teal, including the menus, items, buttons, etc.
>	The menu structures to show the path to load the corresponding page. For example, Advanced > Wireless > WDS means the WDS function page is under the Wireless menu that is located in the Advanced tab.
 Note:	Ignoring this type of note might result in a malfunction or damage to the device.
 Tips:	Indicates important information that helps you make better use of your device.
symbols on the web page	<ul style="list-style-type: none"> Click to edit the corresponding entry. Click to delete the corresponding entry. click to enable or disable the corresponding entry. Click to view more information about items on the page.

More Info

The latest software, management app and utility can be found at [Download Center](https://www.tp-link.com/support/download/) at <https://www.tp-link.com/support/download/>.

The Quick Installation Guide can be found where you find this guide or inside the package of the router.

Specifications can be found on the product page at <https://www.tp-link.com>.

TP-Link Community is provided for you to discuss our products and share knowledge at <https://community.tp-link.com>.

Our Technical Support contact information can be found at the [Contact Technical Support](https://www.tp-link.com/support/) page at <https://www.tp-link.com/support/>.

*Maximum wireless signal rates are the physical rates derived from IEEE Standard 802.11 specifications. Actual wireless data throughput and wireless coverage are not guaranteed and will vary as a result of 1) environmental factors, including building materials, physical objects, and obstacles, 2) network conditions, including local interference, volume and density of traffic, product location, network complexity, and network overhead, and 3) client limitations, including rated performance, location, connection, quality, and client condition.

*Use of Wi-Fi 6 (802.11ax), and features including OFDMA, MU-MIMO, 1024-QAM, and HT160 require clients to also support the corresponding features.

*Saving clients' battery power requires clients to also support the 802.11ax Wi-Fi standard. Actual power reduction may vary as a result of network conditions, client limitations, and environmental factors.

*Use of WPA3 requires clients to also support the corresponding feature.

*This router may not support all the mandatory features as ratified in Draft 3.0 of IEEE 802.11ax specification.

*Further software upgrades for feature availability may be required.

Chapter 1

Get to Know About Your Modem Router

This chapter introduces what the modem router can do and shows its appearance.

It chapter contains the following sections:

- [Product Overview](#)
- [Appearance](#)

1.1. Product Overview

TP-Link's Router is a combined wired/wireless network connection device with integrated WAN router, reducing hassle of configuration and saving space.

With Ethernet ports and antennas, the router provides wired and wireless access for multiple computers and mobile devices.

With various features and functions, the modem router is the perfect hub of your home or business network.

Moreover, it is simple and convenient to set up and use the TP-Link router due to its intuitive Tether app and powerful web interface.

■ **Note:** The appearance of the product is for illustration only, and images may differ from your device, please refer to your actual product.







1.2. Appearance

1.2.1. Top Panel



The router's LEDs (view from top to bottom) are located on the front. You can check the router's working status by following the LED Explanation table.

Some Common LEDs Explanation

LED	Status	Indication
 (Signal Strength)	Solid white	The signal strength is above 75%.
	Solid green	The signal strength is between 50% and 75%.
	Solid yellow	The signal strength is below 50%.
	Off	No mobile network signal.
 (LAN)	On	At least one LAN port is connected.
	Off	No LAN port is connected or LAN port is not connected properly.
 (Wi-Fi)	On	At least one radio interface is enabled.
	Flashing	The WPS pairing is ongoing. If the connection is established successfully, it will return to solid white. If it is not successfully established, it will continue to flash for 2 minutes and then return to solid white. If Wi-Fi is turned off during WPS pairing, the Wi-Fi light will be off.
	Off	Both 2.4 GHz and 5 GHz radio interfaces are disabled.
 (Network Type)	Solid white	The device is on a 5G or 4G+ network (depending on the router).
	Solid green	The device is on a 4G network.
	Solid yellow	The device is on a 3G network.
	Off	The device is not registered on the network.
 (Internet)	On	Internet service is available.
	Off	The router's WAN port is unplugged, or the SIM card is not connected, or the SIM card is connected but dialing fails.
 (Power)	On	The system has started up successfully.
	Flashing	The system is starting up or the firmware is being upgraded. Do not disconnect or power off your router.
	Off	Power is off.

Note:

1. If the Signal Strength LED is off, please check your Internet connection first. Refer to [Connect the Hardware](#) for more information about how to make Internet connection correctly. If you have already made a right connection, please contact your ISP to make sure your Internet service is available now.
2. If the Internet LED is off, please check your Signal Strength LED first. If your Signal Strength LED is also off, please refer to [Note 1](#). If your Signal Strength LED is ON, please check your Internet configuration. You may need to check this part of information with your ISP and make sure everything have been input correctly.
3. If the Network Type LED is off, please check your Internet LED first. If the Internet LED is also off, please check your internet connection. If you have already made a right connection, please contact your ISP to make sure your 5G/4G network service is available.

1.2.2. The Back Panel



The following parts (view from top to bottom) are located on the back panel.

Some Common Buttons and Ports Explanation

Item	Description
RESET	Press and hold this button for at least 5 seconds until the Power LED blinks to reset the router to its factory default settings. The RESET button is actually a shared RESET/Wi-Fi button (short press for 5 seconds or less is for Wi-Fi function, long press for 5 seconds or more is for RESET function). A short press will cause the Wi-Fi in use to turn off.
WPS	Press the button to start a WPS synchronization.
LAN1, LAN2, LAN3/WAN Ports	For connecting the router to your PC or other Ethernet network devices. In wireless router mode, the WAN port is used for connecting to a Cable/FTTH/VDSL/ADSL device.
ON/OFF	The switch for the power. Press it to power on or off the router.
POWER	For connecting the modem router to power socket via the provided power adapter.

Chapter 2

Connect the Hardware

This chapter contains the following sections:

- [Position Your Router](#)
- [Connect Your Router](#)

2.1. Position Your Router

- The product should not be located in a place where it will be exposed to moisture or excessive heat.
- Place the router in a location where it can be connected to multiple devices as well as to a power source.
- Make sure the cables and power cord are safely placed out of the way so they do not create a tripping hazard.
- The router can be placed on a shelf or desktop.
- Keep the router away from devices with strong electromagnetic interference, such as Bluetooth devices, cordless phones and microwaves.
- Generally, the router is placed on a horizontal surface, such as on a shelf or desktop.
- Try relocating the router to a spot that may receive a stronger mobile network signal, such as near a window.

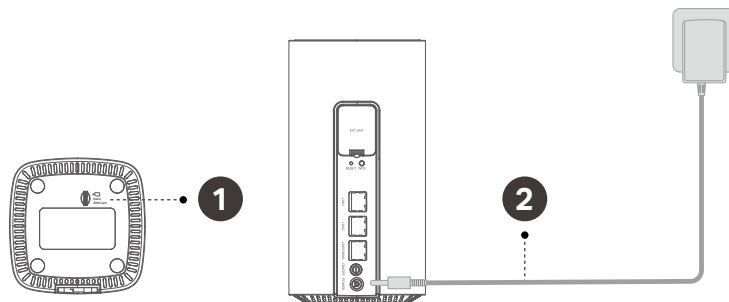
2.2. Connect Your Router

Before you start, turn off your modem, if any, and remove the backup battery if it has one. And place the router horizontally and orient the antennas vertically.

Follow the steps below to connect your router.

There are two dial-up Internet access methods: dial-up Internet access via Mobile WAN (SIM card), and dial-up Internet access via EWAN. You don't need to connect both Mobile WAN (SIM card) and EWAN.

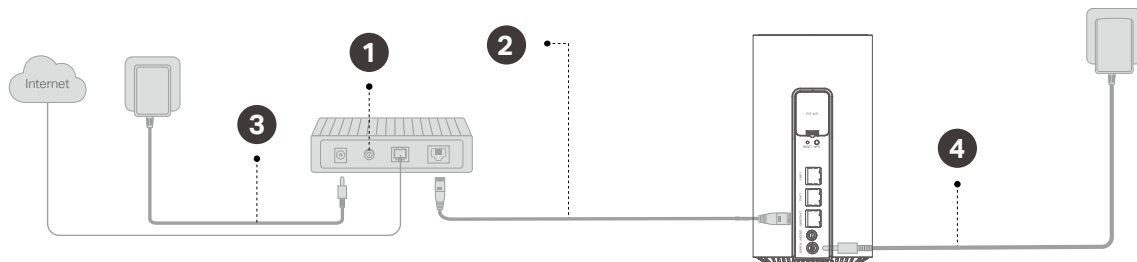
- **Method 1: Via Mobile WAN:**



1. With the gold contacts facing right, insert the nano SIM card into the slot until you hear a click.
2. Connect the power adapter to the router and turn on the router.

Method 2: Via EWAN

If your internet comes from an Ethernet outlet instead of a DSL / Cable / Satellite modem, connect the router's WAN/LAN port to it, then follow steps 4 and 5 to complete the hardware connection.



1. Turn off the modem, and remove the backup battery if it has one.
2. Connect the modem to the router's WAN port with an Ethernet cable.
3. Turn on the modem, and then wait about **2 minutes** for it to restart.
4. Connect the power adapter to the router and turn on the router.
5. Verify that the hardware connection is correct by checking the following LEDs.



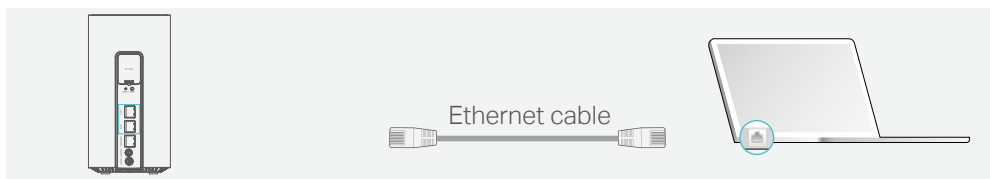
Note:

If the Internet LED and Wi-Fi LED are off, press and hold the RESET button on the back for more than 5 seconds to reset the router. Both the LEDs should turn solid on.

6. Connect your computer to the router.

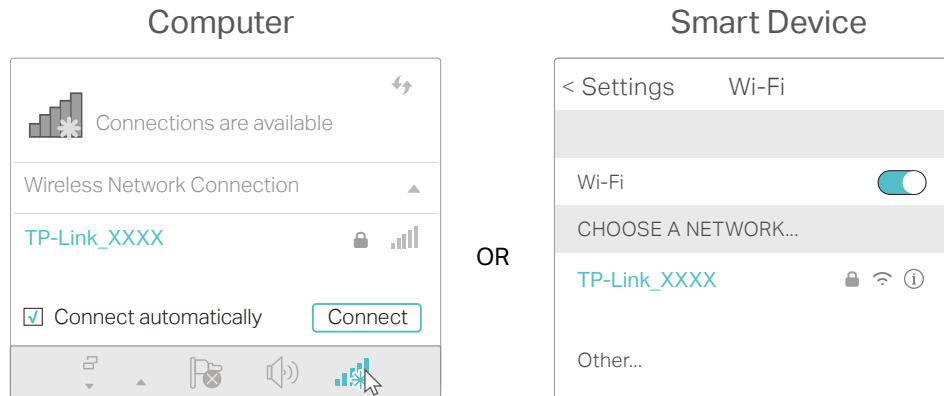
• Method 1: Wired

Turn off the Wi-Fi on your computer and connect the devices as shown below.



• Method 2: Wirelessly

- 1) Find the SSID (Network Name) and Wireless Password printed on the label at the bottom of the router.
- 2) Click the network icon of your computer or go to Wi-Fi Settings of your smart device, and then select the SSID to join the network.



- **Method 3: Use the WPS button**

Wireless devices that support WPS, including Android phones, tablets, and most USB network cards, can be connected to your router through this method.

Note:

- WPS is not supported by iOS devices.
- The WPS function cannot be configured if the wireless function of the router is disabled. Also, the WPS function will be disabled if your wireless encryption is WEP. Please make sure the wireless function is enabled and is configured with the appropriate encryption before configuring the WPS.

- 1) Tap the WPS icon on the device's screen. Here we take an Android phone for instance.
- 2) Within two minutes, press the WPS button on your router.

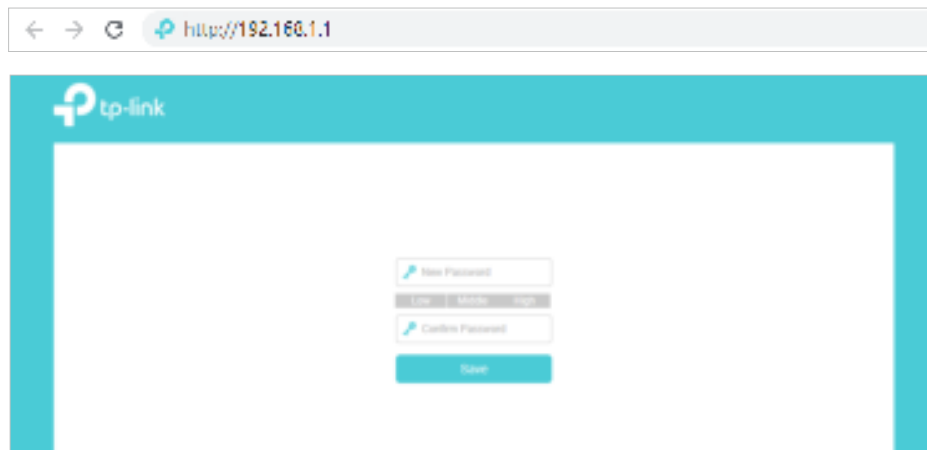
Chapter 3

Log In to Your Router

With a web-based utility, it is easy to configure and manage the router. The web-based utility can be used on any Windows, Mac OS or UNIX OS with a Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari.

Follow the steps below to log in to your router.

1. Set up the TCP/IP Protocol in [Obtain an IP address automatically](#) mode on your computer.
2. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and create a login password for secure management purposes. Then click [Save](#) to log in.



Note:

- If the login window does not appear, please refer to the [FAQ](#) Section.

Chapter 4

Set Up Internet Connection

This chapter introduces how to connect your router to the internet. The router is equipped with a web-based Quick Setup wizard. It has necessary ISP information built in, automates many of the steps and verifies that those steps have been successfully completed. Furthermore, you can also set up an IPv6 connection if your ISP provides IPv6 service.

It contains the following sections:

- [Use Quick Setup Wizard](#)
- [Quick Setup Via TP-Link Tether App](#)
- [Manually Set Up Your Internet Connection](#)
- [Test Internet Connectivity](#)
- [Set Up an IPv6 Internet Connection](#)
- [IPv6 Tunnel](#)
- [Create a Connection Profile](#)
- [Upgrade Your ISP Information](#)
- [PIN Management](#)
- [Data Settings](#)
- [USSD](#)

4.1. Use Quick Setup Wizard

The Quick Setup Wizard will guide you to set up your router.

🔗 Tips:

If you need the IPv6 internet connection, please refer to the section of [Set Up an IPv6 Internet Connection](#).

Follow the steps below to set up your router.

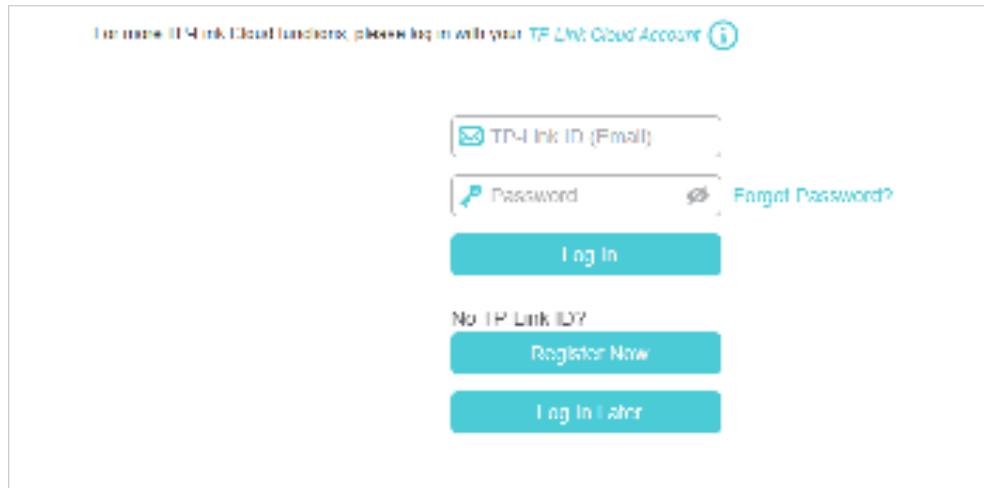
1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.



2. Follow the step-by-step instructions to complete Quick Setup configuration or go to [Quick Setup](#) for configuration to connect your router to the internet. Then follow the step-by-step instructions to connect your router to the internet.



3. To enjoy a more complete service from TP-Link (remote management, TP-Link DDNS, and more.), log in with your TP-Link ID or click [Register Now](#) to get one. Then follow the instructions to bind the cloud router to your TP-Link ID.

**Note:**

- To learn more about the TP-Link Cloud service, please refer to the [TP-Link Cloud Service](#) section.
- If you do not want to register a TP-Link ID now, you may click [Skip](#) to proceed.
- If you have changed the preset wireless network name (SSID) and wireless password during the Quick Setup process, all your wireless devices must use the new SSID and password to connect to the router.

4.2. Quick Setup Via TP-Link Tether App

The Tether 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 Tether” or simply scan the QR code to download and install the app.



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

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

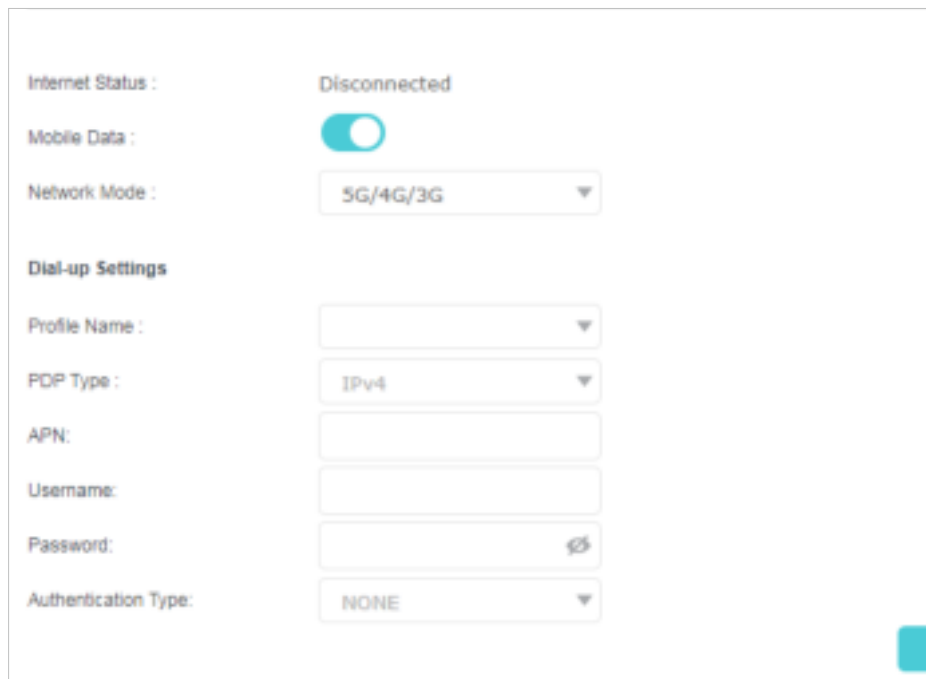
3. Tap the **+** button and select [Add a Router](#). In [Specific 4G/5G Routers](#), find this router and tap it.
4. Follow the steps to complete the setup and connect to the internet.
5. Connect your devices to the newly configured wireless networks of the router and enjoy the internet!

4.3. Manually Set Up Your Internet Connection

In this part, you can check your current internet connection settings. You can also modify the settings according to the service information provided by your ISP.

➤ **Dial-up Internet access via Mobile WAN:**

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Basic](#) > [Internet](#) page and select [MBB](#). You are recommended to keep the default value. If your ISP settings are not detected by the router, you can create an internet connection in [Advanced](#) > [Network](#) > [Mobile WAN](#).
3. Configure Dial-up settings.



The screenshot displays the 'Mobile WAN' configuration page. At the top, 'Internet Status' is 'Disconnected'. Below it, 'Mobile Data' is toggled on. 'Network Mode' is set to '5G/4G/3G'. The 'Dial-up Settings' section includes a 'Profile Name' dropdown, 'PDP Type' set to 'IPv4', and empty input fields for 'APN', 'Username', and 'Password'. The 'Authentication Type' is set to 'NONE'. A blue square button is visible in the bottom right corner of the form area.

- [Mobile Data](#) - It is enabled by default. You can disable it to prohibit Internet access.
 - [Network Mode](#) - The device supports three modes of network connection - 5G/4G/3G, 5G Only, 4G/3G, 4G Only, and 3G. You can select network mode according to your mobile network standard and the current network condition.
 - [Profile Name](#) - The name of the profile you've selected.
 - [PDP Type](#) - Select the type of your PDP (Packet Data Protocol).
 - [APN](#) - Access Point Name, provided by your ISP. You need to set APN only after selecting the static APN type. You are recommended to keep the default value.
 - [Username/Password](#) - Enter the username and password provided by your ISP. These fields are case-sensitive. You are recommended to keep the default value.
 - [Authentication Type](#) - Some ISPs need a specific authentication type, please confirm it with your ISP or keep the default value.
- [NONE](#) - No any authentication is needed.

PAP - Password Authentication Protocol. This protocol allows the device to establish authentication with the peer using two handshakes. Select this option if the ISP requires this authentication type.

CHAP - Challenge Handshake Authentication Protocol. This protocol allows the device to establish authentication with the peer using three handshakes and checking the peer identity periodically. Select this option if the ISP requires this authentication type.

PAP/CHAP - Password Authentication Protocol/Challenge Handshake Authentication Protocol. This protocol allows the device to establish authentication with the peer using two or three handshakes. Select this option if the ISP requires this authentication type.

➤ **Dial-up Internet access via EWAN:**

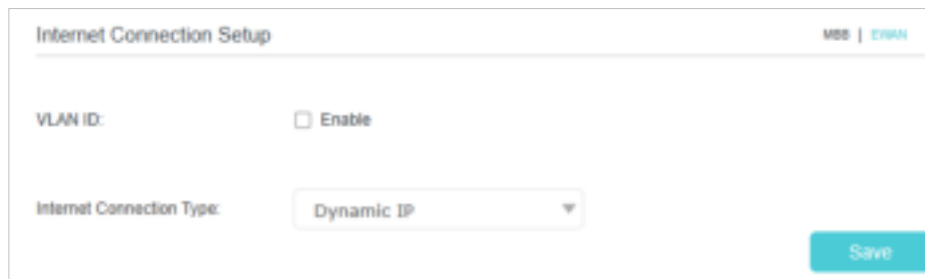
Follow the steps below to check or modify your internet connection settings.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Basic** > **Internet** page and select **EWAN**.
3. Follow the instructions on the page to continue the configuration. Parameters on the figures are just used for demonstration.

■ **Note:**


Since different connection types require different cables and connection information, you can also refer to the demonstrations to determine your connection type.

- 1) If you choose **Dynamic IP**, the IP address and Subnet Mask are assigned automatically by the ISP. Dynamic IP users are usually equipped with a cable TV or fiber cable.



The screenshot shows the 'Internet Connection Setup' page. At the top right, there is a breadcrumb trail 'Basic > Internet'. Below this, there is a section for 'VLAN ID' with an 'Enable' checkbox. Further down, the 'Internet Connection Type' is set to 'Dynamic IP' in a dropdown menu. A 'Save' button is located at the bottom right of the form.

- 2) If you choose **Static IP**, enter the information provided by your ISP in the corresponding fields.



Internet Connection Setup MSS | EMMAN

VLAN ID: ☐ Enable

Internet Connection Type: Static IP ▼

IP Address:

Subnet Mask:


Default Gateway:

Primary DNS:

Secondary DNS: (Optional)

Save

- 3) If you choose [PPPoE](#), enter the [username](#) and [password](#) provided by your ISP. PPPoE users usually have DSL cable modems.



Internet Connection Setup MSS | EMMAN

VLAN ID: ☐ Enable

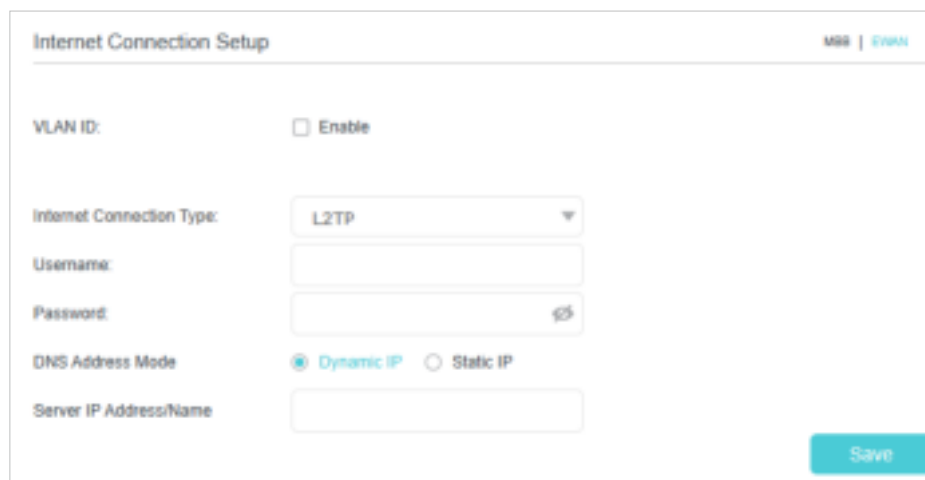
Internet Connection Type: PPPoE ▼

Username:

Password:

Save

- 4) If you choose [L2TP](#), enter the [username](#) and [password](#) and choose the [Secondary Connection](#) provided by your ISP. Different parameters are needed according to the Secondary Connection you have chosen.



Internet Connection Setup MSS | EMMAN

VLAN ID: ☐ Enable

Internet Connection Type: L2TP ▼

Username:

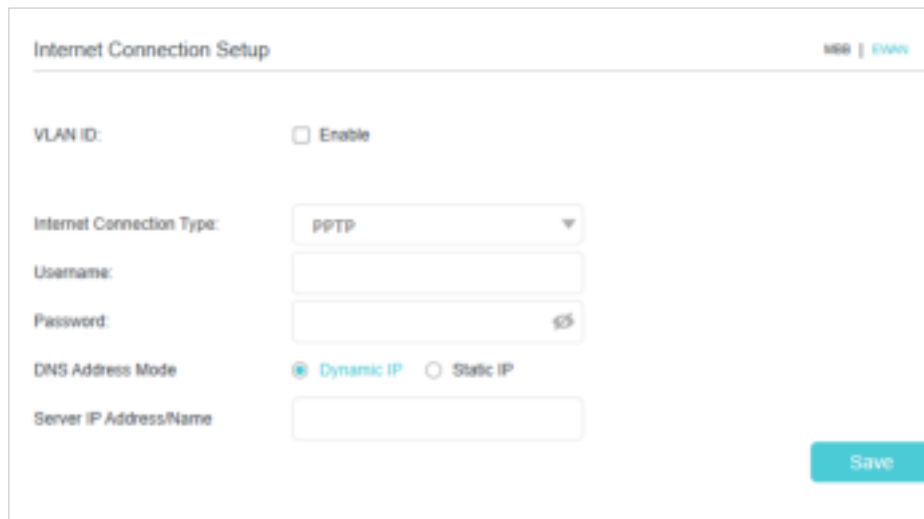
Password:

DNS Address Mode: ☒ Dynamic IP ☐ Static IP

Server IP Address/Name:

Save

- 5) If you choose **PPTP**, enter the **username** and **password**, and choose the **Secondary Connection** provided by your ISP. Different parameters are needed according to the Secondary Connection you have chosen.



4. Click **Save**.

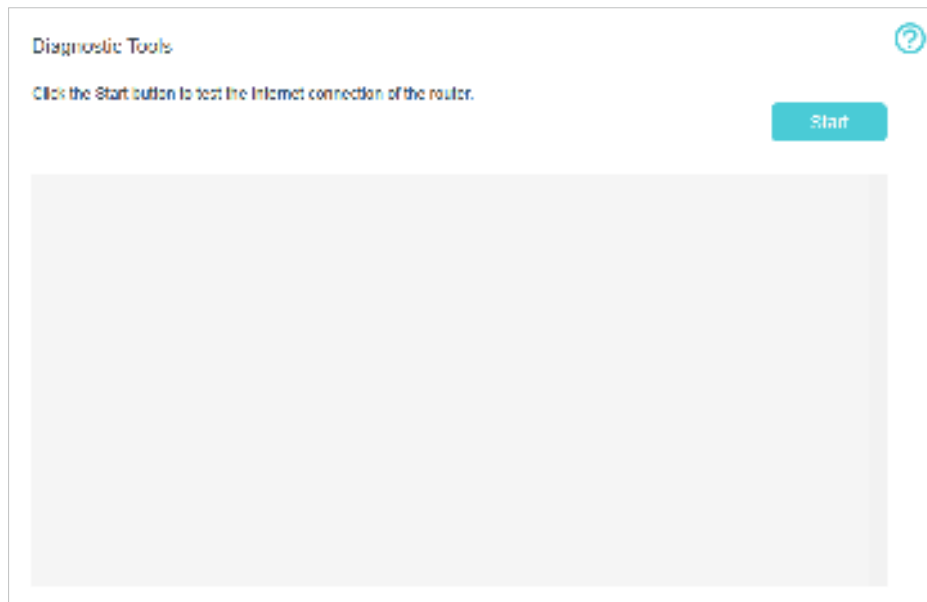
 **Tips:**

- If you use **Dynamic IP** and **PPPoE** and you are provided with any other parameters that are not required on the page, please go to **Advanced > Network > Internet** to complete the configuration.
- If you still cannot access the internet, refer to the [FAQ](#) section for further instructions.

4.4. Test Internet Connectivity

After manually set up the internet connection, you need to know the internet connectivity. The router provides a diagnostic tool to help you locate the malfunction.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > System Tools > Diagnostics** page.



3. Click **Start** to test the internet connectivity and you will see the test result in the gray box.

4.5. Set Up an IPv6 Internet Connection

Your ISP provides information about one of the following IPv6 internet connection types: PPPoE(SLAAC/DHCPv6/AUTO/Passthrough), Dynamic IP(SLAAC/DHCPv6/AUTO/Passthrough), Static IP.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > Network > Internet**.

Default Gateway

Default Gateway

Auto

WAN Priority

☐ None ☐ EWAN ☒ MBB

DNS Lookup:

(Optional)

IPv4 Ping:

0 . 0 . 0 . 0

(Optional)

IPv6 Ping:

::

(Optional)

save

Internet Setup

Refresh

Add

Delete All

Connection Name	Service Type	VLAN ID	Status	Operation	Enable	Modify
ipoe_0_0_d	Internet	N/A	Disconnected	Connect		

3. Click [Add](#) and enable IPv6 and select the internet connection type provided by your ISP.

Tips:

If you do not know what your internet connection type is, contact your ISP or judge according to the already known information provided by your ISP.

4. Fill in information as required by different connection types.

1) [Static IP](#): Fill in blanks and click [OK](#).

Connection Name: (Optional)

☒ Enable This Entry

Service Type: ☒ Internet ☐ IPTV ☐ TR069 ☐ Others

Default Gateway:

Internet Connection Type:

VLAN ID: ☐ Enable

IPv4: ☒ Enable

IP Address:

Subnet Mask:

Default Gateway:

Primary DNS:

Secondary DNS: (Optional)

IPv6: ☒ Enable

IPv6 Address:

Prefix Length:

IPv6 Gateway:

IPv6 DNS Server:

Secondary DNS: (Optional)

IPv6 Tunnel: ☐ Enable

- 2) [Dynamic IP\(SLAAC/DHCPv6/AUTO/Passthrough\)](#): Click [Advanced](#) to input further information if your ISP requires. Click [OK](#).

Connection Name: (Optional)

☒ Enable This Entry

Service Type: ☒ Internet ☐ IPTV ☐ TR069 ☐ Others

Default Gateway:

Internet Connection Type:

VLAN ID: ☐ Enable

IPv4: ☒ Enable

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

IPv6: ☒ Enable

IPv6 Address: ::

Prefix Length: 64

IPv6 Gateway: ::

Addressing Type:

IPv6 Tunnel: ☐ Enable

- 3) PPPOE(SLAAC/DHCPv6/AUTO/Passthrough): Click [Advanced](#) to input further information if your ISP requires. Click [OK](#).

Connection Name: (Optional)

☒ Enable This Entry

Service Type: ☒ Internet ☐ IPTV ☐ TR069 ☐ Others

Default Gateway:

Internet Connection Type:

VLAN ID: ☐ Enable

Username:

Password:

Confirm Password:

Connection Mode: ☒ Auto ☐ On Demand ☐ Manually

Authentication Type:

IPv4: ☒ Enable

IPv6: ☒ Enable

Addressing Type:

IPv6 Tunnel: ☐ Enable

5. Configure LAN ports. Go to [Advanced](#) > [Network](#) > [LAN Settings](#). Fill in [Site Prefix Type](#) provided by your ISP, and click [Save](#).

DHCP Server IPv4 **IPv6**

Group:

IPv6 LAN: ☒ Enable

Address Type: ☒ RADVD ☐ DHCPv6 Server

Enable RDNS: ☐ Enable

Enable ULA Prefix: ☐ Enable

Lifetime: ☐ Enable

Site Prefix Type:

Static: ☐ Static

WAN Connection:

6. Click [Advanced](#) > [Status](#) to check whether you have successfully set up an IPv6 connection.

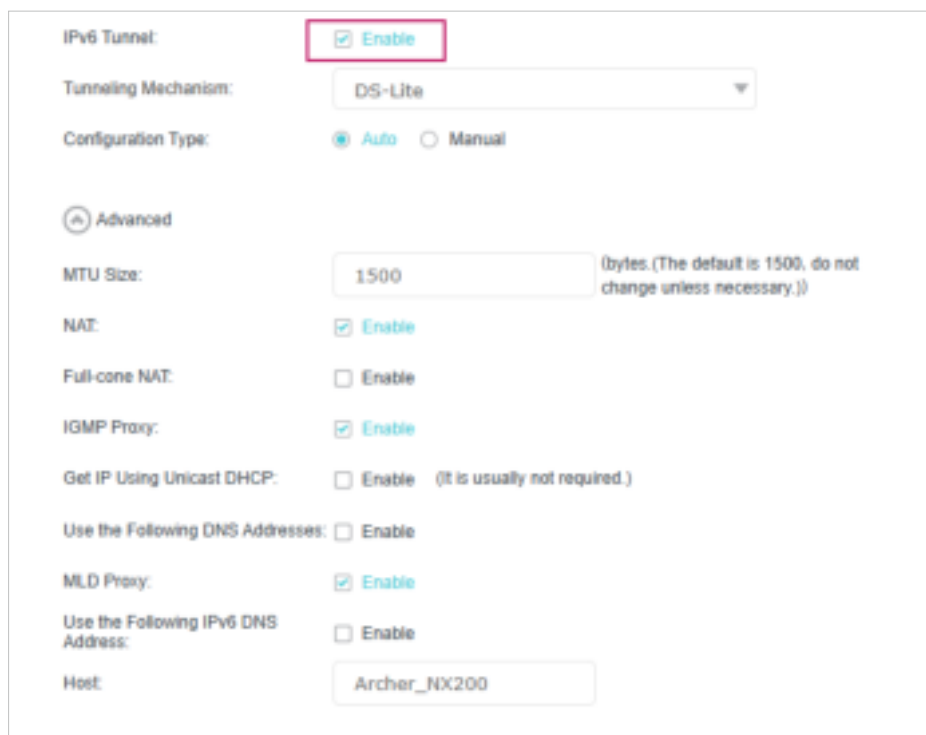
🔗 Tips:

Visit the [FAQ](#) section if there is no internet connection.

4.6. IPv6 Tunnel

IPv6 Tunnel is a transition mechanism that enables IPv6-only hosts to reach IPv4 services or vice versa and allows isolated IPv6 hosts and networks to reach each other over IPv4-only infrastructure before IPv6 completely supplants IPv4. It is a temporary solution for networks that do not support native dual-stack, where both IPv6 and IPv4 run independently.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [Network](#) > [Internet](#).
3. Click [Add](#) and enable IPv6 and Click [Advanced](#) to view more advanced settings.
4. Select the checkbox to enable IPv6 Tunnel.



IPv6 Tunnel: ☒ Enable

Tunneling Mechanism: DS-Lite

Configuration Type: ☒ Auto ☐ Manual

ⓘ Advanced

MTU Size: 1500 (bytes. (The default is 1500, do not change unless necessary.))

NAT: ☒ Enable

Full-cone NAT: ☐ Enable

IGMP Proxy: ☒ Enable

Get IP Using Unicast DHCP: ☐ Enable (It is usually not required.)

Use the Following DNS Addresses: ☐ Enable

MLD Proxy: ☒ Enable

Use the Following IPv6 DNS Address: ☐ Enable

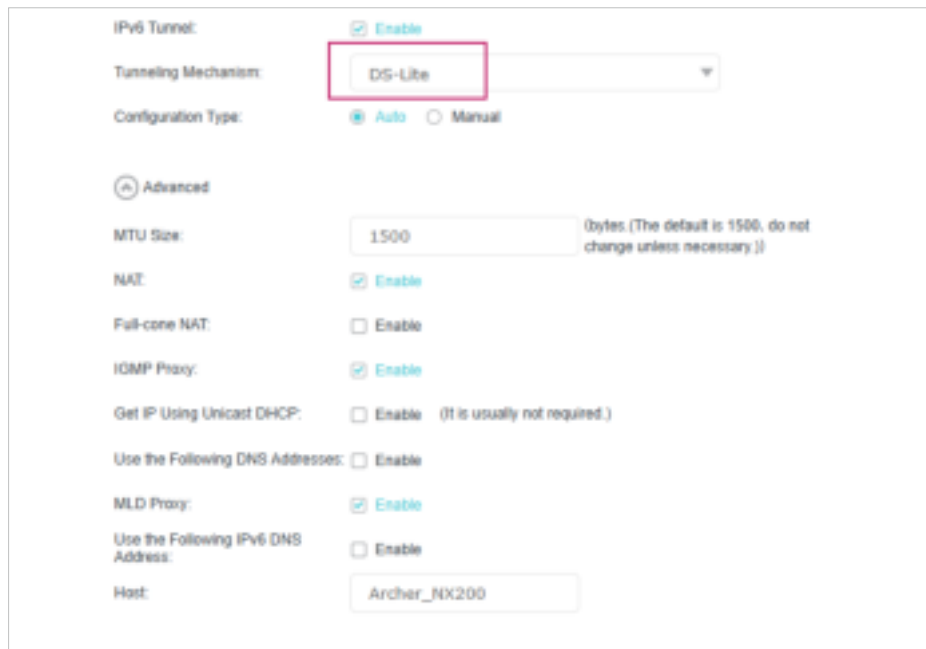
Host: Archer_NX200

📌 Tips:

Please check the IPv6 tunnel settings each time while reconfiguring WAN connection, as WAN connection configuration may take effect on tunnel settings.

5. Fill in information as required by different tunneling mechanisms.

- 1) **DS-Lite**: Fill in blanks and click **OK**. Select this tunneling mechanism if your ISP uses DS-Lite deployment for assigning address.



IPv6 Tunnel: ☒ Enable

Tunneling Mechanism: DS-Lite

Configuration Type: ☒ Auto ☐ Manual

MTU Size: (bytes (The default is 1500, do not change unless necessary.))

NAT: ☒ Enable

Full-cone NAT: ☐ Enable

IGMP Proxy: ☒ Enable

Get IP Using Unicast DHCP: ☐ Enable (It is usually not required.)

Use the Following DNS Addresses: ☐ Enable

MLD Proxy: ☒ Enable

Use the Following IPv6 DNS Address: ☐ Enable

Host:

- 2) [6rd](#): Fill in blanks and click [OK](#). Select this tunneling mechanism if your ISP uses 6rd deployment for assigning address.



IPv6 Tunnel: ☒ Enable

Tunneling Mechanism: 6rd

Configuration Type: ☐ Auto ☒ Manual

IPv4 Mask Length:

6rd Prefix:

6rd Prefix Length:

Border Relay IPv4 Address:

MTU Size: (bytes (The default is 1500, do not change unless necessary.))

NAT: ☒ Enable

Full-cone NAT: ☐ Enable

IGMP Proxy: ☒ Enable

Get IP Using Unicast DHCP: ☐ Enable (It is usually not required.)

Use the Following DNS Addresses: ☐ Enable

MLD Proxy: ☒ Enable

Use the Following IPv6 DNS Address: ☐ Enable

Host:

- 3) [6to4](#): Fill in blanks and click [OK](#). Select this tunneling mechanism if your ISP uses 6to4 deployment for assigning address.



IPv6 Tunnel: ☒ Enable

Tunneling Mechanism: 6to4

☒ Advanced

MTU Size: (bytes. (The default is 1500, do not change unless necessary.))

NAT: ☒ Enable

Full-cone NAT: ☐ Enable

IGMP Proxy: ☒ Enable

Get IP Using Unicast DHCP: ☐ Enable (It is usually not required.)

Use the Following DNS Addresses: ☐ Enable

MLD Proxy: ☒ Enable

Use the Following IPv6 DNS Address: ☐ Enable

Host:

- 4) [MAP-T](#): Fill in blanks and click [OK](#). Select this tunneling mechanism if your ISP uses MAT-P deployment for assigning address



IPv6 Tunnel: ☒ Enable

Tunneling Mechanism: MAP-T

Configuration: ☒ Auto ☐ Static

☒ Advanced

MTU Size: (bytes. (The default is 1500, do not change unless necessary.))

NAT: ☒ Enable

Full-cone NAT: ☐ Enable

IGMP Proxy: ☒ Enable

Get IP Using Unicast DHCP: ☐ Enable (It is usually not required.)

Use the Following DNS Addresses: ☐ Enable

MLD Proxy: ☒ Enable

Use the Following IPv6 DNS Address: ☐ Enable

Host:

4. 7. Create a Connection Profile

If your ISP settings are not detected by the router, you can create an internet connection profile by following the steps below:

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [Network](#) > [Mobile WAN](#) page.

The screenshot shows the 'Mobile WAN' configuration page. At the top, it says 'Mobile WAN'. Below this, there are several settings:

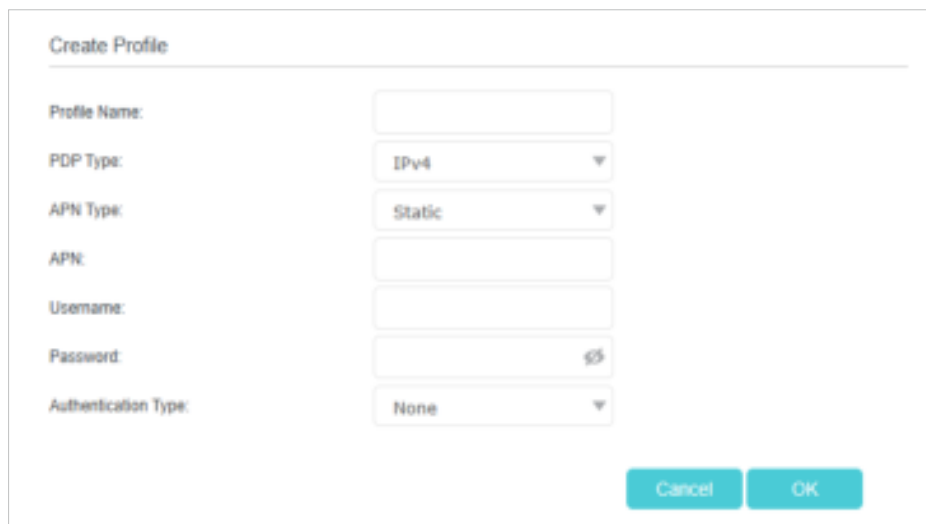
- Internet Status :** Disconnected
- Mobile Data :** ☒
- Data Roaming:** ☐
- NAT:** ☒
- External Antennas:** ☐
- Network Mode :** 5G/4G/3G (dropdown menu)
- Band Search:** Auto (dropdown menu)
- Network Search:** Auto (dropdown menu)
- Dial-up Settings**
 - Profile Name:** (dropdown menu)
 - PDP Type:** IPv4 (dropdown menu)
 - APN Type:** Static (dropdown menu)
 - APN:** (text input field)
 - Username:** (text input field)
 - Password:** (password input field with an eye icon)
 - Authentication Type:** None (dropdown menu)

At the bottom left, there is a [Create Profile](#) link with the text 'Click this button to create a new dial-up profile. Up to 8 profiles can be added.' At the bottom right, there are two buttons: 'delete' and 'Save'.

🔗 Tips:

- You can also upgrade the supported ISP information. Refer to [Upgrade Your ISP Information](#) to configure.
- You can view all internet connections or edit connections that are set up manually on this page.
- You can change the [Network Mode](#) to [5G/4G/3G](#), [5G Only](#), [4G/3G,4G Only](#) or [3G](#) according to your needs.
- You can manually select 5G and 4G bands in [Band Search](#) setting.
- If the [Auto](#) network connection displays a wrong ISP profile, you can select a correct network manually:
 1. Change the [Network Search](#) mode to [Manual](#).
 2. When prompted, select the correct ISP network and click [Save](#).

3. Click [Create Profile](#).
4. Specify the [Profile Name](#), [Username](#) and [Password](#). Select the [PDP Type](#), [APN Type](#) and [Authentication Type](#) according to your ISP.

A dialog box titled "Create Profile" with a light gray border. It contains several input fields and dropdown menus. The fields are: "Profile Name:" (text input), "PDP Type:" (dropdown menu with "IPv4" selected), "APN Type:" (dropdown menu with "Static" selected), "APN:" (text input), "Username:" (text input), "Password:" (password input with a toggle icon), and "Authentication Type:" (dropdown menu with "None" selected). At the bottom right, there are two buttons: "Cancel" and "OK".

Create Profile

Profile Name:

PDP Type:

APN Type:

APN:

Username:

Password:

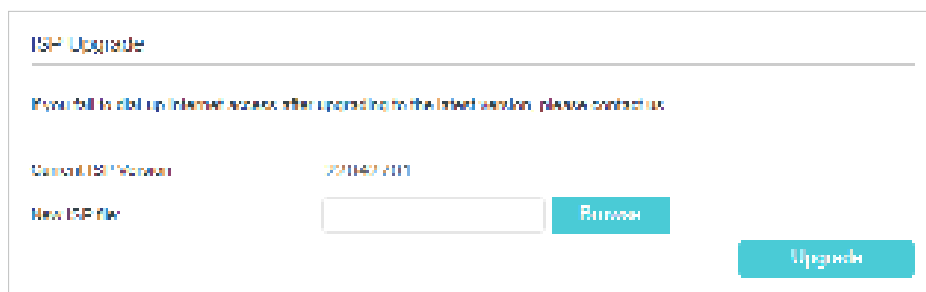
Authentication Type:

5. Click **OK** to make the settings effective and the new profile will be used to set up a new connection.

4.8. Upgrade Your ISP Information

If your ISP information is not detected by the router, you can upgrade ISP information by following the steps below:

1. Download the latest ISP upgrade file from the [Support](#) page at <https://www.tp-link.com> to your computer.
2. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router.
3. Go to **Advanced > Network > ISP Upgrade**.

A dialog box titled "ISP Upgrade" with a light gray border. It contains a message: "If you fail to dial up Internet access after upgrading to the latest version, please contact us". Below the message, it shows "Current ISP Version: 2210497/2011". There is a "New ISP file:" label followed by a text input field and a "Browse" button. At the bottom right, there is an "Upgrade" button.

ISP Upgrade

If you fail to dial up Internet access after upgrading to the latest version, please contact us.

Current ISP Version: 2210497/2011

New ISP file:

4. Click **Browse** to locate and select the latest file.
5. Click **Upgrade**.

Note:

1. If you fail to dial-up Internet access after upgrading to the latest version, please contact the technical support.
2. If your ISP settings are still not detected after upgrading, refer to [Create a Connection Profile](#) to add a new internet connection profile.

4.9. PIN Management

PIN (Personal Identification Number) is used to protect the SIM card from embezzlement. PIN Management allows you to easily change the PIN settings of your SIM card as needed.

Follow the steps below to change your PIN settings.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [Network](#) > [PIN Management](#) page.

The screenshot shows the 'PIN Management' web interface. At the top, there's a title 'PIN Management'. Below it, there are two status indicators: 'SIM Card Status' and 'SIM card prepared'. The 'PIN Lock' toggle is turned on. The 'Auto unlock PIN' toggle is also turned on. There is a text input field for the 'PIN' and a 'Remaining Attempts: 3' indicator. A 'Save' button is located at the bottom right.

- [SIM Card Status](#) - Displays the status of your SIM card.
 - [PIN Lock](#) - Toggle on to enable PIN Lock. Once it is enabled, every time you start the router with this SIM card inserted, you need to enter the PIN.
 - [Auto-unlock PIN](#) - When the PIN is required upon router restarting or inserting a SIM card, it will be validated automatically, saving you the trouble to enter the PIN each time you start the router or insert a SIM card. If validation failed, you need to enter the PIN on this page.
 - [PIN](#) - Enter the PIN to unlock the SIM card. It consists of 4-8 digits.
 - [PUK](#) - PIN Unlocked Key, also known as Personal Unlock Code (PUC), is used to reset a PIN that has been lost or forgotten. The PUK is a SIM-specific code assigned by the service provider. You need to enter the PUK after 3 incorrect login attempts of PIN. Contact your service provider if you do not know the PUK. It consists of 8 digits.
 - [New PIN](#) - Enter 4-8 digits to reset the PIN of your SIM card.
 - [Remaining Attempts](#) - Shows how many attempts are left for you to try entering the PIN or PUK. You have only 3 attempts for entering the PIN and 10 attempts for entering the PUK. If you accidentally fail in 3 attempts, the SIM card will be locked and you will be required to enter the PUK that is written on your SIM card.
3. Click [Save](#) to save the settings.

4. 10. Data Settings

Data Settings is used to monitor the data usage of your router in real-time. You can limit your data usage according to your monthly allowance or total allowance and you will receive a warning if your data usage reaches the specified level.

Follow the steps below to monitor your data usage.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [Network](#) > [Data Settings](#) page.



The screenshot shows the 'Data Settings' page. At the top, it displays 'Monthly Used: 0.000 MB' with a 'Correct' button. Below this is a note: 'You can send messages to your carrier for accurate data usage.' The 'Data Limit' toggle is turned on, with a sub-note: 'The router will automatically disconnect from the network when the data usage limit is reached.' The 'Monthly Allowance' field is empty, with a unit dropdown set to 'MB'. The 'Usage Alert' field is set to '90 %'. The 'SMS Alert for Usage' field is empty, with a 'Send Test Message' button and a note: 'Note: This function may cause SMS charges.' The 'Monthly Data Statistics' toggle is turned on, and the 'Start Date' field is set to '1'. A 'Save' button is at the bottom right.

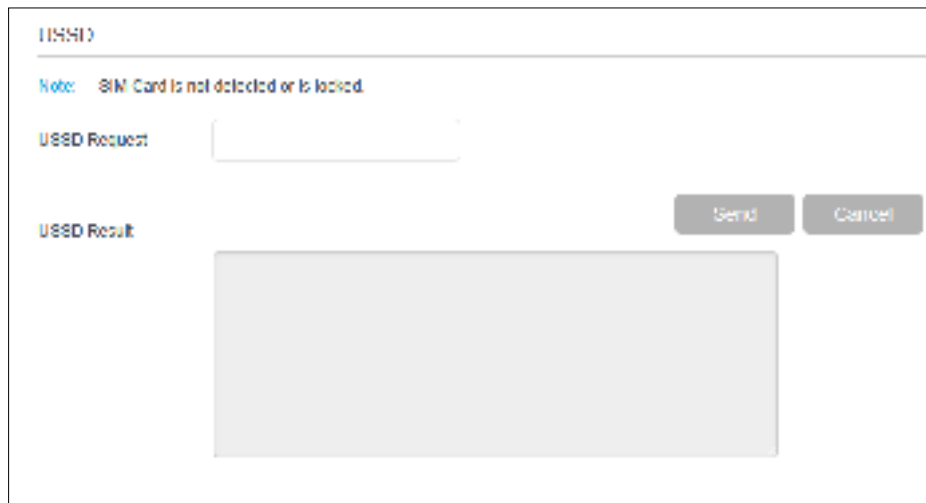
3. Enable [Data Limit](#) to set total/monthly data allowance and usage alert to prevent data overuse.
4. Enter the allowed amount of total/monthly data in the [Total/Monthly Allowance](#) field. When data usage exceeds the allowed level, the router will disconnect from the internet and notify you on the [Basic](#) > [Network Map](#) Page.
5. Enter a percentage in the [Usage Alert](#) field to prevent data overuse. When data usage reaches the alert level, a warning will be shown on the [Basic](#) > [Network Map](#) Page. If you want to receive the alert on your phone, enter your mobile phone number in the [SMS Alert for Usage](#) field.
6. Enable [Monthly Data Statistics](#) to reset data statistics when the next billing cycle starts.
7. Enter the start date of the billing cycle in the [Start Date](#) field.
8. Click [Save](#) to save the settings.

4.11. USSD

USSD (Unstructured Supplementary Service Data) is used to communicate with the service provider's computer. You can query service data on this page.

Follow the steps below to get service data.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [Network](#) > [USSD](#) page.



The screenshot shows the 'USSD' configuration page. At the top, there is a title 'USSD'. Below it, a note in red text states: 'Note: SIM Card is not detected or is locked.' There is a label 'USSD Request' followed by a text input field. To the right of the input field are two buttons: 'Send' and 'Cancel'. Below the input field is a label 'USSD Result' followed by a large, empty rectangular box for displaying the result.

3. Enter the USSD request and click [Send](#). You will see the message returned from the carrier in the [USSD Result](#) box.

Chapter 5

SMS

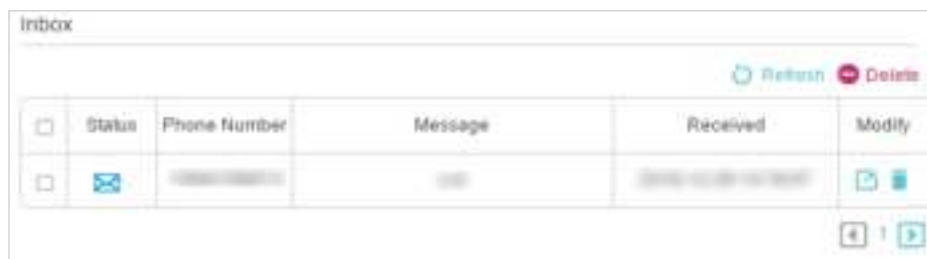
This chapter introduces how to use the SMS functions to view and write messages, keep drafts and specify the message center number. You can easily monitor your data usage by sending a message to your carrier.



This chapter includes the following sections:

- [View Messages](#)
- [Edit and Send a New Message](#)
- [View Sent Messages](#)
- [View Drafts](#)
- [SMS Settings](#)

5.1. View Messages

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [SMS](#) > [Inbox](#) page.



3. Click the  or  icon to unfold and read the content of the message.

ⓘ Tips:

 indicates the message is read, while  indicates the message is unread.

5.2. Edit and Send a New Message

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [SMS](#) > [New Message](#) page.

3. Enter the receiver's phone number in the [Phone Number](#) field.
4. Enter your message in the [Content](#) field.

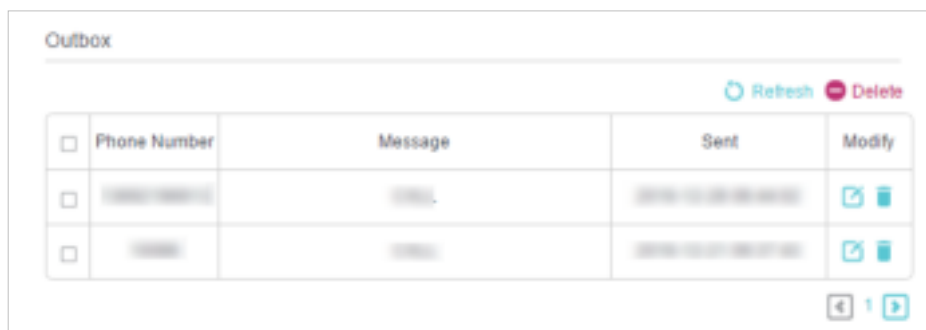
ⓘ Tips:

You can enter up to 160 letters or numbers, and any exceeding characters will be sent in the next message. You can send up to 5 messages each time.

- Click [Send](#) to send the message or click [Save](#) to save the message to the Drafts.

5.3. View Sent Messages

- Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
- Go to [Advanced](#) > [SMS](#) > [Outbox](#) page. All the messages you sent are listed in the [Outbox](#) table.



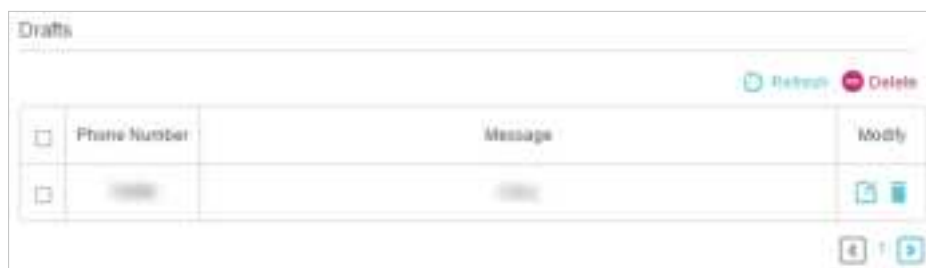
<input type="checkbox"/>	Phone Number	Message	Sent	Modify
<input type="checkbox"/>	15888888888	15888888888	2016-10-20 10:10:10	Edit Delete
<input type="checkbox"/>	15888888888	15888888888	2016-10-20 10:10:10	Edit Delete

Tips:

You can click [Edit](#) to edit and forward the message.

5.4. View Drafts

- Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
- Go to [Advanced](#) > [SMS](#) > [Drafts](#) page. All the unsent messages are listed in the [Drafts](#) table.



<input type="checkbox"/>	Phone Number	Message	Modify
<input type="checkbox"/>	15888888888	15888888888	Edit Delete

Tips:

You can click [Edit](#) to edit and forward the message.

5.5. SMS Settings

SMS Settings allows you to configure the Message Center. When the Message Center is enabled, you can change the Message Center Number via which messages will be

sent. It is not recommended to change it for a wrong message center number will affect the SMS function of the router.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [SMS](#) > [SMS Settings](#) page and enable [Message Center](#).



3. The [Message Center Number](#) is auto-populated. Change it according to your needs.
4. Click [Save](#) to apply your settings.

Chapter 6

Customize Your Network Settings

This chapter introduces how to change the default settings or adjust the basic configuration of the router using the web management page.

It contains the following sections:

- [Configure LAN Settings](#)
- [Configure IPv6 LAN Settings](#)
- [Set Up a Dynamic DNS Service Account](#)
- [Create Static Routes](#)
- [RIP Settings](#)
- [Specify Wireless Settings](#)
- [Schedule Your Wireless Function](#)
- [Use WPS for Wireless Connection](#)

6.1. Configure LAN Settings

6.1.1. Change the LAN IP Address

The router is preset with a default LAN IP 192.168.1.1, which you can use to log in to its web management page. The LAN IP address together with the Subnet Mask also defines the subnet that the connected devices are on. If the IP address conflicts with another device in your local network or your network requires a specific IP subnet, you can change it.

Follow the steps below to change your IP address.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [Network](#) > [LAN Settings](#) page and select [IPv4](#).



DHCP Server

MAC Address: 74:FE:CE:B7:F5:27

IP Address: 192 - 168 - 1 - 1

Subnet Mask: 255.255.255.0

IGMP Snooping: ☒ Enable

Second IP: ☐ Enable

3. Enter a new [IP Address](#) appropriate to your needs.
4. Select the [Subnet Mask](#) from the drop-down list. The subnet mask together with the IP address identifies the local IP subnet.
5. Keep [IGMP Snooping](#) enabled by default. IGMP snooping is the process of listening to IGMP (Internet Group Management Protocol) network traffic. The function prevents hosts on a local network from receiving traffic for a multicast group they have not explicitly joined.
6. You can configure the router's [Second IP](#) and [Subnet Mask](#) for LAN interface through which you can also access the web management page.
7. Keep the rest settings as the default settings.
8. Click [Save](#) to make the settings effective.

6.1.2. Use the Router as a DHCP Server

You can configure the router to act as a DHCP server to assign IP addresses to its clients. To use the DHCP server function of the router, you must configure all computers on the LAN to obtain an IP Address automatically.

Follow the steps below to configure DHCP server.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [Network](#) > [LAN Settings](#) page and select [IPv4](#).



The screenshot shows the DHCP configuration interface. At the top, there is a toggle switch for 'DHCP' which is turned on (labeled 'Enable'). Below this, there are two radio buttons: 'DHCP Server' (which is selected) and 'DHCP Relay'. The 'IP Address Pool' is configured with a start address of 192.168.1.2 and an end address of 192.168.1.249. The 'Address Lease Time' is set to 120 minutes, with a note indicating the range is 1-255 minutes and the default is 120. The 'Default Gateway', 'Default Domain', 'Primary DNS', and 'Secondary DNS' are all set to 0.0.0.0, with a note '(Optional)' next to each. A 'Save' button is located at the bottom right of the form.

3. Enable [DHCP](#) function and select [DHCP Server](#).
4. Specify the [IP Address Pool](#), the start address and end address must be on the same subnet with LAN IP. The router will assign addresses within this specified range to its clients. It is from 192.168.1.2 to 192.168.1.249 by default.
5. Enter a time duration in the [Address Lease Time](#) field. The [Address Lease Time](#) is the amount of time in which a DHCP client can lease its current dynamic IP address assigned by the router. After the dynamic IP address expires, the user will be automatically assigned a new dynamic IP address.
6. Keep the rest settings as the default settings and click [Save](#).

Note:

1. The router can be configured to work as a [DHCP Relay](#). A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. If it is enabled, the DHCP requests from local PCs will be forwarded to the DHCP server that runs on WAN side.
2. You can also appoint IP addresses within a specified range to devices of the same type by using [Condition Pool](#) feature. For example, you can assign IP addresses within the range (192.168.1.50 to 192.168.1.80) to Camera devices, thus facilitating the network management. Enable DHCP feature and configure the parameters according to your situation on the [Advanced](#) > [Network](#) > [LAN Settings](#) page.

6.1.3. Reserve LAN IP Addresses

You can view and add a reserved address for a client. When you specify an IP address for a device on the LAN, that device will always receive the same IP address each time when it accesses the DHCP server. If there are some devices in the LAN that require permanent IP addresses, please configure Address Reservation on the router for the purpose.

Follow the steps below to reserve an IP address for your devices.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [Network](#) > [LAN Settings](#) page, and select [IPv4](#).
3. Scroll down to the [Address Reservation](#) section, and click [Add](#) to add an address reservation entry for your device.

MAC Address	Reserved IP Address	Group	Enable	Modify
-------------	---------------------	-------	--------	--------

MAC Address:

IP Address:

Group:

☐ Enable This Entry

4. Enter the [MAC Address](#) of the device for which you want to reserve IP address.
5. Specify the [IP address](#) which will be reserved by the router.
6. Select the [Enable This Entry](#) check box and click [OK](#) to make the settings effective.

6.2. Configure IPv6 LAN Settings

Based on the IPv6 protocol, the router provides two ways to assign IPv6 LAN addresses:

- Configure the RADVD (Router Advertisement Daemon) address type
- Configure the DHCPv6 Server address type

6.2.1. Configure the RADVD Address Type

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [Network](#) > [LAN Settings](#).
3. Select [IPv6](#) to configure IPv6 LAN parameters.

DHCP Server

IPv6

Group: Default

IPv6 LAN: ☒ Enable

Address Type: ☒ RADVD ☐ DHCPv6 Server

Enable RDNSS: ☐ Enable

Enable ULA Prefix: ☐ Enable

Lifetime: ☐ Enable

Site Prefix Type: ☒ Delegated ☐ Static

WAN Connection: HBB

Save

- 1) Select [RADVD](#) as the address type to make the router assign IPv6 address prefixes to hosts.
- Note:
- Do not select the [Enable RDNSS](#) and [Enable ULA Prefix](#) check boxes unless required by your ISP. Otherwise you may not be able to access the IPv6 network. For more information about RDNSS and ULA Prefix, contact our technical support.
- 2) Keep [Site Prefix Type](#) as the default setting [Delegated](#). If your ISP has provided a specific IPv6 site prefix, select [Static](#) and enter the prefix.
 - 3) Keep [WAN Connection](#) as the default settings.
4. Click [Save](#) to make the settings effective.

6.2.2. Configure the DHCPv6 Server Address Type

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [Network](#) > [LAN Settings](#).
3. Select [IPv6](#) to configure IPv6 LAN parameters.

DHCP Server

IPv4 IPv6

Group: Default

IPv6 LAN: ☒ Enable

Address Type: ☐ RADVD ☒ DHCPv6 Server

Starting IPv6 Address: 1 (1-FFFF)

Ending IPv6 Address: FFFE (1-FFFF)

Address Lease Time: 7200 seconds

Site Prefix Type: ☒ Delegated ☐ Static

WAN Connection: MBB

Save

- 1) Select **DHCPv6 Server** as the address type to make the router assign IPv6 addresses to hosts.
 - 2) Specify the **Starting/Ending IPv6 Address** for the IPv6 suffixes. The router will generate IPv6 addresses within the specified range.
 - 3) Keep **Address Lease Time** as the default setting.
 - 4) Keep **Site Prefix Type** as the default value **Delegated**. If your ISP has provided a specific IPv6 site prefix, select **Static** and enter the prefix.
 - 5) Keep **WAN Connection** as the default setting.
4. Click **Save** to make the settings effective.

6.3. Set Up a Dynamic DNS Service Account

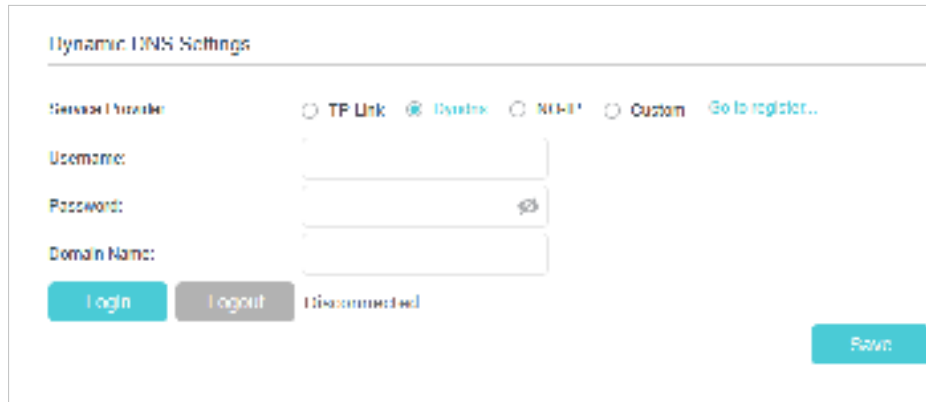
Most ISPs (Internet service providers) assign a dynamic IP address to the router and you can use this IP address to access your router remotely. However, the IP address can change any time and you don't know when it changes. In this case, you might need the DDNS (Dynamic Domain Name Server) feature on the router to allow you and your friends to access your router and local servers (FTP, HTTP, etc.) using domain name, in no need of checking and remembering the IP address.

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

To set up DDNS, please follow the instructions below:

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to **Advanced > Network > Dynamic DNS**.
3. Select the **Service Provider** (TP-Link/Dyndns/NO-IP).

4. Log in with your DDNS account, select a service provider. Enter the username, password and domain name of the account (such as lisa.ddns.net).



5. Click [Log in](#) and [Save](#).

💡 **Tips:** If you want to use a new DDNS account, please log out first, then log in with the new account.

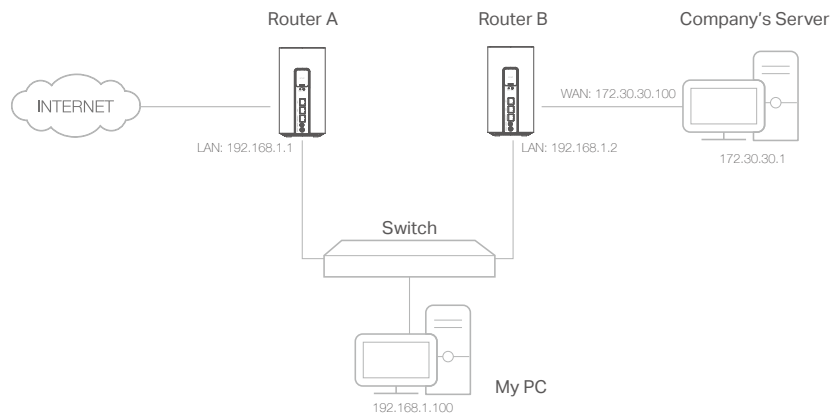
6.4. Create Static Routes

A static route is a pre-determined path that network information must travel to reach a specific host or network. Data from one point to another will always follow the same path regardless of other considerations. Normal internet usage does not require this setting to be configured.

I want to:

Visit multiple networks and multiple servers at the same time.

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

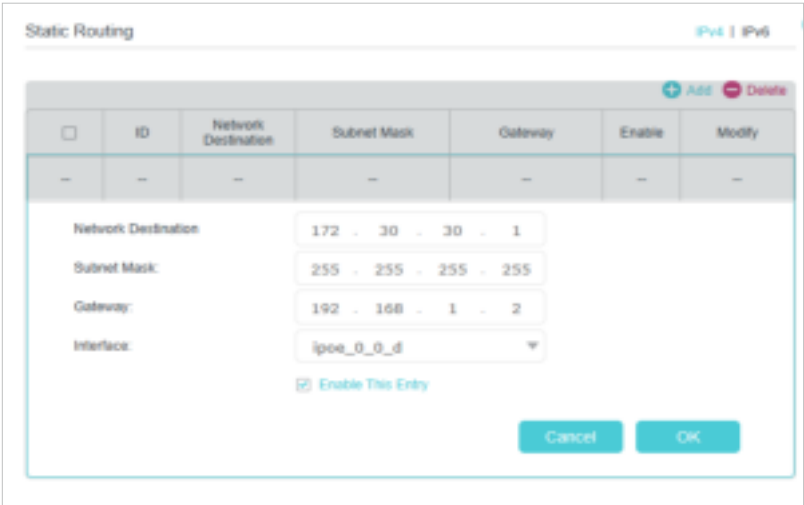


How can I do that?

1. Make sure the routers use different LAN IP addresses on the same subnet. Disable Router B's DHCP function.
2. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the Router A.
3. Go to [Advanced > Network > Static Routing](#). Select your current [WAN Interface](#) and click [Save](#).



4. Click [Add](#) to add a new static routing entry. Finish the settings according to the following explanations:



- **Network Destination:** The destination IP address that you want to assign to a static route. This IP address cannot be on

the same subnet with the WAN IP or LAN IP of the Router A. In the example, the IP address of the company network is the destination IP address, so here we enter 172.30.30.1.

- **Subnet Mask:** Determines the destination network with the destination IP address. If the destination is a single IP address, enter 255.255.255.255; otherwise, enter the subnet mask of the corresponding network IP. In the example, the destination network is a single IP, so here we enter 255.255.255.255.
 - **Gateway:** The IP address of the gateway device to which the data packets will be sent. This IP address must be on the same subnet with the router's IP which sends out the data. In the example, the data packets will be sent to the LAN port of Router B and then to the Server, so the default gateway should be 192.168.1.2.
 - **Interface:** Determined by the port (WAN/LAN) that sends out the data packets. In the example, the data is sent to the gateway through the LAN port of Router A, so **LAN** should be selected.
1. Select the **Enable This Entry** check box to enable this entry.
 5. Click **OK** to make the settings effective.

Done!

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

6.5. RIP Settings

To activate RIP for the WAN interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Save' button to start/stop RIP and save the configuration.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > Network > RIP Settings**.
3. Configure RIP settings.

RIP Settings

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Save' button to start/stop RIP and save the configuration.

(NOTE: RIP cannot be configured on the WAN interface which has NAT enabled.)

MD5 Authentication: Enable

MD5 Key ID 0:

MD5 Key ID 1:

Save

Interface	Version	AcceptRA	SendRA	Enabled	RipngEnabled	Modify
-----------	---------	----------	--------	---------	--------------	--------

- **MD5 Authentication** - Enable MD5 Authentication to enhance the rip RA packets security.
- **MD5 Key ID 0** - Setting the MD5 Key ID 0 value.
- **MD5 Key ID 1** - Setting the MD5 Key ID 1 value.
- **Interface** - The WAN interface name of the RIP rule table's entry used in.
- **Version** - The RIP version (RIPv1/RIPv2) of the RIP rule table's entry used.
- **AcceptRA** - Enable it to make the RIP rule entry can accept the Router Advertisement.
- **SendRA** - Enable it to make the RIP rule entry can send the Router Advertisement.
- **Enabled** - Enable it to make the RIP rule entry active for IPv4.
- **RipngEnabled** - Enable it to make the RIP rule entry active for IPv6, which is also known as Ripng.
- **Modify** - Click here to modify the RIP rule entry.

6. 6. Specify Wireless Settings

6. 6. 1. Change Basic Wireless Settings

The router's wireless network name (SSID) and password, and security option are preset in the factory. The preset SSID and password can be found on the product label. You can customize the wireless settings according to your needs.

Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.

➤ **To enable or disable OFDMA:**

OFDMA enables multiple users to transmit data simultaneously, and thus greatly improves speed and efficiency. Note that only when your clients also support OFDMA, can you fully enjoy the benefits.

1. Go to [Advanced](#) > [Wireless](#) > [Wireless Settings](#).
2. Enable [OFDMA](#).

➤ **To enable or disable TWT:**

TWT (Target Wake Time) allows 802.11ax routers and clients to negotiate their periods to transmit and receive data packets. Clients only wake up at TWT sessions and remain in sleep mode for the rest of the time, which significantly extends their battery life. It is disabled by default.

1. Go to [Advanced](#) > [Wireless](#) > [Wireless Settings](#).
2. Enable [TWT](#).

➤ **To enable or disable the BSS Color function:**

BSS Coloring is a way to address the increased spatial reuse rate due to overlapping basic service sets (OBSS) and to reduce the competitive overhead of the MAC tier due to overlapping BSS.

1. Go to [Advanced](#) > [Wireless](#) > [Wireless Settings](#).
2. Enable [BSS Color](#).

➤ **To enable or disable the wireless function:**

1. Go to [Basic](#) > [Wireless](#) or [Advanced](#) > [Wireless](#) > [Wireless Settings](#).
2. The wireless radio is enabled by default. If you want to disable the wireless function of the router, just clear the [Enable](#) check boxes. In this case, all the wireless settings will be invalid.

➤ **To change the wireless network name (SSID) and wireless password:**

1. Go to [Basic](#) > [Wireless](#) or [Advanced](#) > [Wireless](#) > [Wireless Settings](#).
2. Enter a new SSID (32 characters at most) in the [Network Name \(SSID\)](#) field and a new password in the [Password](#) field and click [Save](#). The SSID and password are case-sensitive.

■ **Note:**

If you use a wireless device to change the wireless settings, you will be disconnected after the new settings are effective. Please write down the new SSID and password for future use.

➤ **To hide SSID:**

1. Go to [Basic](#) > [Wireless](#) or [Advanced](#) > [Wireless](#) > [Wireless Settings](#).

2. Select **Hide SSID**, and your SSID will not be broadcast. Your SSID won't display on your wireless devices when you scan for local wireless networks and you need to manually join the network.

➤ **To change the mode or channel:**

1. Go to **Advanced > Wireless > Wireless Settings**.

Wireless Radio: ☒ Enable

Network Name (SSID): ☒ Hide SSID

Security:

Password:

Transmit Power: ☐ Low ☐ Middle ☒ High

ⓘ Advanced

2.4GHz Mode:

2.4GHz Channel:

2.4GHz Channel Width:

5GHz Mode:

5GHz Channel:

5GHz Channel Width:

Save

2. Select the wireless network mode or channel and click **Save** to make the settings effective.

Mode: Select the desired transmission mode.

- 802.11b/g/n mixed: Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.
- 802.11b/g/n/ax mixed: Select if you are using a mix of 802.11b, 11g, 11n and 11ax wireless clients.
- 802.11a/n/ac mixed: Select if you are using a mix of 802.11a, 11n, and 11ac wireless clients.
- 802.11a/n/ac/ax mixed: Select if you are using a mix of 802.11a, 11n, 11ac and 11ax wireless clients.

Channel: Select the channel you want to use from the drop-down list. This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

Channel Width: Select the channel width from the drop-down list. The default setting is **Auto**, which can adjust the channel width for your clients automatically.

Transmit Power: Select Low, Middle, or High to specify the data transmit power. The default and recommended setting is **High**.

➤ **To change the security option:**

1. Go to **Advanced > Wireless > Wireless Settings**.



2. Select an option from the **Security** drop-down list and configure the related parameters. The router provides five options, No Security, WPA-PSK[TKIP]+WPA2-PSK[AES], WPA2-PSK[AES], WPA2-PSK[AES]+WPA3-Personal, WEP. WPA3 uses the newest standard and the security level is the highest. We recommend you don't change the default settings unless necessary.
3. Click **Save** to make the settings effective.

➤ **To enable network roaming:**

Network roaming helps devices choose better AP based on actual conditions to balance network demands.

1. Go to **Basic > Wireless** or **Advanced > Wireless > Wireless Settings**.
2. Locate the **Band Steering** section, select the **Enable** check box to make the settings effective.



6.6.2. Advanced Wireless Settings

Advanced wireless settings are for those who want more network controls. You can follow the instructions below to configure your router.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for your router.
2. Go to **Advanced > Wireless > Advanced Settings**.

➤ **To change basic advanced settings:**

Locate the [Advanced Settings](#) section and configure the advanced settings according to the explanation below, and then click [Save](#).

Setting	Value	Range/Unit
Beacon Interval	100	(40-1000) ms
RTS Threshold	2347	(1-2347)
DTIM Interval	1	(1-255)
Group Key Update Period	0	seconds
WMM	<input checked="" type="checkbox"/> Enable	
Short GI	<input checked="" type="checkbox"/> Enable	
AP Isolation	<input type="checkbox"/> Enable	
Authentication Protocol	<input type="checkbox"/> Enable	
Load Balancing (RIP-11a)	<input type="checkbox"/> Enable	

[Save](#)

- **Beacon Interval:** Enter a value between 40 and 1000 in milliseconds to determine the duration between which beacon packets are broadcast by the router to synchronize the wireless network. The default is 100 milliseconds.
- **RTS Threshold:** Enter a value between 1 and 2346 to determine the packet size of data transmission through the router. By default, the RTS (Request to Send) Threshold size is 2347. If the packet size is greater than the preset threshold, the router sends Request to Send frames to a particular receiving station and negotiates the sending of a data frame, or else the packet will be sent immediately.
- **DTIM Interval:** Enter a value between 1 and 255 to determine the interval of the Delivery Traffic Indication Message (DTIM). 1 indicates the DTIM Interval is the same as [Beacon Interval](#).
- **Group Key Update Period:** Enter the number of seconds to control the time interval for the encryption key automatic renewal. The default is 0, indicating no key renewal.
- **WMM:** This feature guarantees the packets with high-priority messages being transmitted preferentially. WMM is enabled compulsively under 802.11n or 802.11ac mode.
- **Short GI:** This feature is enabled by default and recommended to increase the data capacity by reducing the Guard Interval (GI) time.
- **AP Isolation:** Select this check box to enable the AP Isolation feature that allows you to confine and restrict all wireless devices on your network from interacting with each other, but still able to access the internet.

- **Airtime fairness:** Select this checkbox to enable the Airtime Fairness(ATF) feature that allows you to optimize the throughput of each flow. The ATF traffic scheduler uses the per-destination airtime targets to balance airtime usage across flow destinations.
- **Fast Roaming (802.11r):** This feature allows a client device to roam quickly in environments implementing the WPA2 Enterprise security, by ensuring that the client device does not need to re-authenticate to the RADIUS server every time it roams from one access point to another. It's recommended that you keep the feature enabled for better roaming experiences.

Note:

If you are not familiar with the settings mentioned above, it's strongly recommended that you keep the provided default settings; otherwise it may result in lower wireless network performance.

➤ **To enable or disable WPS function:**

WPS (Wi-Fi Protected Setup) provides you with an easier approach to set up a security-protected Wi-Fi connection. This function is enabled by default, but if you do not need this function, clear the WPS **Enable** check box.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for your router.
2. Go to **Advanced > Wireless > WPS**.



➤ **To create multi-SSID network:**

The router supports additional up to three multi-SSID wireless networks for client access in each wireless band. You can specify the access and security settings to ensure network security and privacy according to your situation.

Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for your router.

➤ **Method 1: Advanced Settings**

1. Go to [Advanced](#) > [Wireless](#) > [Multi-SSID](#), create the multi-SSID network as needed.
 - 1) Select the [Enable MSSID 1](#) or [2](#) check box(es) to enable the corresponding multi-SSID network.

The screenshot shows the 'Multi-SSID' configuration page. It contains two identical sections for MSSID1 and MSSID2. In the MSSID1 section, the 'Enable' checkbox is checked, the 'Network Name (SSID)' is 'TP-Link_F527_1', the 'Hide SSID' checkbox is unchecked, the 'Security' dropdown is set to 'No Security', and the 'Allow guests to see each other' checkbox is checked. The MSSID2 section has the same settings. A 'Save' button is located at the bottom right of the form.

- 2) Enter a new [Network Name \(SSID\)](#) or use the default name, this field is case sensitive. Don't select [Hide SSID](#) unless you want your guests to manually input the SSID for Wi-Fi access.
 - 3) Select the [Security](#) option for the multi-SSID network, [WPA2-PSK\[AES\]+WPA3-Personal](#) is recommended, and you can set a password for the network.

If you want to allow the clients in your Multi-SSID network to communicate with each other via methods such as Network Neighborhood and Ping, select the [Allow Guests to See Each Other](#) check box.
2. Repeat step 1) to step 2) to set other wireless networks if needed, and click [Save](#) to make the settings effective.

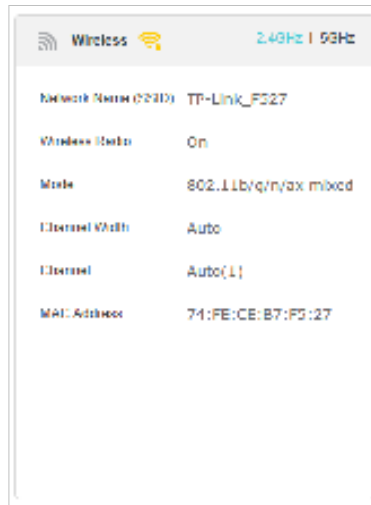
➤ **Method 2: Basic Settings**

6.6.3. View Wireless Information

➤ **To view the detailed wireless network settings:**

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.

2. Go to [Advanced](#) > [Status](#) page. You will find the [Wireless](#) panel.
3. Click [2.4GHz](#) or [5GHz](#) to view the wireless details.



💡 **Tips:** You can also see the wireless details by clicking the router icon on [Basic](#) > [Network Map](#).

6.7. Schedule Your Wireless Function

You can automatically turn off your wireless networks when you do not need the wireless connection.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [Wireless](#) > [Wireless Schedule](#).
3. Enable the [Wireless Schedule](#) function.

The image shows a 'Wireless Schedule' configuration window. At the top, there is a toggle switch labeled 'Wireless Schedule' which is currently turned on. Below the toggle is a 24-hour grid. The grid has columns for the days of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat) and rows for each hour from 0:00 to 24:00. Yellow bars are placed in the grid to indicate when the wireless network is scheduled to be turned off. The bars are located in the following time slots: 5:00-7:00 on Friday and Saturday; 10:00-11:00 on Tuesday and Wednesday; 12:00-13:00 on Thursday; 13:00-15:00 on Thursday; 16:00-19:00 on Tuesday and Wednesday. At the bottom of the grid, there is a legend showing a yellow square next to the text 'Wireless Off'. Below the legend are two buttons: 'Restore' and 'Save'.

4. Click [Add](#) to set the [Wireless Off Time](#), and click [Save](#) to make the settings effective.

Note:

1. Make sure that the time of the router is correct before using this function. For details, refer to [Set System Time](#).
2. The wireless LED will turn off if the corresponding wireless network is disabled.
3. The wireless network will be automatically turned on after the time period you set.

6.8. Use WPS for Wireless Connection

You can use WPS (Wi-Fi Protected Setup) to add a new wireless device to your existing network quickly and easily.

Method 1: Use the WPS button

Use this method if your client device has a WPS button.

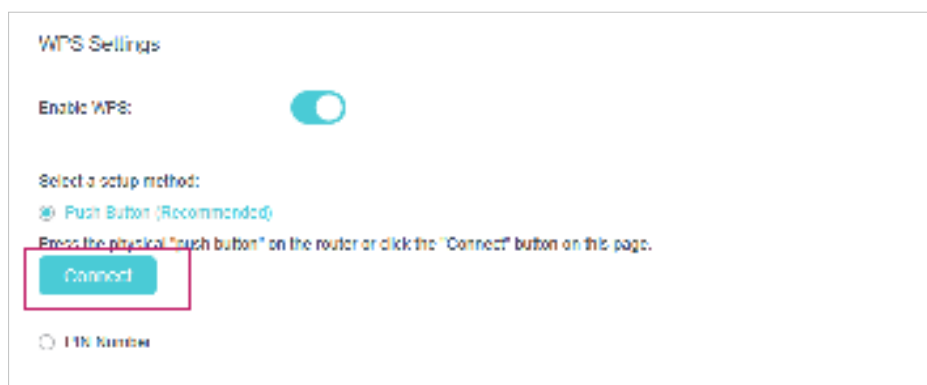
1. Press the WPS button of the router.
2. Press the WPS button of the client device directly.
3. The WLAN LED flashes for about 2 minutes during the WPS process.

4. When the WLAN LED is on, the client device has successfully connected to the router.

Method 2: Use the “Connect” button on the web management page

Use this method if your client device has a WPS button.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [Wireless](#) > [WPS](#) page.

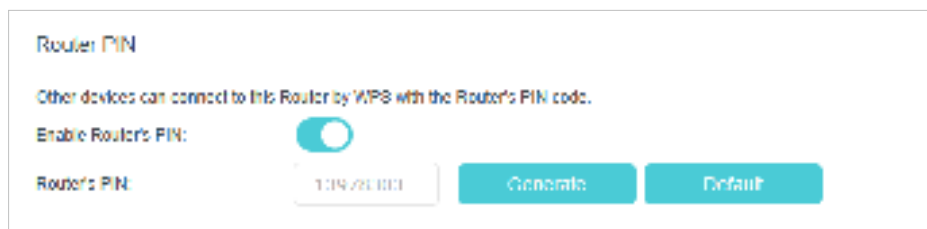


3. Click [Connect](#) on the page.
4. Press the WPS button of the client device directly.
5. The WPS LED of the router flashes for about 2 minutes during the WPS process.
6. When the WPS LED is on, the client device has successfully connected to the router.

Method 3: Enter the router's PIN on your client device

Use this method if your client device asks for the router's PIN.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [Wireless](#) > [WPS](#), and enable [Router's PIN](#).



3. Take a note of the current PIN of the router. You can also click the [Generate](#) button to get a new PIN.
4. Enter the router's PIN on the client device. (The default PIN is also printed on the label of the router.)

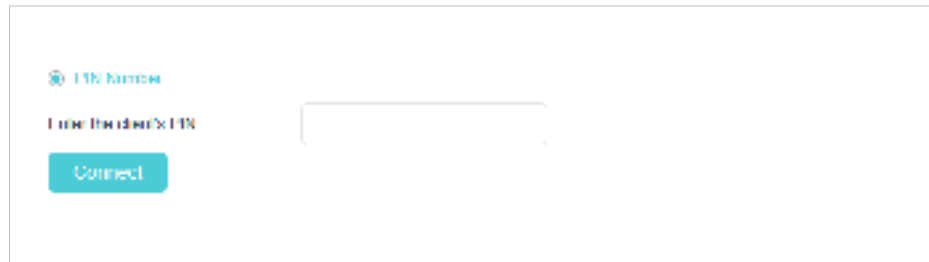
5. The WPS LED flashes for about 2 minutes during the WPS process.
6. When the WPS LED is on, the client device has successfully connected to the router.

■ Note:

1. The WPS LED on the router will light on for five minutes if the device has been successfully added to the network.
2. The WPS function cannot be configured if the wireless function of the router is disabled. Please make sure the wireless function is enabled before configuring WPS.

Method 4: Enter the client device's PIN on the router

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [Wireless](#) > [WPS](#), and click [PIN Number](#).
3. Enter the [Client's PIN](#).



4. Then click the [Connect](#) button.
5. [Device has been added successfully!](#) or the similar information will appear on the web page, which means the client device has successfully connected to the router.

Chapter 7

TP-Link Cloud Service

TP-Link Cloud service provides a better way to manage your cloud devices. Log in to your router with a TP-Link ID, and you can easily monitor and manage your home network when you are out and about via the Tether app. To ensure that your router stays new and gets better over time, the TP-Link Cloud will notify you when an important firmware upgrade is available. Surely you can also manage multiple TP-Link Cloud devices with a single TP-Link ID.

This chapter introduces how to register a new TP-Link ID, bind or unbind TP-Link IDs to manage your router, and the Tether app with which you can manage your home network no matter where you may find yourself.

It contains the following sections:

- **Register a TP-Link ID**
- **Change Your TP-Link ID Information**
- **Manage the User TP-Link IDs**
- **Manage the Router via the TP-Link Tether App**

7.1. Register a TP-Link ID

If you have skipped the registration during the Quick Setup process, you can:

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to **Basic > TP-Link Cloud**.
3. Click **Register Now** and follow the instructions to register a TP-Link ID.



4. After activating your TP-Link ID, come back to the TP-Link Cloud page to log in. The TP-Link ID used to log in to the router for the first time will be automatically bound as an **Admin**.

Note:


- To learn more about the **Admin** and **User** TP-Link ID, refer to [Manage the User TP-Link IDs](#).
- Once you have registered a TP-Link ID on the web management page, you can only register another TP-Link ID via the Tether APP. Please refer to [Manage the Router via the TP-Link Tether App](#) to install the app.
- If you want to unbind the admin TP-Link ID from your router, please go to **Basic > TP-Link Cloud**, and click **Unbind** in the **Device Information** section.

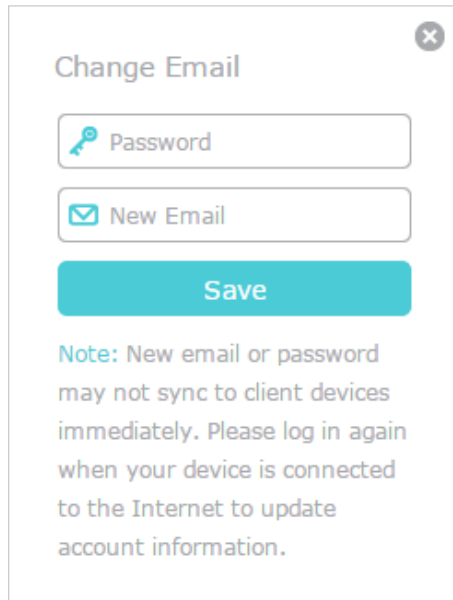
7.2. Change Your TP-Link ID Information

Follow the steps below to change your email address and password of your TP-Link ID as needed.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID.
2. Go to **Basic > TP-Link Cloud**, and focus on the **Account Information** section.


➤ **To change your email address:**

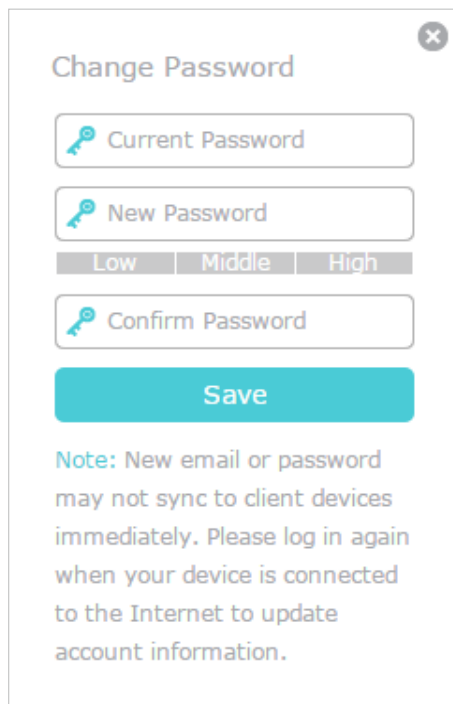
1. Click  behind the Email.
2. Enter the password of your TP-Link ID, then a new email address. And click **Save**.



A dialog box titled "Change Email" with a close button (X) in the top right corner. It contains two input fields: "Password" with a key icon and "New Email" with an envelope icon. Below the fields is a teal "Save" button. A note at the bottom states: "Note: New email or password may not sync to client devices immediately. Please log in again when your device is connected to the Internet to update account information."

➤ **To change your password:**

1. Click  behind the Password.
2. Enter the current password, then a new password twice. And click **Save**.



A dialog box titled "Change Password" with a close button (X) in the top right corner. It contains three input fields: "Current Password" with a key icon, "New Password" with a key icon, and "Confirm Password" with a key icon. Below the "New Password" field are three tabs: "Low", "Middle", and "High". Below the fields is a teal "Save" button. A note at the bottom states: "Note: New email or password may not sync to client devices immediately. Please log in again when your device is connected to the Internet to update account information."

7.3. Manage the User TP-Link IDs

The TP-Link ID used to log in to the router for the first time will be automatically bound as the **Admin** account. An admin account can add or remove other TP-Link IDs to or

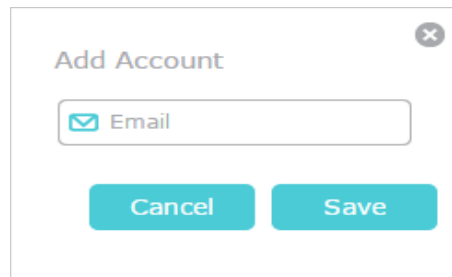
from the same router as **Users**. All accounts can monitor and manage the router locally or remotely, but user accounts cannot:

- Reset the router to its factory default settings either on the web management page or in the Tether app.
- Add/remove other TP-Link IDs to/from the router.

7.3.1. Add TP-Link ID to Manage the Router

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID.
2. Go to **Basic > TP-Link Cloud**, and focus on the **Bound Accounts** section.
3. Click **+ Bind**, enter another TP-Link ID as needed and click **Save**.

Note: If you need another TP-Link ID, please register a new one via the Tether app. Refer to [Manage the Router via the TP-Link Tether App](#) to install the app and register a new TP-Link ID.



The image shows a modal dialog box titled "Add Account" with a close button (X) in the top right corner. Inside the dialog, there is a text input field with a blue envelope icon and the label "Email". Below the input field are two buttons: "Cancel" and "Save", both in a teal color.

4. The new TP-Link ID will be displayed in the Bound Accounts table as a **User**.



The image shows a screenshot of the "Bound Accounts" section in the TP-Link Cloud management interface. At the top right, there are two buttons: "+ Bind" (teal) and "- Unbind" (purple). Below these buttons is a table with the following columns: a checkbox, ID, Email, Binding Date, and Role. There are two rows of data. The first row has ID 1, an email address, a binding date, and the role "Admin". The second row has ID 2, an email address, a binding date, and the role "User", which is highlighted with a yellow box.

	ID	Email	Binding Date	Role
<input type="checkbox"/>	1	admin@tplink.com	2020-10-10	Admin
<input type="checkbox"/>	2	user@tplink.com	2020-10-10	User

7.3.2. Remove TP-Link ID(s) from Managing the Router

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID.
2. Go to **Basic > TP-Link Cloud**, and focus on the **Bound Accounts** section.
3. Tick the checkbox(es) of the TP-Link ID(s) you want to remove and click **Unbind**.



Chapter 8

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

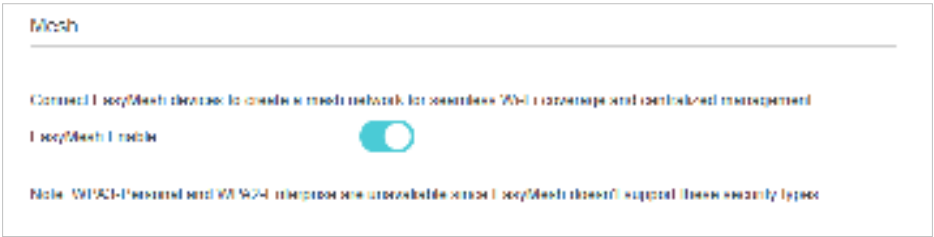
Devices automatically switch between your controller and agents as you move through your home for the fastest possible speeds.

Easy Setup and Management

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

8. 1. Set Up a EasyMesh Network

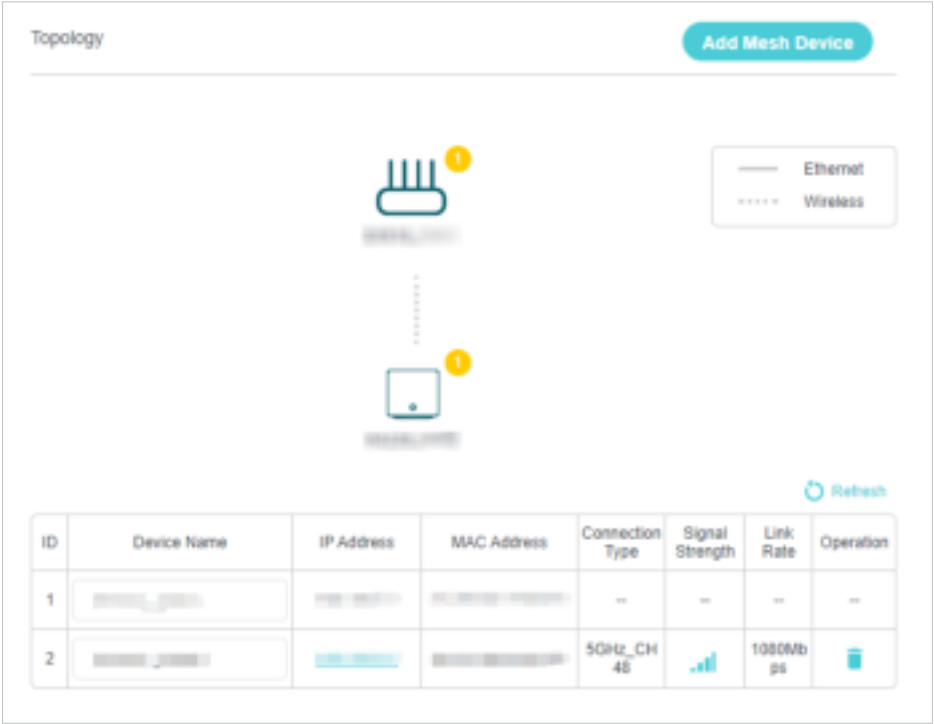
1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router.
1. Go to **Basic > Mesh** or **Advanced > Wireless > Mesh**.



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.






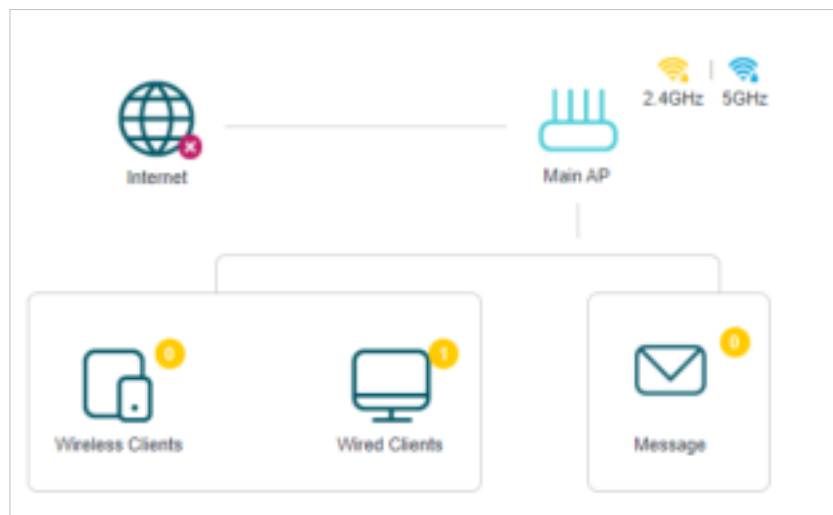
Done! Now your controller and agents successfully form a EasyMesh network!

8. 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://tplinkmodem.net> or <http://192.168.1.1>, 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://tplinkmodem.net> or <http://192.168.1.1>, 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 9

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](#)

9.1. Create a Network for Guests

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Basic > Guest Network](#) or [Advanced > Guest Network](#).
3. Create a guest network as needed.
 - 1) Tick the Enable checkbox for the 2.4GHz/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.



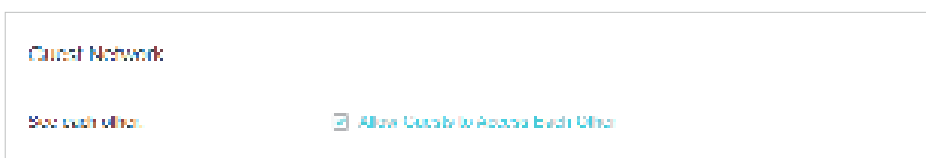
4. Click [Save](#). Now your guests can access your guest network using the SSID and password you set!

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.

9.2. Customize Guest Network Options

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Basic > Guest Network](#) or [Advanced > Guest Network](#).
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 10

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:

- [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](#)

10.1. 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://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router. Go to **Advanced > NAT Forwarding > ALG**.

ALG	
PPTP Pass through:	<input checked="" type="checkbox"/> Enable
L2TP Pass through:	<input checked="" type="checkbox"/> Enable
IPSec Pass through:	<input checked="" type="checkbox"/> Enable
FTP ALG:	<input checked="" type="checkbox"/> Enable
TFTP ALG:	<input checked="" type="checkbox"/> Enable
H323 ALG:	<input checked="" type="checkbox"/> Enable
RTSP ALG:	<input checked="" type="checkbox"/> Enable
SIP ALG:	<input checked="" type="checkbox"/> Enable


Save

10.2. 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://tplinkmodem.net> or <http://192.168.1.1>, 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.

Virtual Servers

+

Full

-

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 CVMPP, Virtual Server will not take effect.

Interface Name

ipsec_0_0_0

Service Type

View Existing Applications

External Port

(XX-XX or XX)

Internal IP

Internal Port

(XX or Blank, 1-65535)

Protocol

TCP

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

<input type="checkbox"/>	ID	Service Type	External Port	Internal IP	Internal Port	Protocol	Status	Modif
...

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

Interface Name:

ipoe_0_0_d

Service Type:

FTP

View Existing Applications

External Port:

21

(XX-XX or XX)

Internal IP:

- - -

Internal Port:

21

(XX or Blank, 1-65535)

Protocol:

TCP

☒ 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.

10.3. 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://tplinkmodem.net> or <http://192.168.1.1>, 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](#).

Port Triggering

Interface Name:

igmp_0_0_d

Application:

View Existing Applications

Triggering Port:

(XX, 1-65535)

Triggering Protocol:

TCP

External Port:

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

External Protocol:

TCP

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

Interface Name:

igmp_0_0_d

Application:

MSN Gaming Zone

View Existing Applications

Triggering Port:

47524

(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

<input type="checkbox"/>	ID	Application	Triggering Port	Triggering Protocol	External Port	External Protocol	Status	Modify
<input type="checkbox"/>	1	MSN Gaming Zone	47624	ICMP or UDP	24000-24005, 24006-24010	ICMP 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.

10.4. 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 192.168.1.100.
2. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router.
3. Go to [Advanced](#) > [NAT Forwarding](#) > [DMZ](#) and tick to enable DMZ.
4. Enter the PC's IP address 192.168.1.100 manually in the [DMZ Host IP Address](#) field.

5. Click **SAVE**.

Done!

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

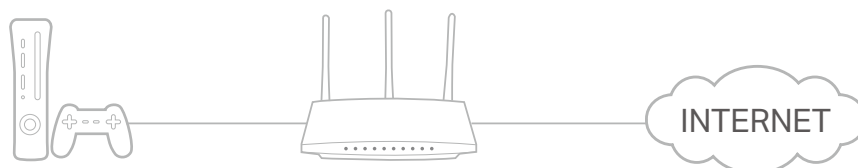
10.5. Make Xbox Online Games Run Smoothly by UPnP

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).

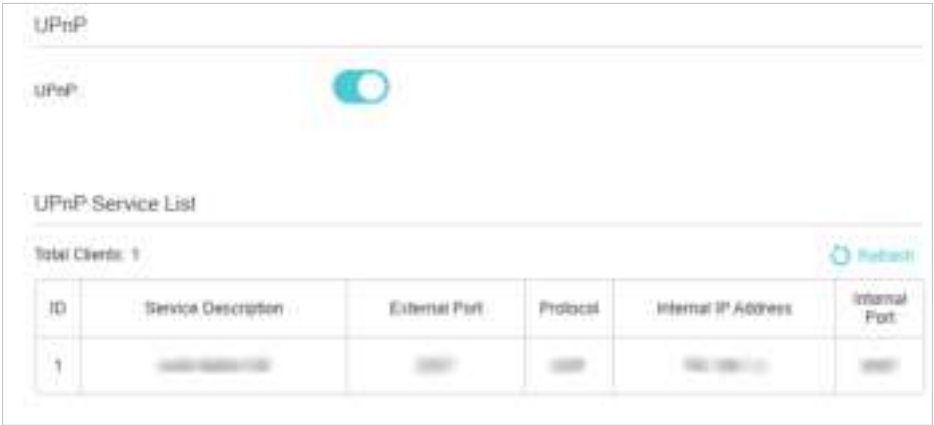
For example, when you connect your Xbox to the router which has connected to the internet to play online games, UPnP will send request to the router to open the corresponding ports allowing the following data penetrating the NAT to transmit. Therefore, you can play Xbox online games without a hitch.



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

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, 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 11

Parental Controls

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

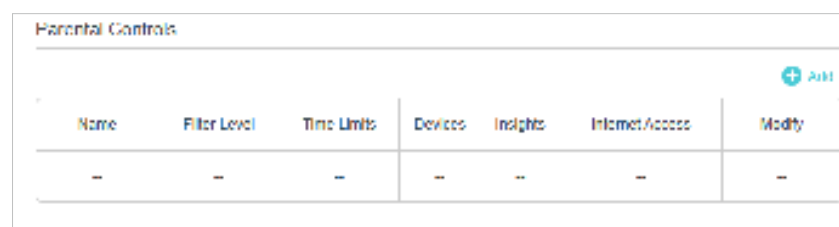
I want to:

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://tplinkmodem.net> or <http://192.168.1.1>, 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**.

Parental Controls

[+ Add](#)

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

Filter Level

Basic Info ————— Time Controls

Child (0-7) Pre-Teen (8-12) Teen (13-17) Adult (>17)

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

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.

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

05 : 00 AM

Weekends

☒ Enable

From

10 : 00 PM

To

05 : 00 AM

Cancel

Back

Save

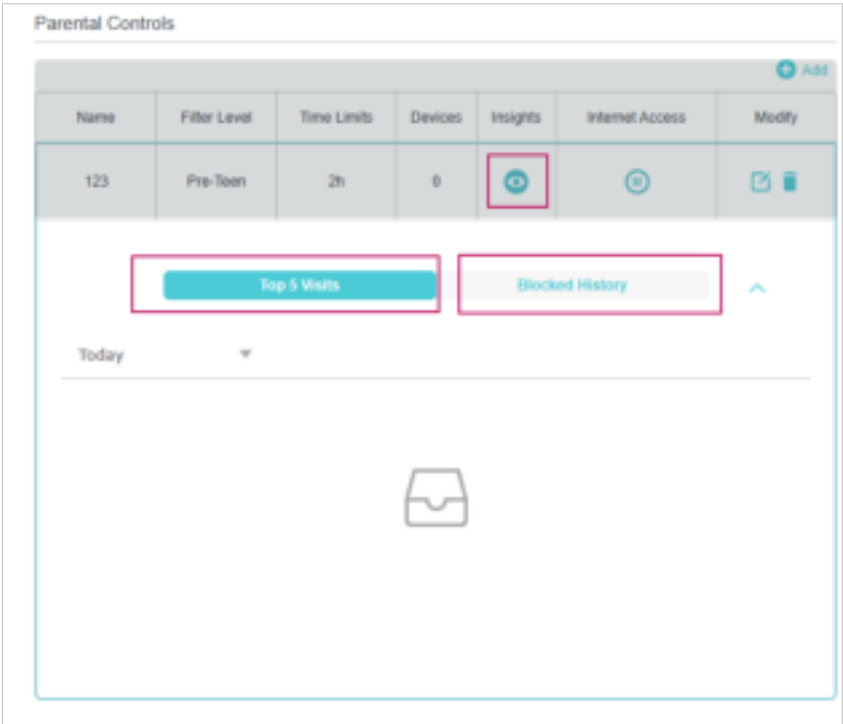
7. Click [Save](#).

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.



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



Chapter 12

Quality of Service

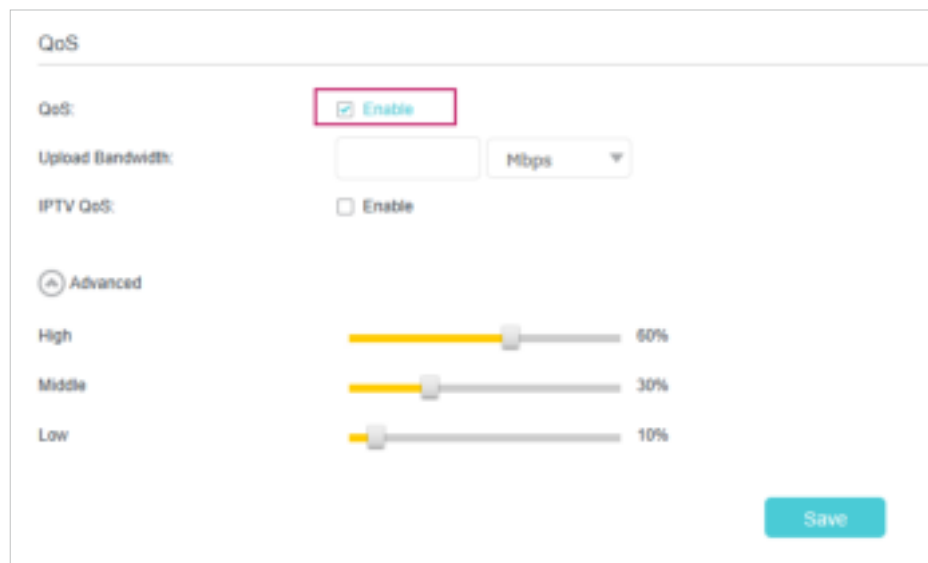
This function allows you to specify the priority of traffic and minimizes the impact of network congestion.

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://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [QoS](#).
3. Enable [QoS](#).



The screenshot shows the 'QoS' configuration page. At the top, the title 'QoS' is displayed. Below it, the 'QoS' section has a checkbox labeled 'Enable' which is checked and highlighted with a red box. Underneath, there is a field for 'Upload Bandwidth' with a unit dropdown menu set to 'Mbps'. Below that, the 'IPTV QoS' section has an unchecked 'Enable' checkbox. A section titled 'Advanced' is expanded, showing three sliders for traffic prioritization: 'High' is set to 60%, 'Middle' is set to 30%, and 'Low' is set to 10%. A 'Save' button is located at the bottom right of the configuration area.

4. Enter the upload bandwidths provided by your ISP.

QoS

QoS: ☒ Enable

Upload Bandwidth: Mbps

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.

QoS

QoS: ☒ Enable

Upload Bandwidth: Mbps

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: Mbps

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://tplinkmodem.net> or <http://192.168.1.1>, 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](#).

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.

QuS Rule

Type: By Device

Device Name:

Unknown

Scan

MAC Address:

Cancel

OK

ID	Device Name	IP Address	MAC Address	Operation
1	Unknown			<div></div>

Chapter 13

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](#)

13.1. Firewall & DoS Protection

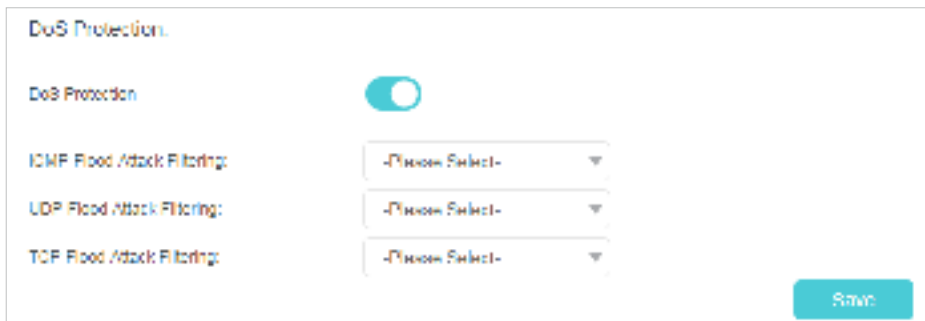
The SPI (Stateful Packet Inspection) Firewall and DoS (Denial of Service) Protection protect the router from cyber attacks.

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://tplinkmodem.net> or <http://192.168.1.1>, 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](#).

Dos Protection Level Settings

ICMP-Flood Protection Level:

Low:

3600

(5-3600) packets/sec

Middle:

2400

(5-3600) packets/sec

High:

1200

(5-3600) packets/sec

UDP-Flood Protection Level:

Low:

3600

(5-3600) packets/sec

Middle:

2400

(5-3600) packets/sec

High:

1200

(5-3600) packets/sec

TCP-SYN-Flood Protection Level:

Low:

3600

(5-3600) packets/sec

Middle:

2400

(5-3600) packets/sec

High:

1200

(5-3600) packets/sec

Save

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](#).

Blocked DoS Host List

Host Number 0

Refresh

Delete

<input type="checkbox"/>	ID	IP Address	MAC Address

13.2. Service Filtering

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

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [Security](#) > [Service Filtering](#), and enable [Service Filtering](#).

Service Filtering

Service Filtering: ☒

3. Click [Add](#).

The screenshot shows a 'Filtering List' configuration window. At the top, there are buttons for 'Return', 'Add', and 'Delete'. Below is a table with the following columns: Service Type, Port, IP Address, Status, and Modify. The table is currently empty. Below the table, there are several input fields: 'Service Type' is set to 'Any(ALL)', 'Protocol' is set to 'TCP/UDP', 'Starting Port' is '1', 'Ending Port' is '65535', and 'Filter Service For' is set to 'All IP Addresses'. There are also buttons for 'Cancel' and 'Save' at the bottom right.

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.

13.3. 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://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to **Advanced > Security > Access Control** and enable **Access Control**.

The screenshot shows the 'Access Control' settings page. At the top, it says 'Access Control'. Below that, there is a toggle switch labeled 'Access Control' which is currently turned on (indicated by a blue circle).

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**.

The screenshot shows the 'Access Mode' configuration interface. It has a title 'Access Mode' and a label 'Access Mode:'. Below the label are two radio buttons: 'Blacklist' (which is selected) and 'Whitelist'. A teal 'Save' button is located at the bottom right.

- 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.

The screenshot shows the network management interface. It has two main sections: 'Devices in Blacklist' and 'Online Devices'.

Devices in Blacklist: This section has a title 'Devices in Blacklist' and two buttons: '+ Add' and 'Unblock'. Below the buttons is a table with the following columns: ID, Device Name, MAC Address, and Modify. The table is currently empty.

Online Devices: This section has a title 'Online Devices' and two buttons: 'Refresh' and 'Block'. Below the buttons is a table with the following columns: ID, Device Name, IP Address, MAC Address, and Connection Type. The table contains one row with the following data:

ID	Device Name	IP Address	MAC Address	Connection Type
1	Unknown	192.168.1.157	08:BF:BF:3F:29:05	Wired

To allow specific device(s):

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

The screenshot shows the 'Access Mode' configuration interface. It has a title 'Access Mode' and a label 'Access Mode:'. Below the label are two radio buttons: 'Blacklist' and 'Whitelist' (which is selected). A teal 'Save' button is located at the bottom right.

- 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" and "- Delete" buttons. Below this is a table with the following columns: ID, Device Name, MAC Address, and Priority. The table is currently empty. Below the table, there is a form to add a new device. It has two input fields: "Device Name:" and "MAC Address:". To the right of the "Device Name" field is a "Scan" button. Below the "MAC Address" field are "Cancel" and "OK" 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](#).

13.4. 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://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [Security](#) > [IP & MAC Binding](#), and enable [IP & MAC Binding](#).

IP & MAC Binding

IP & MAC Binding: ☒

Binding List

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

<input type="checkbox"/>	ID	MAC Address	IP Address	Status	Enable	Modify
<input type="checkbox"/>	--	--	--	--	--	--

ARP List

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

<input type="checkbox"/>	ID	Device Name	MAC Address	IP Address	Status	Modify
<input type="checkbox"/>	1	Unknown	08:EF:B8:3F:29:05	192.168.1.197	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](#)

<input type="checkbox"/>	ID	MAC Address	IP Address	Status	Enable	Modify
<input type="checkbox"/>	--	--	--	--	--	--

MAC Address: 74 - FE - CE - 87 - F3 - 27

IP Address: 192 - 168 - 1 - 100

☒ 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 [OK](#).

Done!

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

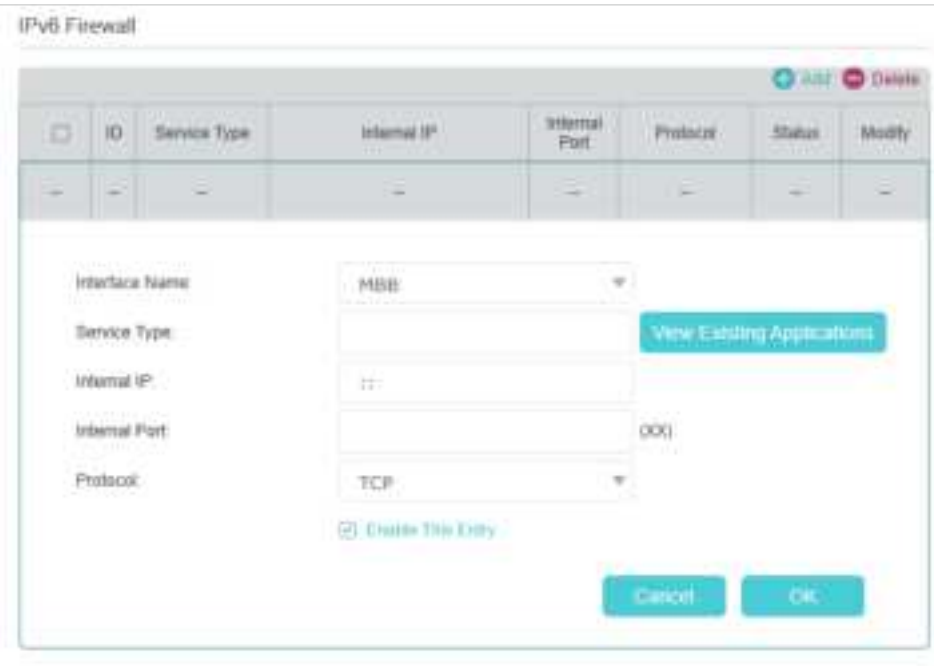
13.5. IPv6 Firewall

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://tplinkmodem.net> or <http://192.168.1.1>, 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 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

ID	Service Type	Internal IP	Internal Port	Protocol	Status	Modify

Interface Name: PEER

Service Type: FTP [View Existing Applications](#)

Internal IP: ::

Internal Port: 21 (000)

Protocol: TCP

☒ 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 14

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.

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](#)

14. 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

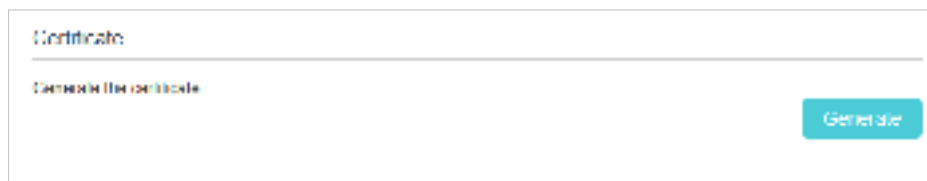
1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > VPN > OpenVPN**, and tick the box of **Enable VPN Server**.

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.

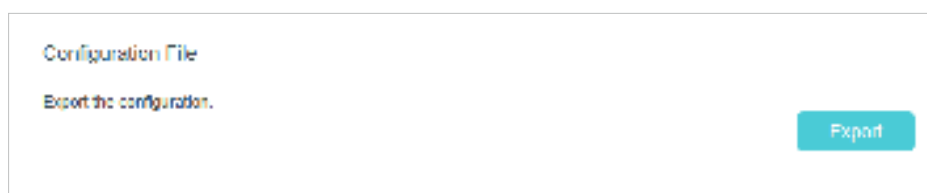
3. Select the **Service Type** (communication protocol) for OpenVPN Server: UDP, TCP.
4. Enter a VPN **Service Port** to which a VPN device connects, and the port number should be between 1024 and 65535.
5. In the **VPN Subnet/Netmask** fields, enter the range of IP addresses that can be leased to the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

14. 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://tplinkmodem.net> or <http://192.168.1.1>, 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**.



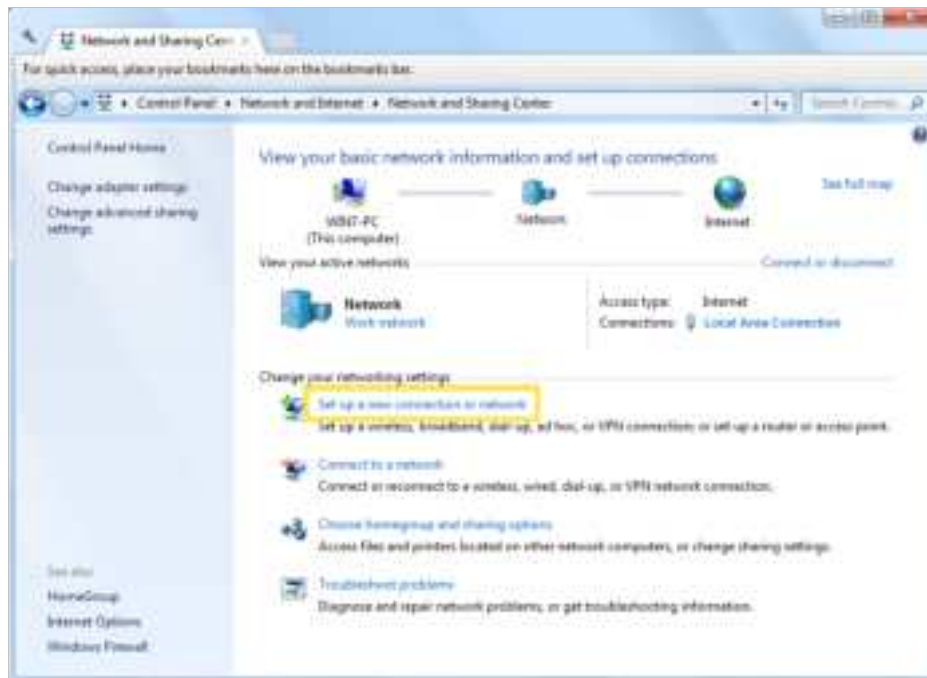
Note: Before you enable [VPN Server](#), we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router's WAN port and synchronize your [System Time](#) with internet.

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.

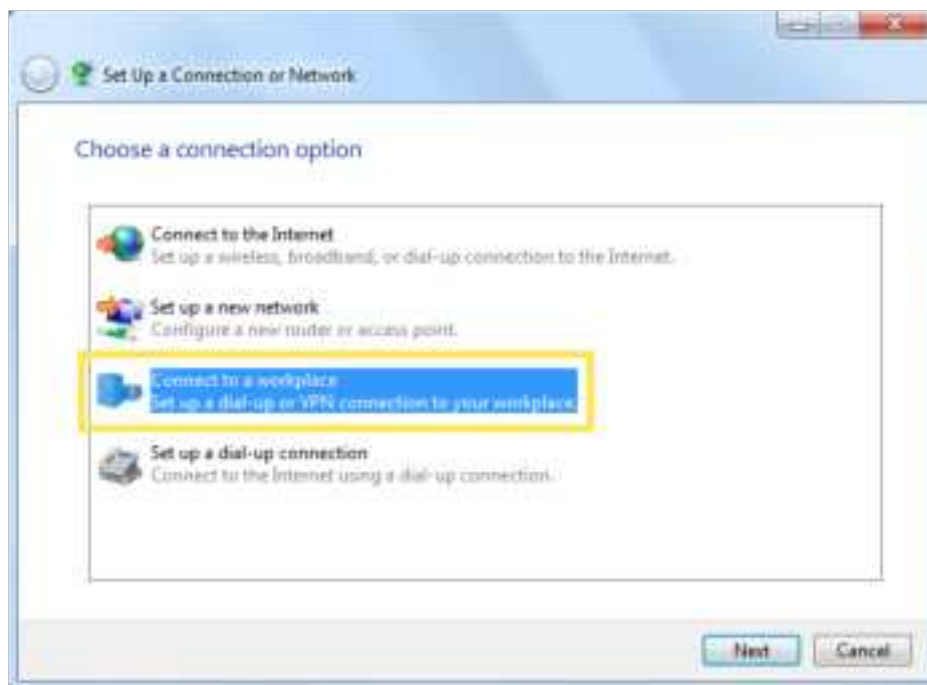
Step 2. Configure PPTP VPN Connection on Your Remote Device

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 \(VPN\)](#).



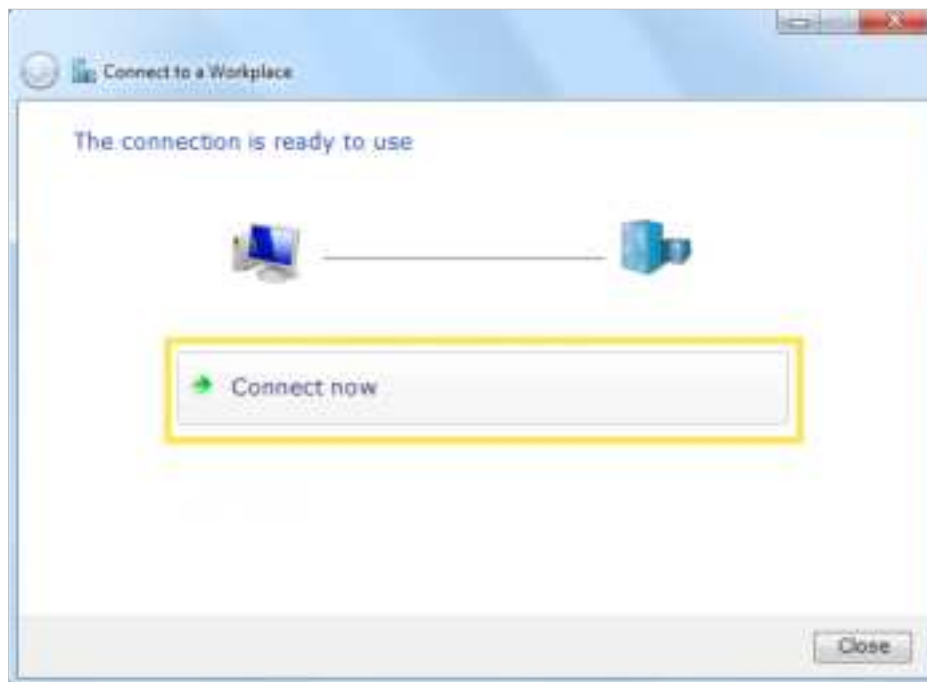
5. Enter the internet IP address of the router (for example: 218.18.1.73) in the [Internet address](#) field. Click [Next](#).



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.



14.3. 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 the IPsec connection on remote devices. Please follow the steps below to set up the IPsec VPN connection.

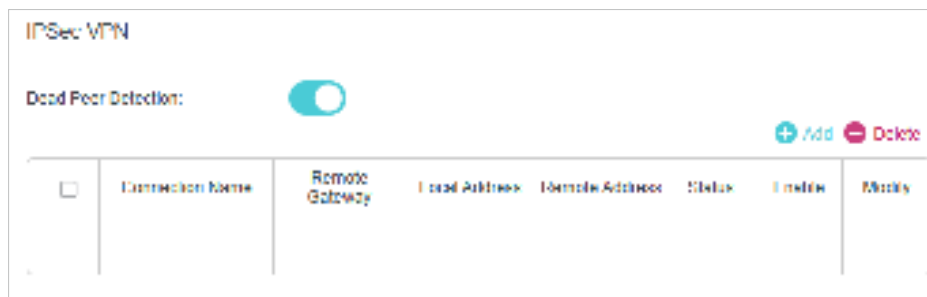


Step 1. Set up IPsec VPN Server on Your Router

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, 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.

Dead Peer Detection ☒

+ Add - Delete

	Connection Name	Remote Gateway	Local Address	Remote Address	Status	Enable	Modify

IPSec Connection Name:

Remote IPSec Gateway (URL):

Tunnel access from local IP addresses:

IP Address for VPN:

Subnet Mask:

Tunnel access from remote IP addresses:

IP Address for VPN:

Subnet Mask:

Key Exchange Method:

Authentication Method:

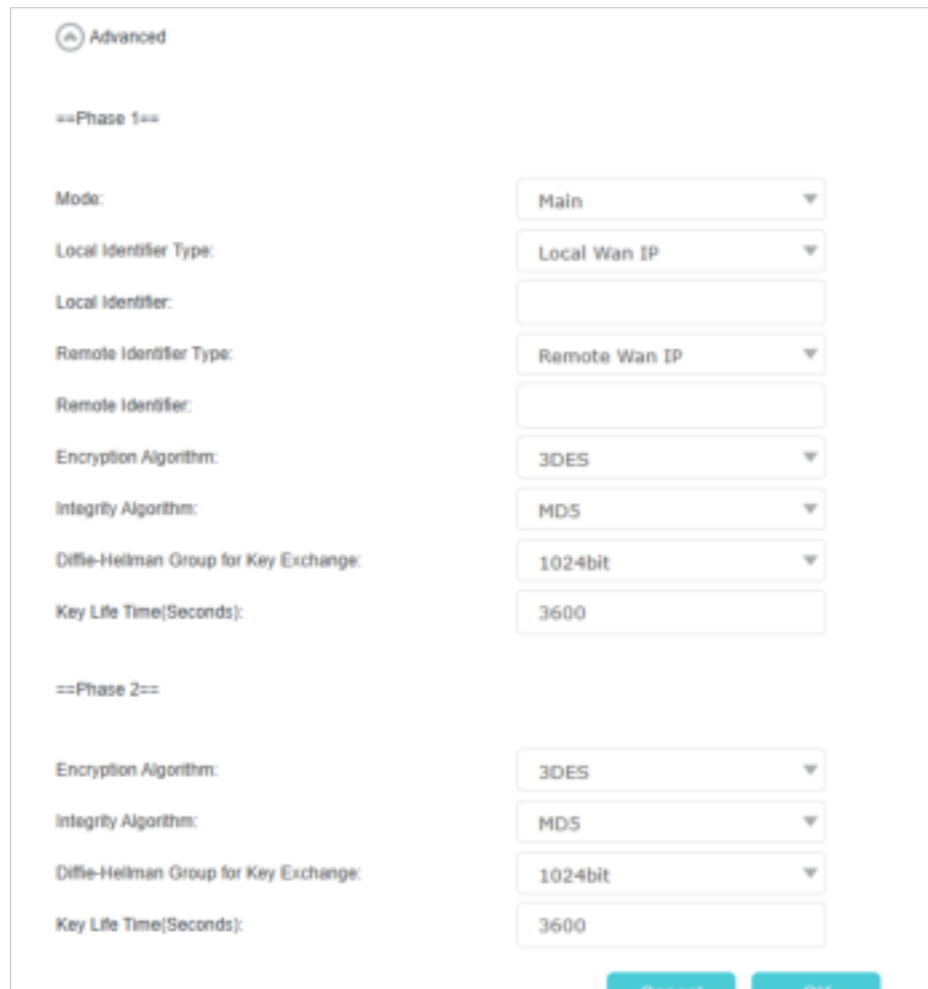
Pre-Shared Key:

Perfect Forward Secrecy:

☒ Advanced

Cancel OK

5. 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 back arrow icon. 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 two buttons: "Previous" and "OK".

6. Click **OK**.

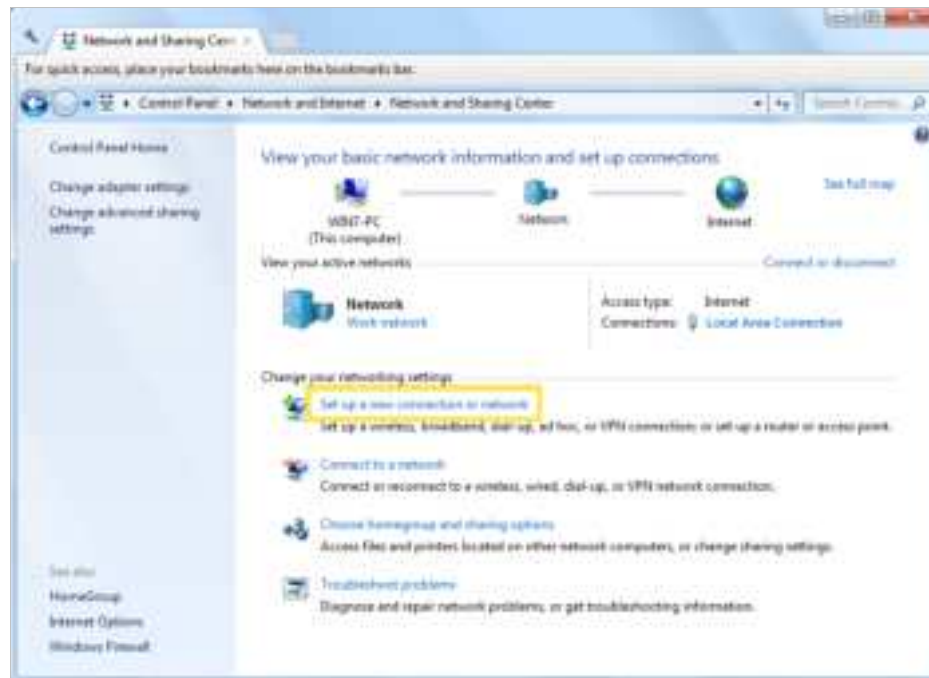
Note:

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

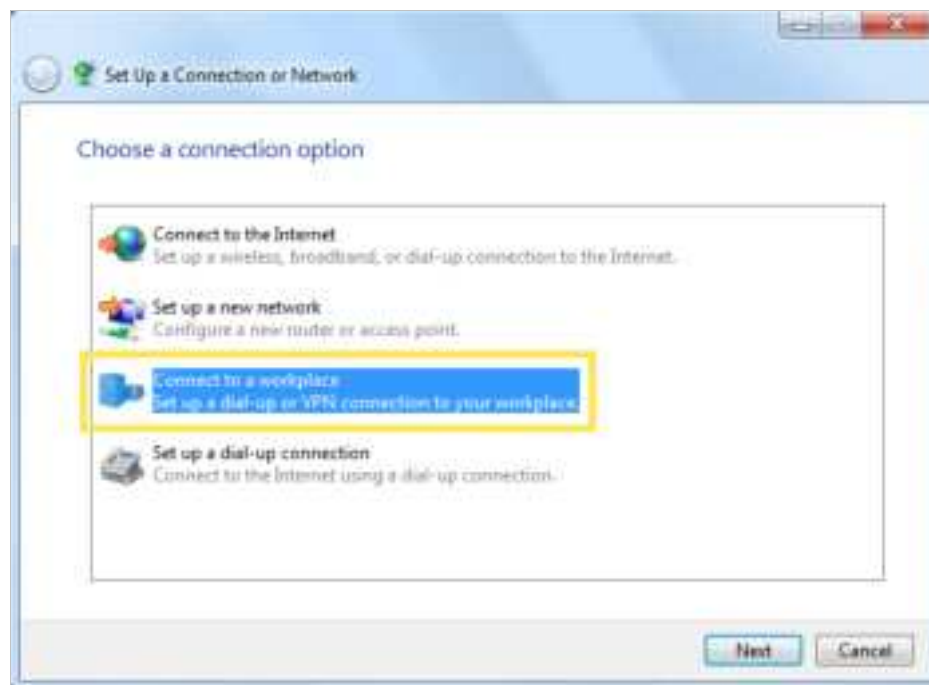
Step 2. Configure IPSec VPN Connection on Your Remote Device

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.

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



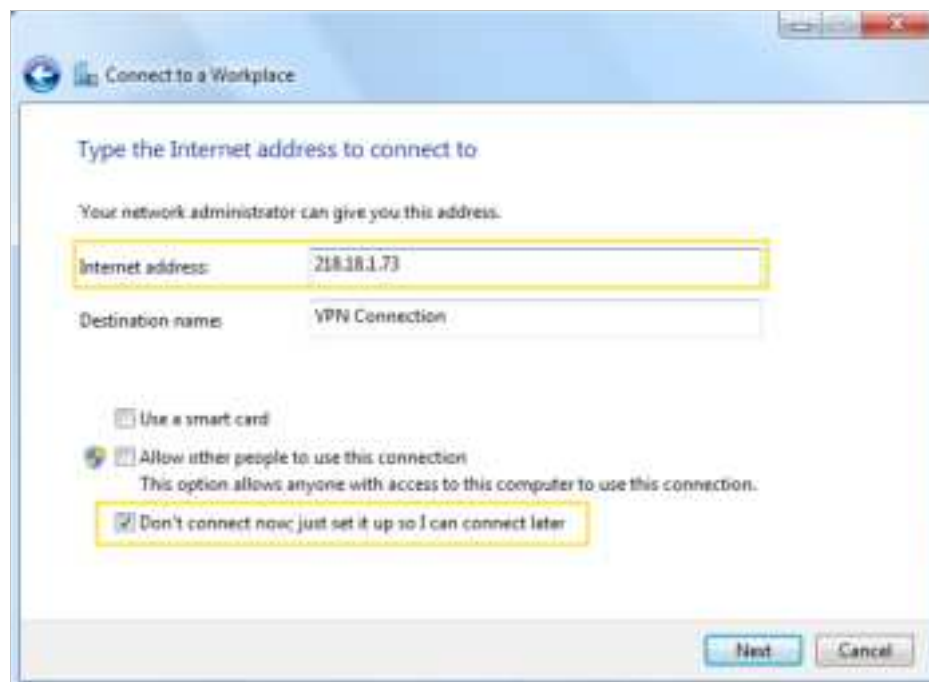
3. Select [Connect to a workplace](#) and click [Next](#).



4. Select [Use my Internet connection \(VPN\)](#).



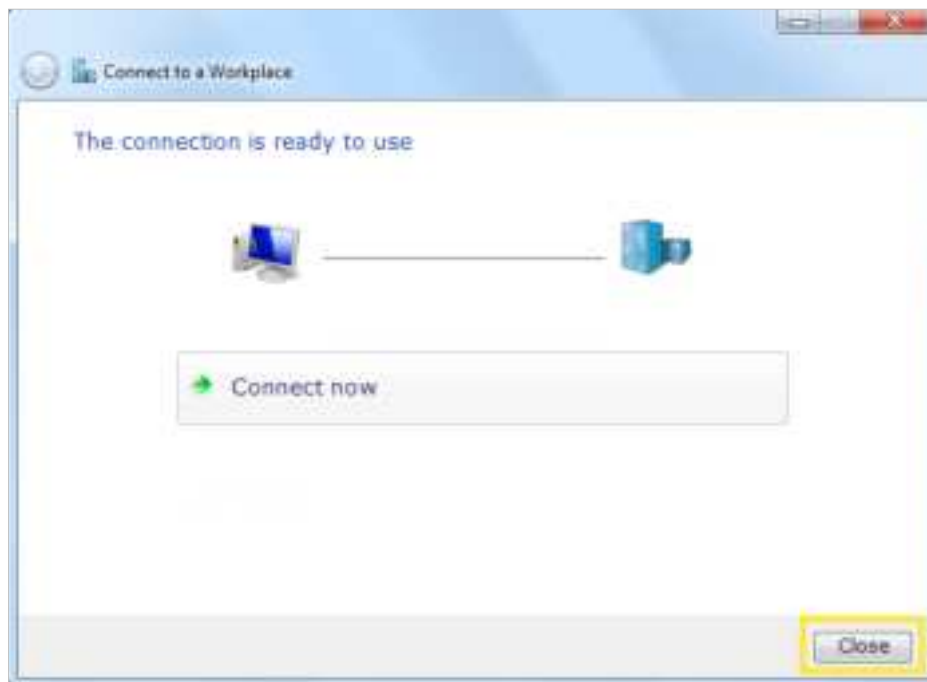
5. Enter the internet IP address of the router (for example: 218.18.1.73) in the **Internet address** field, and select the checkbox **Don't connect now; just set it up so I can connect later**. Click **Next**.



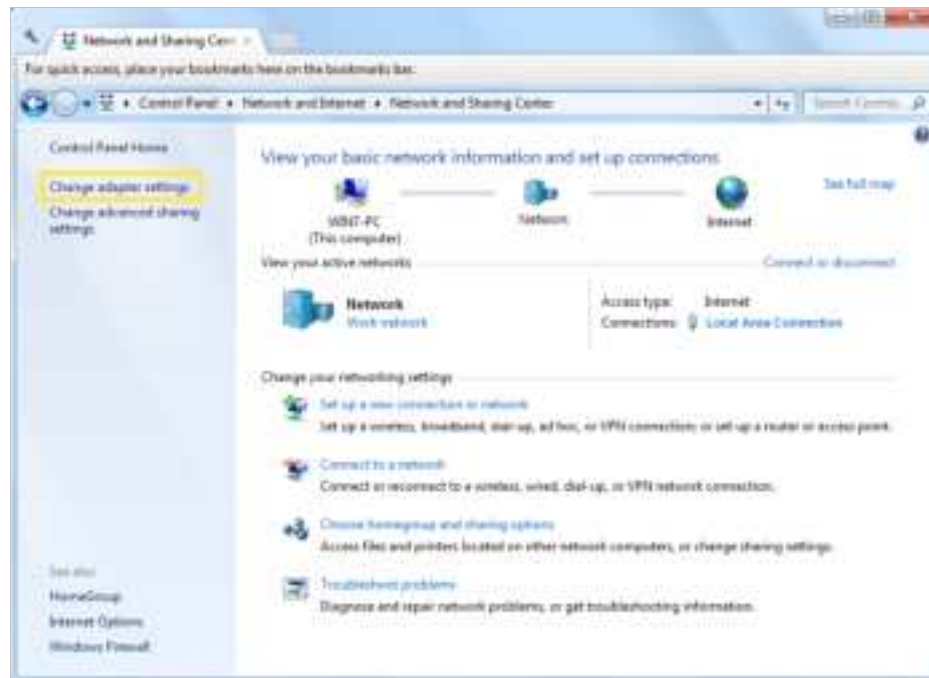
6. Enter the **User name** and **Password** you have set for the IPSec VPN server on your remote device, and click **Connect**.



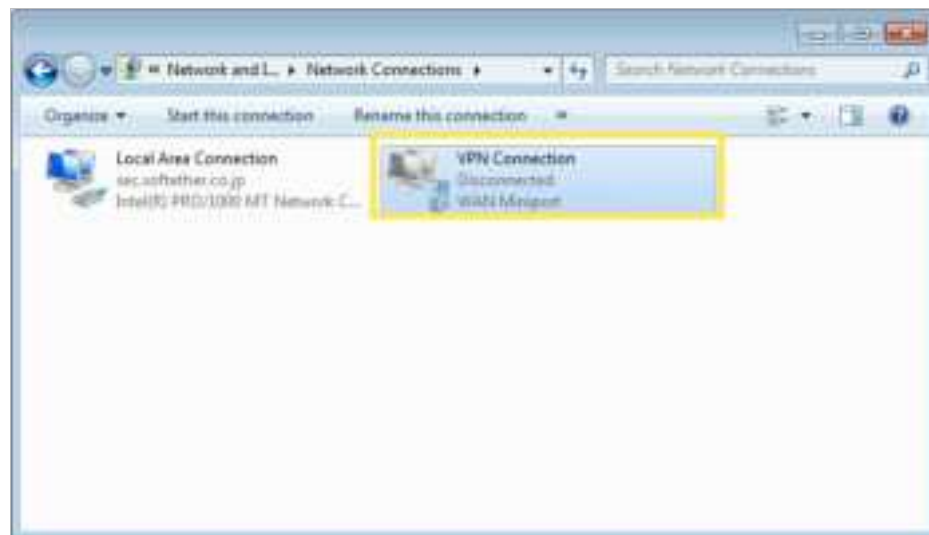
7. Click [Close](#) when the VPN connection is ready to use.



8. Go to [Network and Sharing Center](#) and click [Change adapter settings](#).



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



10. Enter the **User name** and **Password** you have set for the IPSec VPN server on your remote device, and click **Properties**.



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



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



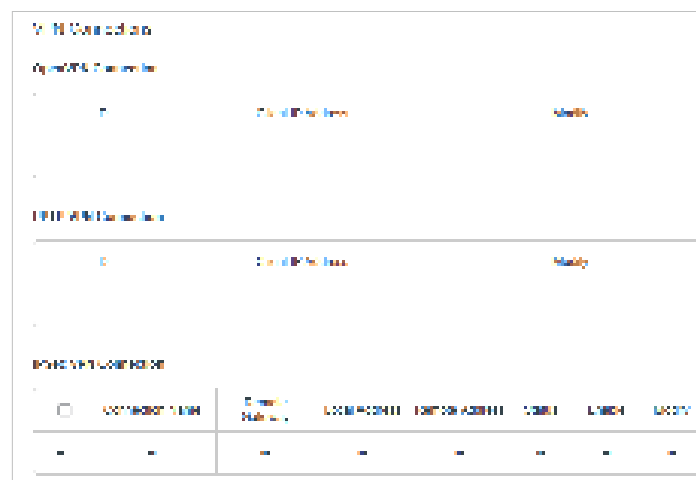
Done! Click **Connect** to start VPN connection.



14.4. VPN Connections

VPN Connections page displays the clients that are currently connected to the OpenVPN servers, PPTP VPN servers and IPSec VPN hosted on the router.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced** > **VPN** > **VPN connections**.



Chapter 15

Manage Your Router

This chapter introduces how to change the system settings and administrate your router's network.

This chapter contains the following sections:

- [Set System Time](#)
- [Control the LED](#)
- [Test Internet Connectivity](#)
- [Update the Firmware](#)
- [Back Up and Restore Configuration Settings](#)
- [Reboot the Router](#)
- [Administration Management](#)
- [System Log](#)
- [Monitor the Internet Traffic Statistics](#)

15.1. Set System Time

System time is the time displayed while the router is running. The system time you configure here will be used for other time-based functions like Parental Controls and Wireless Schedule. You can manually set how to get the system time.

Follow the steps below to set your system time.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [System Tools](#) > [Time Settings](#) page.

The screenshot shows the 'System Time' configuration page. It includes a 'Time Zone' dropdown menu set to '(GMT+01:00) Amsterdam, Berlin, Rome, Stockholm, Paris, Prague, Bratisl...'. The 'Date' field is set to '4/5/2024' with a '(MM/DD/YYYY)' label. The 'Time' field is set to '10 : 1 : 14'. The 'NTP' checkbox is checked and labeled 'Enable'. Below it are two 'NTP Server' fields, both set to '0.0.0.0' with '(Optional)' labels. At the bottom, there are two buttons: 'Get from PC' and 'Get from the Internet', and a 'Save' button on the right.

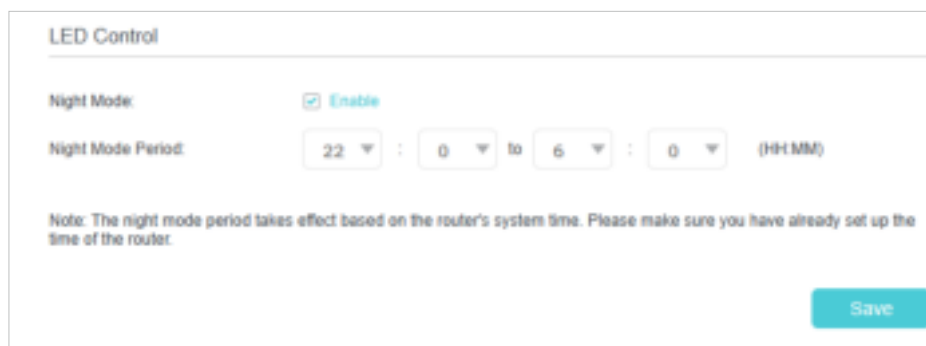
3. Configure the system time using the following methods:
[Get from PC](#): Click this button if you want to use the current time of your PC.
[Get from the Internet](#): Click this button if you want to get time from the internet. Make sure your router can access the internet before you select this way to get system time.
4. Click [Save](#).
5. After setting the system time, you can set [Daylight Saving Time](#) according to your needs. Enable [Daylight Saving Time](#), and set the start and end time and then click [Save](#) to make the settings effective.

The screenshot shows the 'Daylight Saving Time' configuration page. It features a checkbox labeled 'Enable Daylight Saving Time'. Below this, there are two rows of settings for 'Start' and 'End'. The 'Start' row is set for the year '2024', with a dropdown for 'Sun', 'M', 'Last', 'W', and 'Th', and a time dropdown set to '(00:00)'. The 'End' row is set for the year '2024', with a dropdown for 'Sun', 'M', 'Last', 'W', and 'Th', and a time dropdown set to '(03:00)'. A 'Save' button is located at the bottom right.

15.2. Control the LED

The LED of the router indicates its activities and status. You can enable the Night Mode feature to specify a time period during which the LED is off.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router.
2. Go to [Advanced](#) > [System](#) > [LED Control](#).
3. Enable [Night Mode](#).
4. Specify the LED off time, and the LED will be off during this period every day.
5. Click [Save](#).



The screenshot shows the 'LED Control' configuration page. At the top, the title 'LED Control' is displayed. Below it, the 'Night Mode' is set to 'Enable' with a checked checkbox. The 'Night Mode Period' is configured as '22 : 0' to '6 : 0' in HH:MM format. A note below the period settings states: 'Note: The night mode period takes effect based on the router's system time. Please make sure you have already set up the time of the router.' A 'Save' button is located at the bottom right of the form.

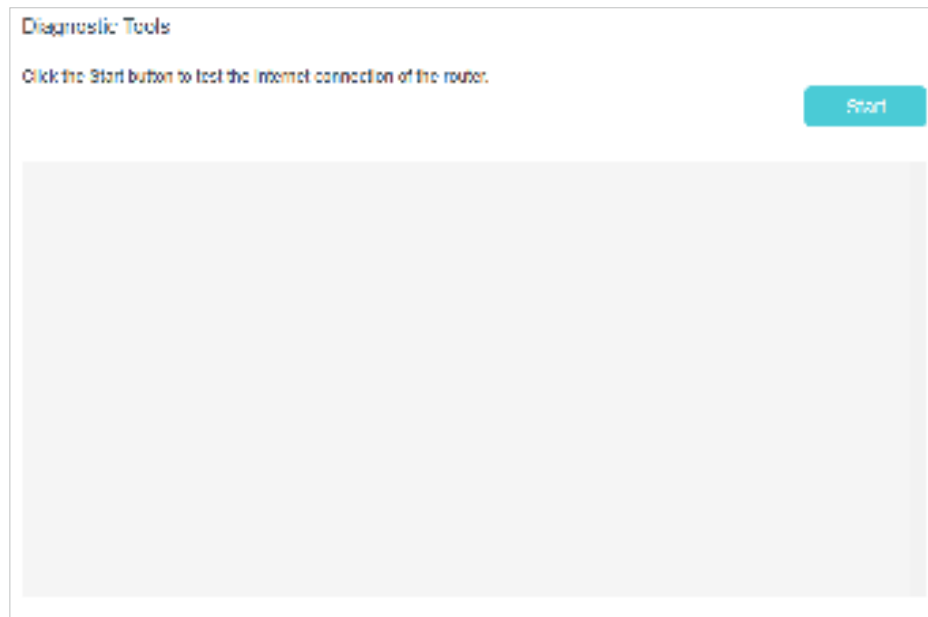
15.3. Test Internet Connectivity

Diagnostics function is used to test the connectivity between the router and the host or other network devices.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [System Tools](#) > [Diagnostics](#) page.

➤ **To test the internet connection of the router:**

Locate the [Diagnostic Tools](#) section, and click the [Start](#) to test the internet connectivity and you will find the test results in the gray box.



➤ **To run ping and traceroute tools:**

- 1) Locate the [Diagnostic Tools](#) section.

- 2) Select [Ping](#) or [Traceroute](#) or [Nslookup](#) as the diagnostic tool to test the connectivity.
 - [Ping](#) is used to test the connectivity between the router and the tested host, and measure the round-trip time.
 - [Traceroute](#) is used to display the route (path) your router has passed to reach the tested host, and measure transit delays of packets across an internet Protocol network.
 - [Nslookup](#) is used to queries the Domain Name System (DNS) to obtain the mapping between a domain name and IP address, or other DNS records.
- 3) Enter the [Target IP Address/Domain Name](#) of the tested host. You can change the default test options if necessary.

- 4) Click [Start](#) to begin the diagnostics, and you will find the test results in the gray box.

15.4. Update the Firmware

TP-Link is dedicated to improving product features, giving you a better network experience.

We will inform you through the web management page if there's any update firmware available for your router. The latest firmware can also be downloaded from the [Support](#) page of our website www.tp-link.com for free.

Note:

1. Make sure that you have a stable connection between the router and your computer. It is NOT recommended to upgrade the firmware wirelessly.
2. Back up your router configuration before upgrading the firmware.
3. DO NOT turn off the router during the firmware upgrade.

➤ Follow the steps below to upgrade the firmware online:

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [System Tools](#) > [Firmware Upgrade](#).
3. Click Check for Upgrades.



4. If a new firmware is displayed, click Upgrade and click Yes when prompted, then the router will automatically download the latest firmware file and upgrade.

➤ Follow the steps below to manually update the firmware:

1. Download the latest firmware file for the router from our website www.tp-link.com.
2. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
3. Go to [Advanced](#) > [System Tools](#) > [Firmware Upgrade](#).
4. Focus on the [Device Information](#) section. Make sure the downloaded firmware file matches with the [Hardware Version](#).

Device Information

Firmware Version:

1.0.0.0 (1.0.0.0) (1.0.0.0) (1.0.0.0) (1.0.0.0) (1.0.0.0)

Hardware Version:

1.0.0.0 (1.0.0.0) (1.0.0.0) (1.0.0.0) (1.0.0.0)

Serial Number:

1.0.0.0 (1.0.0.0) (1.0.0.0) (1.0.0.0) (1.0.0.0)

IMEI:

1.0.0.0 (1.0.0.0) (1.0.0.0) (1.0.0.0) (1.0.0.0)

Module version:

1.0.0.0 (1.0.0.0) (1.0.0.0) (1.0.0.0) (1.0.0.0)

Module SN:

1.0.0.0 (1.0.0.0) (1.0.0.0) (1.0.0.0) (1.0.0.0)

5. Focus on the [Local Upgrade](#) section. Click [Browse](#) to locate the downloaded new firmware file, and click [Upgrade](#).

Local Upgrade

-	ID	Device Name	Model Name	MAC Address	Firmware Version
<input checked="" type="checkbox"/>	1	Archer NX200_F527	Archer NX200	1.0.0.0 (1.0.0.0) (1.0.0.0) (1.0.0.0) (1.0.0.0)	1.0.0.0 (1.0.0.0) (1.0.0.0) (1.0.0.0) (1.0.0.0)

New Firmware File:

Browse

Upgrade

6. Wait a few minutes for the upgrading and rebooting.

15.5. Back Up and Restore Configuration Settings

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

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [System Tools](#) > [Backup & Restore](#).

➤ To back up configuration settings:

Click [Backup](#) to save a copy of the current settings to your local computer. A conf.bin file will be stored to your computer.

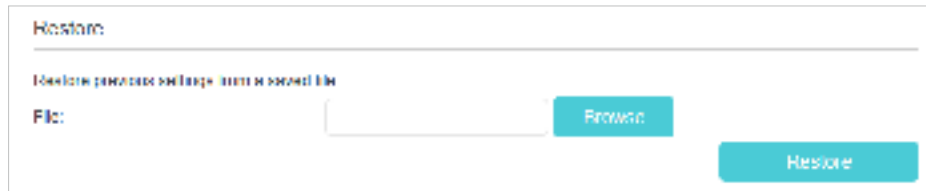
Backup

Save a copy of your current settings.

Backup

➤ **To restore configuration settings:**

- 1) Click [Browse](#) to locate the previous backup configuration file, and click [Restore](#).

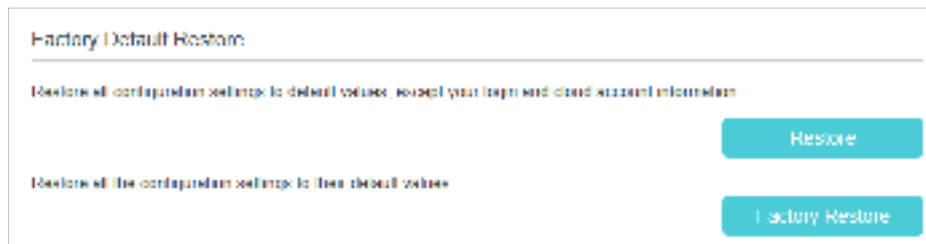


The screenshot shows a web interface titled "Restore". Below the title is a subtitle: "Restore previous settings from a saved file". There is a text input field labeled "File:" followed by a "Browse" button. To the right of the input field is a "Restore" button.

- 2) Wait a few seconds for the restoring and rebooting.

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

- 1) Locate the [Factory Default Restore](#) section, and click [Factory Restore](#) to reset the router.



The screenshot shows a web interface titled "Factory Default Restore". Below the title is a subtitle: "Restore all configuration settings to default values, except your login and cloud account information". There are two buttons: "Restore" and "Factory Restore".

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

■ **Note:**

1. During the resetting process, do not turn off the router.
2. We strongly recommend you back up the current configuration settings before resetting the router.


15.6. Reboot the Router

The Reboot feature cleans the cache to enhance the running performance of the router. You can reboot the router manually or set it to reboot regularly.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [System Tools](#) > [Reboot Schedule](#), and you can restart your router.

➤ **To reboot the router manually:**

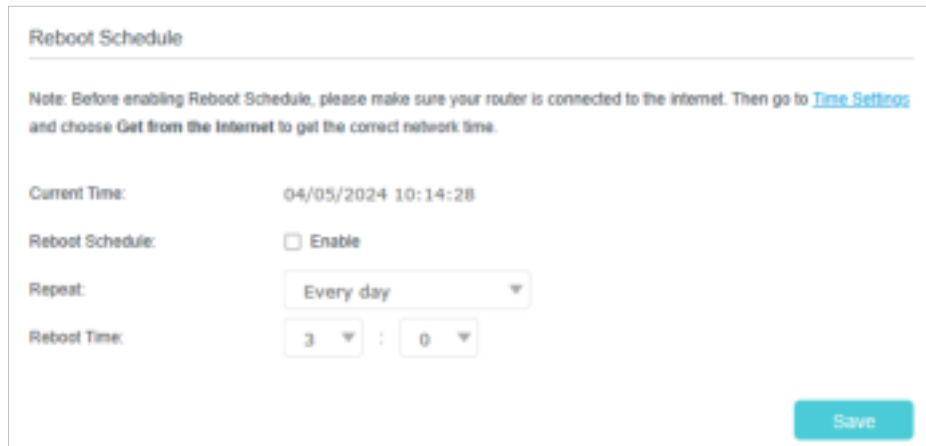
Click [Reboot](#), and wait a few minutes for the router to rebooting.



The screenshot shows a web interface titled "System Reboot". Below the title is a subtitle: "Reboot the router". There is a "Reboot" button.

➤ **To schedule the router to reboot at a specific time:**

- 1) Enable [Reboot Schedule](#).
- 2) Specify the [Time](#) when the router reboots.



- 3) Click [Save](#) to make the settings effective.

Some settings of the router may take effect only after rebooting, including:

- Change the LAN IP Address (system will reboot automatically).
- Change the Operation Mode (system will reboot automatically).
- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router to its factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically).

Note:

The Auto Reboot feature takes effect based on the router's system time. Please make sure you have already set up the time of the router.

15.7. Administration Management

15.7.1. Change the Login Password

A login password is required to log in to the router's web management page. You are asked to set a login password at first login. You can change it with the account management feature.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [System Tools](#) > [Administration](#), and locate the [Account Management](#) section.



The screenshot shows the 'Account Management' section of a router's web interface. It contains three input fields: 'Old Password', 'New Password', and 'Confirm New Password'. Each field has a small eye icon to the right for toggling visibility. The 'New Password' field has a dropdown menu with options 'Lower', 'Mixed', and 'Upper'. A teal 'Save' button is located at the bottom right of the form.

3. Enter the old password and a new password twice (both case-sensitive).
4. Click [Save](#) to make the settings effective.

15.7.2. Local Management

You can control the local devices' authority to manage the router via Local Management feature. By default all local connected devices are allowed to manage the router. You can also specify one device to manage the router and enable local management over a more secure way, HTTPS.

Follow the steps below to allow only the specific device to manage the router via the local management over HTTPS.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [System Tools](#) > [Administration](#), and locate the [Local Management](#) section.
3. Enable [Local Management over HTTPS](#) and keep the [Port for HTTP](#) and [Port for HTTPS](#) as the default settings. Enter the [IP address](#) or [MAC address](#) of the local device to manage the router.



The screenshot shows the 'Local Management' section. It includes four settings: 'Port for HTTP' (set to 80), 'Local Management via HTTPS' (checked 'Enable'), 'Port for HTTPS' (set to 443), and 'IP/MAC Address' (empty). A teal 'Save' button is at the bottom right.

4. Click [Save](#).

Now, you can manage the router over both HTTP (<http://tplinkmodem.net>) and HTTPS (<https://tplinkmodem.net>).

Note:

If you want all local devices can manage the router, just leave the [IP/MAC Address](#) field blank.

15. 7. 3. Remote Management

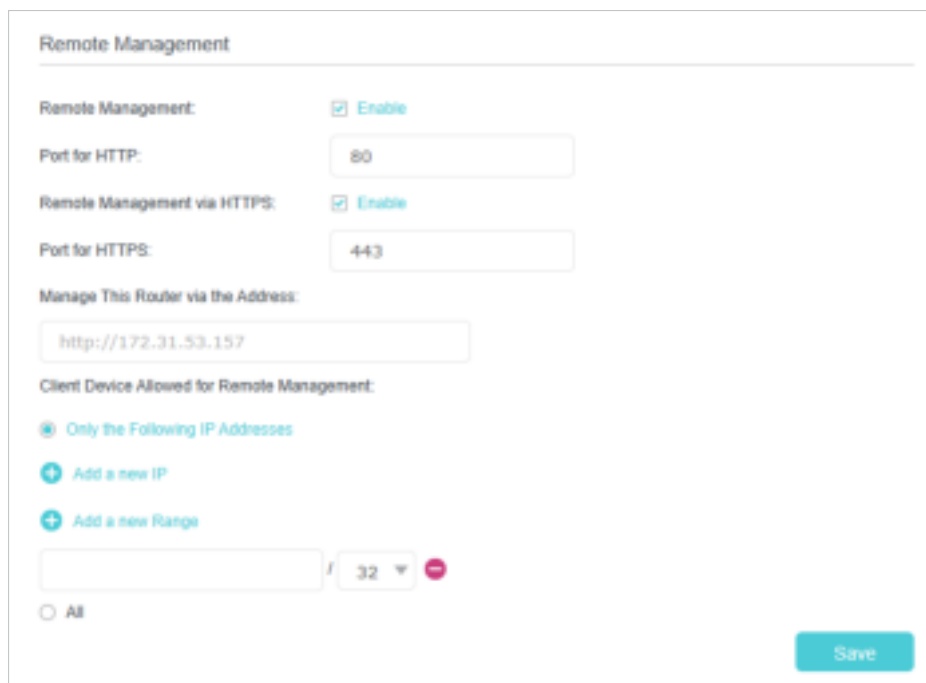
By default, the remote devices are not allowed to manage the router from the internet. You can enable remote management over HTTP and/or HTTPS if needed. HTTPS is a more secure way to access the router.

Note:

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

Follow the steps below to allow remote devices to manage the router over HTTPS.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [System Tools](#) > [Administration](#), and locate the [Remote Management](#) section.



The screenshot shows the 'Remote Management' configuration page. It includes the following settings:

- Remote Management:** ☒ [Enable](#)
- Port for HTTP:**
- Remote Management via HTTPS:** ☒ [Enable](#)
- Port for HTTPS:**
- Manage This Router via the Address:**
- Client Device Allowed for Remote Management:**
 - ☒ [Only the Following IP Addresses](#)
 - [+ Add a new IP](#)
 - [+ Add a new Range](#)
 - / [-](#)
 - ☐ [All](#)

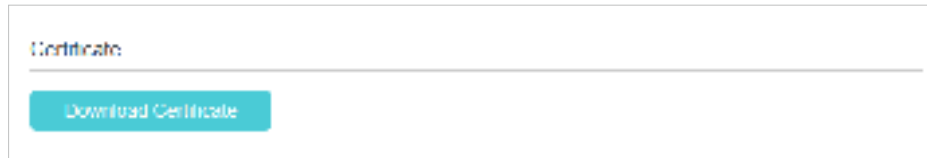
A [Save](#) button is located at the bottom right of the form.

3. Enable [Remote Management](#) and [Remote Management via HTTPS](#) to allow for HTTPS connection. Keep the [Port](#) as the default setting.
4. Set the client device allowed for remote management. Select [All](#) to allow all remote devices to manage the router. If you just want to allow a specific device to manage the router, select [Only the Following IP/MAC Address](#) and enter the IP/MAC address of the remote device.
5. Click [Save](#).

All devices or the specific device on the internet can log in to your router using the address displayed on the [Manage This Router via the Address](#) field to manage the router.

 **Tips:**

1. If you were warned about the certificate when visiting the web management page remotely, click [Trust](#) (or a similar option) to continue. To avoid this warning, you can download and install the certificate on the router's web management page at [Advanced > System Tools > Administration](#).



2. The router's WAN IP is usually a dynamic IP. Please refer to [Set Up a Dynamic DNS Service Account](#) if you want to log in to the router through a domain name.

15.7.4. HTTP Referer Head Check

HTTP referer header check function can protect your networks against CSRF attacks. This function is enabled by default. You can disable this function if needed.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced > System Tools > Administration](#), and locate the [HTTP Referer Head Check](#) section.
3. Clear the [Enable](#) check box and click [Save](#) if you want to disable this function.

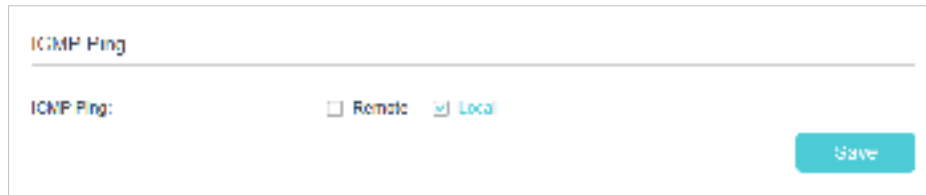


15.7.5. ICMP Ping

ICMP (Internet Control Message Protocol) Ping is used to diagnose the network by sending ICMP echo request packets to the target remote or local host and waiting for an ICMP response.

You can control the router's replies to ICMP Ping requests.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced > System Tools > Administration](#), and locate the [ICMP Ping](#) section.



3. Specify the ICMP Ping reply options.
 - **Remote:** Select it if you want the computers on a public network to ping the router's WAN IP address.
 - **Local:** Enabled by default, if enabled, the computers on a private network can ping the router's LAN IP address.
4. Click **Save** to make the settings effective.

15.7.6. Session ID

When Session ID function is enabled, it will be saved into Flash every time the PPP connection is updated. This can prevent some problems of PPPoE/L2TP/PPTP connection being rejected to reconnect to servers when the device is powered off or the network disconnect accidentally.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to **Advanced > System Tools > Administration**, and locate the **Session ID** section.



3. Enable the **Update Session ID** and Click **Save** to make the settings effective.

15.8. System Log

System Log can help you know what happened to your router, facilitating you to locate the malfunctions. For example when your router does not work properly, you may need to save the system log and send it to the technical support for troubleshooting.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to **Advanced > System Tools > System Log** page.

System Log

Type: ALL ▼

Level: Debug ▼

[Refresh](#) [Delete All](#)

ID	Time	Type	Level	Log Content
1	2024-04-05 10:30:06	HTTPD	Notice	Clear log.

[Log Settings](#) [Save Log](#)

➤ **To view the system logs:**

You can view specific system logs by selecting the log type and level.

Click [Refresh](#) to refresh the log list.

➤ **To save the system logs:**

You can save the system logs to your local computer or a remote server.

Click [Save Log](#) to save the logs in a txt file to your computer.

Click [Log Settings](#) to set the storage path of logs.

Log Settings

☒ [Save Locally](#)

Minimum Level: Information ▼

☒ [Save Remotely](#)

Minimum Level: Warning ▼

Server IP:

Server Port: 514

Local Facility Name: User ▼

[Back](#) [Save](#)

- [Save Locally](#): Select this option to cache the system log to the router's local memory, select the minimum level of system log to be saved from the drop-down list. The logs will be shown in the table in descending order on the System Log page.
- [Save Remotely](#): Select this option to send the system log to a remote server, select the minimum level of system log to be saved from the drop-down list and enter the information of the remote server. If the remote server has a log viewer client or a sniffer tool implemented, you can view and analyze the system log remotely in real-time.

15.9. Monitor the Internet Traffic Statistics

The traffic statistics function allows you to monitor the volume of internet traffic statistics. You can view the network traffic of the LAN, WAN and WLAN sent and received packets.

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [System Tools](#) > [Traffic Statistics](#).
3. Turn on [Enable Traffic Statistics](#) to enable traffic statistics function, you can view the total number of packets and bytes received and transmitted by the router within the selected [Statistics Interval](#). This function is disabled by default.



4. You can refer to [Traffic Statistics List](#) for the detailed information about the traffic usage of all devices.

Traffic Statistics List								
<div><div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div></div></div>								

FAQ

Q1. What should I do if I forget my wireless password?

The default wireless password is printed on the label of the router. If the password has been altered:

1. Connect your computer to the router using an Ethernet cable.
2. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with the password you set for the router.
3. Go to [Wireless](#) to retrieve or reset your wireless password.

Q2. What should I do if I forget my web management password?

- If you are using a TP-Link ID to log in, click [Forgot Password](#) on the login page and then follow the instructions to reset it.
- Alternatively, press and hold the [Reset](#) button of the router until the Power LED blinks to restore factory default settings, and then Visit <http://tplinkmodem.net> or <http://192.168.1.1> to create a new login password.

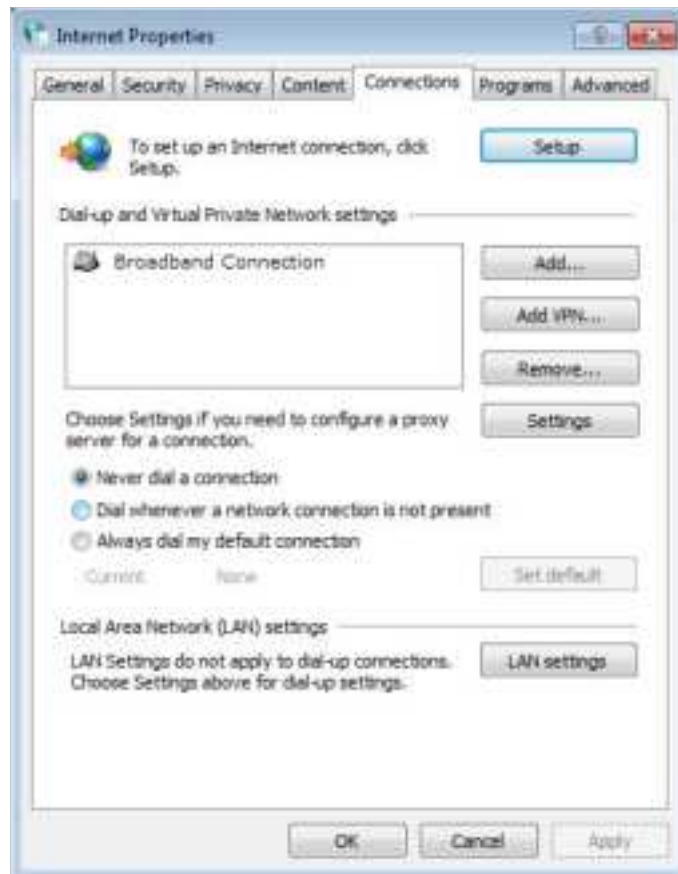
Note:

- You'll need to reconfigure the router to surf the internet once the router is reset, and please mark down your new password for future use.

Q3. What should I do if I can't log in to the router's web management page?

This can happen for a variety of reasons. Please try the methods below to log in again.

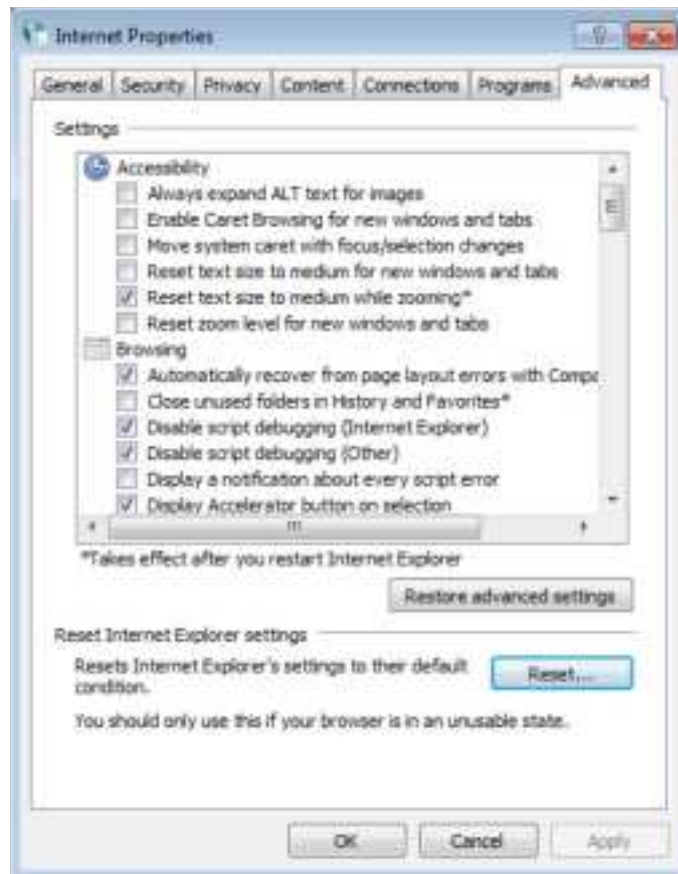
- Make sure your computer is connected to the router correctly and the corresponding LED indicator(s) light up.
- Make sure the IP address of your computer is configured as [Obtain an IP address automatically](#) and [Obtain DNS server address automatically](#).
- Make sure <http://tplinkmodem.net> or <http://192.168.1.1> is correctly entered.
- Check your computer's settings:
 - 1) Go to [Start](#) > [Control Panel](#) > [Network and Sharing Center](#).
 - 2) Click [Internet Options](#) on the bottom left.
 - 3) Click [Connections](#) and select [Never dial a connection](#).



4) Click [LAN settings](#) and deselect the following three options and click [OK](#).



5) Go to [Advanced](#) > [Restore advanced settings](#), click [OK](#) to save the settings.



- Use another web browser or computer to log in again.
- Reset the router to factory default settings and try again. If login still fails, please contact the technical support.

Note: You'll need to reconfigure the router to surf the internet once the router is reset.

Q4. What should I do if I can't access the internet even though the EWAN configuration is finished?

1. Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router.
2. Go to **Advanced > Status** to check internet status:

If IP Address is a valid one, please try the methods below and try again:

- Your computer might not recognize any DNS server addresses. Please manually configure the DNS server.
 - 1) Go to **Advanced > Network > LAN Settings > DHCP Server**.
 - 2) Enter 8.8.8.8 as Primary DNS, click **SAVE**.

Tips: 8.8.8.8 is a safe and public DNS server operated by Google.

DHCP Server
IPv4 | IPv6

MAC Address:

74:FE:CE:B7:F5:27

IP Address:

192 . 168 . 1 . 1

Subnet Mask:

255.255.255.0

IGMP Snooping:

☒ Enable

Second IP:

☐ Enable

DHCP:

☒ Enable

☒ DHCP Server ☐ DHCP Relay

IP Address Pool:

192 . 168 . 1 . 2 - 192 . 168 . 1 . 249

Address Lease Time:

120 minutes. (1-2880. The default value is 120.)

Default Gateway:

0 . 0 . 0 . 0 (Optional)

Default Domain:

(Optional)

Primary DNS:

0 . 0 . 0 . 0 (Optional)

Secondary DNS:

0 . 0 . 0 . 0 (Optional)

Save

- Restart the modem and the router.
 - 1) Power off your modem and router, and leave them off for 1 minute.
 - 2) Power on your modem first, and wait about 2 minutes until it gets a solid cable or Internet light.
 - 3) Power on the router.
 - 4) Wait another 1 or 2 minutes and check the internet access.
- Reset the router to factory default settings and reconfigure the router.
- Upgrade the firmware of the router.
- Check the TCP/IP settings on the particular device if all other devices can get internet from the router.

As the picture below shows, if the IP Address is 0.0.0.0, please try the methods below and try again:

Internet	
WAN Interface Name	lpo0_0_0_d
MAC Address	7E:FE:CE:B7:F5:28
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Connection Type	Dynamic IP
Up time	0 days 00:00:00

- Make sure the physical connection between the router and the modem is proper.
- Clone the MAC address of your computer.
 - 1) Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router.
 - 2) Go to [Internet](#) or [Advanced](#) > [Network](#) > [Internet](#) and focus on the [MAC Clone](#) section.
 - 3) Choose an option as needed (enter the MAC address if [Use Custom MAC Address](#) is selected), and click [SAVE](#).

MAC Clone:

☒ Use Default MAC Address
☐ Clone Current Computer MAC Address
☐ Use Custom MAC Address

Tips:

- Some ISP will register the MAC address of your computer when you access the internet for the first time through their Cable modem, if you add a router into your network to share your internet connection, the ISP will not accept it as the MAC address is changed, so we need to clone your computer's MAC address to the router.
- The MAC addresses of a computer in wired connection and wireless connection are different.

- **Modify the LAN IP address of the router.**

Note:

Most TP-Link routers use 192.168.0.1/192.168.1.1 as their default LAN IP address, which may conflict with the IP range of your existing ADSL modem/router. If so, the router is not able to communicate with your modem and you

can't access the internet. To resolve this problem, we need to change the LAN IP address of the router to avoid such conflict, for example, 192.168.2.1.

- 1) Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router.
- 2) Go to [Advanced](#) > [Network](#) > [LAN Settings](#).
- 3) Modify the LAN IP address as the follow picture shows. Here we take 192.168.2.1 as an example.
- 4) Click [Save](#).



DHCP Server		IPv4 IPv6
MAC Address:	74:FE:CE:B7:F5:27	
IP Address:	192 - 168 - 2 - 1	
Subnet Mask:	255.255.255.0 ▼	

- Restart the modem and the router.
 - 1) Power off your modem and router, and leave them off for 1 minute.
 - 2) Power on your modem first, and wait about 2 minutes until it get a solid cable or Internet light.
 - 3) Power on the router.
 - 4) Wait another 1 or 2 minutes and check the internet access.
- Double check the internet connection type.
 - 1) Confirm your internet connection type, which can be learned from the ISP.
 - 2) Visit <http://tplinkmodem.net> or <http://192.168.1.1>, and log in with your TP-Link ID or the password you set for the router.
 - 3) Go to [Advanced](#) > [Network](#) > [Internet](#).
 - 4) Select your [Internet Connection Type](#) and fill in other parameters.
 - 5) Click [Save](#).

Internet Setup

Connection Name	Service Type	VLAN ID	Status	Operation	Enable	Modify
ipoe_0_0_d	Internet	AAA	Connected	Disconnect		

Connection Name: (Optional)

☒ Enable This Entry

Service Type: ☒ Internet ☐ IPTV ☐ TR069 ☐ Others

Default Gateway:

Internet Connection Type:

VLAN ID:

IPv4

IP Address:

Subnet Mask:

Gateway:

IPv6

IPv6 Tunnel:

☐ Enable

☒ Advanced

6) Restart the modem and the router again.

- Please upgrade the firmware of the router.

If you've tried every method above but still cannot access the internet, please contact the technical support.

Q5.What should I do if I can't find my wireless network or I cannot connect the wireless network?

If you fail to find any wireless network, please follow the steps below:

- Make sure the wireless function of your device is enabled if you're using a laptop with built-in wireless adapter. You can refer to the relevant document or contact the laptop manufacturer.
- Make sure the wireless adapter driver is installed successfully and the wireless adapter is enabled.
 - **On Windows 7/8/10/11**
 - 1) If you see the message [No connections are available](#), it is usually because the wireless function is disabled or blocked somehow.
 - 2) Click [Troubleshoot](#) and windows might be able to fix the problem by itself.

- **On Windows XP**

- 1) If you see the message [Windows cannot configure this wireless connection](#), this is usually because windows configuration utility is disabled or you are running another wireless configuration tool to connect the wireless.
- 2) Exit the wireless configuration tool (the TP-Link Utility, for example).
- 3) Select and right click on [My Computer](#) on desktop, select [Manage](#) to open Computer Management window.
- 4) Expand [Services and Applications](#) > [Services](#), find and locate [Wireless Zero Configuration](#) in the Services list on the right side.
- 5) Right click [Wireless Zero Configuration](#), and then select [Properties](#).
- 6) Change [Startup type](#) to [Automatic](#), click on Start button and make sure the Service status is [Started](#). And then click [OK](#).

If you can find other wireless network except your own, please follow the steps below:

- Check the WLAN LED indicator on your wireless router/modem.
- Make sure your computer/device is still in the range of your router/modem. Move it closer if it is currently too far away.
- Go to [Wireless](#) or [Advanced](#) > [Wireless](#) > [Wireless Settings](#), and check the wireless settings. Double check your wireless Network Name and SSID is not hidid.

If you can find your wireless network but fail to connect, please follow the steps below:

- **Authenticating problem/password mismatch:**

- 1) Sometimes you will be asked to type in a PIN number when you connect to the wireless network for the first time. This PIN number is different from the Wireless Password/Network Security Key, usually you can only find it on the label of your router.



- 2) If you cannot find the PIN or PIN failed, you may choose [Connecting using a security key instead](#), and then type in the [Wireless Password/Network Security Key](#).

- 3) If it continues to show note of [Network Security Key Mismatch](#), it is suggested to confirm the wireless password of your wireless router.

 **Note:** Wireless Password/Network Security Key is case sensitive.

- **Windows unable to connect to XXXX / Can not join this network / Taking longer than usual to connect to this network:**
 - Check the wireless signal strength of your network. If it is weak (1~3 bars), please move the router closer and try again.
 - Change the wireless Channel of the router to reduce interference from other networks.
 - Re-install or update the driver for your wireless adapter of the computer.

Q6. What should I do if I can't access the internet even though the Mobile WAN (SIM card) configuration is finished?

- Verify that your SIM card is a 5G/4G or WCDMA card.
- Verify that your SIM card is in your internet service provider's service area.
- Verify that your SIM card has sufficient credit.
- Check the LAN connection: Open a web browser and enter <http://tplinkmodem.net> or <http://192.168.1.1> in the address bar. If the login page does not appear, refer to Q1 and then try again.
- Launch a web browser, log in to the web management page, and check the following:
 - 1) Go to [Advanced](#) > [Network](#) > [Mobile WAN](#) to verify the parameters provided by your ISP are correctly entered. If the parameters are incorrect, click [Create Profile](#) and enter the correct parameters, then select the new profile from the [Profile Name](#) list.
 - 2) Go to [Advanced](#) > [Network](#) > [PIN Management](#) to verify if PIN is required. If it is, enter the correct PIN provided by your ISP, and click [Save](#).
 - 3) Go to [Advanced](#) > [Network](#) > [Data Settings](#) to verify if the Total/Monthly Used exceeds the Total/Monthly Allowance. If it does, click [Correct](#) and set Total/Monthly Used to 0 (zero), or disable [Data Limit](#).
 - 4) Go to [Advanced](#) > [Network](#) > [Mobile WAN](#) to verify that [Mobile Data](#) is enabled. If it is not, enable it to access the internet.
 - 5) Confirm with your ISP if you are in a roaming service area. If you are, go to [Advanced](#) > [Network](#) > [Mobile WAN](#) to enable [Data Roaming](#).
 - 6) Confirm the selection of [Antenna Type](#).
If it is determined that an external antenna is connected, enable [External Antennas](#).
If you are sure that no external antenna is connected, disable [External Antennas](#).

CE Mark Warning



OPERATING FREQUENCY(the maximum transmitted power)

2400MHz~2483.5MHz (20dBm)

5150MHz~5250MHz (23dBm)

5250MHz~5350MHz (23dBm)

5470MHz~5725MHz (30dBm)

5G n1,3,5,7,8,20,28,38(23 dBm \pm 2 dB)

5G n40,41,77,78(26 dBm +2/-3 dB)

LTE Band1,3,5,7,8,20,28,32,38,40,41,42,43 (23 dBm \pm 2 dB)

WCDMA Band 1,5,8(23 dBm \pm 2 dB)

Frequency band: 5150 - 5250 MHz:

Indoor use: Inside buildings only. Installations and use inside road vehicles and train carriages are not permitted. Limited outdoor use: If used outdoors, equipment shall not be attached to a fixed installation or to the external body of road vehicles, a fixed infrastructure or a fixed outdoor antenna. Use by unmanned aircraft systems (UAS) is limited to within the 5170 - 5250 MHz band.

Frequency band: 5250 - 5350 MHz:

Indoor use: Inside buildings only. Installations and use in road vehicles, trains and aircraft are not permitted. Outdoor use is not permitted.

Frequency band: 5470 - 5725 MHz:

Installations and use in road vehicles, trains and aircraft and use for unmanned aircraft systems (UAS) are not permitted.

EU Declaration of Conformity

TP-Link hereby declares that the device is in compliance with the essential requirements and other relevant provisions of directives 2014/53/EU, 2009/125/EC, 2011/65/EU and (EU)2015/863.


The original EU Declaration of Conformity may be found at
<https://www.tp-link.com/en/support/ce/>

RF Exposure Information

This device meets the EU requirements (2014/53/EU Article 3.1a) on the limitation of exposure of the general public to electromagnetic fields by way of health protection.

The device complies with RF specifications when the device is used at 20 cm from your body.

National Restrictions

	AT	BE	BG	CH	CY	CZ	DE	DK
	EE	EL	ES	FI	FR	HR	HU	IE
	IS	IT	LI	LT	LU	LV	MT	NL
	NO	PL	PT	RO	SE	SI	SK	UK(IN)

UKCA Mark



UK Declaration of Conformity

TP-Link hereby declares that the device is in compliance with the essential requirements and other relevant provisions of the Radio Equipment Regulations 2017.

The original UK Declaration of Conformity may be found at <https://www.tp-link.com/support/ukca/>

National Restrictions

Attention: This device may only be used indoors in Great Britain.



Korea Warning Statements:

당해 무선설비는 운용중 전파혼신 가능성이 있음.



NCC Notice & BSMI Notice:

注意!

取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前述合法通信，指依電信管理法規定作業之無線電通信。

低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

應避免影響附近雷達系統之操作。

減少電磁波影響，請妥適使用。

電波功率密度 MPE 標準值：1 mW/cm²，送測產品實測值：0.3604 mW/cm²，建議使用時設備天線至少距離人體20公分。

安全諮詢及注意事項

- 請使用原裝電源供應器或只能按照本產品注明的電源類型使用本產品。
- 清潔本產品之前請先拔掉電源線。請勿使用液體、噴霧清潔劑或濕布進行清潔。
- 注意防潮，請勿將水或其他液體潑灑到本產品上。
- 插槽與開口供通風使用，以確保本產品的操作可靠並防止過熱，請勿堵塞或覆蓋開口。
- 請勿將本產品置放於靠近熱源的地方。除非有正常的通風，否則不可放在密閉位置中。
- 不要私自拆開機殼或自行維修，如產品有故障請與原廠或代理商聯繫。

限用物質含有情況標示聲明書

設備名稱：5G AX1800 Wireless Dual Band Gigabit Router Equipment name				型號（型式）：Archer NX200/Archer NX210 Type designation (Type)		
單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛 Lead (Pb)	汞 Mercury (Hg)	鎘 Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr ⁺⁶)	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
PCB	○	○	○	○	○	○
外殼	○	○	○	○	○	○
電源供應器	—	○	○	○	○	○
其他及其 配件	—	○	○	○	○	○

備考1. “超出0.1 wt %” 及 “超出0.01 wt %” 係指限用物質之百分比含量超出百分比含量基準值。

Note 1: “Exceeding 0.1 wt %” and “exceeding 0.01 wt %” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2. “○” 係指該項限用物質之百分比含量未超出百分比含量基準值。

Note 2: “○” indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3. “—” 係指該項限用物質為排除項目。

Note 3: The “—” indicates that the restricted substance corresponds to the exemption.



Продукт сертифіковано згідно с правилами системи УкрСЕПРО на відповідність вимогам нормативних документів та вимогам, що передбачені чинними законодавчими актами України.



Safety Information

- Keep the device away from water, fire, humidity or hot environments.
- Do not attempt to disassemble, repair, or modify the device. If you need service, please contact us.
- Do not use damaged charger or USB cable to charge the device.
- Do not use any other chargers than those recommended.
- Do not use the device where wireless devices are not allowed.
- Adapter shall be installed near the equipment and shall be easily accessible.
- Use only power supplies which are provided by manufacturer and in the original packing of this product. If you have any questions, please don't hesitate to contact us.

Operating Temperature: 0°C~40°C

This product uses radios and other components that emit electromagnetic fields. Electromagnetic fields and magnets may interfere with pacemakers and other implanted medical devices. Always keep the product and its power adapter more than 15 cm (6 inches) away from any pacemakers or other implanted medical devices. If you suspect your product is interfering with your pacemaker or any other implanted medical device, turn off your product and consult your physician for information specific to your medical device.

















Please read and follow the above safety information when operating the device. We cannot guarantee that no accidents or damage will occur due to improper use of the device. Please use this product with care and operate at your own risk.

- 請勿使用損壞的充電器或USB線來供應設備充電。

- 請勿使用推薦充電器以外的任何其他充電器。
- 變壓器應安裝在設備附近且易於操作。
- 運作溫度: 0°C~40°C (32°F~104°F)

Explanations of the symbols on the product label

Note: The product label can be found at the bottom of the product and its I.T.E. power supply. Symbols may vary from products.

Symbol	Explanation
	Class II equipment
	Class II equipment with functional earthing
	Alternating current
	Direct current
	Polarity of d.c. power connector
	For indoor use only
	Dangerous voltage
	Caution, risk of electric shock
	Energy efficiency Marking
	Protective earth
	Earth
	Frame or chassis
	Functional earthing
	Caution, hot surface
	Caution
	Operator's manual

Symbol	Explanation
	Stand-by
	"ON" / "OFF" (push-push)
	Fuse
	Fuse is used in neutral N
	<p>RECYCLING</p> <p>This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/EU in order to be recycled or dismantled to minimize its impact on the environment.</p> <p>User has the choice to give his product to a competent recycling organization or to the retailer when he buys a new electrical or electronic equipment.</p>
	Caution, avoid listening at high volume levels for long periods
	Disconnection, all power plugs
m	Switch of mini-gap construction
μ	<p>Switch of micro-gap construction (for US version)</p> <p>Switch of micro-gap / micro-disconnection construction (for other versions except US)</p>
ε	Switch without contact gap (Semiconductor switching device)

產品標籤上符號的解釋

注意：產品標籤可以在產品底部和其I.T.E.電源供應器上找到。

符號可能因產品而異

符號	說明
	II類設備
	具有功能接地的II類設備
	交流
	直流
	輸出端點的極性

符號	說明
	僅供室內使用
	危險電壓
	請注意，有觸電的危險
	能源效率標誌
	保護接地
	接地
	功能接地
	功能接地
	請注意，表面過熱
	警告
	操作手冊
	待機
	“開啟” / “關閉”（按壓式）
	保險絲
	保險絲用於中性線N
	<p>回收</p> <p>這個產品帶有歐盟指令2012/19/EU中關於廢棄電氣電子設備（WEEE）的選擇性分類標誌。這意味著，該產品必須按照該指令處理，以便進行回收或拆解，從而最大限度地減少對環境的影響。用戶可以選擇將產品交給有資格的回收機構，或在購買新的電器或電子設備時將其交給零售商進行回收。</p>
	請小心，避免長時間以高音量收聽。
	斷線，所有電源插頭

符號	說明
m	迷你間隙結構開關
μ	小間隙結構開關（US版本） 小間隙/小斷開結構的開關（非US版）
ε	無接觸間隙的開關（半導體開關設備）