User Guide

300Mbps Wireless N Router
TL-WR850N

1910020832 REV2.0.0

Contents

About This Guide

This guide is a complement to Quick Installation Guide. The Quick Installation Guide provides instructions for quick internet setup, while this guide contains details of each function and demonstrates how to configure them.

Please note that features of your router may vary slightly depending on the model and software version you have, and on your location, language and internet service provider. All images, parameters and descriptions documented in this guide are used for demonstration only.

Conventions

In this guide the following conventions are used:

Convention	Description
Underlined	Hyperlinks are in teal and underlined. You can click to redirect to a website or a specific section.
Teal	Key information appears in teal, including management page text such as menus, items, buttons and so on.
>	The menu structures to show the path to load the corresponding page. For example, Advanced > Wireless > Wireless Settings means the Wireless Settings 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	• 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 firmware is available from the Download Center at www.tp-link.com/support.

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 http://www.tp-link.com.

A Technical Support Forum is provided for you to discuss our products at http://forum.tp-link.com.

Our Technical Support contact information can be found at the Contact Technical Support page at www.tp-link.com/support.

Chapter 1

Get to Know Your Router

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

This chapter contains the following sections:

1. 1. Product Overview

The TP-Link router is designed to fully meet the need of Small Office/Home Office (SOHO) networks and users demanding higher networking performance. The powerful antennas ensure continuous Wi-Fi signal to all your devices while boosting widespread coverage throughout your home, and the built-in Ethernet ports supply high-speed connection to your wired devices.

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

1. 2. Appearance

1. 2. 1. Top Panel

The router's LEDs are located on the top panel. You can check the router's working status by following the LED Explanation table.

LED Explanation

Name	Status	Indication
(Power)	On	The system has started up successfully.
	Flashing	The system is starting up or the router is updating the firmware. Do not disconnect or power off the router.
	Off	Power is off.
(Wi-Fi)	On	The wireless function is working properly.
	Off	The wireless function is disabled.
(Ethernet)	On	At least one of router's Ethernet ports is connected.
	Off	No Ethernet port is connected.
(Internet)	On	The internet service is available.
	Flashing	The router's WAN port is connected, but the internet service is unavailable.
	Off	The router's WAN port is not connected.
(WPS)	On/Off	Turns on when a WPS connection is established, and goes off about 5 minutes later.
	Flashing	A wireless device is trying to connect to the network via WPS. This process may take up to 2 minutes.

1. 2. 2. Back Panel

The router's back panel contains the connection ports, buttons and antennas. Refer to the following for detailed instructions.

Item	Description
Power Port	For connecting the router to a power socket via the provided power adapter.
WAN Port	For connecting the router to a DSL/Cable modem, or an Ethernet port.
Ethernet Ports (1/2/3/4)	For connecting your PCs or other Ethernet network devices to the router.
WPS/RESET Button	Press this button to establish a WPS connection. If you have a WPS-supported device, you can press this button, and immediately press the WPS button on your device to quickly establish connection between the router and the client device.
	Press and hold this button for about 8 seconds until all LEDs blink to reset the router to its factory default settings.
Antennas	Used for wireless operation and data transmitting. Upright them for the best Wi-Fi performance.

Chapter 2

Connect the Hardware

This chapter contains the following sections:

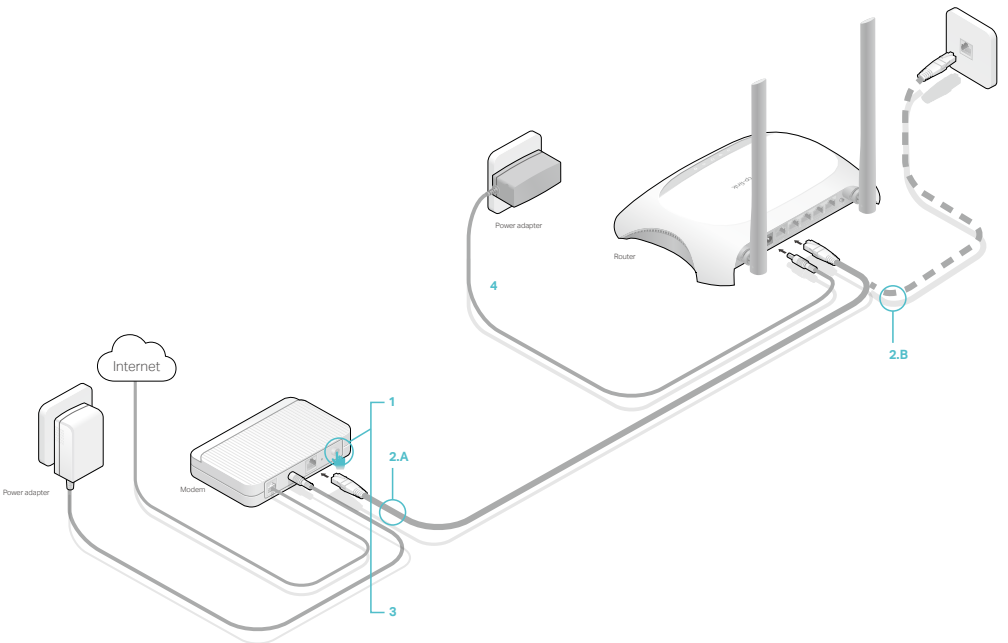
2. 1. Position Your Router

- 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 strong devices with strong electromagnetic interference, such as Bluetooth devices, cordless phones and microwaves.

2. 2. Connect Your Router

Follow the steps below to connect your router.

If your internet connection is through an Ethernet cable from the wall instead of through a DSL / Cable / Satellite modem, connect the Ethernet cable directly to the router's WAN port as step 2B, and then follow step 4 and 5 to complete the hardware connection.

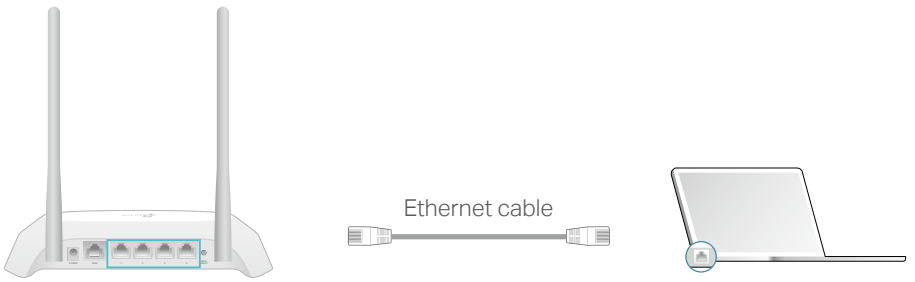


1. Turn off the modem, and remove the backup battery if it has one.
2. Connect the modem to the router's WAN port with an Ethernet cable.
3. Turn on the modem, and then wait about **2 minutes** for it to restart.
4. Connect the power adapter to the router.
5. Verify that the following LEDs are solid on before continuing with the configuration.

6. Connect your computer to the router.

- **Method 1: Wired**

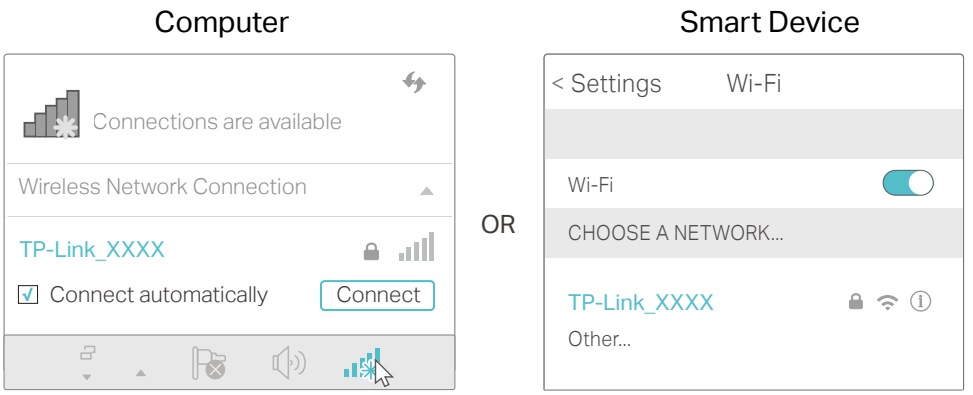
Turn off the Wi-Fi on your computer and connect the devices as shown below.



- **Method 2: Wireless**

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**

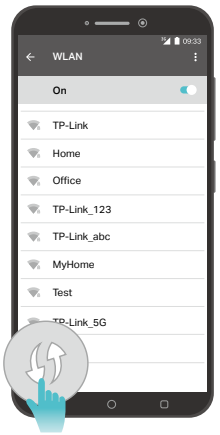
Wireless devices that support WPS, including Android phones, tablets, most USB network cards, can be connected to your router through this method.

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) Tab the WPS icon on the device's screen. Here we take an Android phone as an example.

2) Immediately press the WPS/RESET button on your router.



Close to

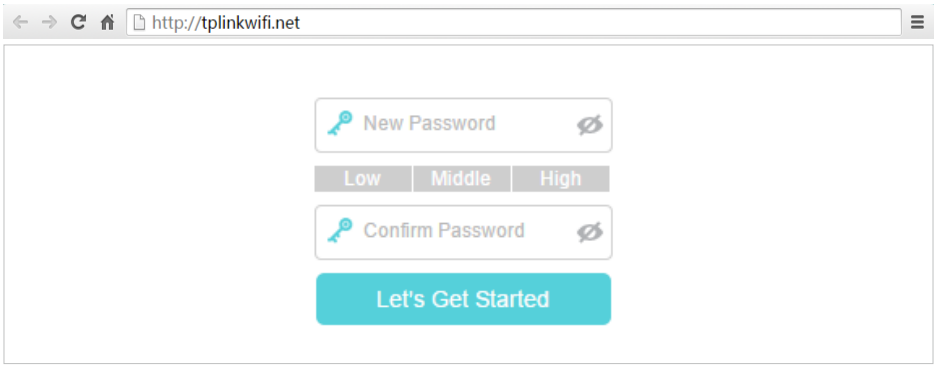
Chapter 3

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, Macintosh or UNIX OS with a Web browser, such as Microsoft the 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://tplinkwifi.net, and create a login password for secure management. Then click Let's Get Started 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:

4. 1. Use Quick Setup Wizard

The Quick Setup Wizard will guide you through the process 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://tplinkwifi.net, and log in with the password you set for the router.
2. Click Quick Setup on the top of the page. Then follow the step-by-step instructions to connect your router to the internet.

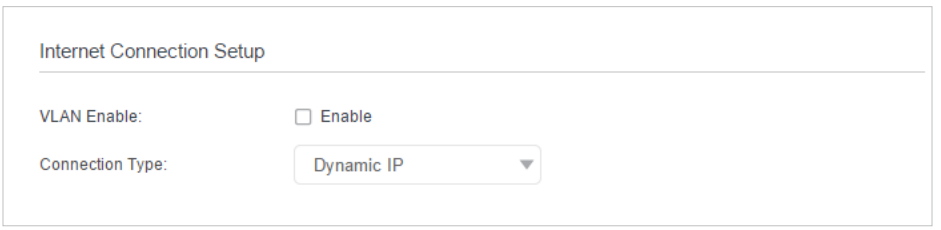
Note:
If you have changed the preset wireless network name (SSID) and wireless password during the Quick Setup process, all your wireless devices must use the new SSID and password to connect to the router.

4. 2. 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.

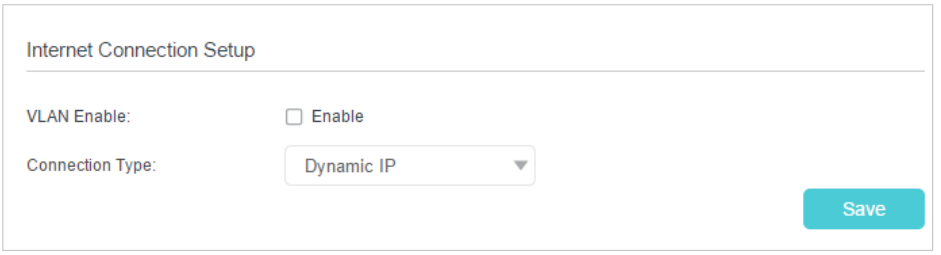
Follow the steps below to check or modify your internet connection settings.

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Basic > Internet.
3. Select your internet connection type from the drop-down list.

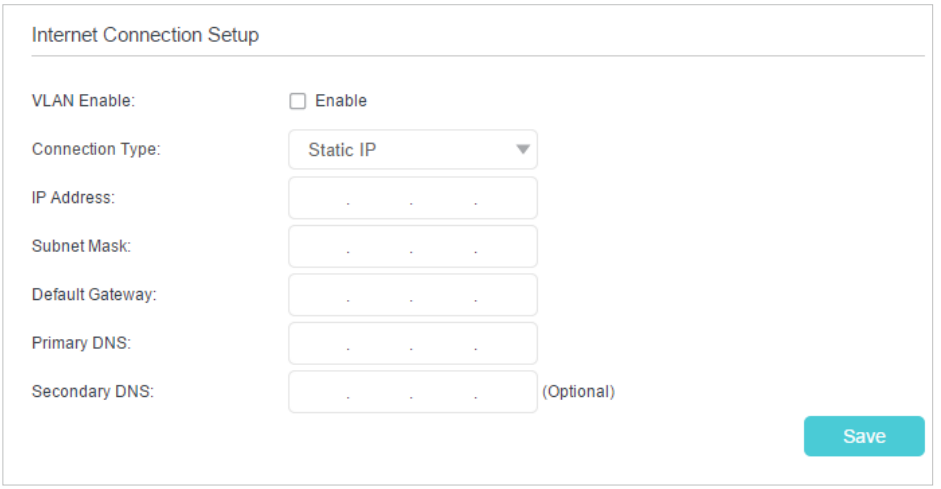


Note:
If you are unsure of what your connection type is, you can consult your ISP. Since different connection types require different cables and connection information, you can also refer to the demonstrations in Step 4 to determine your connection type.

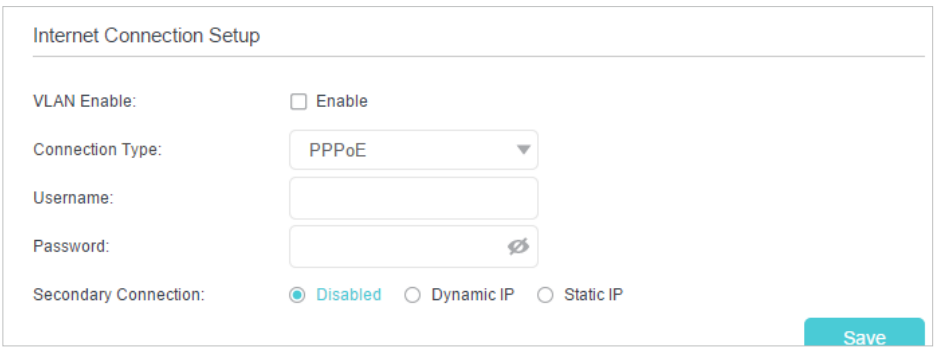
4. Follow the instructions on the page to continue the configuration. Parameters on the images are used for demonstration only.
   1) If you choose Dynamic IP, you just need to click Save the make the settings effective. Dynamic IP users are usually equipped with a cable TV or fiber cable.



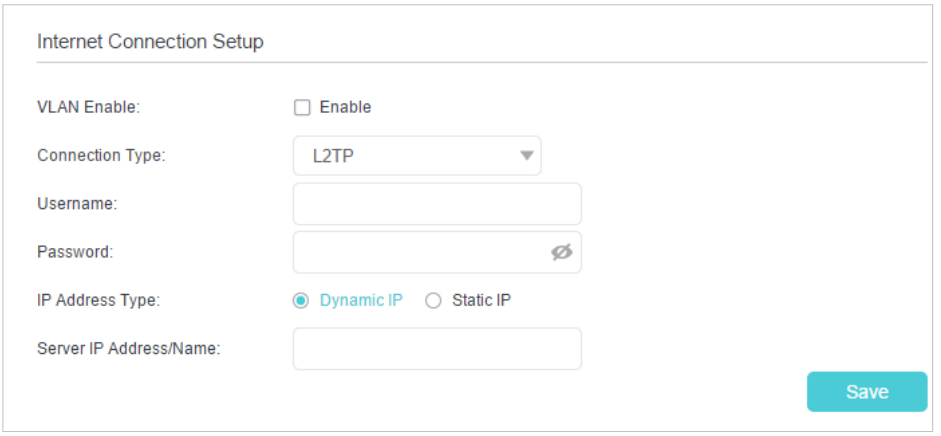
2) If you choose Static IP, enter the information provided by your ISP in the corresponding fields.



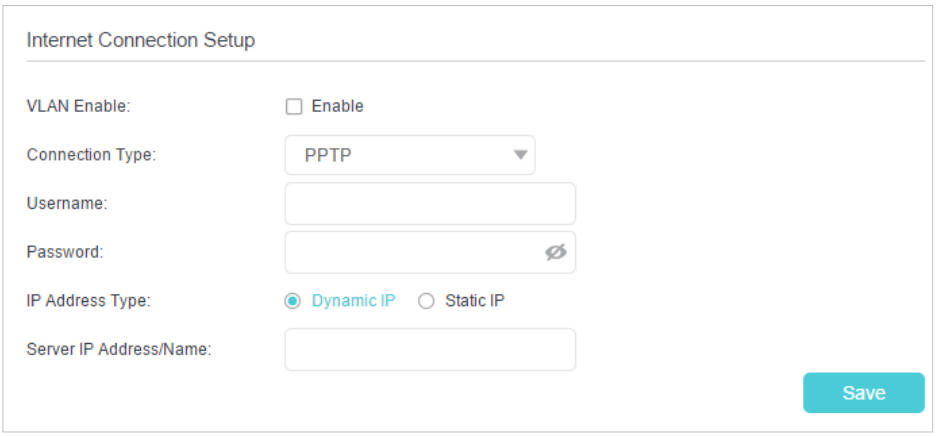
3) If you choose PPPoE, enter the Username and Password and choose Secondary Connection provided by your ISP. Different parameters are needed according to the Secondary Connection type you have chosen. PPPoE users usually have DSL cable modems.



4) If you choose L2TP, enter the Username and Password, and select the IP Address Type provided by your ISP. Different parameters are needed according to the IP address type you selected.



5) If you choose PPTP, enter the Username and Password, and select the IP Address Type provided by your ISP. Different parameters are needed according to the IP address type you selected.



5. Click Save to make the settings effective, and you can refer to Test Internet Connectivity to test the Internet connection.

Note:

It may take 1-2 minutes to make the settings effective.

Tips:

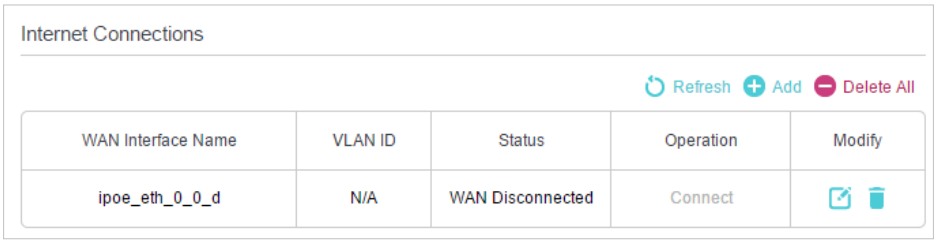
1. You can check your internet connection by clicking Network Map on the left of the page.
2. If you use Dynamic IP and PPPoE and you are provided with any other parameters that are not required on the page, please go to Advanced > Network > Internet to complete the configuration.
3. If you still cannot access the internet, refer to the FAQ section for further instructions.

4. 3. Set Up an IPv6 Internet Connection

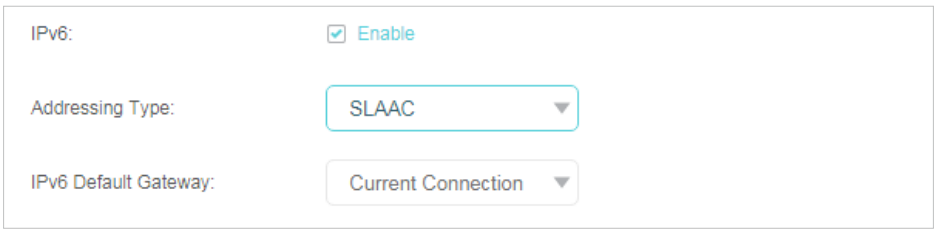
If your ISP provides information about one of the following IPv6 internet connection types: PPPoE, Dynamic IP(SLAAC/DHCPv6), and Static IP, you can manually set up an IPv6 connection.

If your ISP provides an IPv4-only connection or IPv6 tunnel service, permit IPv6 connection by referring to Set Up the IPv6 Tunnel.

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



3. Select your WAN Interface Name (Status should be Connected) and click the (edit) icon.
4. Scroll down the page, enable IPv6, and configure the IPv6 parameters.



- Addressing Type: Consult your ISP for the addressing type (DHCPv6 or SLAAC). SLAAC is the most commonly used addressing type.
- IPv6 Gateway: Keep the default setting as Current Connection.

Note: If your ISP has provided the IPv6 address, click Advanced to reveal more settings. You can check the detailed settings of IPv6 and enter the parameters provided by your ISP.

5. Click Save to make the settings effective. Now IPv6 service is available for your network.

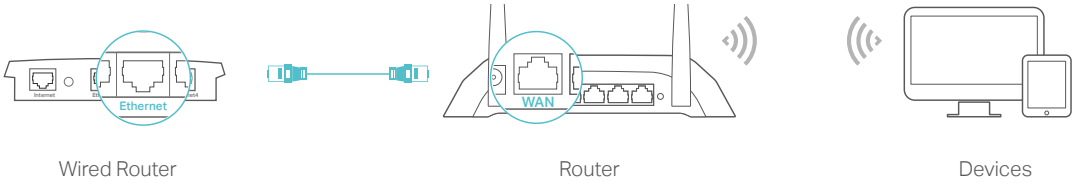
4. 4. More Operation Modes

The router supports two more operation modes: Access Point mode and Range Extender mode. You can change the operation mode according to your needs.

4. 4. 1. Configure the Router in Access Point Mode

In Access Point mode, the device can be connected to a wired network and transform the wired access into wireless one to extend the wireless coverage of your existing network. Advanced functions like NAT, Parental Controls and QoS are not supported in this mode.

If you already have a wired router, you can use this mode. To switch to Access Point mode:



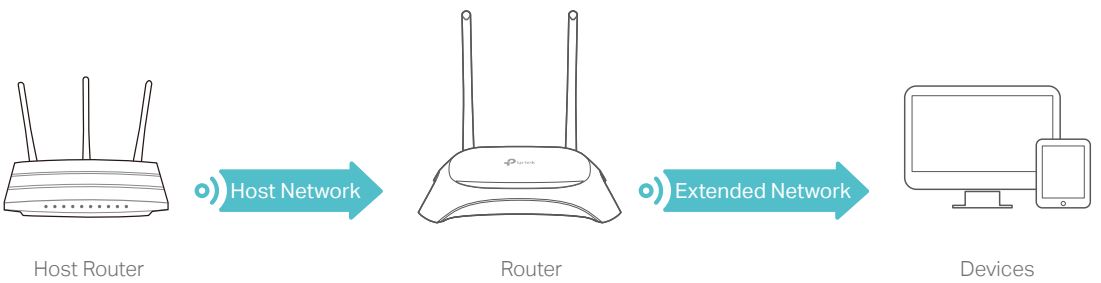
1. Connect the router's WAN port to your wired router's Ethernet port via an Ethernet cable as shown above. And power on the router.
2. Connect a computer to the router via an Ethernet cable or wirelessly by using the SSID (network name) and Wireless Password printed on the label at the bottom of the router.
3. Visit http://tplinkwifi.net, and log in with the password you set for the router.
4. Go to Settings or Advanced > Operation Mode, select Access Point and click Save. Log in to the router via http://tplinkwifi.net after the router reboots.
5. Go to Quick Setup or Settings > Wireless > Wireless Settings and set the network name(SSID) and passwords for the wireless network.

Now, you can connect to the SSID and enjoy your existing network.

4. 4. 2. Configure the Router in Range Extender Mode

In Range Extender mode, the device can copy and reinforce the existing wireless signal to extend the coverage of the signal, especially for a large space to eliminate signal-blind corners. Advanced functions like NAT, Parental Controls and QoS are not supported in this mode.

To switch to Range Extender mode:



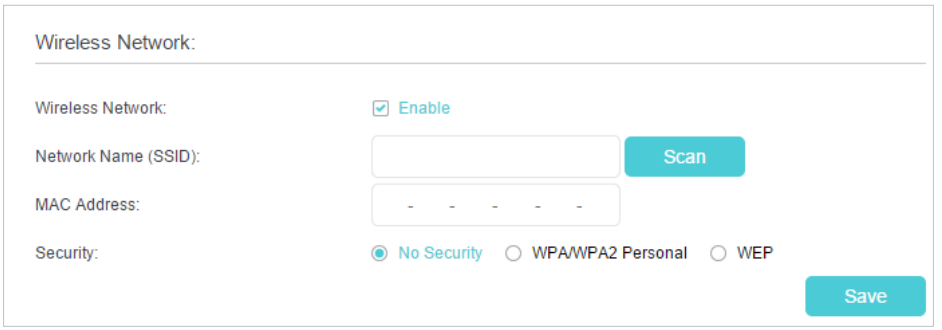
1. Place the router next to your host router and power it on.
2. Connect a computer to the router via an Ethernet cable or wirelessly by using the SSID (network name) and Wireless Password printed on the label at the bottom of the router.
3. Visit http://tplinkwifi.net, and log in with the password you set for the router.

4. Go to Settings or Advanced > Operation Mode, select Range Extender and click Save. Log in to the router via http://tplinkwifi.net after the router reboots.
5. Configure the basic settings of the wireless network.
   - **Method 1: Use Quick Setup wizard**

   Go to Quick Setup to connect to the host network and specify your extended wireless network name(SSID).
   - **Method 2: Manually configure the network connection**

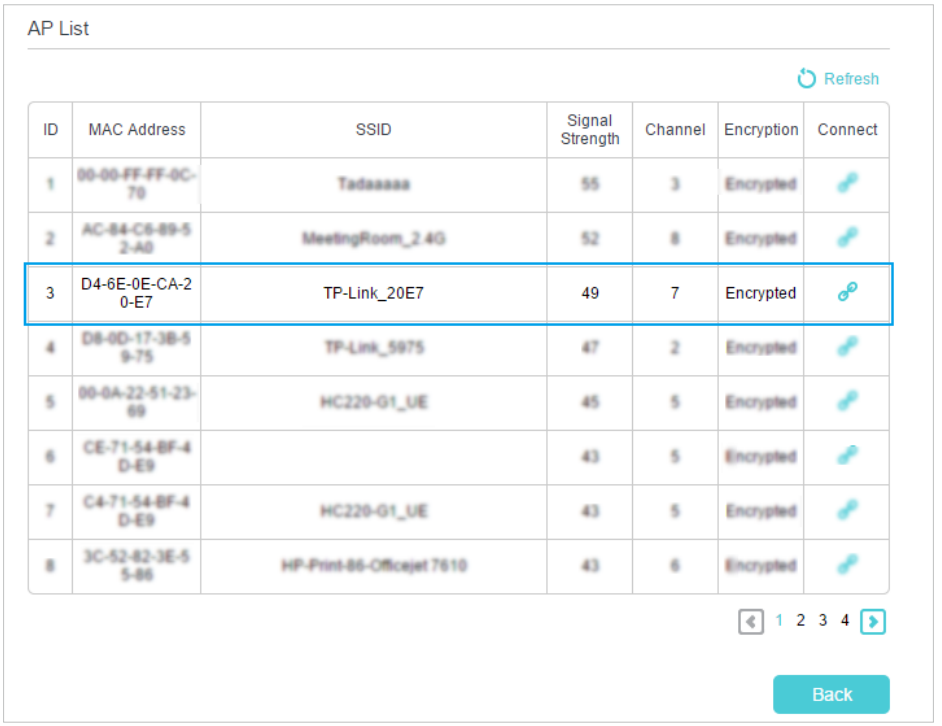
   ➢ **To connect to the host network:**

   1) Go to Settings > Wireless > Connect to Network, click Scan to detect all available wireless networks.

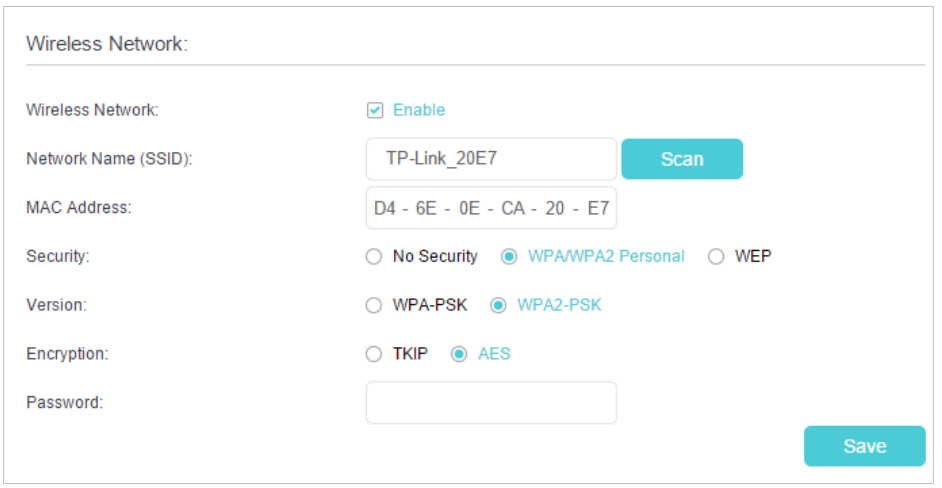


Tips: You can also enter the SSID and MAC address of the host network in the corresponding fields and select the security settings of the host network.

   2) Select the wireless network you want to connect to by clicking the connect icon in the Connect column. Once the host network is selected, the SSID and security settings of that network will be automatically filled in.

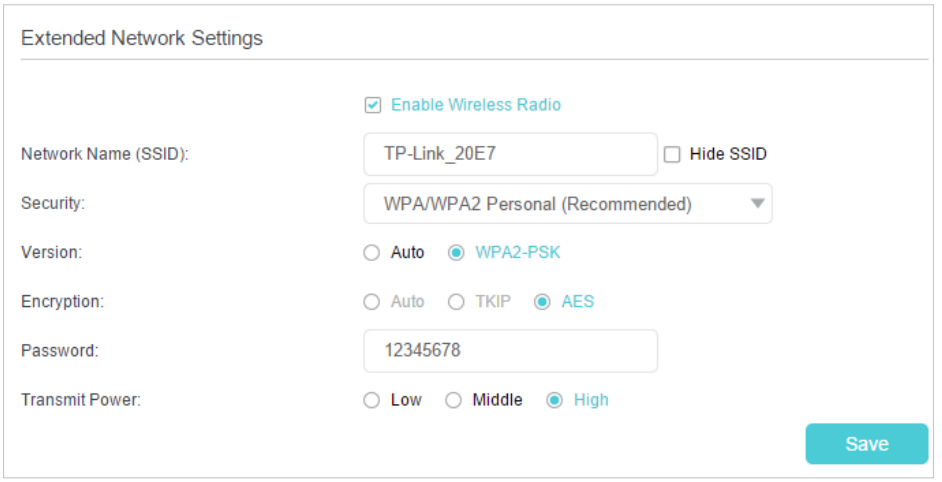


3) Enter the Password of the host network you selected, and click Save to make the settings effective.



➢ **To specify the extended network:**

1) Go to Settings > Wireless > Extended Network, and configure the basic settings of the extended network.



- Network Name (SSID): Enter a new SSID (up to 32 characters long) or just use the SSID of the default name copied from the host network. This field is case-sensitive. Do not select Hide SSID unless you want the client devices to join the network manually.
- Security: Select one of the security options and configure the corresponding settings for the extended wireless network.
    - No Security - This option disables the wireless security.
    - WPA/WPA2(Reconmmended) - Select this option to enable the wireless security. This is highly recommended to protect the wireless network from unauthorized access. And then you can select a security version and encryption type.
    - WEP - This option is the most basic form of wireless security that can be used if your client devices can only access wireless using WEP (Wired Equivalent Privacy).
- Transmit Power: Select Low, Middle, or High to specify the data transmit power. The default and recommended setting is High.

2) Click Save to make the settings effective.

Now, you can connect to the SSID and enjoy the extended network.

Chapter 5

Parental Controls

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

I want

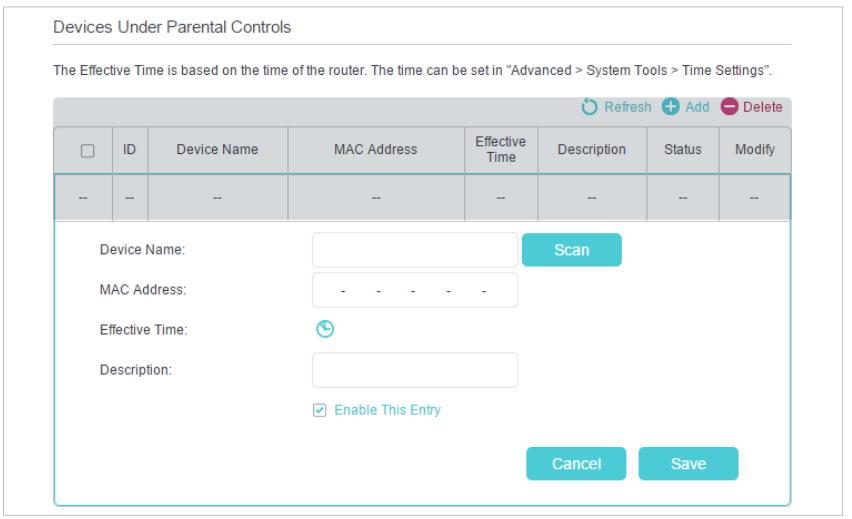
Control what types of websites my children or other home network users can visit and the time of day they are allowed to access the internet.

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

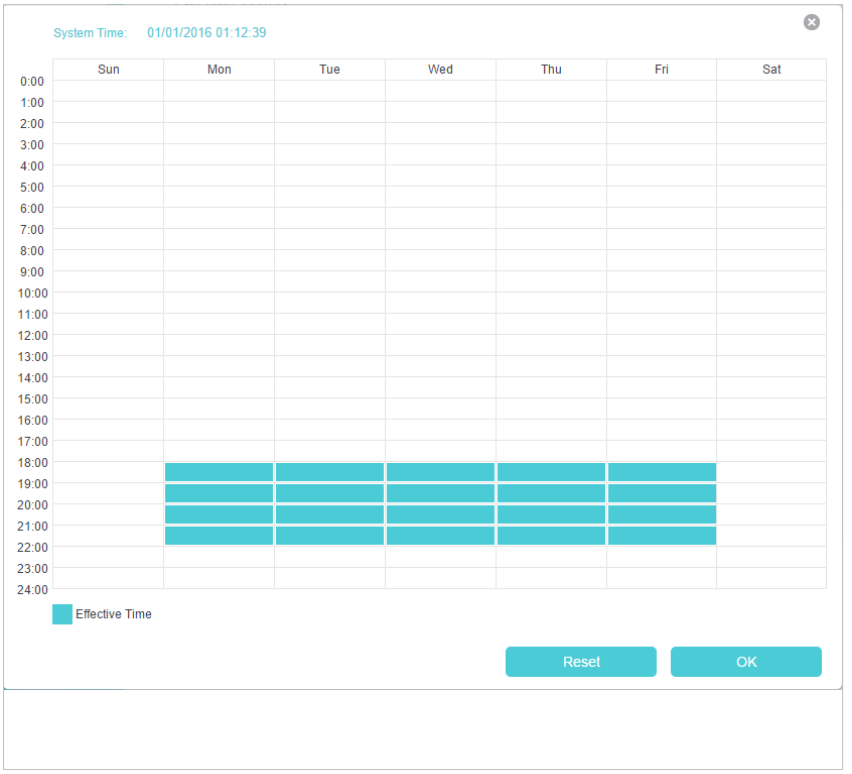
How can I do that?

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

3. Click Add, and then click Scan to select the connected device to be controlled. Or, enter the Device Name and MAC Address manually.

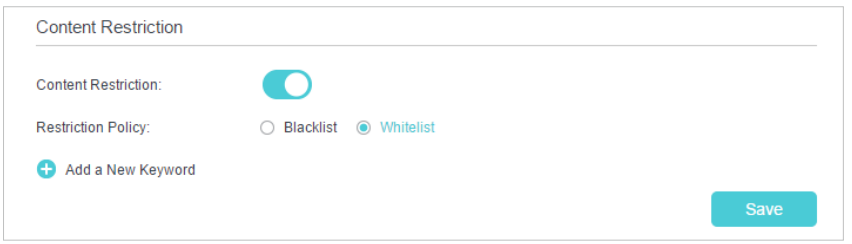


4. Click the icon to set the Effective Time. Drag the cursor over the appropriate cell(s) and click OK.



5. Enter a Description for the entry, keep the Enable This Entry check box selected, and then click Save.

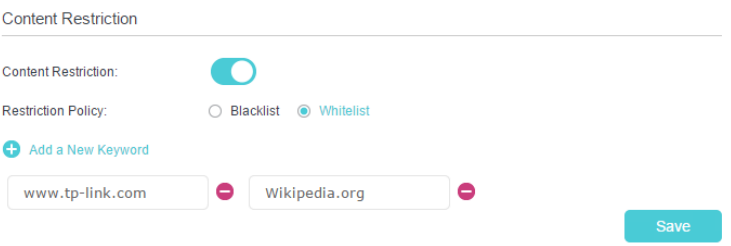
6. Enable Content Restriction, and select Whitelist as the restriction policy.



Tips:

- With Blacklist selected, the controlled devices cannot access any websites containing the specified keywords during the Effective Time period.
- With Whitelist selected, the controlled devices can only access websites containing the specified keywords during the Effective Time period.

7. Click Add a New Keyword and enter “www.tp-link.com” and “Wikipedia.org” as the keywords and click Save.



8. You can add up to 32 keywords for either Blacklist or Whitelist. Below are some sample entries for your reference.
   - For Whitelist: Enter a web address (e.g. wikipedia.org) to allow access only to its related websites. If you wish to block all Internet browsing access, do not add any keyword to the Whitelist.
   - For Blacklist: Specify a web address (e.g. wikipedia.org), a web address keyword (e.g. wikipedia) or a domain suffix (e.g. .edu or .org) to block access only to the websites containing that keyword or suffix.

Done!

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

Chapter 6

Bandwidth Control

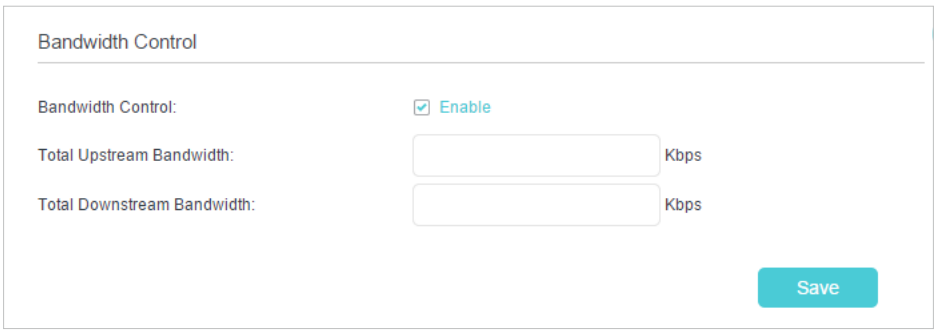
This chapter describes how to use the Bandwidth Control function to control the bandwidth by configuring rules for limiting various data flows. In this way, the network bandwidth can be reasonably distributed and utilized.

It contains the following sections:

6. 1. Configure the Bandwidth Control

Bandwidth Control allows you to configure the Upstream Bandwidth and Downstream Bandwidth of the network, follow the steps below to configure the bandwidth.

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Bandwidth Control, and enable Bandwidth Control.
3. Input the total upload and download speed through the WAN port in the Total Upstream Bandwidth and Total Downstream Bandwidth field. For optimal bandwidth control, please consult your ISP for the total allowed bandwidth for upstream and downstream.

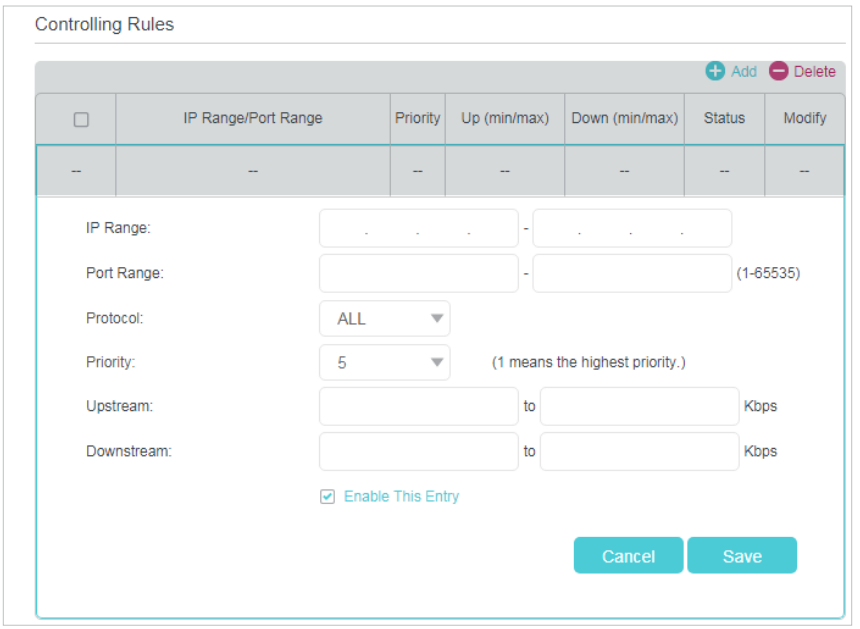


4. Click Save to make the settings effective.

6. 2. Controlling Rules

To add a new rule for the Bandwidth Control:

1. Click Add.



2. Enter a range of IP addresses and port numbers to be controlled.

   IP Range: The field can be a single IP address or IP address range according to your needs. If you set the IP Range to a single IP address, the computer with this IP address will get independent given bandwidth. If you set the IP Range to an IP address range, all computers in the range will share the given bandwidth.

   Port Range: Enter a range of port numbers to be controlled.

3. Select the protocol type for this rule.
4. Select a priority level for this rule. 1 is the highest priority level and 8 is the lowest priority level. The total upload and download bandwidth will be allocated to guarantee the minimal rate of all bandwidth control rules.
5. Enter the minimum and maximum upload bandwidth and download bandwidth through the WAN port.
6. Select the Enable This Entry check box.
7. Click Save to make the settings effective.

Chapter 7

Network Security

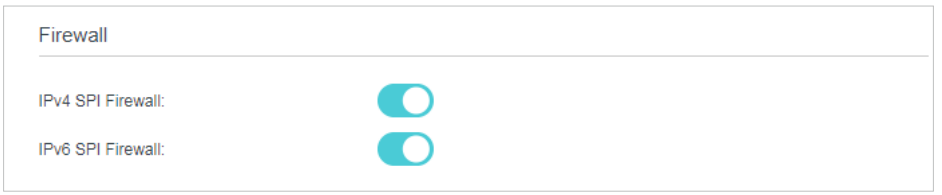
This chapter guides you on how to protect your home network from unauthorized users by implementing network security functions. You can block or allow specific client devices to access your wireless network using MAC Filtering, or using Access Control for wired and wireless networks, or you can prevent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

This chapter contains the following sections:

7. 1. Firewall & DoS Protection

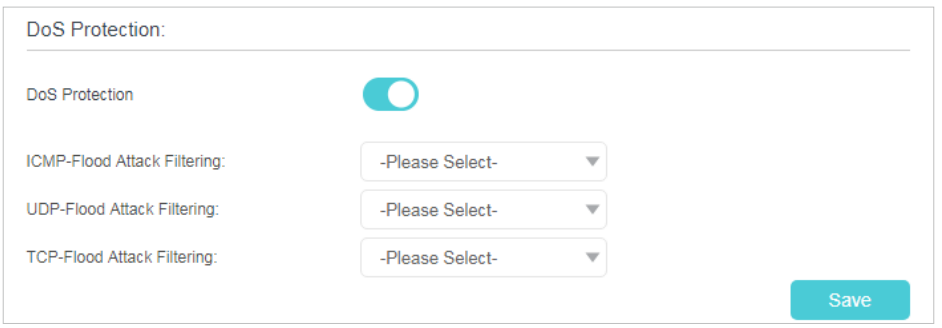
The SPI (Stateful Packet Inspection) Firewall and DoS (Denial of Service) Protection protect the router from cyber attacks.

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



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

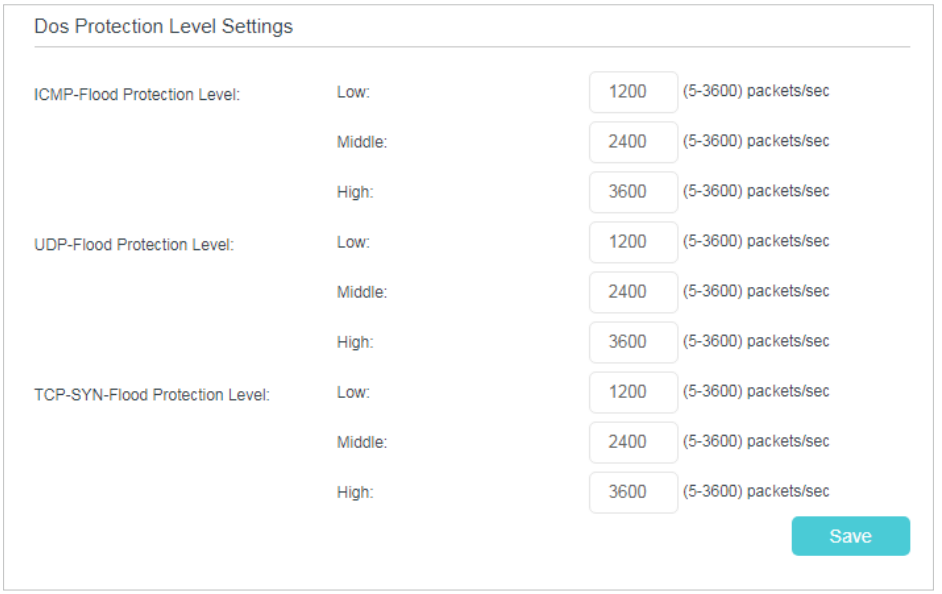
1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Security > Firewall & DoS Protection.



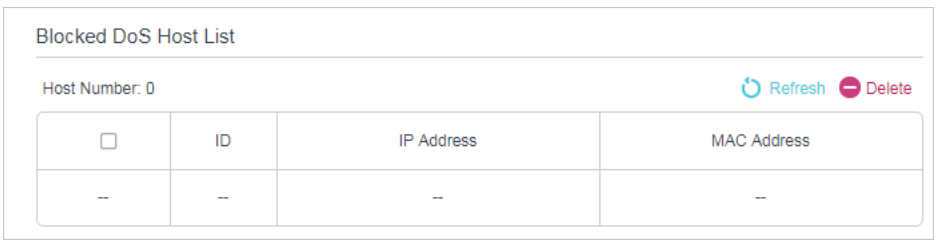
3. Enable DoS Protection.
4. Set the protection level (Low, Middle or High) for ICMP-Flood Attack Filtering, UDP-Flood Attack Filtering and TCP-Flood Attack Filtering.
   - ICMP-Flood Attack Filtering - Enable to prevent the ICMP (Internet Control Message Protocol) flood attack.
   - UDP-Flood Attack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

Tips:

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



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

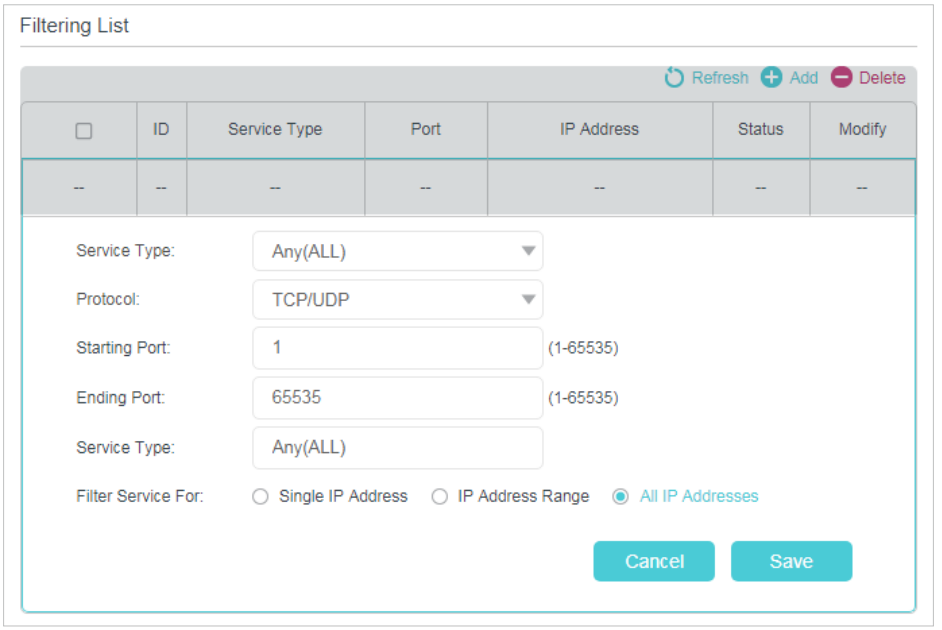


7. 2. Service Filtering

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

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

3. Click Add.



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

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

7. 3. Access Control

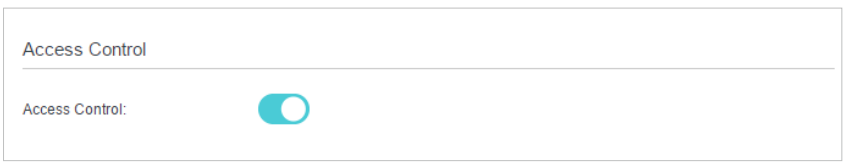
Access Control is used to block or allow specific client devices to access your network (via wired or wireless) based on a list of blocked devices (Blacklist) or a list of allowed devices (Whitelist).

I want to:

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

How can I do that?

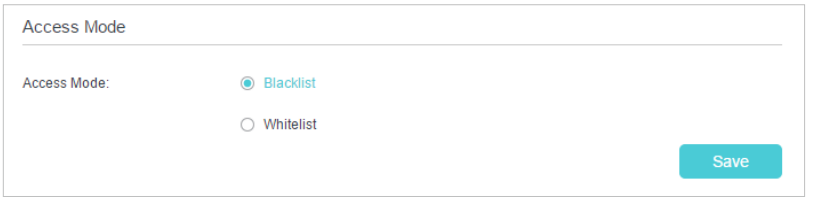
1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Security > Access Control and enable Access Control.



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

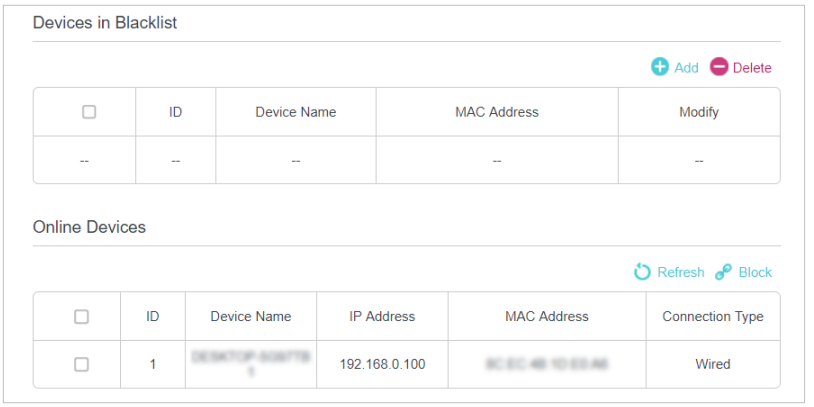
To block specific device(s):

1) Select Blacklist and click Save.



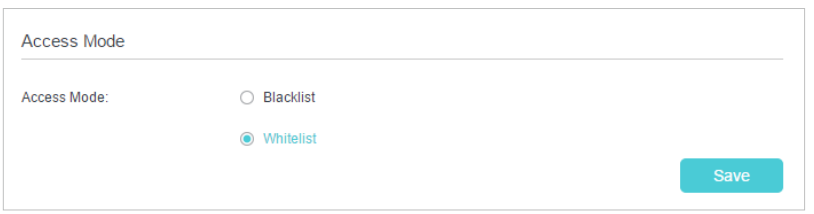
2) Select the device(s) to be blocked in the Online Devices table (or click the Add under the Devices in Blacklist and enter the Device Name and MAC Address manually).

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

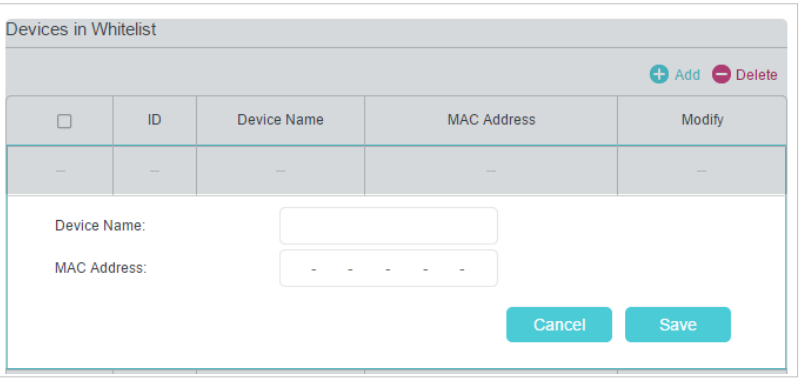


To allow specific device(s):

1) Select Whitelist and click Save.



2) Click Add in the Devices in Whitelist section.



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

4) Click Save.

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

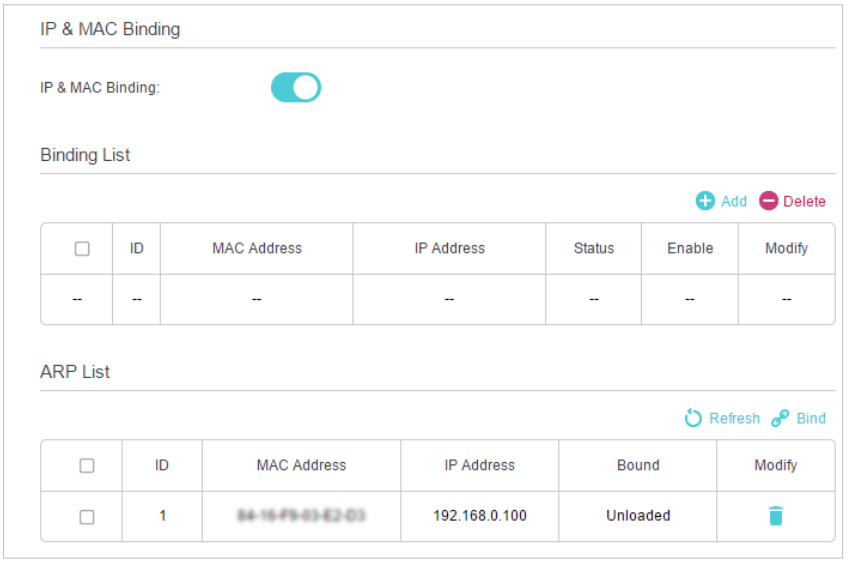
7. 4. IP & MAC Binding

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

I want to: Prevent ARP spoofing and ARP attacks.

How can I do that?

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



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

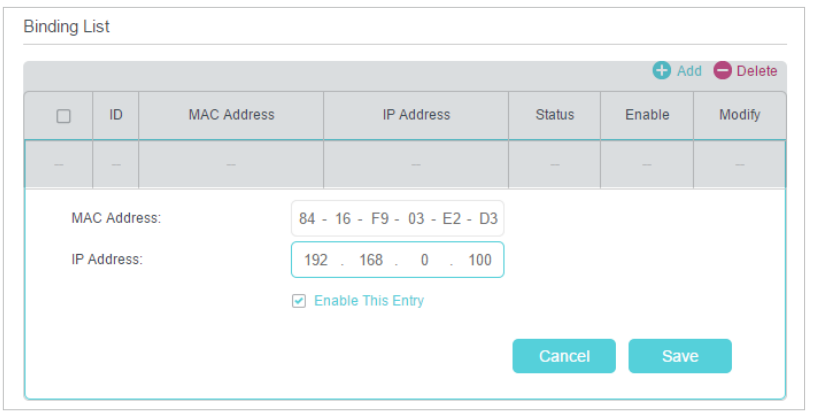
To bind the connected device(s):

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

2) Click Bind to add to the Binding List.

To bind the unconnected device:

1) Click Add in the Binding List section.



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

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

Done!

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

Chapter 8

NAT Forwarding

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

The router can use a forwarding feature to remove the isolation of NAT and allow external internet hosts to initiatively communicate with the devices in the local network, thus enabling some special features.

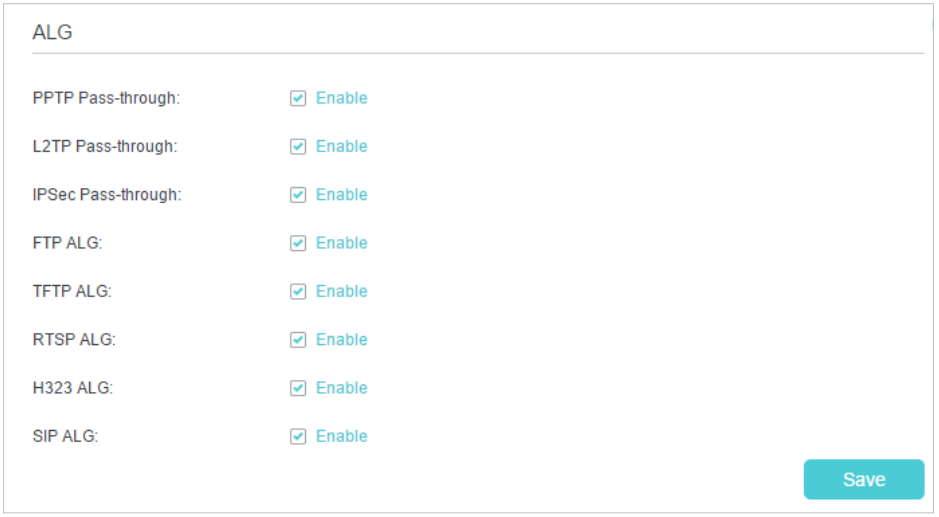
TP-Link router includes four forwarding rules. If two or more rules are set, the priority of implementation from high to low is Virtual Servers, Port Triggering, UPnP and DMZ.

This chapter contains the following sections:

8. 1. Translate Address and Port by ALG

ALG (Application Layer Gateway) allows customized NAT (Network Address Translation) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols: FTP, TFTP etc. Enabling ALG is recommended.

Visit http://tplinkwifi.net, and log in with the password you set for the router. Go to Advanced > NAT Forwarding > ALG.



- PPTP Pass-through: If enabled, it allows Point-to-Point sessions to be tunneled through an IP network and passed through the router.
- L2TP Pass-through: If enabled, it allows Layer 2 Point-to-Point sessions to be tunneled through an IP network and passed through the router.
- IPSec Pass-through: If enabled, it allows IPSec (Internet Protocol Security) to be tunneled through an IP network and passed through the router. IPSec uses cryptographic security services to ensure private and secure communications over IP networks.
- FTP ALG: If enabled, it allows FTP (File Transfer Protocol) clients and servers to transfer data via NAT.
- TFTP ALG: If enabled, it allows TFTP (Trivial File Transfer Protocol) clients and servers to transfer data via NAT.
- RTSP ALG: If selected, it allows media player clients to communicate with streaming media servers via NAT.
- H323 ALG: If enabled, it allows Microsoft NetMeeting clients to communicate via NAT.
- SIP ALG: If enabled, it allows clients communicate with SIP (Session Initiation Protocol) servers via NAT.

8. 2. Share Local Resources over the Internet by Virtual Server

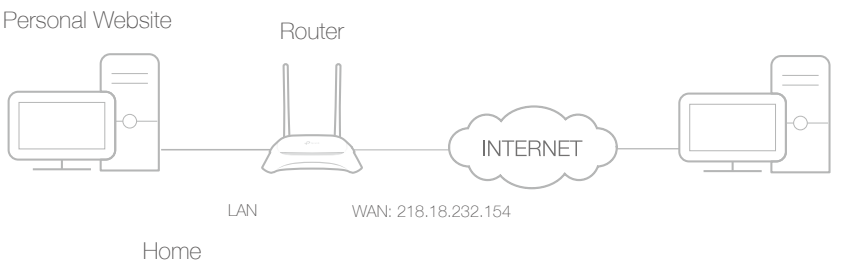
When you build up a server in the local network and want to share it on the internet, Virtual Server can realize the service and provide it to the internet users. At the same time virtual server can keep the local network safe as other services are still invisible from the internet.

Virtual server can be used for setting up public services in your local network, such as HTTP, FTP, DNS, POP3/SMTP and Telnet. Different service uses different service port. Port 80 is used in HTTP service, port 21 in FTP service, port 25 in SMTP service and port 110 in POP3 service. Please verify the service port number before configuration.

I want to:

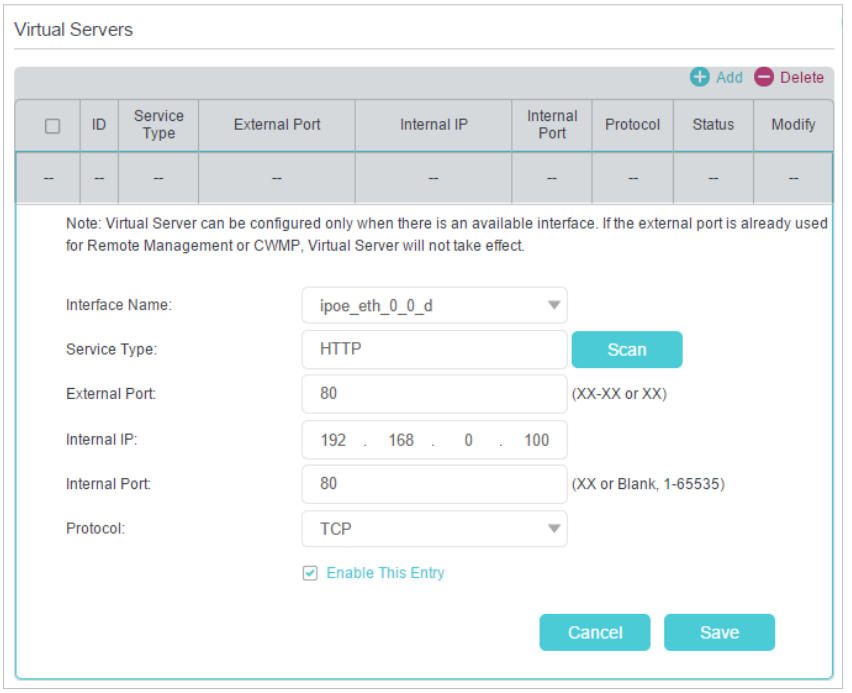
Share my personal website I've built in a local network with my friends through the internet.

For example, the personal website has been built on my home PC (192.168.0.100). I hope that my friends can visit my website. The PC is connected to the router with the WAN IP address 218.18.232.154.



How can I do that?

1. Assign a static IP address to your PC, for example 192.168.0.100.
2. Visit http://tplinkwifi.net, and log in with the password you set for the router.
3. Go to Advanced > NAT Forwarding > Virtual Servers, click Add.



4. Click Scan, and select HTTP. The external port, internal port and protocol will be automatically filled in. Enter the PC's IP address 192.168.0.100 in the Internal IP field.

5. Click Save to save the settings.

Tips:

1. It is recommended to keep the default settings of Internal Port and Protocol if you are not clear about which port and protocol to use.
2. If the service you want to use is not in the Service Type, you can enter the corresponding parameters manually. You should verify the port number that the service needs.
3. You can add multiple virtual server rules if you want to provide several services from a router. Please note that the External Port cannot be overlapped.

Done!

Internet users can enter http://WAN IP (in this example: http://218.18.232.154) to visit your personal website.

Tips:

1. For a WAN IP that is assigned dynamically by ISP, it is recommended to apply and register a domain name for the WAN by DDNS, go to Set Up a Dynamic DNS Service Account for more information. Then you can use http://domain name to visit the website.
2. If you have changed the default External Port, you should use http://WAN IP: External Port or http://domain name: External Port to visit the website.

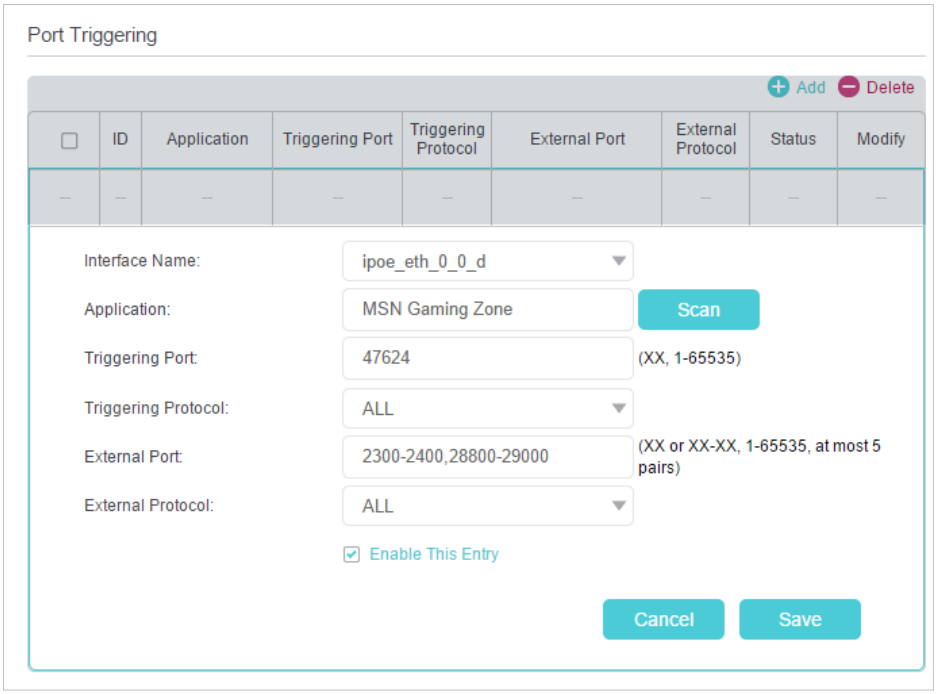
8. 3. Open Ports Dynamically by Port Triggering

Port triggering can specify a triggering port and its corresponding external ports. When a host in 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 returns to the external ports, the router can forward them to the corresponding host. Port triggering is mainly applied to online games, VoIPs and video players. Common applications include MSN Gaming Zone, Dialpad, Quick Time 4 players, and so on.

Follow the steps below to configure the port triggering rules:

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > NAT Forwarding > Port Triggering, and click Add.



3. Click Scan, and select the desired application. The triggering port and protocol, the external port and protocol will be automatically filled in. Here we take MSN Gaming Zone as an example.
4. Click Save to make the settings effective.

Tips:

1. You can add multiple port triggering rules according to your network needs.
2. If the application you need is not listed in the Existing Applications list, you can 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 suggested.

8. 4. Make Applications Free from Port Restriction by DMZ

When a PC is set to be a DMZ (Demilitarized Zone) host in 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, like IP camera and database software, you can set the PC to be a DMZ host.

Note:

DMZ is most applicable when you don't know which ports to open. When it 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 with all ports opened.

How can I do that?

1. Assign a static IP address to your PC, for example 192.168.0.100.
2. Visit http://tplinkwifi.net, and log in with the password you set for your router.
3. Go to Advanced > NAT Forwarding > DMZ and select the Enable check box to enable DMZ.

4. Enter the IP address 192.168.0.100 in the DMZ Host IP Address filed.
5. Click Save to save the settings.

Done!

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

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

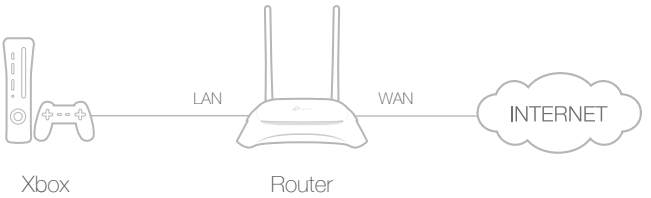
UPnP (Universal Plug and Play) protocol allows the applications or host devices to automatically find the front-end NAT device and send request to it to open the corresponding ports. With UPnP enabled, the applications or host devices in the both sides of NAT device can freely communicate with each other realizing the seamless connection of the network. You need to enable the UPnP if you want to use applications

such as multiplayer gaming, peer-to-peer connections, real-time communication (for example, VoIP or telephone conference), or remote assistance.

Tips:

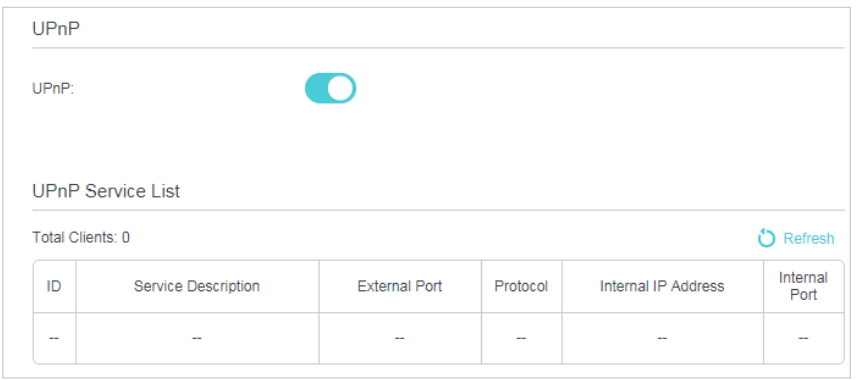
1. Only the application supporting UPnP protocol can use this feature.
2. UPnP feature needs the support of operating system (e.g. Windows Vista/ Windows 7/ Windows 8, etc. Some operating systems need to install the UPnP components).

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.



You can follow the steps to change the status of UPnP.

1. Visit http://tplinkwifi.net, and log in with the password you set for your router.
2. Go to Advanced > NAT Forwarding > UPnP and enable or disable UPnP according to your needs.



Chapter 9

VPN Server

The VPN (Virtual Private Networking) Server allows you to access your home network in a secured way through internet when you are out of home. The router offers two ways to setup VPN connection: OpenVPN and PPTP (Point to Point Tunneling Protocol) VPN.

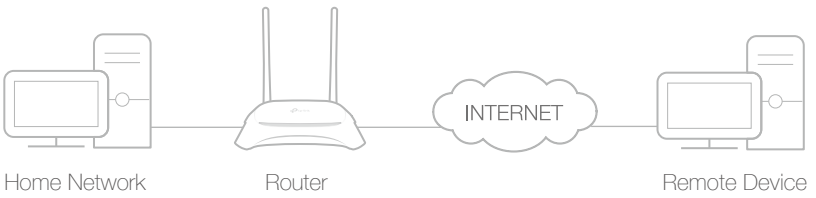
OpenVPN is somewhat complex but with greater security and more stable. It is suitable for restricted environment, such as campus network and company intranet.

PPTP VPN is more easily used and its speed is faster, it's compatible with most operating systems and also supports mobile devices. Its security is poor and your packets may be cracked easily, and PPTP VPN connection may be prevented by some ISP.

This chapter contains the following sections, you can choose the appropriate VPN server connection type as needed.

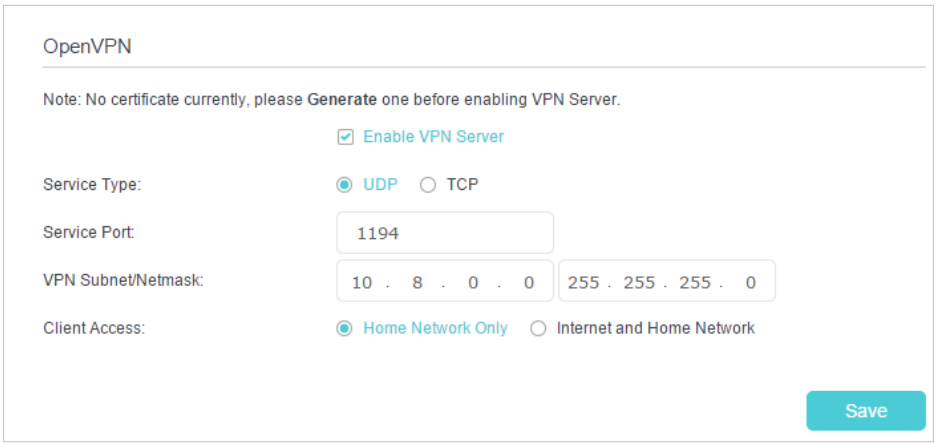
9. 1. Use OpenVPN to Access Your Home Network

In the OpenVPN connection, the home network can act as a server, and the remote device can access the server through the router which acts as an OpenVPN Server gateway. To use the VPN feature, you should enable OpenVPN Server on your router, and install and run VPN client software on the remote device. Please follow the steps below to set up an OpenVPN connection.



Step1. Set Up OpenVPN Server on Your Router

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > VPN > OpenVPN, and select Enable VPN Server.

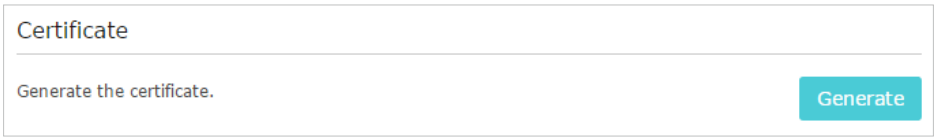


Note:

1. 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.
2. 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.

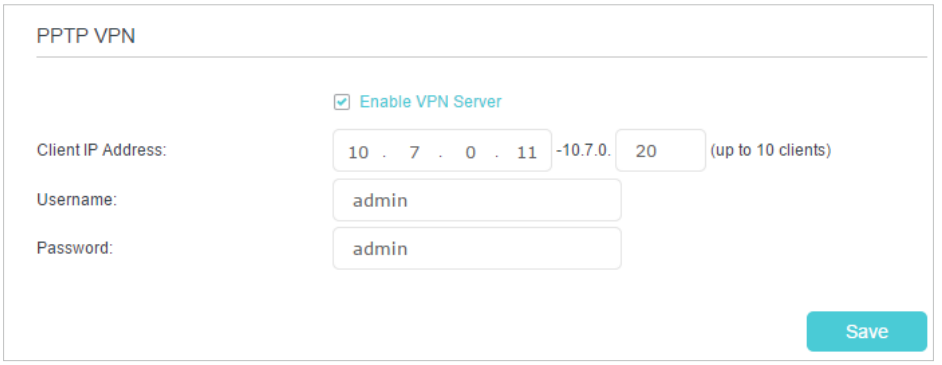
Tips:
You can go to Advanced > VPN > VPN Connections to view the clients that are currently connected to the OpenVPN servers.

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

PPTP VPN Server is used to create a VPN connection for remote device. To use the VPN feature, you should enable PPTP VPN Server on your router, and configure the PPTP connection on the remote device. Please follow the steps below to set up a PPTP VPN connection.

Step 1. Set Up PPTP VPN Server on Your Router

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > VPN Server > PPTP VPN, and select Enable VPN Server.



Note:

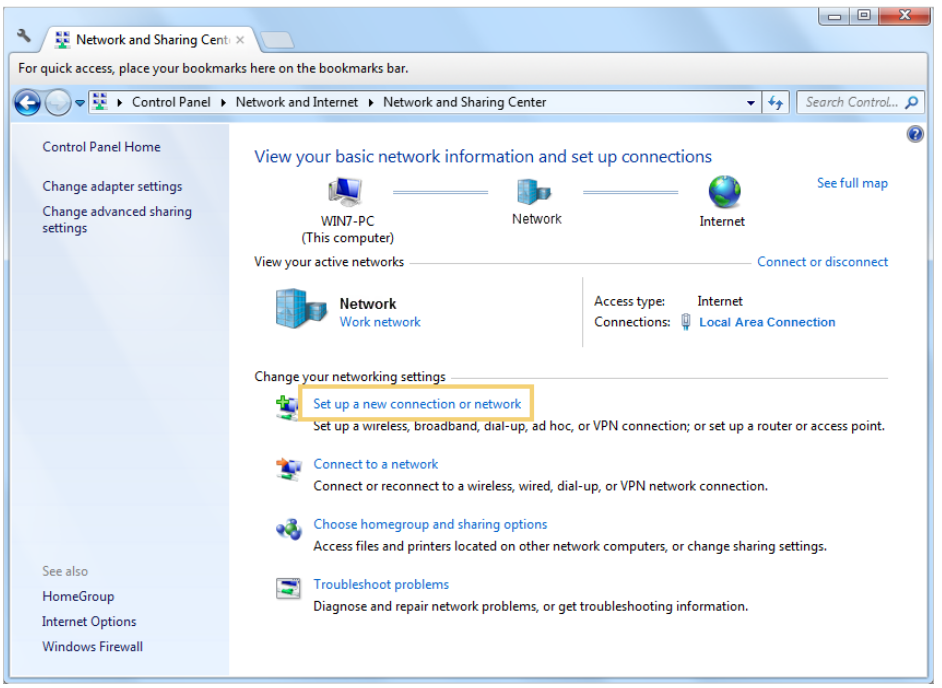
Before you enable VPN Server, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router's WAN port and synchronize your System Time with internet.

3. In the Client IP Address filed, 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 to make the settings effective.

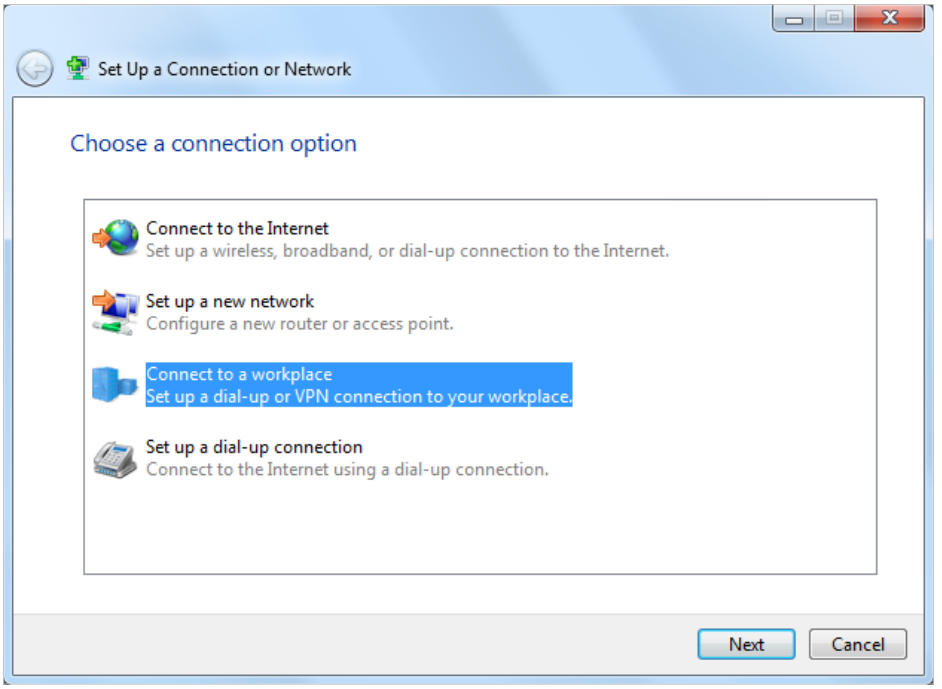
Step 2. Configure PPTP VPN Connection on Your Remote Device

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.

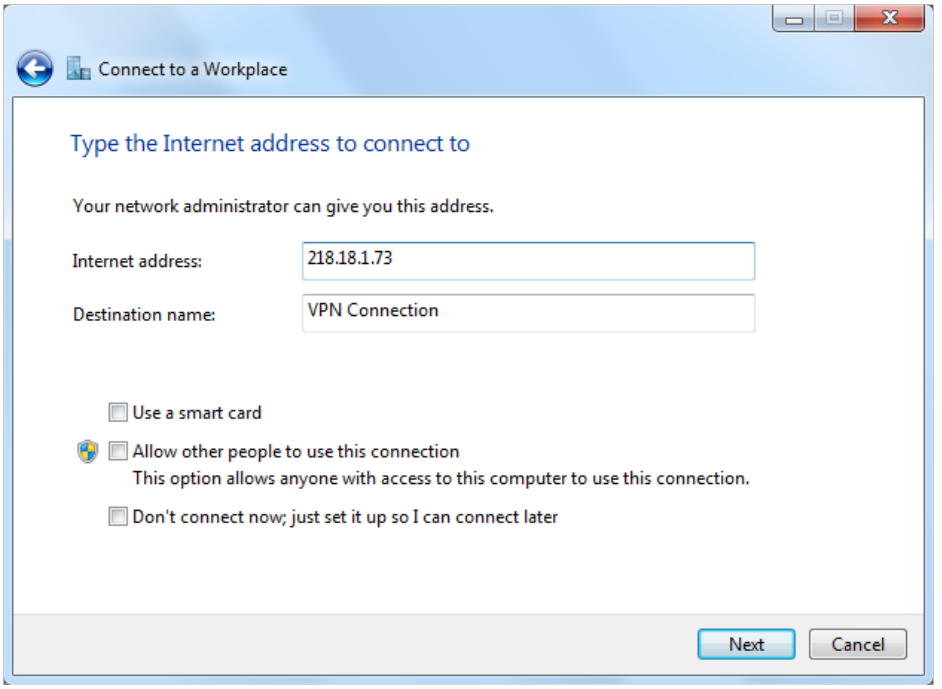


3. Select Connect to a workplace and click Next.

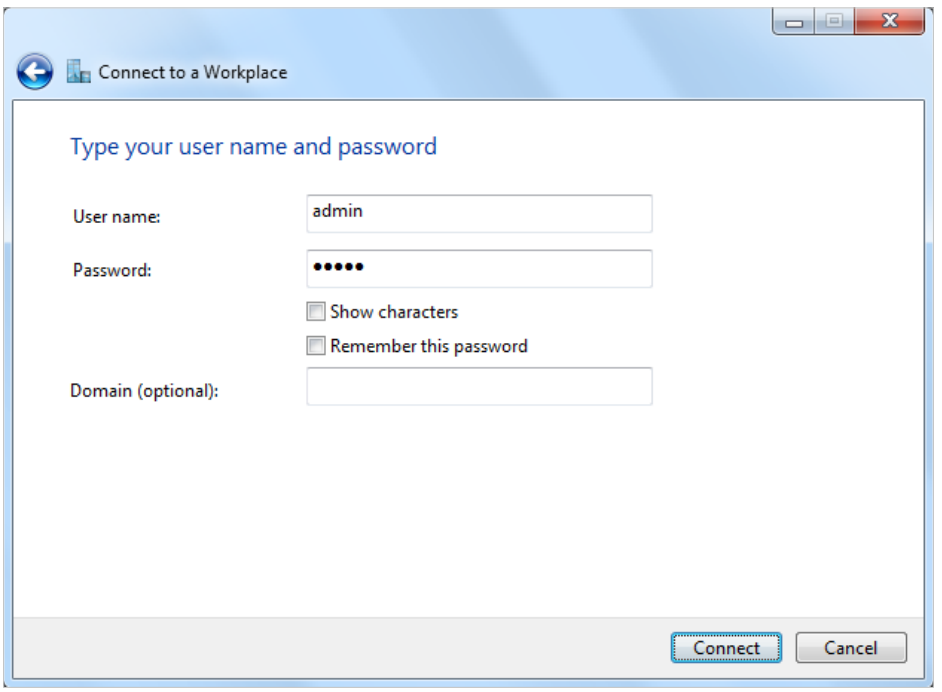


4. Select Use my Internet connection (VPN).

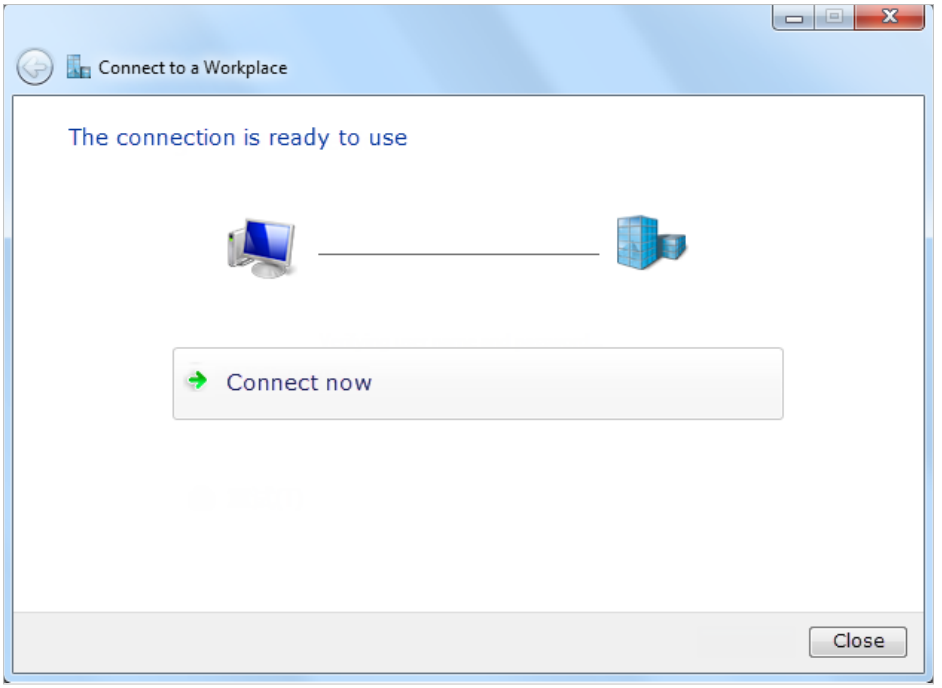
5. Enter the internet IP address of the router (for example: 218.18.1.73) in the Internet address field. Click Next.



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



7. The PPTP VPN connection is created and ready to use.



Tips:
You can go to Advanced > VPN > VPN Connections to view the clients that are currently connected to the PPTP VPN servers.

Chapter 10

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:

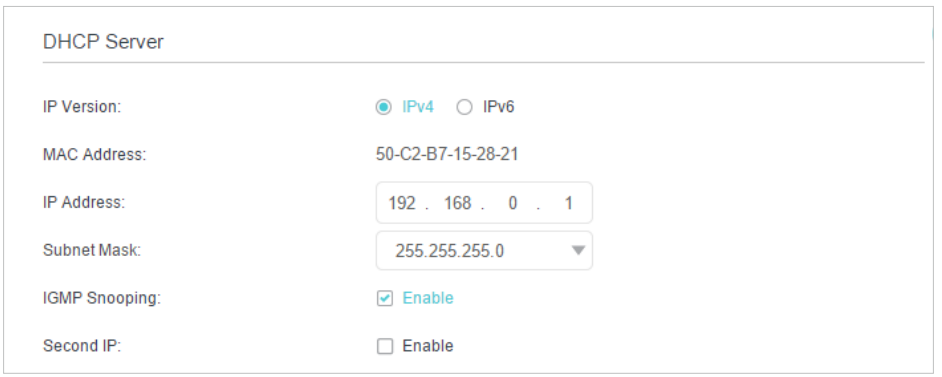
10. 1. Configure LAN Settings

10. 1. 1. Change the LAN IP Address

The router is preset with a default LAN IP 192.168.0.1, which you can use to log in to its web management page. The LAN IP address together with the Subnet Mask also defines the subnet that the connected devices are on. If the IP address conflicts with another device 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://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Network > LAN Settings page and select IPv4.



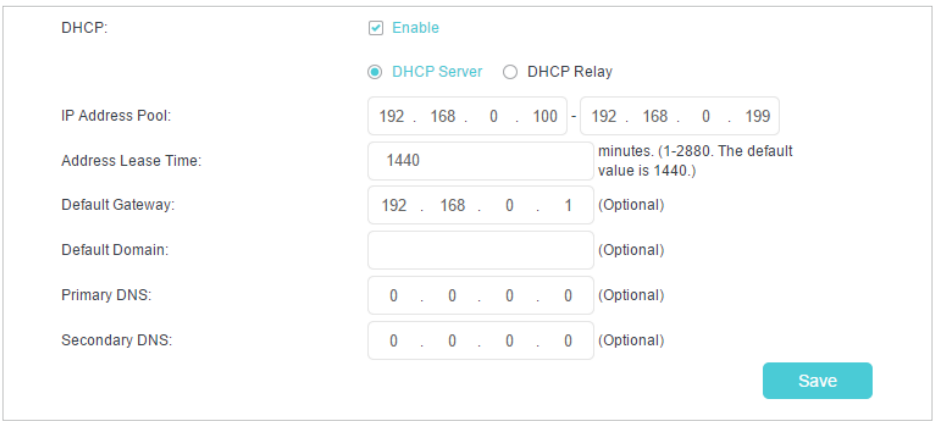
3. Enter a new IP Address appropriate to your needs.
4. Select the Subnet Mask from the drop-down list. The subnet mask together with the IP address identifies the local IP subnet.
5. Keep IGMP Snooping enabled by default. IGMP snooping is the process of listening to IGMP (Internet Group Management Protocol) 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.

10. 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://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Network > LAN Settings page and select IPv4.



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 192.168.0.100 to 192.168.0.199 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 (192.168.0.50 to192.168.0.80) 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.

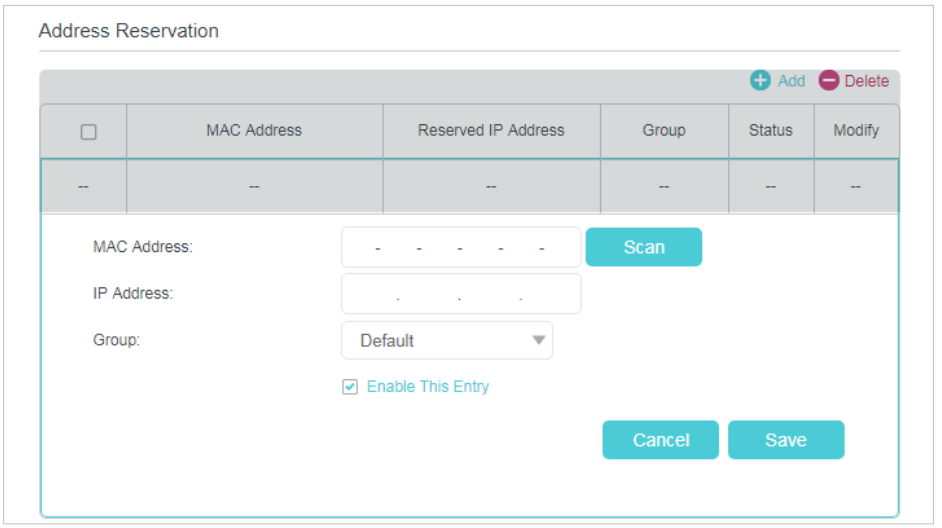
10. 1. 3. Reserve LAN IP Addresses

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://tplinkwifi.net, 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.



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 Save to make the settings effective.

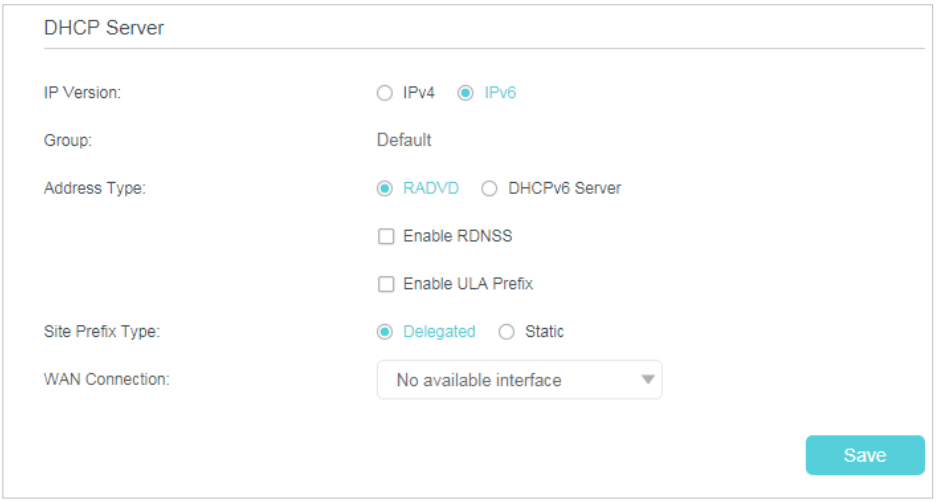
10. 2. Configure IPv6 LAN Settings

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

10. 2. 1. Configure the RADVD Address Type

1. Visit http://tplinkwifi.net, 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.



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.

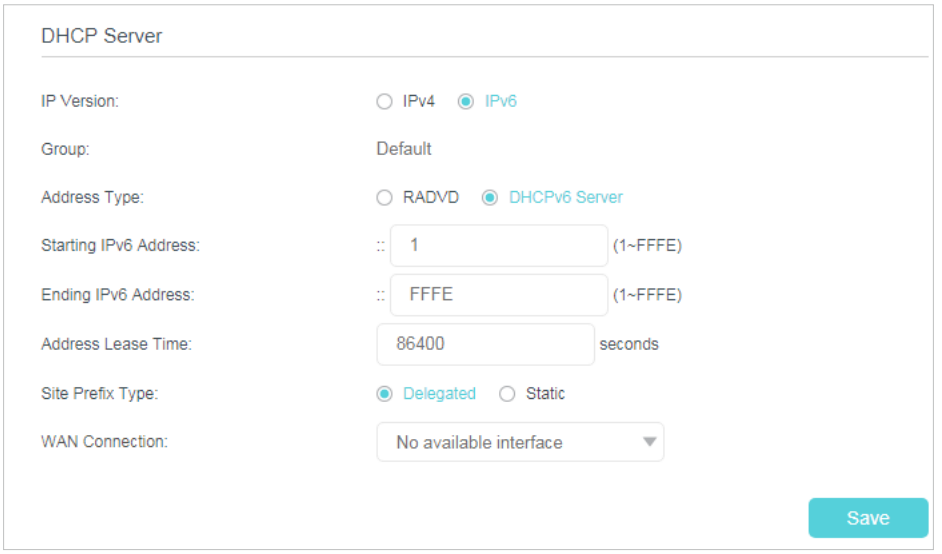
2) Keep Site Prefix Type as the default setting Delegated. If your ISP has provided a specific IPv6 site prefix, select Static and enter the prefix.

3) Keep WAN Connection as the default settings.

4. Click Save to make the settings effective.

10. 2. 2. Configure the DHCPv6 Server Address Type

1. Visit http://tplinkwifi.net, 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.



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.

10. 3. Set Up a Dynamic DNS Service Account

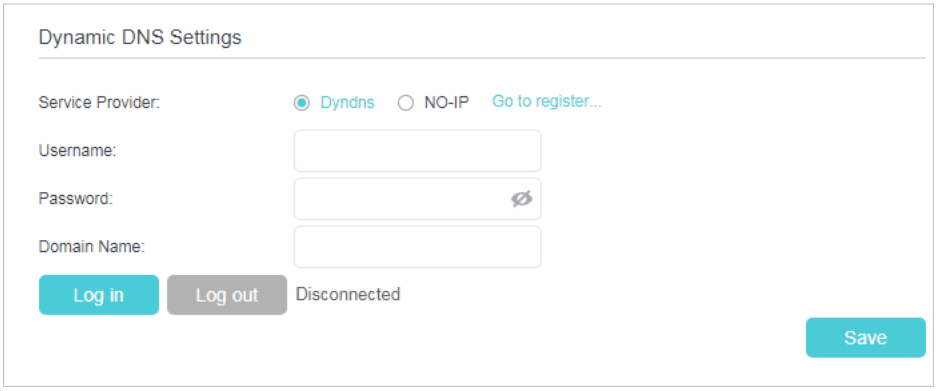
Most ISPs (Internet service providers) assign a dynamic IP address to the router and you can use this IP address to access your router remotely. However, the IP address can change any time and you don't know when it changes. In this case, you might need the DDNS (Dynamic Domain Name Server) feature on 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://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Network > Dynamic DNS.
3. Select the Service Provider (Dyndns or NO-IP).

4. Log in with your DDNS account, select a service provider and click Go to register ... 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.

10. 4. Create Interface Groups

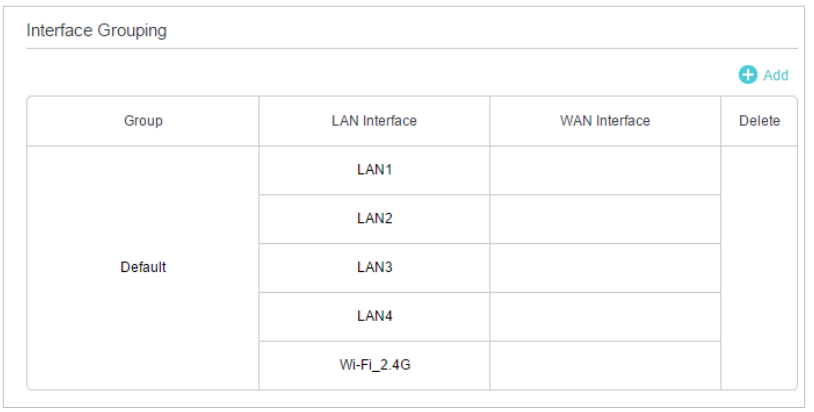
I want to:

Divide my devices connected to the router into different groups and disallow devices' cross-group communication.

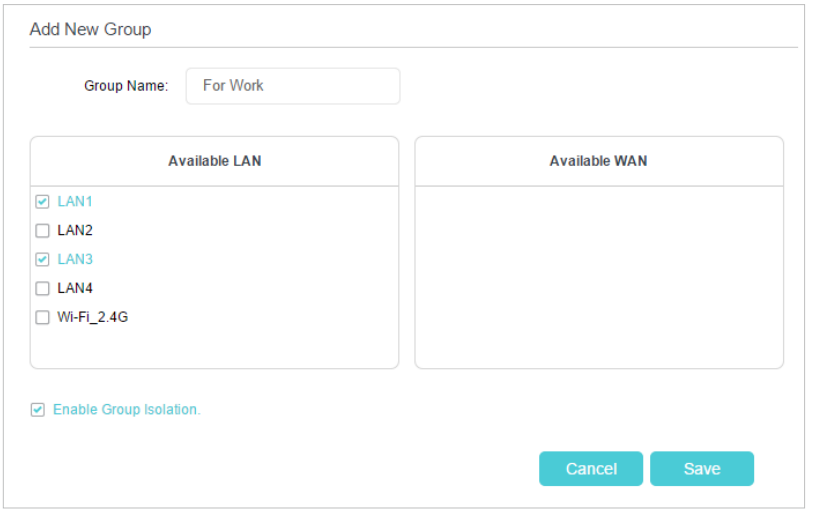
For example, in my house, devices connected to LAN1 and LAN3 are for work, while others for entertainment. I want to isolate working devices from others while keep all devices' access to the internet.

How can I do that?

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Network > Interface Grouping page to open the configuration page where some interfaces can be grouped together.



3. Click Add to create a new group.



4. Name the group.
5. Select LAN1 and LAN3 in Available LAN. Wireless network Wi-Fi 2.4G is viewed as a LAN interface.
6. Select the Enable Group Isolation check box to isolate working devices and disallow other devices from communicating with them.
7. Click Save to make the settings effective.

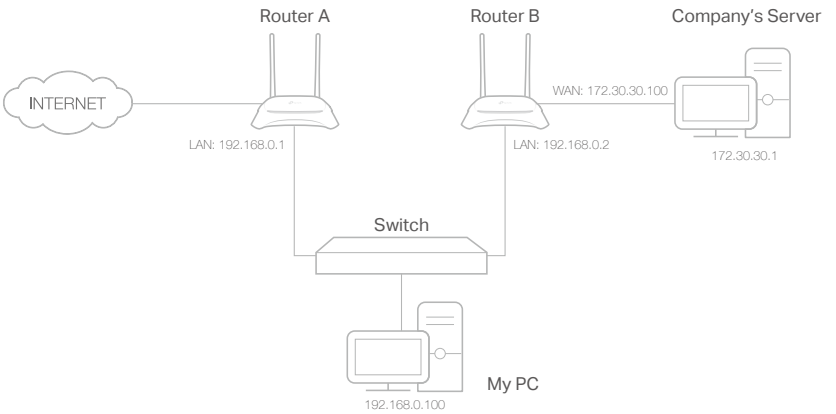
Done! Now your working devices connected to LAN1 and LAN3 are in an isolated group!

10. 5. 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.

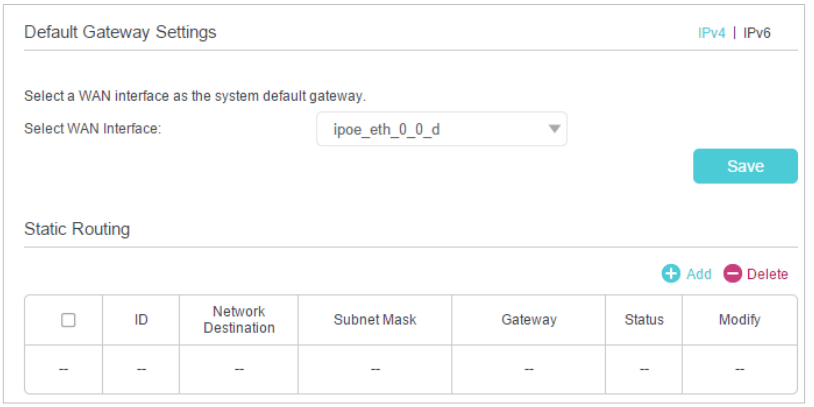
I want to: Visit multiple networks and multiple servers at the same time.

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.

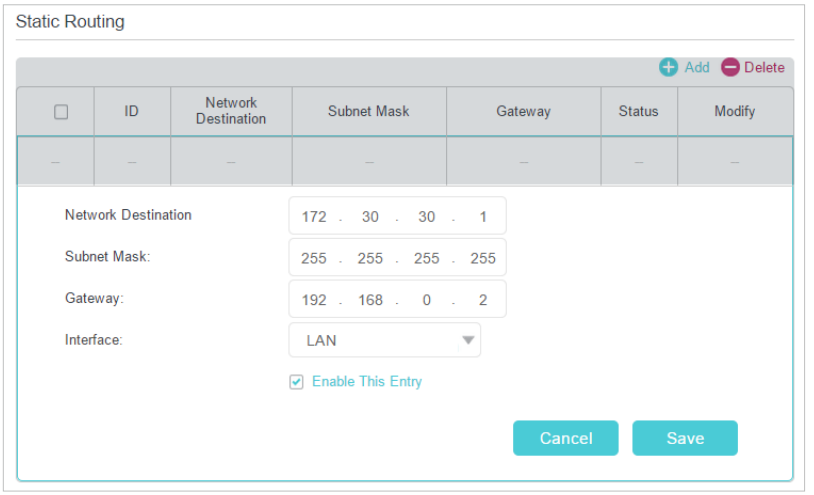


How can I do that?

1. Make sure the routers use different LAN IP addresses on the same subnet. Disable Router B's DHCP function.
2. Visit http://tplinkwifi.net, 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 192.168.0.2.
- 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.

5. Select the Enable This Entry check box to enable this entry.
6. Click Save 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.

10. 6. Set Up the IPv6 Tunnel

The IPv6 Tunnel feature helps you obtain IPv6 resources based on an IPv4 WAN connection or vice versa.

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.

The router provides three tunneling mechanisms: 6to4, 6rd and DS-Lite. The methods of setting up 6rd and DS-Lite tunnel are similar.

10. 6. 1. Use the Public IPv6 Tunnel Service-6to4

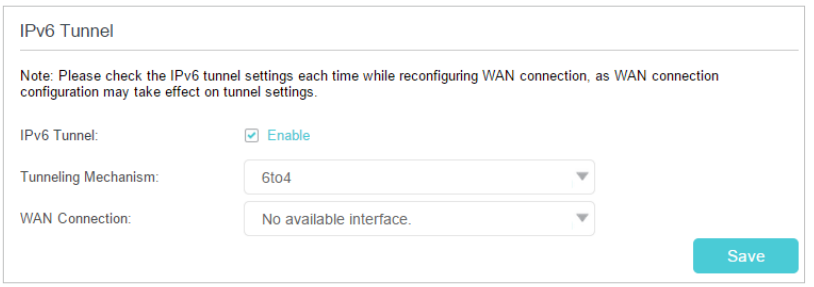
The 6to4 tunnel is a kind of public service. If there are any 6to4 servers on your network, you can use this mechanism to access IPv6 service. If your ISP provides you with an IPv4-only connection but you want to visit IPv6 websites, you can try to set up a 6to4 tunnel.

I want to:

Set up the IPv6 tunnel though my ISP doesn't provide me with the tunnel service.

How can I do that?

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Network > IPv6 Tunnel.
3. Enable IPv6 Tunnel, and select 6to4 as the tunneling mechanism and select a WAN connection from the drop-down list, then click Save.



Note:

If there is no available WAN connection to choose, make sure you have connected to the internet and the connection type is not Bridge.

Done!

Now you can visit the IPv6 websites with the 6to4 tunnel.

Note:

If you still can't access IPv6 resources, it may means that no 6to4 public server was found in your network. You can contact your ISP to sign up for IPv6 connection service.

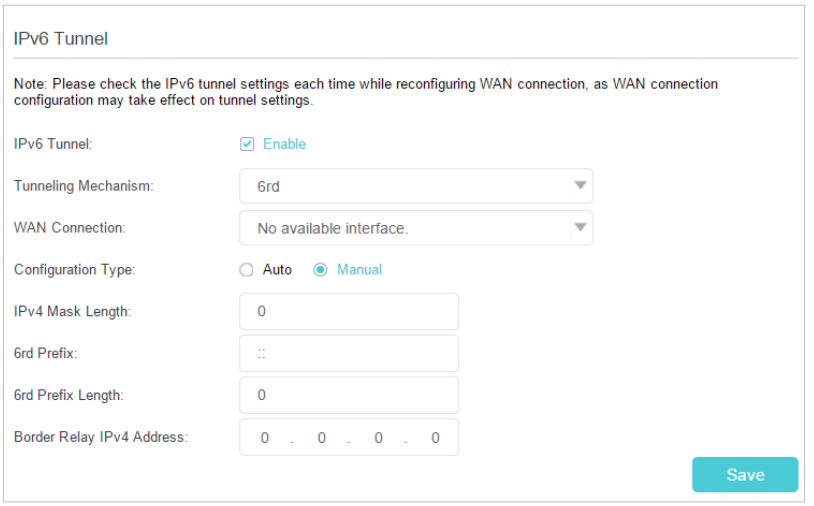
10. 6. 2. Specify the 6rd Tunnel with Parameters Provided by Your ISP

I want to:

Specify the 6rd tunnel with the parameters provided by my 6rd tunnel service provider.

How can I do that?

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Network > IPv6 Tunnel.
3. Enable IPv6 Tunnel, and select 6rd as the tunneling mechanism and select a WAN connection from the drop-down list.
4. According to the parameters provided by your ISP, choose Auto or Manual. More parameters are needed if you choose Manual.
5. Click Save.



Note:

If there is no available WAN connection to choose, make sure you have connected to the internet and the connection type is not Bridge.

Done!

Now you can visit the IPv6 websites with the 6rd tunnel.

Tips:

The way to set up DS-Lite tunnel is similar to that of 6rd tunnel. If you are provided with an IPv6-only WAN connection and have signed up for DS-Lite tunnel service, specify the DS-Lite tunnel by referring to the steps above.

10. 7. Specify Wireless Settings

10. 7. 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://tplinkwifi.net, and log in with the password you set for the router.

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

1. Go to Basic > Wireless.
2. The wireless radio is enabled by default. If you want to disable the wireless function of the router, just clear the Enable check box. 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.
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.

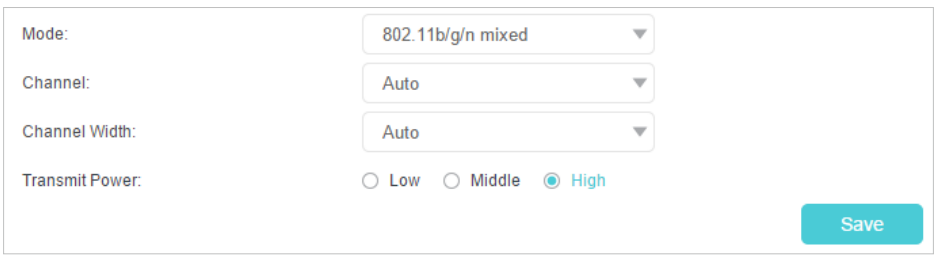
Note:
If you use a wireless device to change the wireless settings, you will be disconnected after the new settings are effective. Please write down the new SSID and password for future use.

➢ **To hide SSID:**

1. Go to Basic > Wireless.
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.



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

Mode: Select the desired transmission mode.

- 802.11n only: Select only if all of your wireless clients are 802.11n devices.
- 802.11g/n mixed: Select if you are using both 802.11g and 802.11n wireless clients.
- 802.11b/g/n mixed: Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.

Note: When 802.11n only mode is selected, only 802.11n wireless stations can connect to the router. It is strongly recommended that you select 802.11b/g/n mixed, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the router.

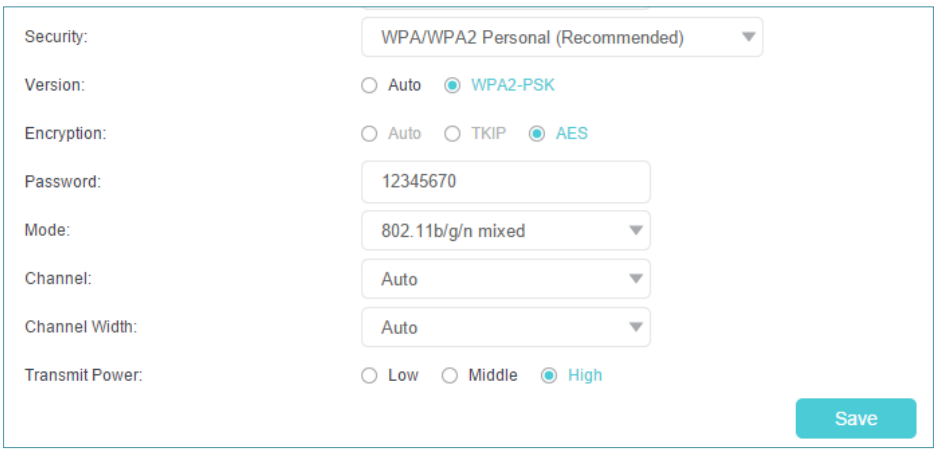
Channel: Select the channel you want to use from the drop-down list. This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

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 four options, No Security, WPA/WPA2 Personal (Recommended), WPA/WPA2 Enterprise, WEP. WPA2 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.

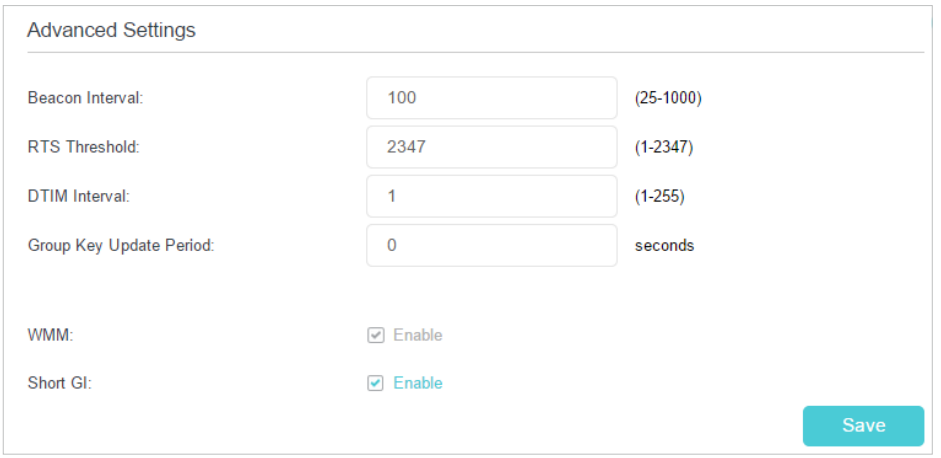
10. 7. 2. Advanced Wireless Settings

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

1. Visit http://tplinkwifi.net, and log in with the password you set for your router.
2. Go to Advanced > Wireless > Advanced Settings page.

➢ **To change basic advanced settings:**

Locate the Advanced Settings section and configure the advanced settings according to the explanation below, and then click Save.



- Beacon Interval: Enter a value between 25 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 2347 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.

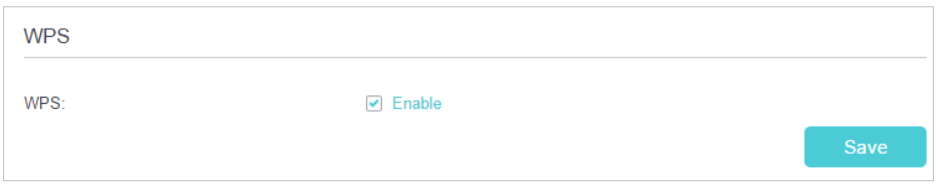
Note:
If you are not familiar with the settings on this page, it's strongly recommended that you keep the provided default values; otherwise it may result in lower wireless network performance.

➢ **To enable WDS bridging function:**

Locate the WDS section and select the Enable WDS Bridging check box. And then set the information of the router to be bridged. Refer to FAQ for detailed instructions.

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

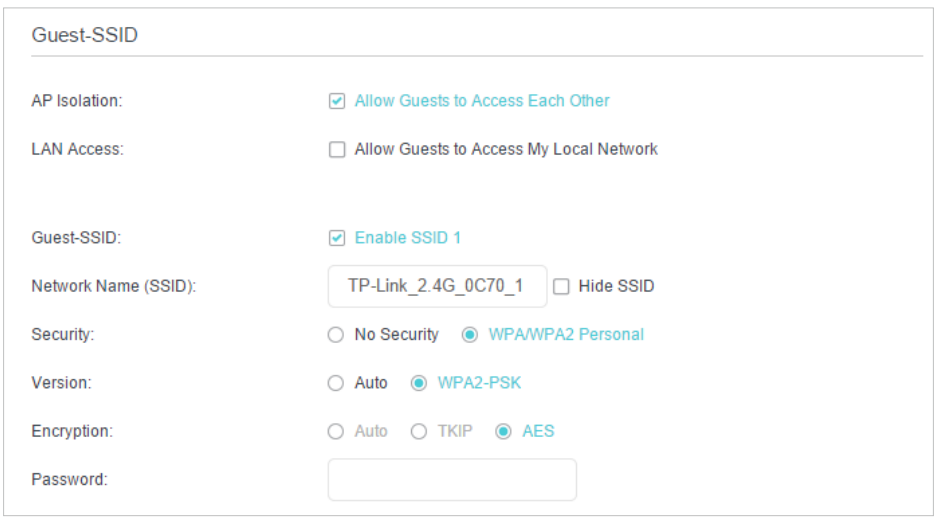
WPS (Wi-Fi Protected Setup) provides you with an easier approach to set up a security-protected Wi-Fi connection. This function is enabled by default, but if you do not need this function, clear the WPS Enable check box and then click Save.



➢ **To create guest-SSID network:**

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

1) Locate the Guest-SSID section, and select the Enable SSID 1 (2 or 3) check box(es) to enable the corresponding guest-SSID network.



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 guest-SSID network, WPA/WPA2 Personal is recommended, and you can set a password for the network.

If you want to allow the wireless devices on the guest-SSID network to communicate with each other via methods such as network neighbors, Samba, Ping, and FTP, select the Allow Guests to Access Each Other check box.

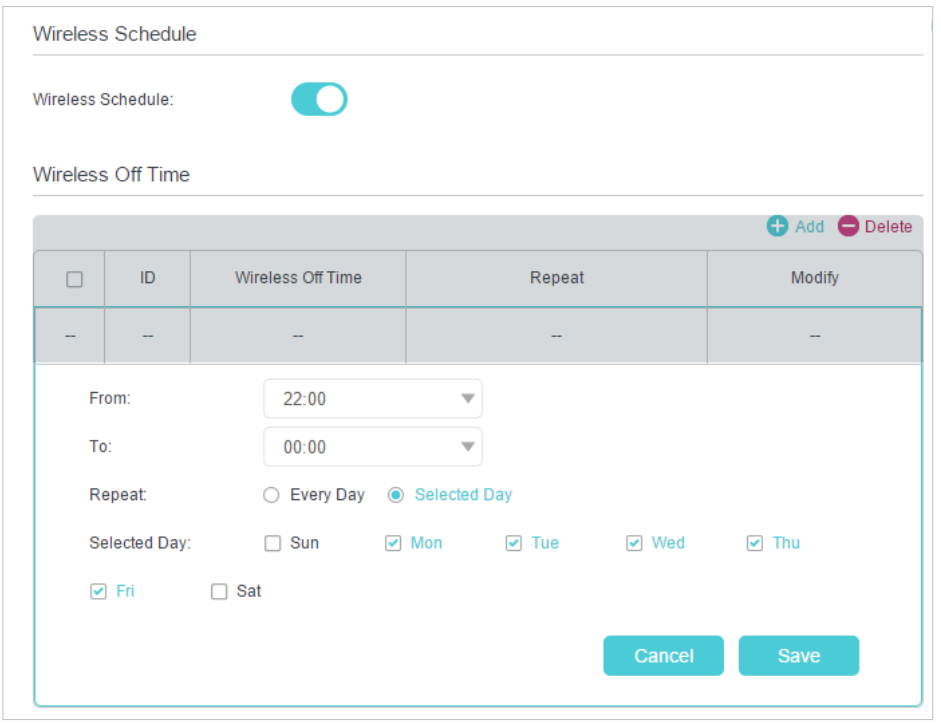
If you want to allow the wireless devices on the guest-SSID network to communicate with the devices connected to the router's LAN ports or main network via methods such as network neighbors, Samba, Ping, and FTP, select the Allow Guests to Access My Local Network check box.

4) Repeat Step 1) to Step 3) to set other two wireless networks if needed, and click Save to make the settings effective.

10. 7. 3. Schedule Your Wireless Function

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

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



4. Click Add to set the Wireless Off Time, and click Save to make the settings effective.

Note:

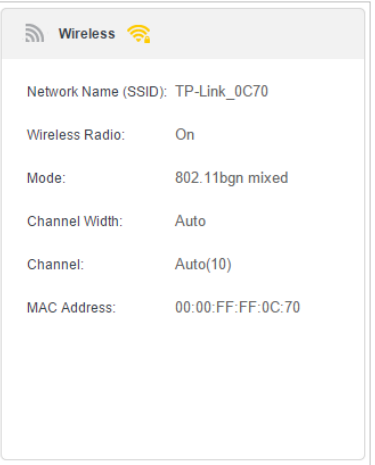
1. Make sure that the time of the router is correct before using this function. For details, refer to Set System Time.

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.

10. 7. 4. View Wireless Information

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

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Status page. You will find the Wireless panel.



Tips: You can also see the wireless details by clicking the router icon on Basic> Network Map.

➢ **To view the detailed information of the connected wireless clients:**

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Wireless > Statistics page.
3. You can view the detailed information of the wireless clients, including its connection type and security option as well as the packets transmitted.

Tips: You can also see the wireless details by clicking the wireless clients icon on Basic > Network Map.

10. 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.

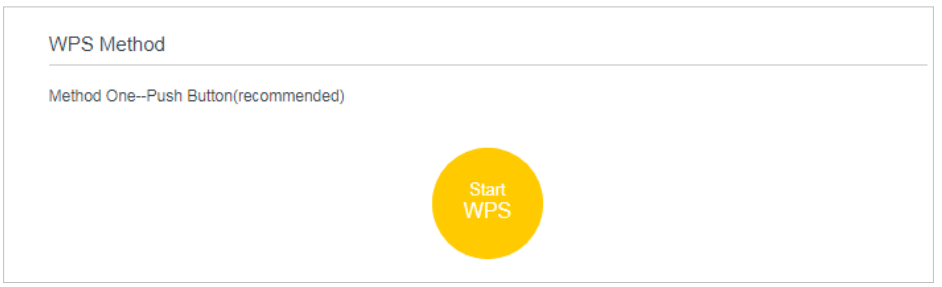
1. Press the WPS/RESET button of the router.
2. Press the WPS button of the client device directly.
3. The WPS LED flashes for about 2 minutes during the WPS process.

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

Method 2: Use the WPS button on the web management page

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

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Wireless > WPS page.



3. Click Start WPS 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://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Wireless > WPS, and click Method Two--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.

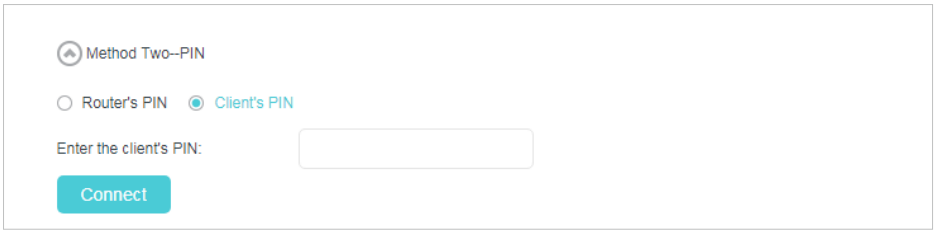
Note:

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://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Wireless > WPS, and click Method Two--PIN.
3. Select Client's PIN.



4. Enter the client device's PIN. 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 11

Manage Your Router

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

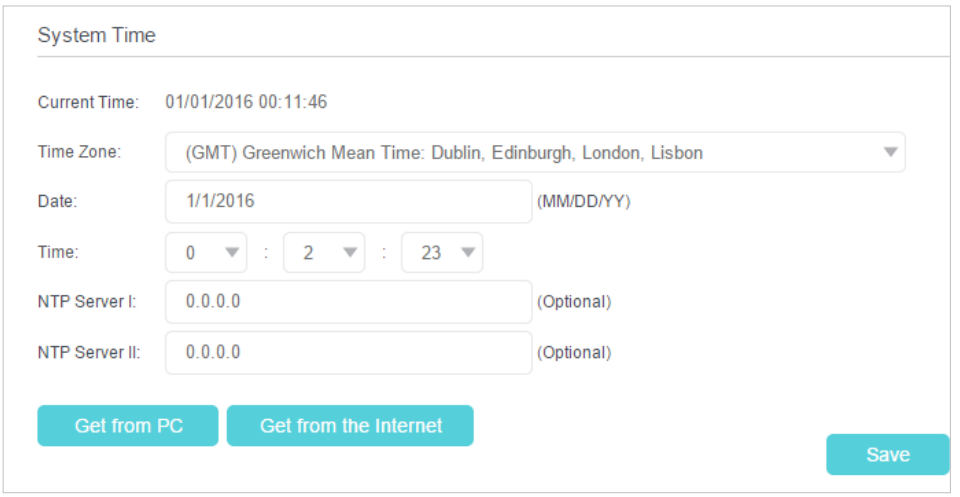
This chapter contains the following sections:

11. 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://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > System Tools > Time Settings page.



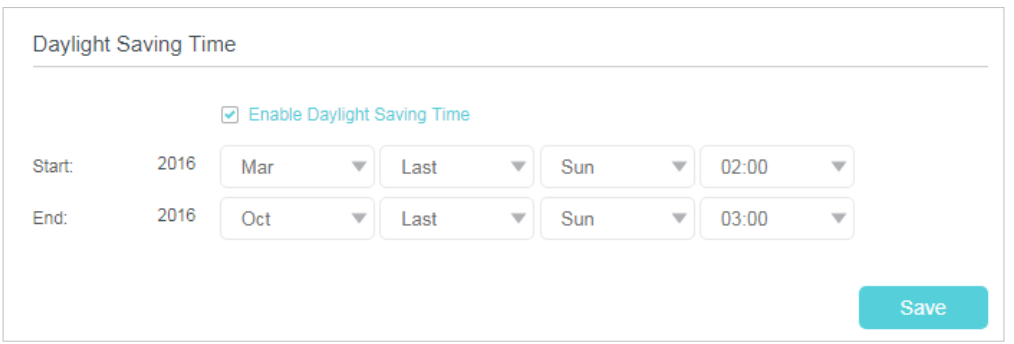
3. Configure the system time using the following methods:

   Manually: Select your time zone, enter the date and select the local time.

   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.



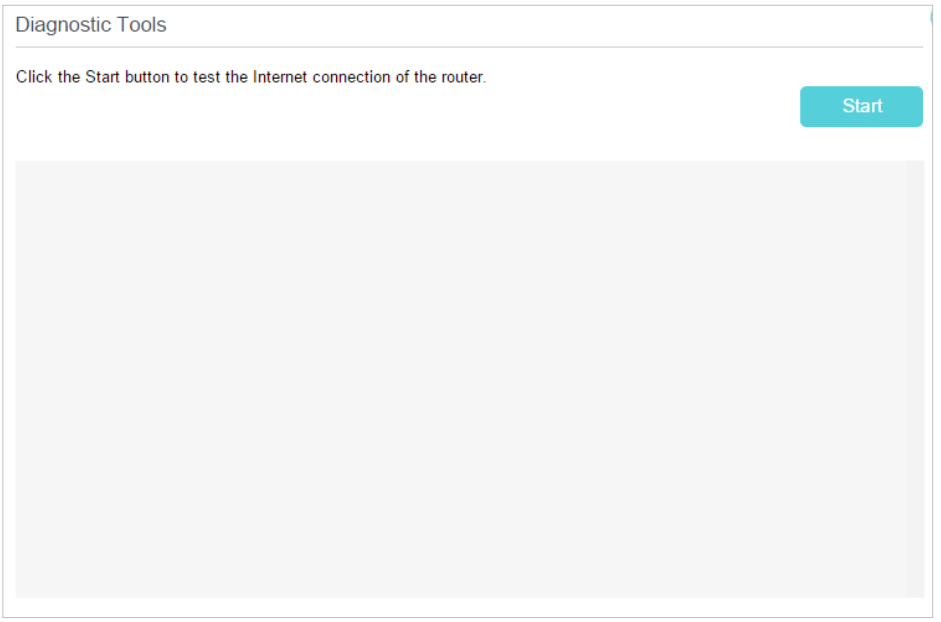
11. 2. Test Internet Connectivity

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

1. Visit http://tplinkwifi.net, and log in with the password you set for your router.
2. Go to Advanced > System Tools > Diagnostics page.

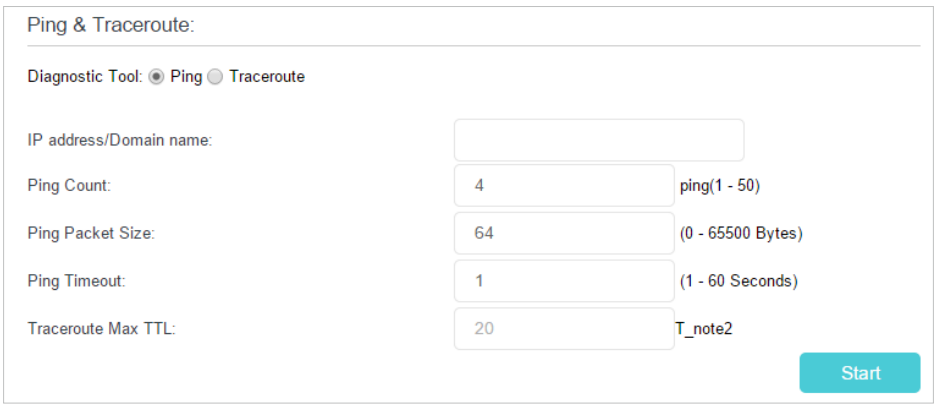
➢ **To test the internet connection of the router:**

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 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.

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.

11. 3. Update the Firmware

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

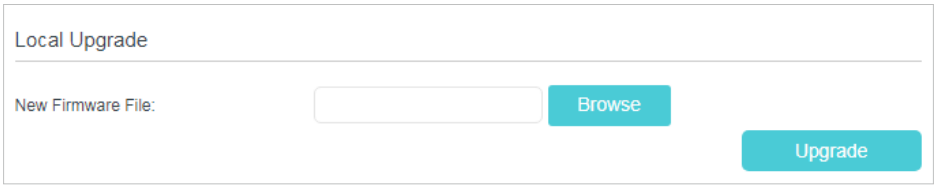
We will inform you through the web management page if there's any update firmware available for your router. The latest firmware can also be downloaded from the Support page of our website www.tp-link.com for free.

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.

You can 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://tplinkwifi.net, 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.
5. Focus on the Local Upgrade section. Click Browse to locate the downloaded new firmware file, and click Upgrade.



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

11. 4. Back Up and Restore Configuration Settings

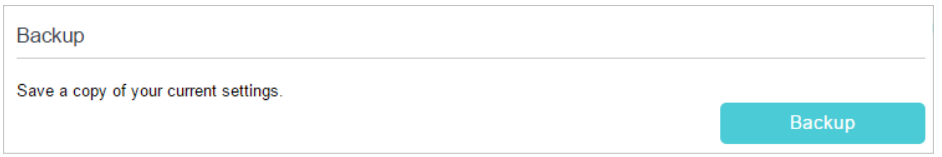
The configuration settings are stored as a configuration file in the router. You can back up the configuration file to your computer for future use and restore the router to a previous settings from the backup file when needed. Moreover, if needed you can erase the current settings and reset the router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

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.

2. Go to Advanced > System Tools > Backup & Restore.

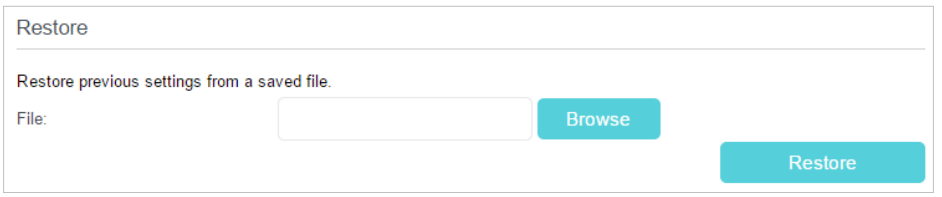
➢ **To back up configuration settings:**

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



➢ **To restore configuration settings:**

1) Click Browse to locate the previous backup configuration file, and click Restore.



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.

2) Wait a few seconds 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.

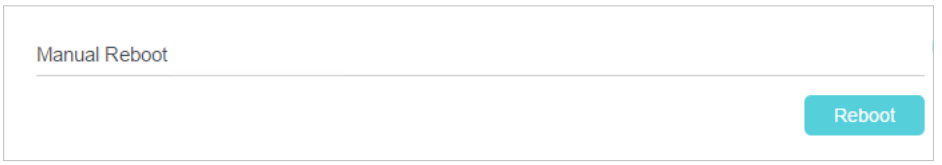
11. 5. Reboot the Router

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://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > System Tools > Reboot, and you can restart your router.

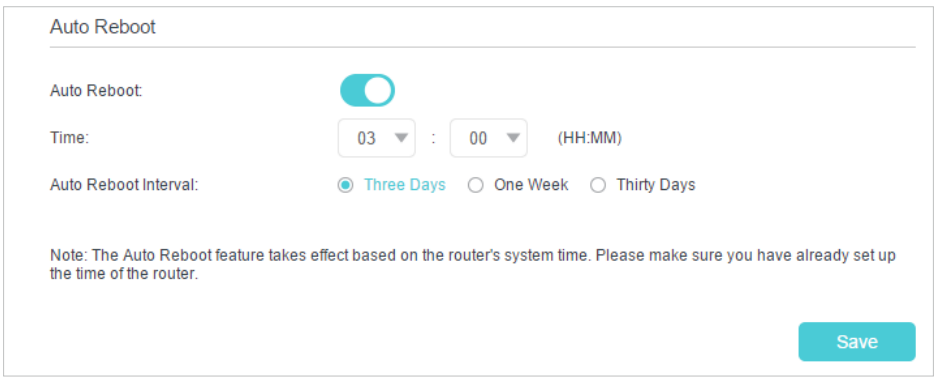
➢ **To reboot the router manually:**

Click Reboot, and wait a few minutes for the router to rebooting.



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

1. Enable Auto Reboot.
2. Specify the Time when the router reboots and the Auto Reboot Interval to decide how often it 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 DHCP Settings.
- Change the Operation Mode.
- Change the Web Management Port.
- 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).

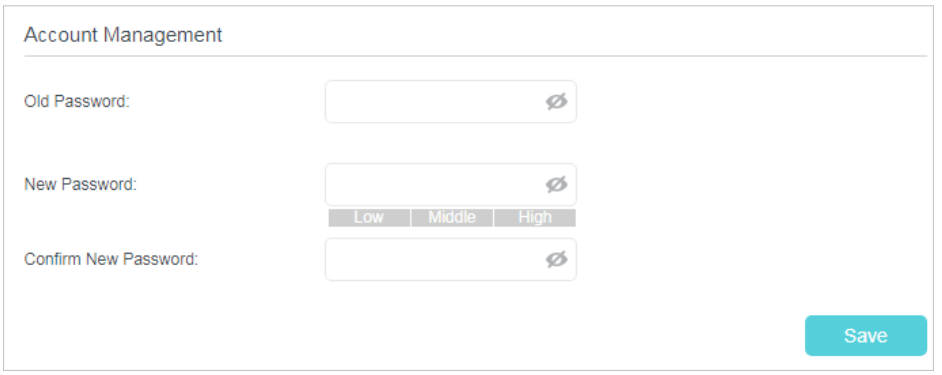
Note:
The Auto Reboot feature takes effect based on the router's system time. Please make sure you have already set up the time of the router.

11. 6. Administration Management

11. 6. 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://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > System Tools > Administration, and locate the Account Management section.



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

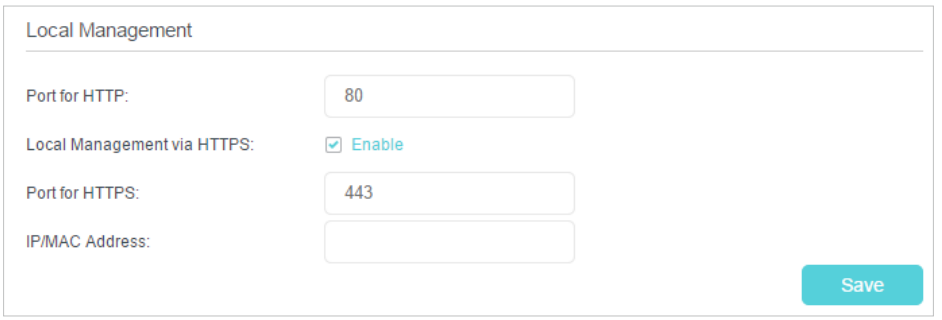
11. 6. 2. Local Management

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://tplinkwifi.net, 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.



4. Click Save.

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

Note:
If you want all local devices can manage the router, just leave the IP/MAC Address field blank.

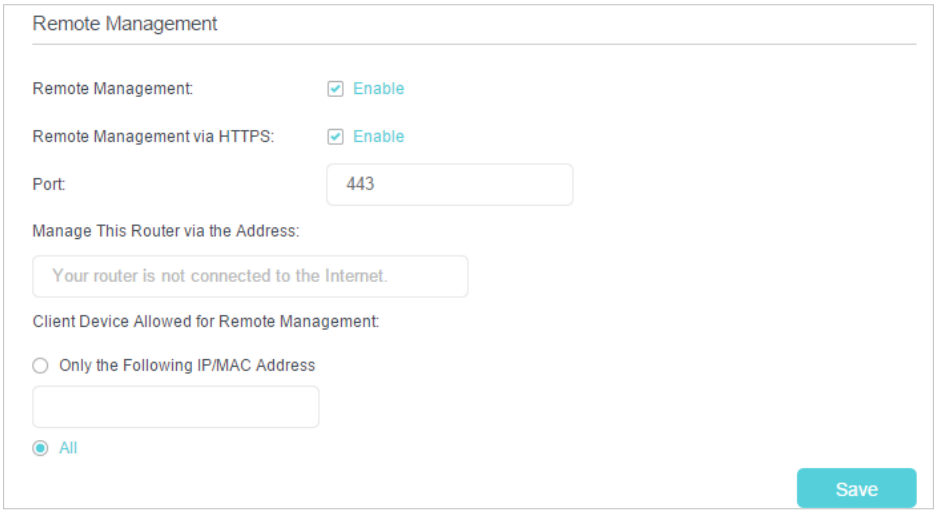
11. 6. 3. Remote Management

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://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > System Tools > Administration, and locate the Remote Management section.

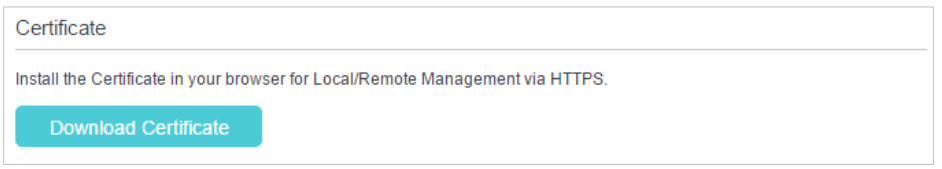


3. Enable Remote Management and Remote Management via HTTPS to allow for HTTPS connection. Keep the Port as the default setting.
4. Set the client device allowed for remote management. Select All to allow all remote devices to manage the router. If you just want to allow a specific device to manage the 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.



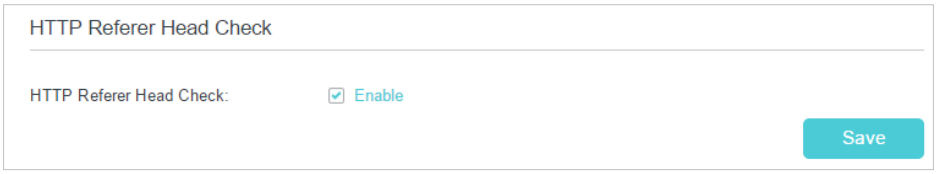
2. The router's WAN IP is usually a dynamic IP. Please refer to Set Up a Dynamic DNS Service Account if you want to log in to the router through a domain name.

11. 6. 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://tplinkwifi.net, 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.

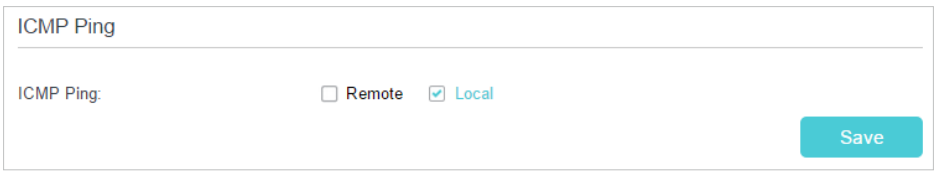


11. 6. 5. ICMP Ping

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://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > System Tools > Administration, and locate the ICMP Ping section.

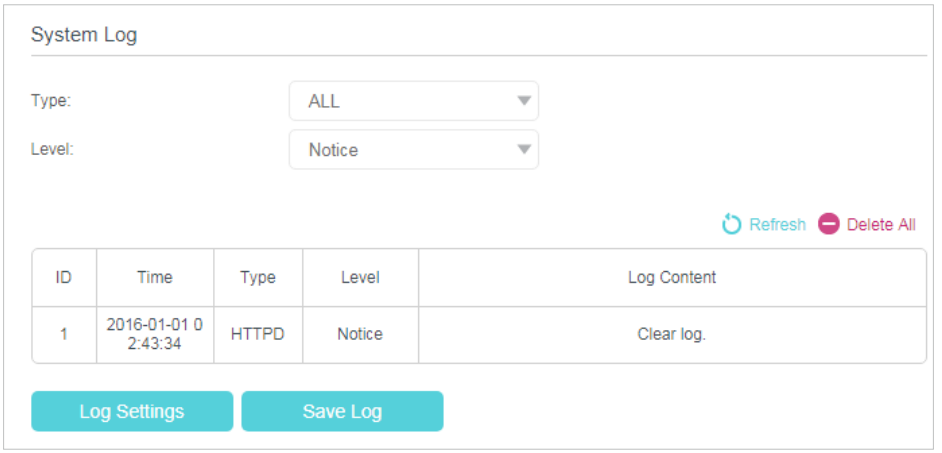


3. Specify the ICMP Ping reply options.
   - Remote: Select it if you want the computers on a public network to ping the router's WAN IP address.
   - Local: Enabled by default, if enabled, the computers on a private network can ping the router's LAN IP address.
4. Click Save to make the settings effective.

11. 7. 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://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > System Tools > System Log page.



➢ **To view the system logs:**

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

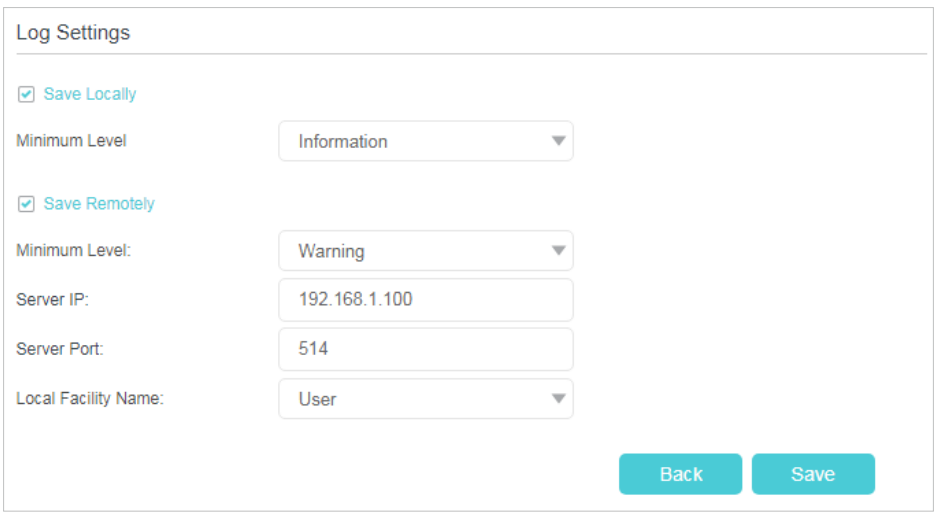
Click Refresh to refresh the log list.

➢ **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.

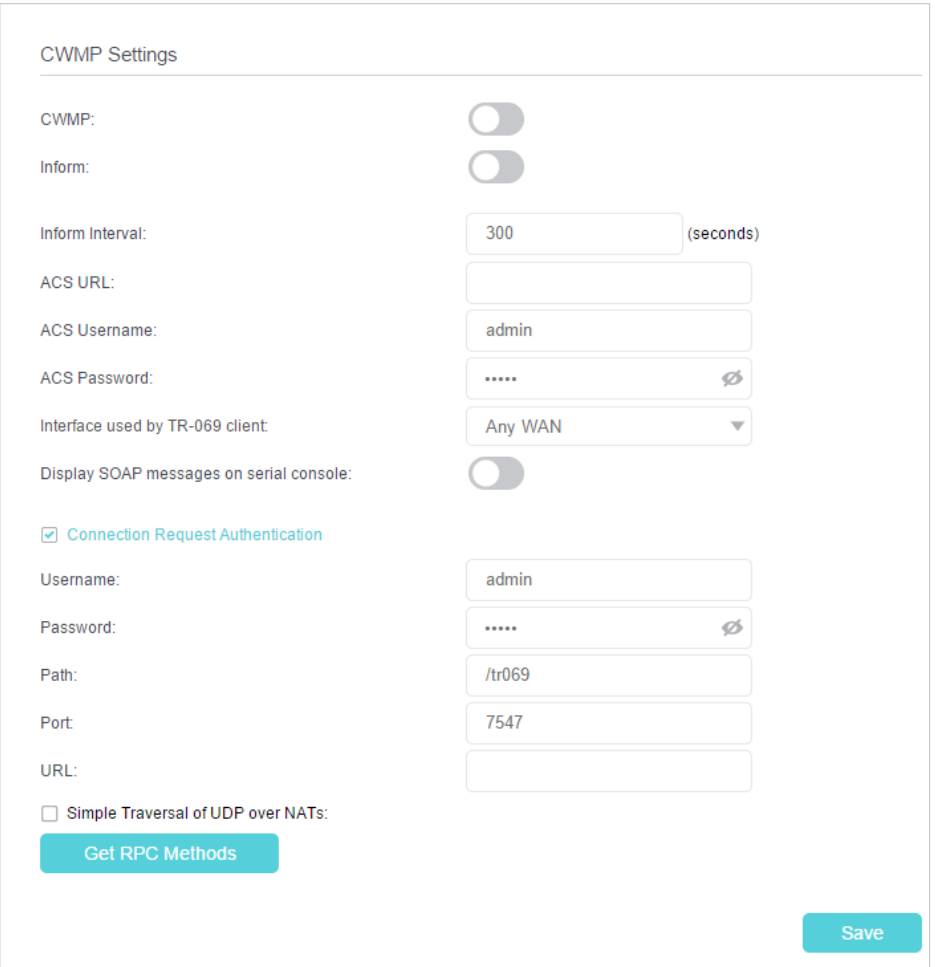


- Save Locally: Select this option to cache the system log to the router's local memory, select the minimum level of system log to be saved from the drop-down list. The logs will be shown in the table in descending order on the System Log page.
- Save Remotely: Select this option to send the system log 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.

11. 8. CWMP Settings

The router supports CWMP (CPE WAN Management Protocol), also called TR-069. This collects information, performs diagnostics and configures the devices automatically via ACS (Auto-Configuration Server).

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > System Tools > CWMP Settings page.



- CWMP: Enable or disable the CWMP (CPE WAN Management Protocol) function.
- Inform: Enable or disable the function of sending an inform message to the ACS (Auto Configuration Server) periodically.
- Inform Interval: Set the time interval in seconds when the Inform message will be sent to the ACS.
- ACS URL: Enter the web address of the ACS which is provided by your ISP.
- ACS Username/Password: Enter the username/password to log in to the ACS server.
- Interface used by TR-069 client: Select which interface to be used by the TR-069 client.

- Display SOAP messages on serial console: Enable or disable this function.
- Connection Request Authentication: Select this check box to enable authentication for the connection request.
- Username/Password: Enter the username/password for the ACS server to log in to the router.
- Path: Enter the path for the ACS server to log in to the router.
- Port: Enter the port that connects to the ACS server.
- URL: Enter the URL that connects to the ACS server.
- Simple Traversal of UDP over NATs: Select this check box to enable STUN for the connection request and set the STUN maximum and minimum keep alive period, server address and port.
- Get RPC Methods: Click to get the methods to support CWMP.

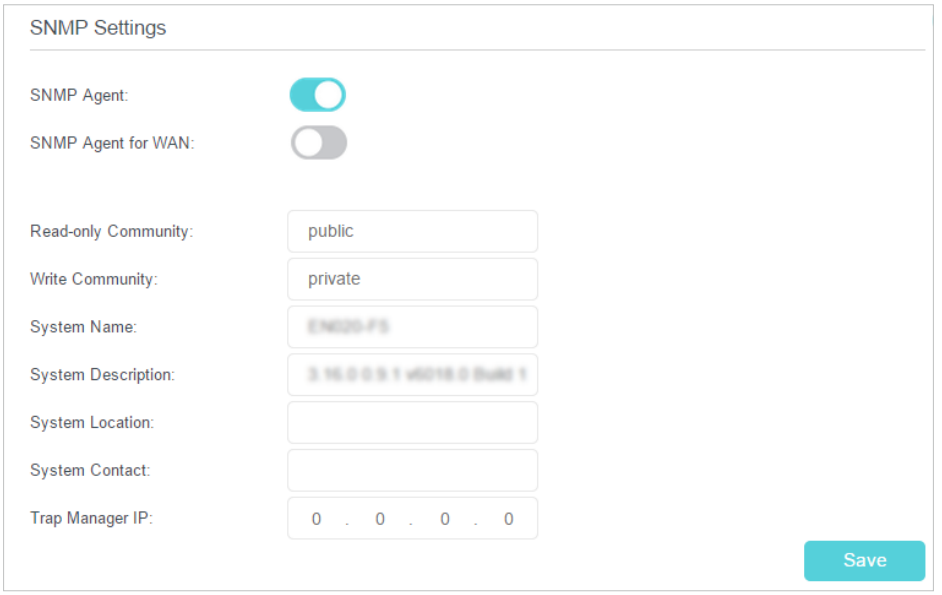
Click Save to make the settings effective.

11. 9. SNMP Settings

SNMP (Simple Network Management Protocol) is widely used in network management for network monitoring. It allows management applications to retrieve status updates and statistics from the SNMP agent within this device. In this way, network administrators can easily search and modify the information on any node on the network. Meanwhile, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating.

The SNMP Agent is an application running on the router that performs the operational role of receiving and processing SNMP messages, sending responses to the SNMP manager, and sending traps when an event occurs. So a router contains SNMP "agent" software can be monitored and/or controlled by SNMP Manager using SNMP messages.

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > System Tools > SNMP Settings page.



- SNMP Agent/SNMP Agent for WAN: Turn on to enable the built-in SNMP agent that allows the router to operate as the operational role in receiving and processing of SNMP messages, sending responses to the SNMP manager, and triggering SNMP traps when an event occurs.
- Read-only Community: Displays the default public community string that protects the router from unauthorized access.
- Write Community: Displays the default write community string that protects the router from unauthorized changes.
- System Name: Displays the administratively-assigned name for this managed device.
- System Description: Displays the textual description of the managed device. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software.
- System Location: Displays the physical location of this device (for example, the telephone closet, 3rd floor).
- System Contact: Displays the textual identification of the contact person for this managed device, together with information on how to contact this person.
- Trap Manager IP: Displays the IP address of the host to receive the traps.

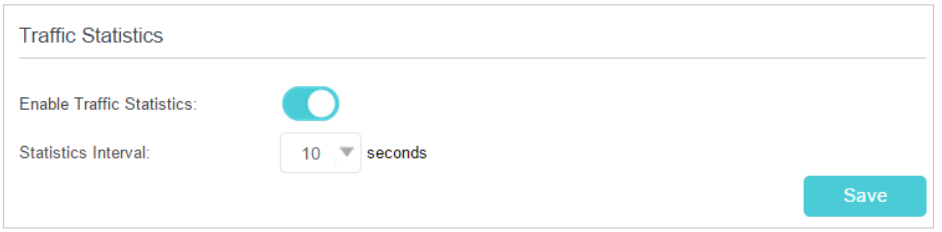
You are suggested to keep the default settings. Click Save to make the settings effective.

11. 10. Monitor the Internet Traffic Statistics

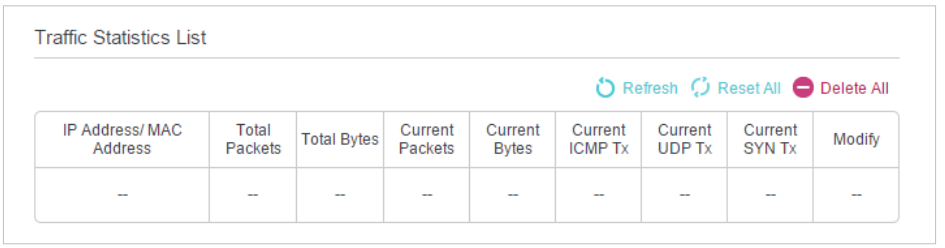
The traffic statistics function allows you to monitor the volume of internet traffic statistics. You can view the network traffic of the LAN, WAN and WLAN sent and received packets.

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.

2. Go to Advanced > System Tools > 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.



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 changed:

1. Connect your computer to the router using an Ethernet cable.
2. Visit http://tplinkwifi.net, and log in with the password you set for the router.
3. Go to Basic > Wireless to retrieve or reset your wireless password.

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

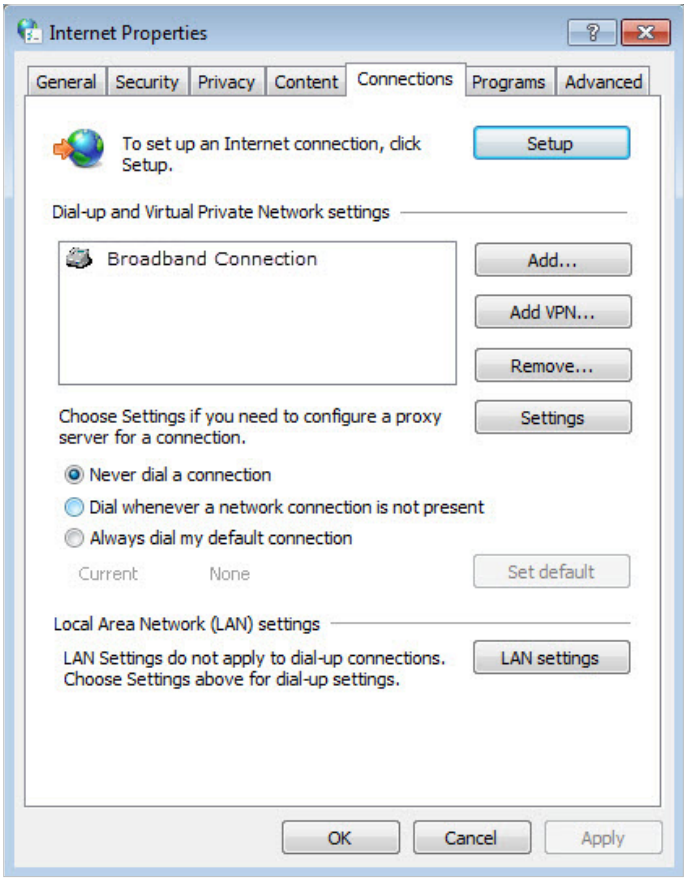
- If you are using a web browser to log in, click Forgot password on the login page and then follow the instructions to reset it.
- Alternatively, press and hold the WPS/RESET button of the router for about 8 seconds, and then visit http://tplinkwifi.net to create a new login password.

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.

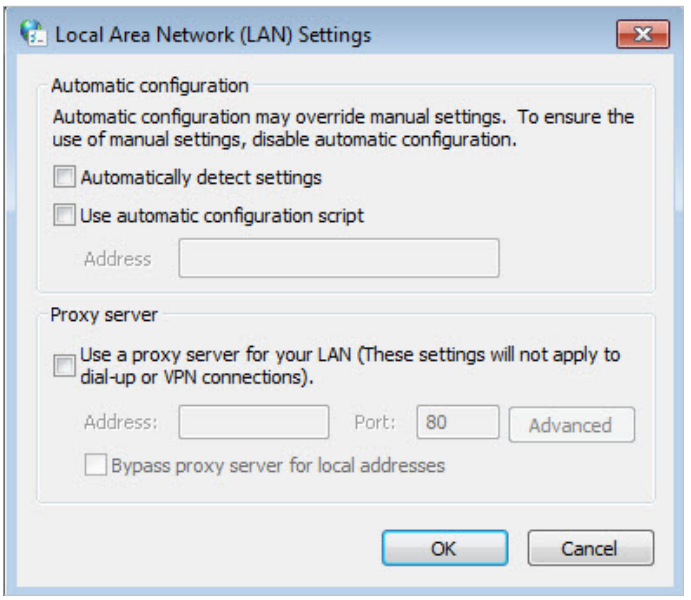
Q3. What should I do if I cannot log in to the router's web management page?

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

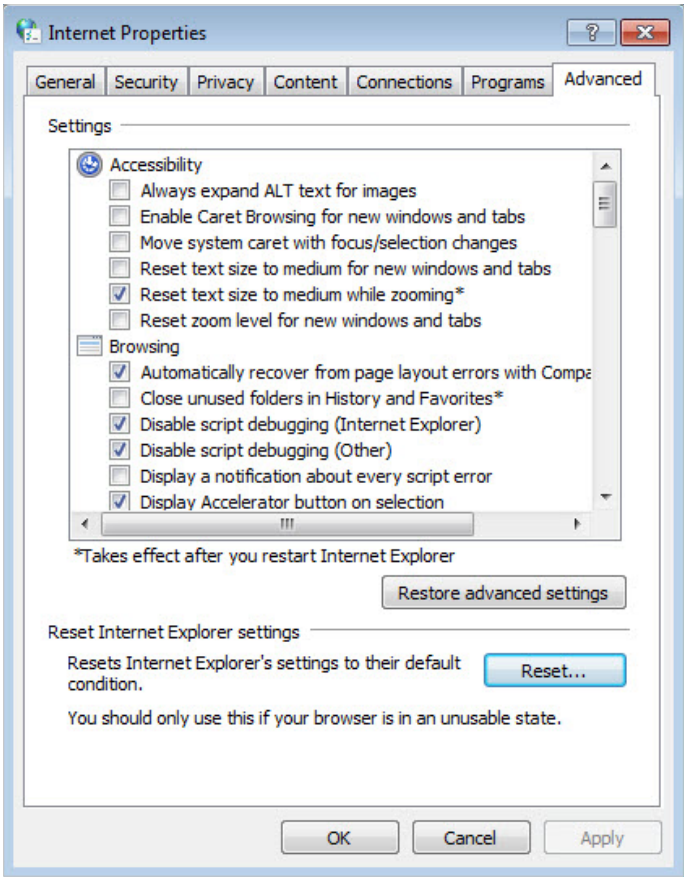
- Make sure your computer is connected to the router correctly and the corresponding LED indicator(s) light up.
- Make sure the IP address of your computer is configured as Obtain an IP address automatically and Obtain DNS server address automatically.
- Make sure http://tplinkwifi.net or http://192.168.0.1 is correctly entered.
- Check your computer's settings:
  1) Go to Start > Control Panel > Network and Internet, and click View network status and tasks.
  2) Click Internet Options on the bottom left.
  3) Click Connections and select Never dial a connection.



4) Click LAN settings and clear 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.

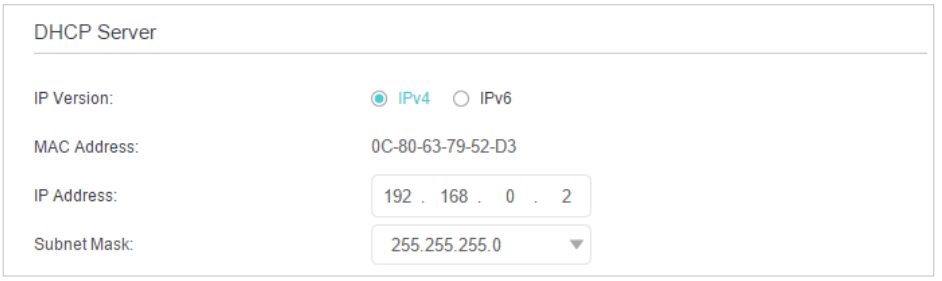
Q4. How do I use the WDS Bridging function to extend my wireless network?

For example, my house covers a large area. The wireless coverage of the router I'm using (the root router) is limited. I want to use an extended router to boost the wireless network of the root router.

Note:

WDS bridging only requires configuration on the extended router.

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Configure the IP address of the router:
   1) Go to Advanced > Network > LAN Settings, configure the IP address of the extended router to be in the same subnet with the root router; (For example, the IP address of the root router is 192.168.0.1, the IP address of the extended router can be 192.168.0.2~192.168.0.254. We take 192.168.0.2 as example.)

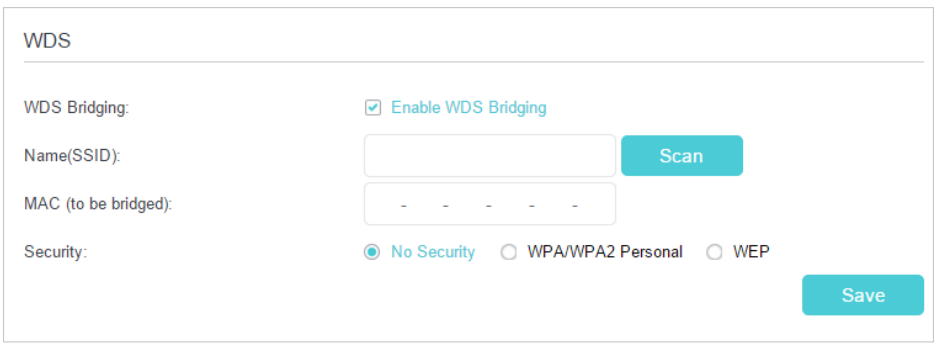


2) Click Save to make the settings effective.

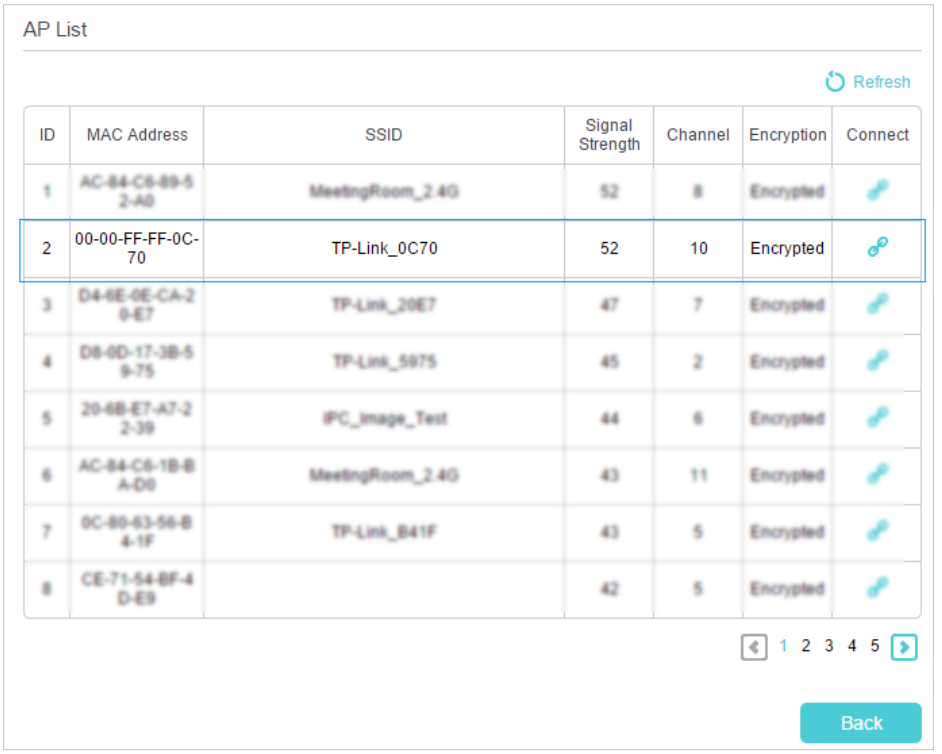
Note: Log in to the web management page again if the IP address of the router is altered.

3. Select the SSID to be bridged:

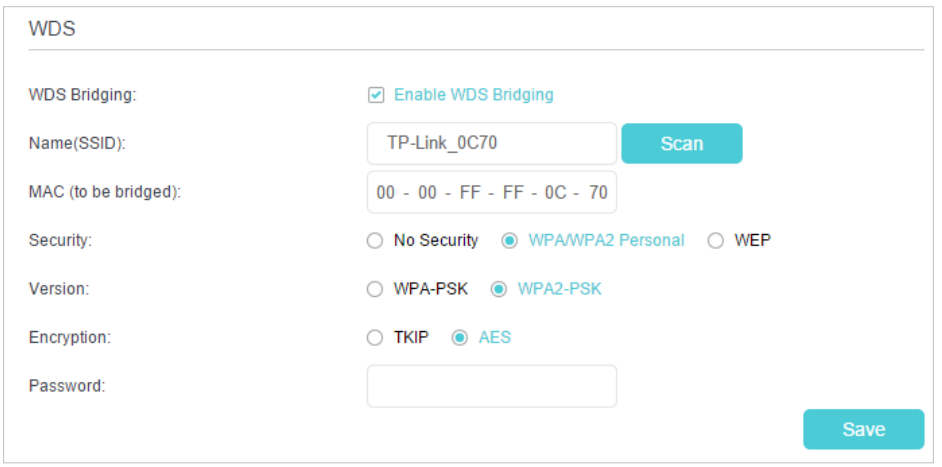
1) Go to Advanced > Wireless > Advanced Settings page. Locate the WDS section and select the Enable WDS Bridging check box to enable the WDS Bridging function.



2) Click Scan to detect all available AP devices and locate the network you want to bridge with.



3) Click the connect icon and then the SSID and MAC will be automatically filled in. If the root router has wireless password, you should enter the wireless password of the root router.



4) Click Save to make the settings effective.

4. Disable DHCP:

1) Go to Advanced > Network > LAN Settings page.

2) Clear the Enable check box of DHCP and click Save.

Now, the root's wireless network is extended and you can use the router's SSID and password to enjoy the network.

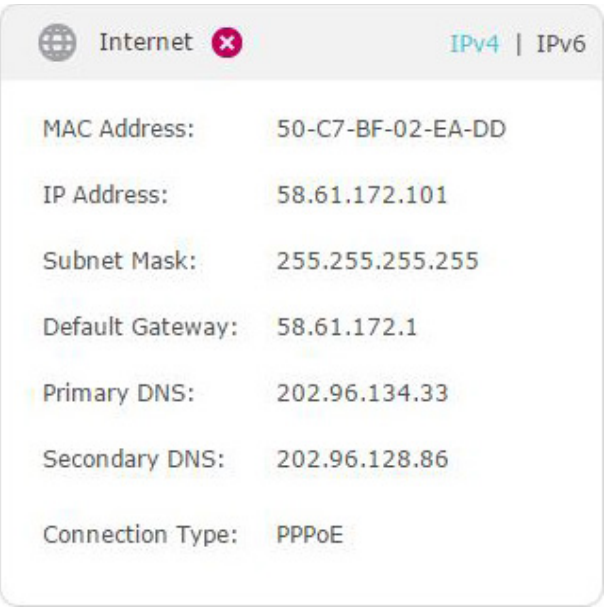
Note:

- The extended router can have different SSID and password from the root router, you can change your router's SSID and password on Basic > Wireless page.
- You can also bridge a network manually: enter the SSID (network name) and MAC Address of the network to be bridged. Select a security type and enter related parameters, which should be the same as the network to be bridged.

Q5. What should I do if I cannot access the internet even though the configuration is finished?

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Status to check internet status:

As the following image shows, if IP Address is a valid one, please try the methods below and try again:

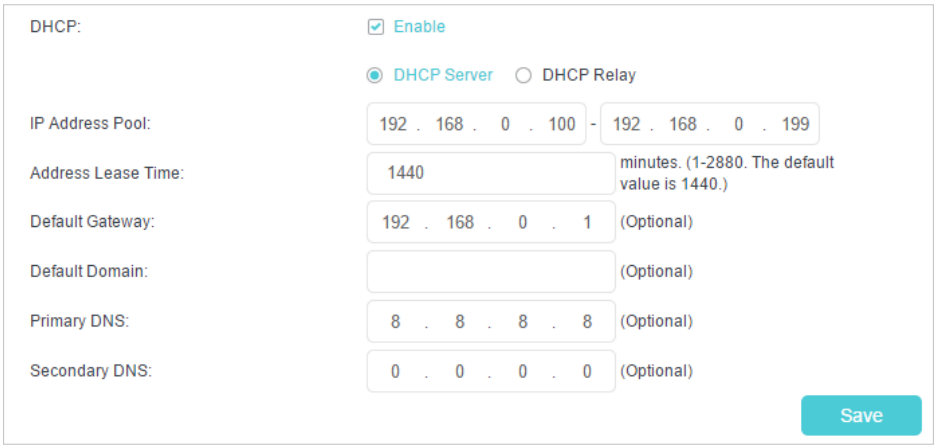


- Your computer might not recognize any DNS server addresses. Please manually configure the DNS server.

  1) Go to Advanced > Network > LAN Settings.

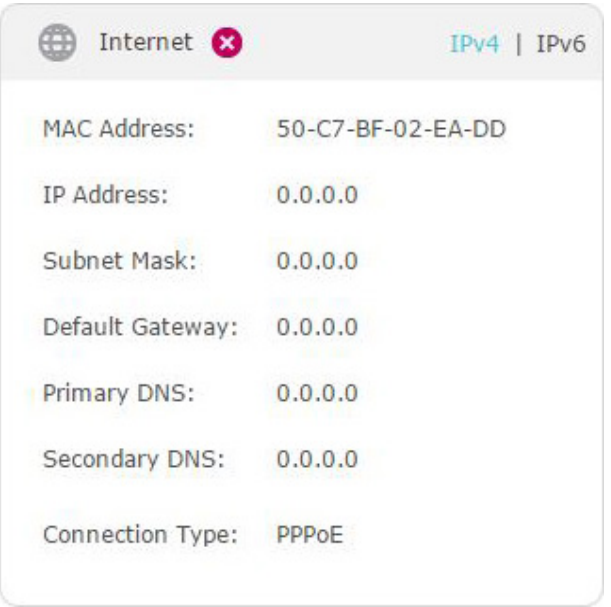
  2) Enter 8.8.8.8 as Primary DNS, click Save.

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



- 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 following image shows, if the IP Address is 0.0.0.0, please try the methods below and try again:



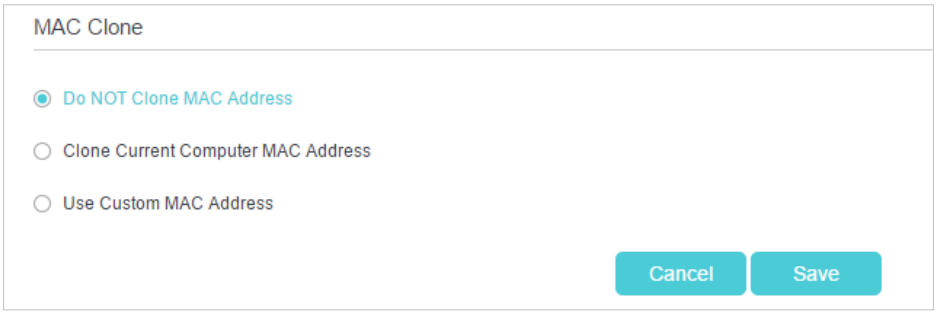
- Make sure the physical connection between the router and the modem is proper.

- Clone the MAC address of your computer.

  1) Visit http://tplinkwifi.net, and log in with the password you set for the router.

  2) Go to Advanced > Network > Internet and click the edit icon to find the MAC Clone section.

  3) Choose an option as needed (enter the MAC address if Use Custom MAC Address is selected), and click Save.



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:

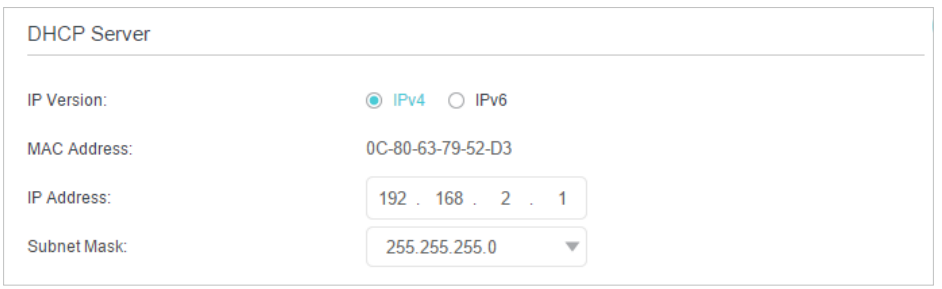
Most TP-Link routers use 192.168.0.1/192.168.1.1 as their default LAN IP address, which may conflict with the IP range of your existing ADSL modem/router. If so, the router is not able to communicate with your modem and you can't access the internet. To resolve this problem, we need to change the LAN IP address of the router to avoid such conflict, for example, 192.168.2.1.

  1) Visit http://tplinkwifi.net, and log in with the password you set for the router.

  2) Go to Advanced > Network > LAN Settings.

  3) Modify the LAN IP address as the following image shows. Here we take 192.168.2.1 as an example.

  4) Click 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 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.

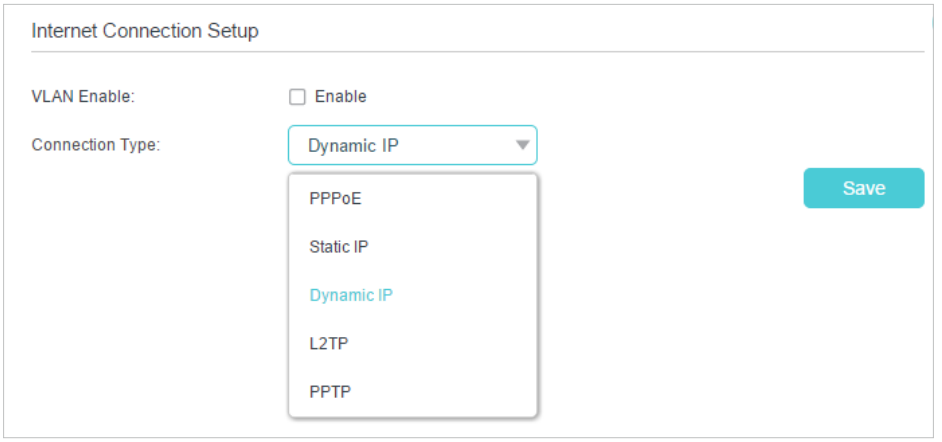
1) Confirm your internet connection type, which can be learned from the ISP.

2) Visit http://tplinkwifi.net, and log in with the password you set for the router.

3) Go to Basic > Internet.

4) Select your Internet Connection Type and enter other parameters if required.

5) Click Save.



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.

Q6. What should I do if I cannot 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**

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.

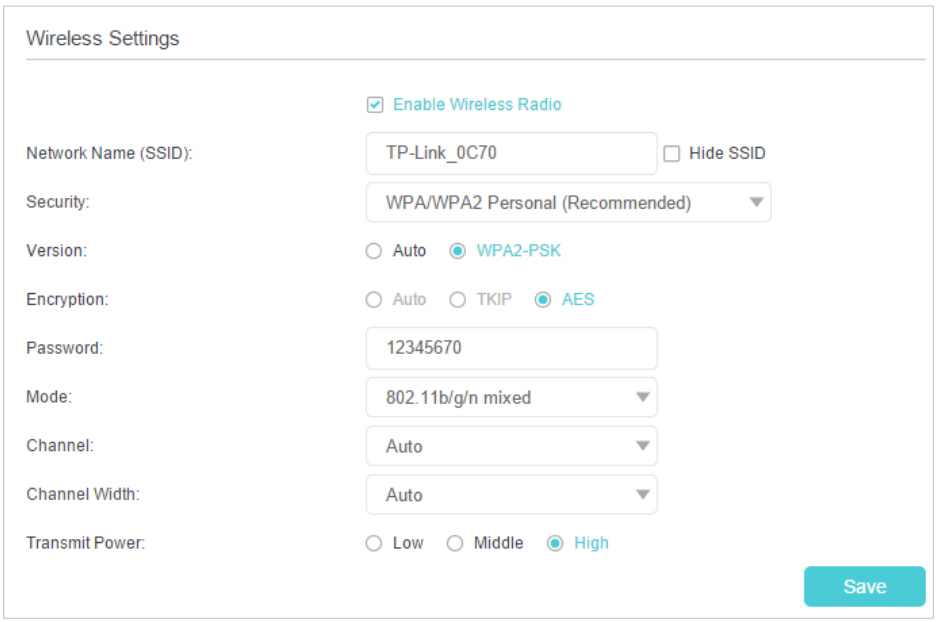
4) Expand Services and Applications > Services, find and locate Wireless Zero Configuration in the Services list on the right side.

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 Advanced > Wireless > Wireless Settings, and check the wireless settings. Double check your Wireless Network Name and SSID is not hidden.



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 1, 6 or 11 to reduce interference from other networks.
  - Re-install or update the driver for your wireless adapter of the computer.

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. tp-link is a registered trademark of TP-Link Technologies Co., Ltd. Other brands and product names are trademarks or registered trademarks of their respective holders.

FCC STATEMENT

Product Name: 300Mbps Wireless N Router

Model Number: TL-WR850N

Component Name	Model
I.T.E POWER SUPPLY	AMS195-0900600FU

Responsible party:

TP-Link USA Corporation, d/b/a TP-Link North America, Inc.

Address: 145 South State College Blvd. Suite 400, Brea, CA 92821

Website: http://www.tp-link.com/us/

Tel: +1 626 333 0234

Fax: +1 909 527 6803

E-mail: sales.usa@tp-link.com

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

"To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

The device is restricted in indoor environment only.

We, **TP-Link USA Corporatio**n, has determined that the equipment shown as above has been shown to comply with the applicable technical standards, FCC part 15. There is no unauthorized change is made in the equipment and the equipment is properly maintained and operated.

Issue Date: 2019.03.08

FCC compliance information statement

Product Name: I.T.E POWER SUPPLY

Model Number: AMS195-0900600FU

Responsible party:

TP-Link USA Corporation, d/b/a TP-Link North America, Inc.

Address: 145 South State College Blvd. Suite 400, Brea, CA 92821

Website: http://www.tp-link.com/us/

Tel: +1 626 333 0234

Fax: +1 909 527 6803

E-mail: sales.usa@tp-link.com

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency

energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

We, **TP-Link USA Corporation**, has determined that the equipment shown as above has been shown to comply with the applicable technical standards, FCC part 15. There is no unauthorized change is made in the equipment and the equipment is properly maintained and operated.

Issue Date: 2019.03.08

CE Mark Warning

CE

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

OPERATING FREQUENCY(the maximum transmitted power)

2400 MHz - 2483.5 MHz (20dBm)

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 and 2011/65/EU.

The original EU declaration of conformity may be found at http://www.tp-link.com/en/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 used at 20 cm from your body.

Canadian Compliance Statement

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. l'appareil ne doit pas produire de brouillage;
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, meme si le brouillage est susceptible d'en compromettre le fonctionnement

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Industry Canada Statement

CAN ICES-3 (B)/NMB-3(B)

Korea Warning Statements:

당해 무선설비는 운용중 전파혼신 가능성이 있음.

NCC Notice:

注意！

依據 低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，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或功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通行；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。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機需忍受合法通信或工業、科學以及醫療用電波輻射性電機設備之干擾。

BSMI Notice

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。
- 請不要私自打開機殼，不要嘗試自行維修本產品，請由授權的專業人士進行此項工作。

限用物質含有情況標示聲明書

產品元件名稱	限用物質及其化學符號					
	鉛 Pb	鎘 Cd	汞 Hg	六價鉻 CrVI	多溴聯苯 PBB	多溴二苯醚 PBDE
PCB	○	○	○	○	○	○
外殼	○	○	○	○	○	○
電源適配器	–	○	○	○	○	○

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

備考2. “○” 系指該項限用物質之百分比含量未超出百分比含量基準值。

備考3. “ – “ 系指該項限用物質為排除項目。

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

EAC

Safety Information

- Keep the device away from water, fire, humidity or hot environments.
- Do not attempt to disassemble, repair, or modify the device.
- 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.

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.

Explanations of the symbols on the product label

Symbol	Explanation
⎓	DC voltage
	Indoor use only
	RECYCLING 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. 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.