Portable 3G/4G Wireless N Router

Pocket-sized for
Travel-Ready Wi-Fi

TL-MR3020

3G/4G Sharing | 300Mbps Wireless Speed | Multi-Mode

Highlights

Share internet from anywhere you have a 3G or 4G mobile connection

Compatible with iOS/Android smartphones, tablets, Windows/Mac laptops and other Wi-Fi enable devices.

3G/4G modem

(Connect to internet through a 3G or 4G modem*)

* Compatible with LTE/HSPA+/HSUPA/HSDPA/UMTS/EVDO modem

Quick Mode Selection

Select an operation mode to best fit your internet need.

Mode Selection

3G/4G Router Mode

WISP Client Router Mode

AP Mode

Features

Reliability

- Wireless N Speed – 300Mbps Wi-Fi speed meets your daily internet needs
- 802.11n – Backward compatible with 802.11b/g products
- Easy Bandwidth Management– Bandwidth Control allocates necessary speed of each connected device to ensure quality of multimedia streaming

Ease of Use

- Intuitive Web UI – Ensures quick and simple Installation without hassle
- Fast Encryption – One-touch WPA wireless security encryption with the WPS button

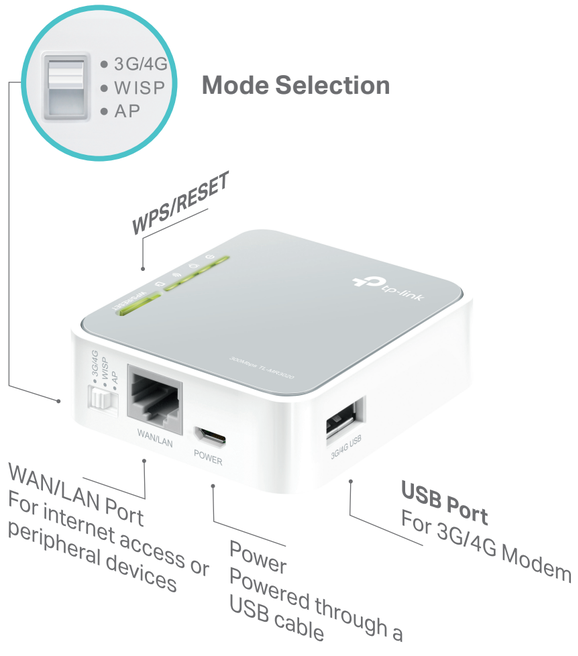
Security

- Guest Network – Keeps your main network secure by creating a separate network for friends and visitors
- Access Control – Establishes a whitelist or blacklist to allow or restrict certain devices to access the internet
- Parental Controls – Restricts internet access time and contents for children devices
- Encryptions for Secure Network – WPA-PSK and WPA2-PSK encryptions provide active protection against security threats

Specifications

Hardware

- Ports: 1 10/100Mbps WAN/LAN Port, 1 USB 2.0 Port, 1 Micro USB Port
- Buttons: WPS/Reset Button, Mode Switch
- Antennas: Internal Antennas
- External Power Supply: 5VDC/1A
- Dimensions (W x D x H): 2.9× 2.6×0.9 in. (74×67×22mm)



Wireless

- Wireless Standards: IEEE 802.11b/g/n
- Frequency: 2.4GHz
- Signal Rate: 300Mbps
- Transmit Power: < 20dBm
- Reception Sensitivity:

  2.4GHz:

  270M: -70dBm@10% PER

  130M: -73dBm@10% PER

  108M: -74dBm@10% PER

  54M: -75dBm@10% PER

  11M: -86dBm@8% PER

  6M: -92dBm@10% PER

  1M: -95dBm@8% PER
- Wireless Function: Enable/Disable Wireless Radio, WMM, Wireless Statistics
- Wireless Security: 64/128-bit WEP, WPA/WPA2, WPA-PSK/WPA2-PSK encryptions

Specifications

Software

- Quality of Service: WMM, Bandwidth Control
- WAN Type: Dynamic IP/Static IP/PPPoE/PPTP(Dual Access)/L2TP(Dual Access)
- Management: Access Control, Local Management, Remote Management
- DHCP: Server, DHCP Client List, Address Reservation
- Port Forwarding: Virtual Server, Port Triggering, UPnP, DMZ
- Dynamic DNS: DynDns, NO-IP
- Access Control: Parental Controls, Local Management Control, Host List, White List, Black List
- Firewall Security: DoS, SPI Firewall, IP and MAC Address Binding
- Protocols: IPv4, IPv6
- Guest Network: 2.4GHz guest network

Others

- Certification:

  CE, RoHS
- System Requirements:

  Microsoft Windows 98SE/NT/2000/XP/Vista™/7/8/8.1/10, MAC OS, NetWare, UNIX or Linux

  Internet Explorer 11, Firefox 12.0, Chrome 20.0, Safari 4.0, or other Java-enabled browser
- Environment:

  Operating Temperature: 0℃~40℃ (32℉ ~104℉)

  Storage Temperature: -40℃~70℃ (-40℉ ~158℉)

  Operating Humidity: 10%~90% non-condensing

  Storage Humidity: 5%~90% non-condensing
- Package Contents

  3G/4G Portable Wireless N Router TL-MR3020

  Ethernet Cable

  USB Cable

  Quick Installation Guide

For more information, please visit
http://www.tp-link.com/en/products/details/TL-MR3020.html
or scan the QR code left

User Guide

Portable 3G/4G Wireless N Router
TL-MR3020

REV3.0.0 1910012156

Contents

About This Guide

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

When using this guide, please notice that features of the router may vary slightly depending on the model and software version you have, and on your location, language, and internet service provider. All screenshots, 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	Underlined words or phrases are hyperlinks. You can click to redirect to a website or a specific section.
Teal	Contents to be emphasized and texts on the web page are in teal, including the menus, items, buttons, etc.
>	The menu structures to show the path to load the corresponding page. For example, Advanced > Wireless > MAC Filtering means the MAC Filtering 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 software, management app and utility can be found at Download Center at http://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 http://www.tp-link.com/support.

Chapter 1

Get to Know About Your Router

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

It contains the following sections:

1. 1. Product Overview

To meet the wireless needs of almost any situation you might encounter, the TP-Link portable router, with multiple operation modes, is designed for home and travel use. The portable size of the router means that you can put it in your pocket and take it with you wherever you go.

1. 2. Appearance

LED Explanation

LED	Status	Indication
(Power)	On	The router is on.
	Off	The router is off.
(Internet)	On	The internet is available.
	Off	The internet is unavailable.
(Wireless)	On	The wireless network is enabled.
	Off	The wireless network is disabled.
(WAN/LAN)	On	The Ethernet port is connected.
	Off	The Ethernet port is not connected.

LED	Status	Indication
WPS/RESET	On	WPS connection has been established.
	Flashing	WPS connection is being established.
	Off	No WPS connection is established.

Port and Button Description

Item	Description
Mode Switch	This switch is used to determine the operation mode of the router.
WAN/LAN Port	LAN: 3G/4G (3G/4G Router), WISP, Access Point, Repeater/Bridge
	WAN: 3G/4G (3G/4G Router Mode With Ewan Backup, Wireless Router Mode, Wireless Router Mode With 3G/4G Backup)
Power Port	This port is used to connect to the power adapter.
WPS/RESET Button	To establish WPS connection, press the WPS button on your device and then press the WPS/RESET button on this router.
	To reset the router, press and hold this button until all the LEDs turn on and then release it.
3G/4G USB Port	This port is used to plug a 3G/4G USB modem into.

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 product away from the devices with strong electromagnetic interference, such as Bluetooth devices, cordless phones and microwaves.

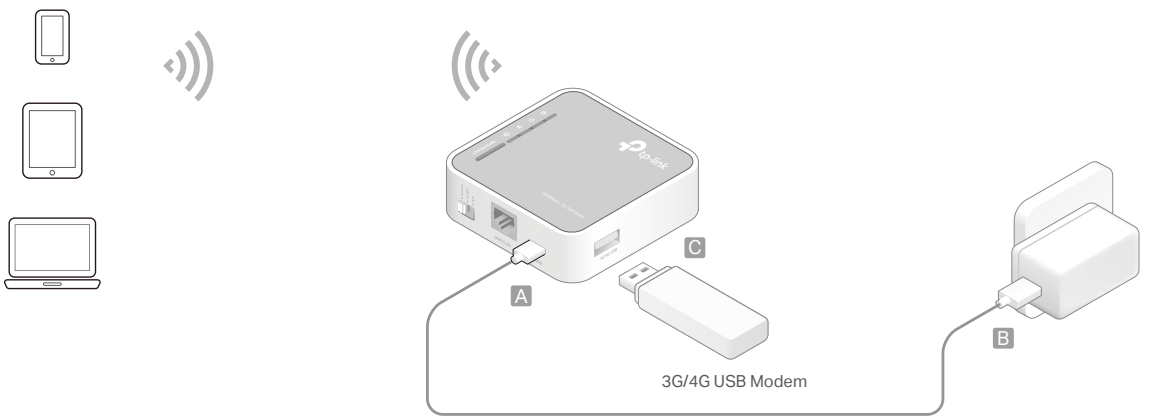
2. 2. Connect Your Router

There are five operation modes supported by this router: 3G/4G Router, Wireless Router, WISP Router, Access Point, and Repeater/Bridge. Please determine which operation mode you need and carry out the corresponding steps.

2. 2. 1. 3G/4G Router Mode

Create a private wireless network instantly and share the 3G/4G network with local devices.

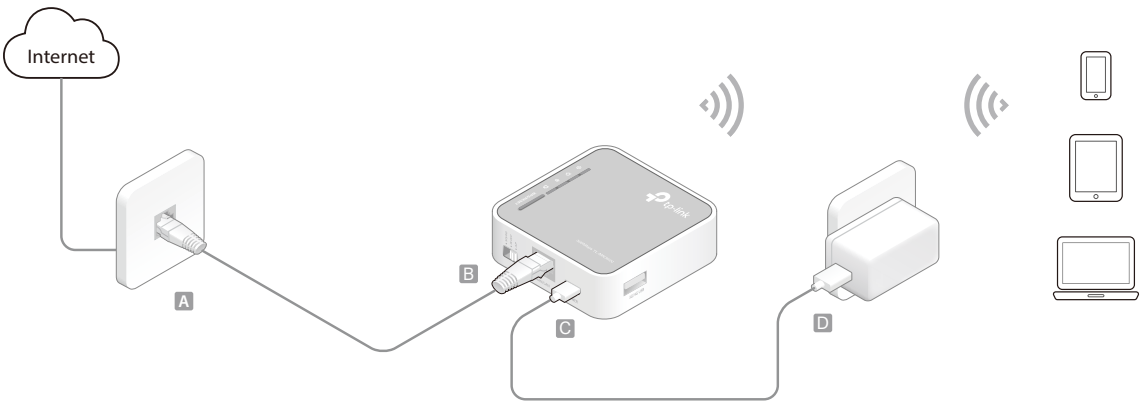
1. Switch the operation mode to 3G/4G and connect the hardware according to Step A to C.
2. Connect your device to the router wirelessly. The SSID (wireless network name) and password are on the router's label.



2. 2. 2. Wireless Router Mode

In Wireless Router Mode, the router shares internet access with multiple wireless devices.

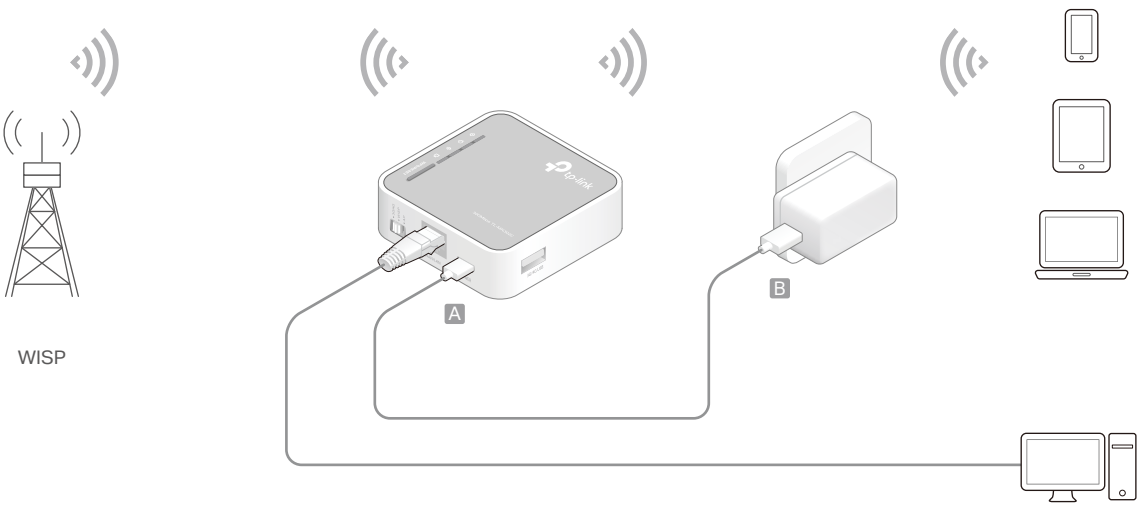
1. Switch the operation mode to 3G/4G and connect the hardware according to Step A to D.
2. Connect your device to the router wirelessly. The SSID (wireless network name) and password are on the router's label.



2. 2. 3. WISP Client Router Mode

In WISP Client Router mode, the router enables multiple users to share internet connection from WISP.

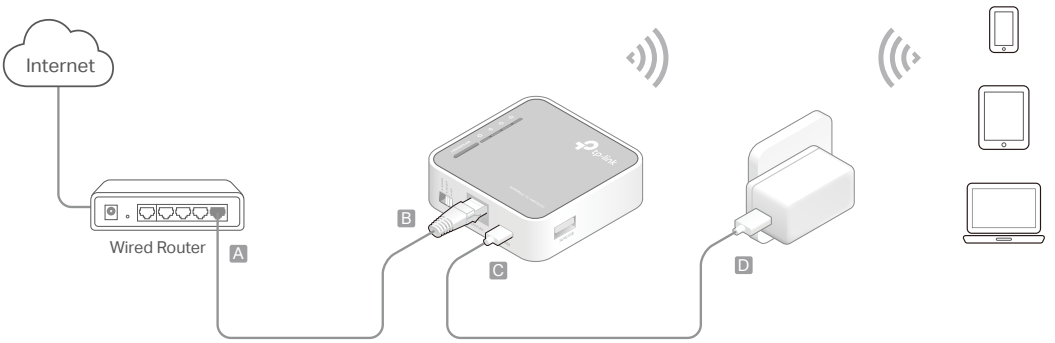
1. Switch the operation mode to WISP and connect the hardware according to Step A and B.
2. Connect your device to the router wirelessly or via an Ethernet cable. The SSID (wireless network name) and password are on the router's label.



2. 2. 4. Access Point Mode

Create a wireless network from an Ethernet connection. This mode is suitable for dorm rooms or homes where there's already a wired router but you need a wireless connection.

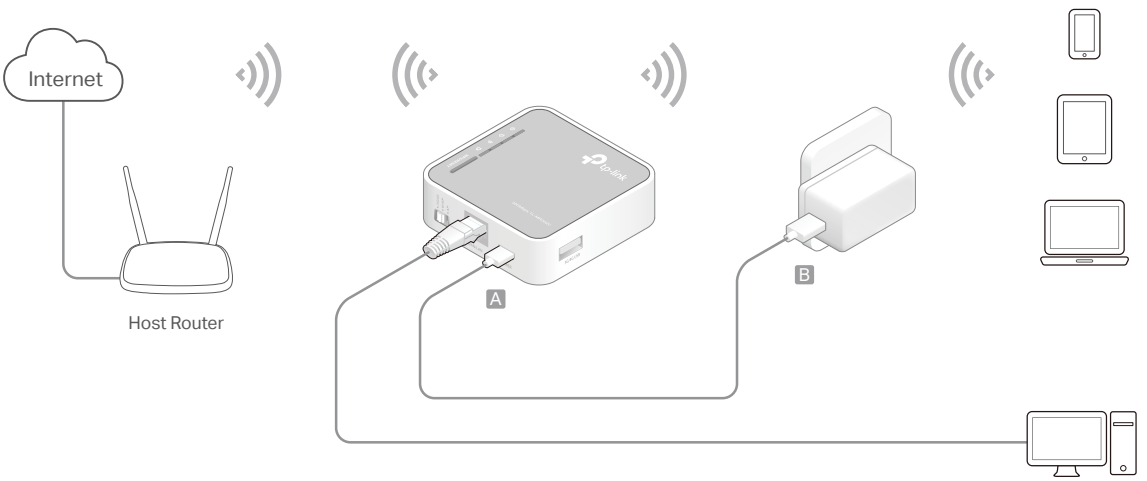
1. Switch the operation mode to AP and connect the hardware according to Step A to D.
2. Connect your device to the router wirelessly. The SSID (wireless network name) and password are on the router's label.



2. 2. 5. Repeater/Bridge Mode

Repeat signal from an existing wireless network. This mode is suitable to extend wireless coverage, reaching devices that were previously too far from your host router to maintain stable wireless connection.

1. Switch the operation mode to AP and connect the hardware according to Step A and B.
2. Connect your device to the router wirelessly or via an Ethernet cable. The SSID (wireless network name) and password are on the router's label.



Chapter 3

Set Up Internet Connection Via Quick Setup Wizard

This chapter introduces how to connect your router to the internet via the web-based Quick Setup Wizard.

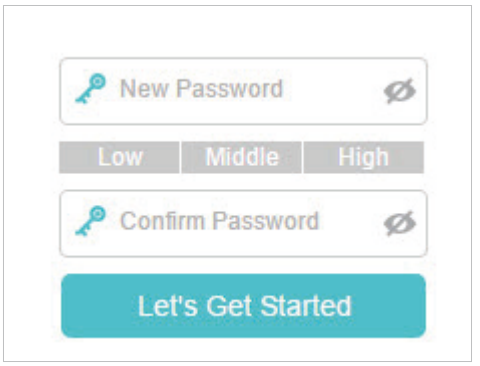
It contains the following sections:

3. 1. Log In to the Router

With the 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 into 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 password for future logins.



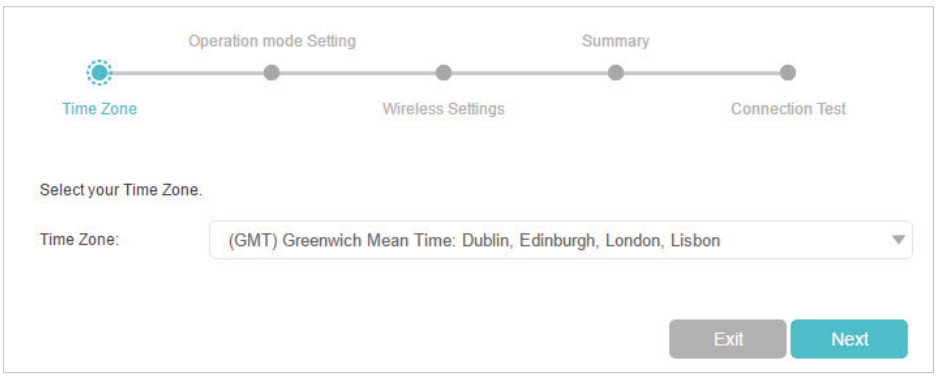
Note: If the login window does not appear, please refer to the FAQ section.

3. 2. Configure the Router

The Quick Setup Wizard will walk you through the process to set up your router.

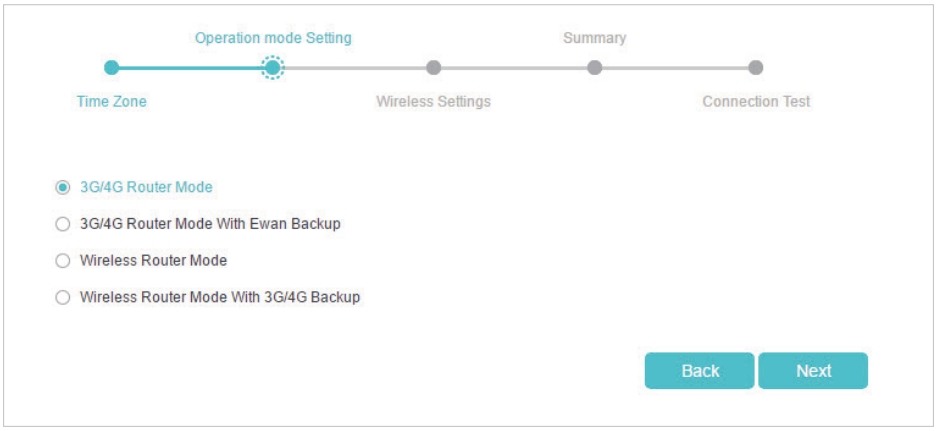
3. 2. 1. 3G/4G Router Mode

1. Select your Time Zone and click Next.

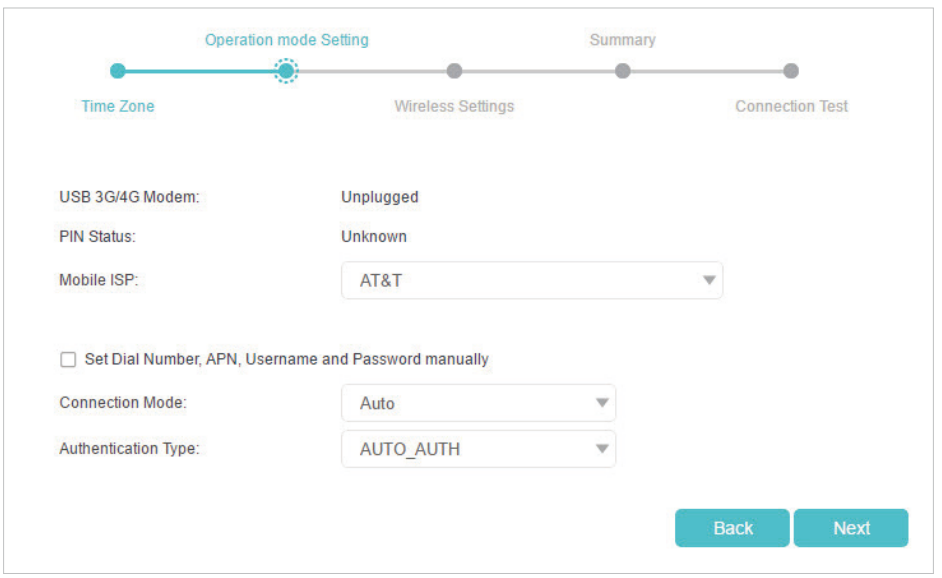


2. Select 3G/4G Router Mode and click Next.

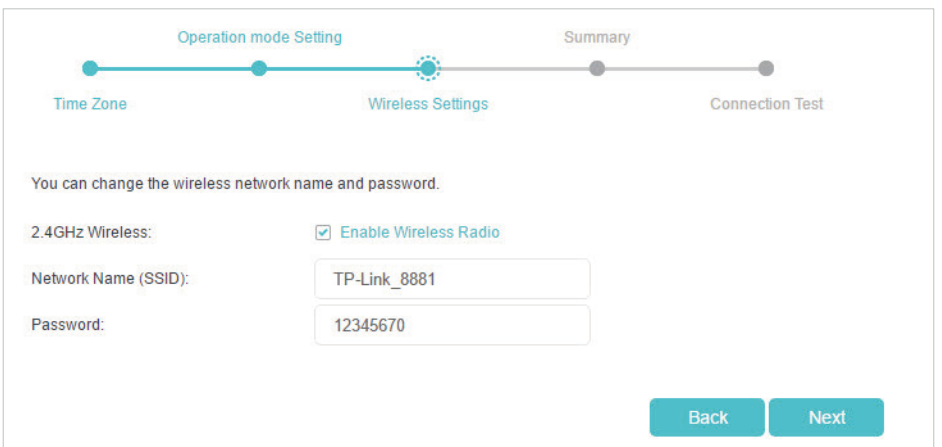
Note: The router can be configured with a primary 3G/4G connection and WAN connection as a backup solution to ensure "always-on" internet connectivity.



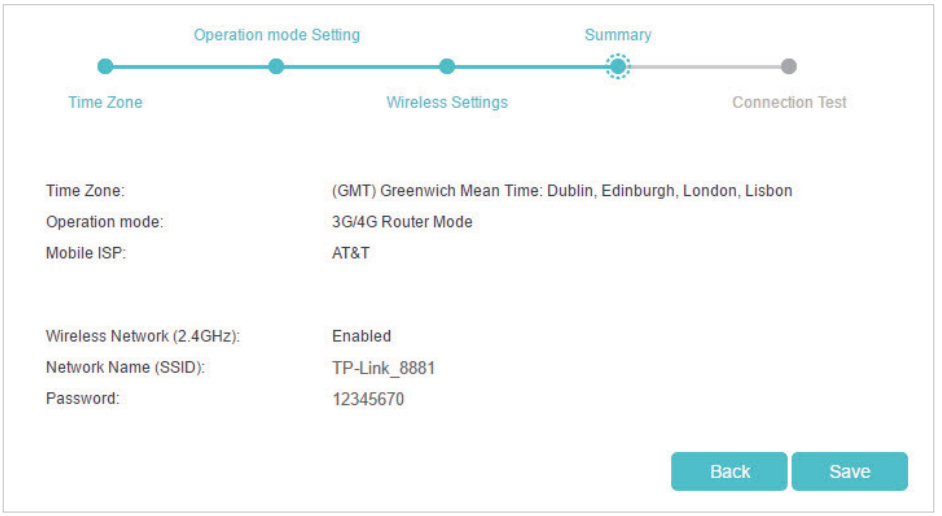
3. Select your Mobile ISP or manually set them if your ISP is not listed. Then click Next.



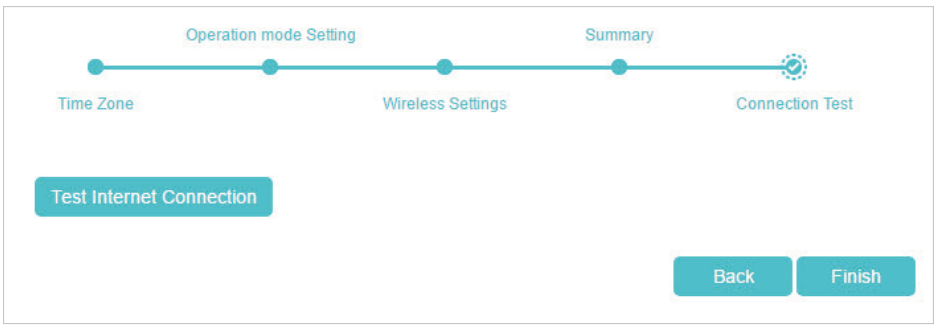
4. Either customize your Network Name (SSID) and Password or keep the default ones, and then click Next.



5. Check the wireless settings and click Save.

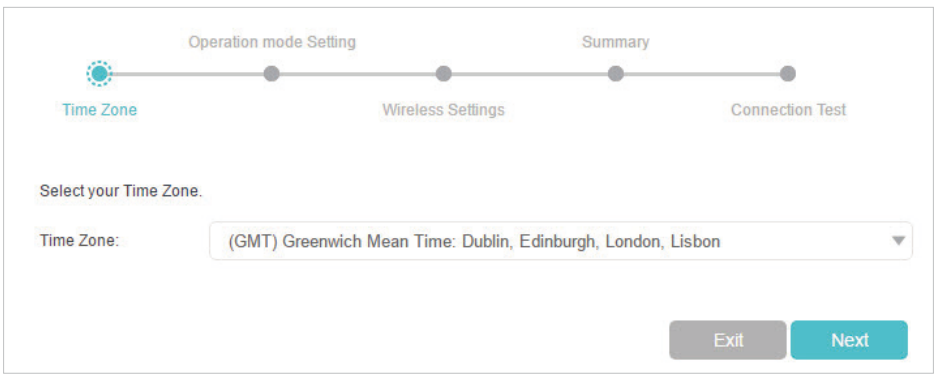


6. Click Finish to complete the configuration. Now connect your devices to the internet!



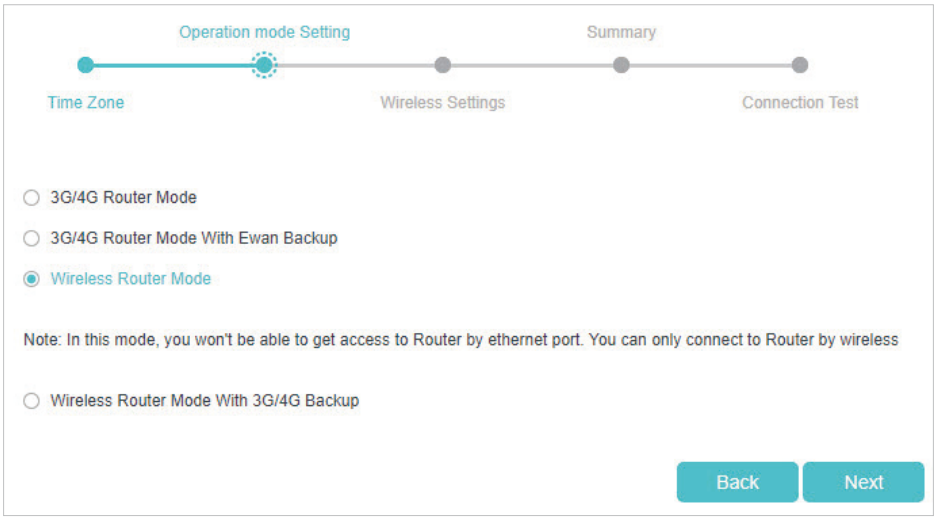
3. 2. 2. Wireless Router Mode

1. Select your Time Zone and click Next.

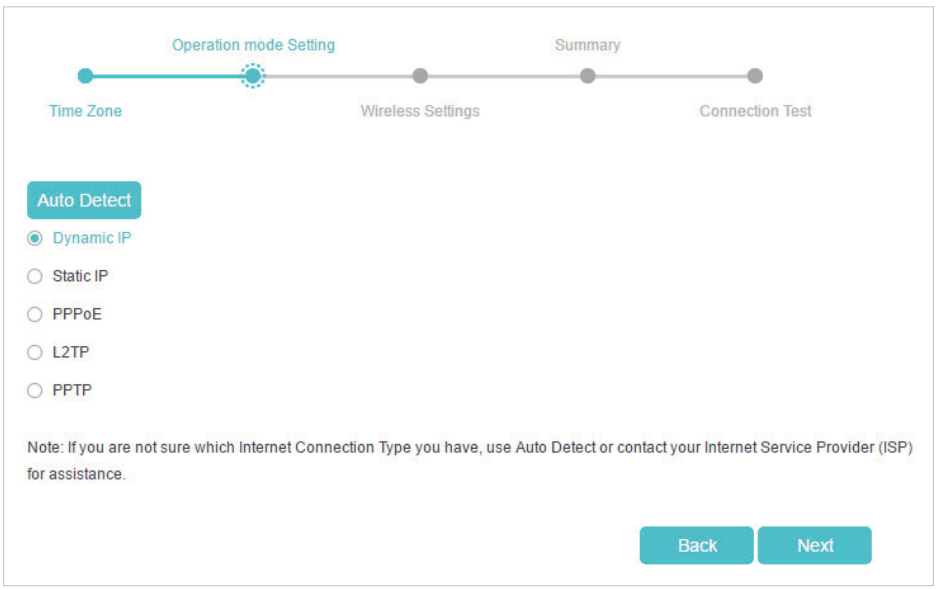


2. Select Wireless Router Mode and click Next.

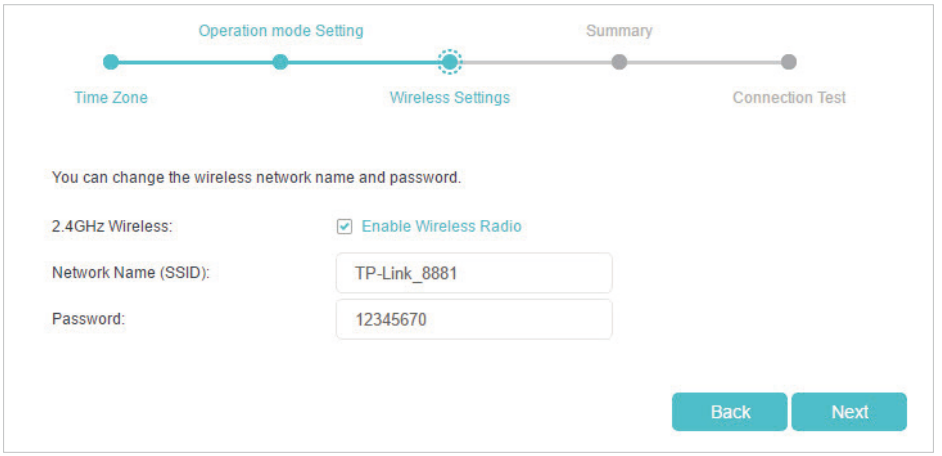
Note: The router can be configured with a primary WAN connection and a 3G/4G USB modem as a backup solution to ensure "always-on" internet connectivity.



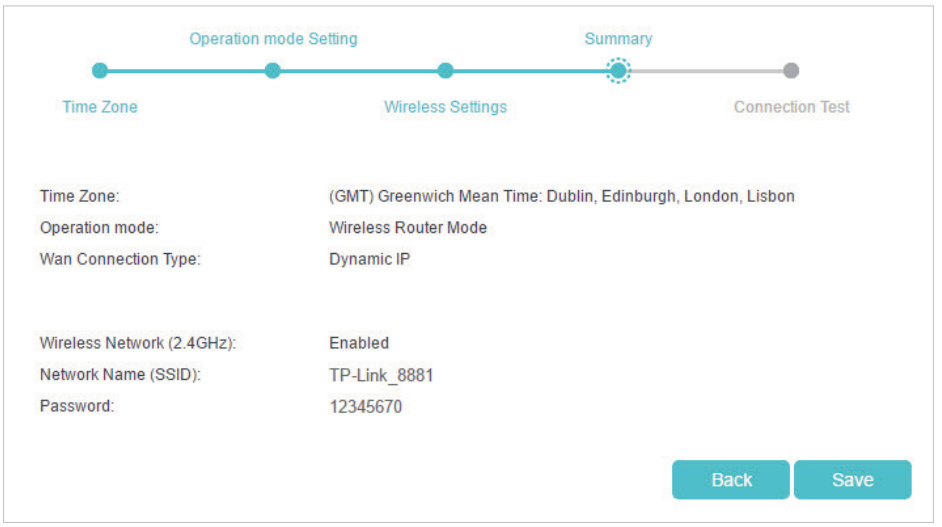
3. Select Internet Connection Type and enter corresponding parameters. If you are not sure, click Auto Detect. Then click Next and enter corresponding parameters.



4. Either customize your Network Name (SSID) and Password or keep the default ones, and then click Next.

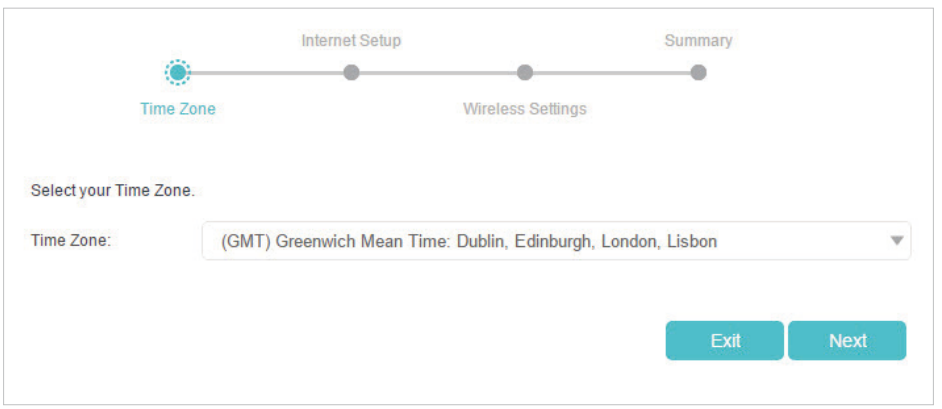


5. Check the wireless settings and click Save.

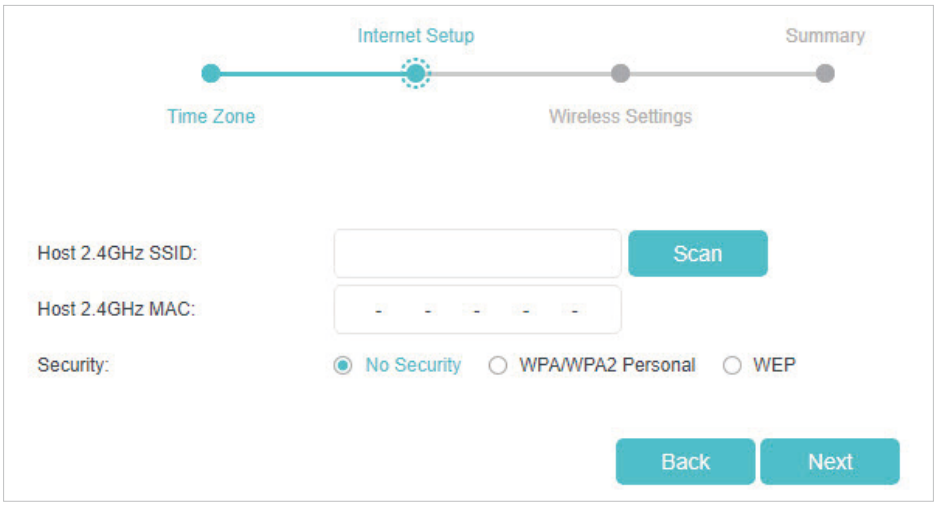


3. 2. 3. WISP Client Router Mode

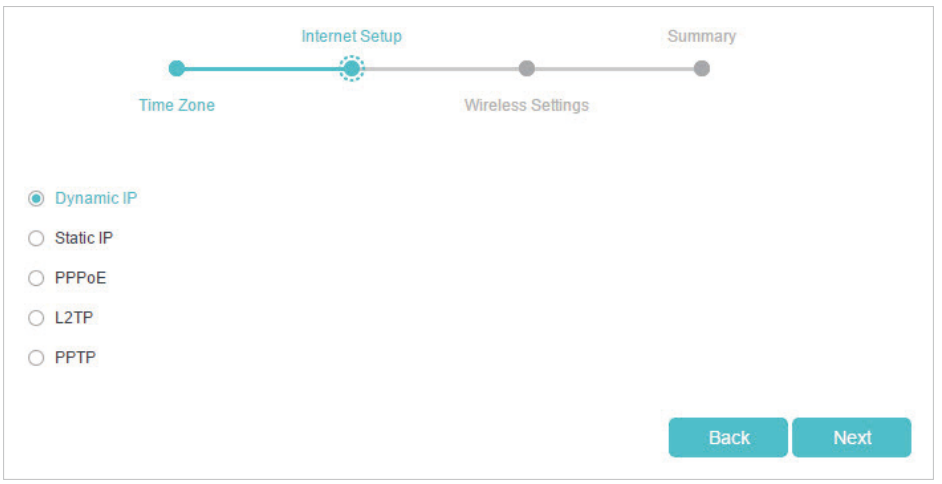
1. Select your Time Zone and click Next.



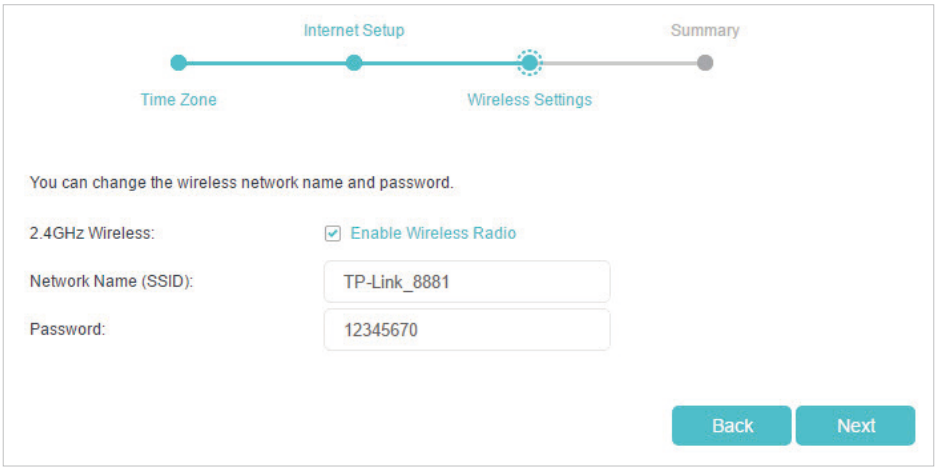
2. Click Scan to find the corresponding network of your WISP. Enter the Password for the selected wireless network if it is encrypted. Then click Next.



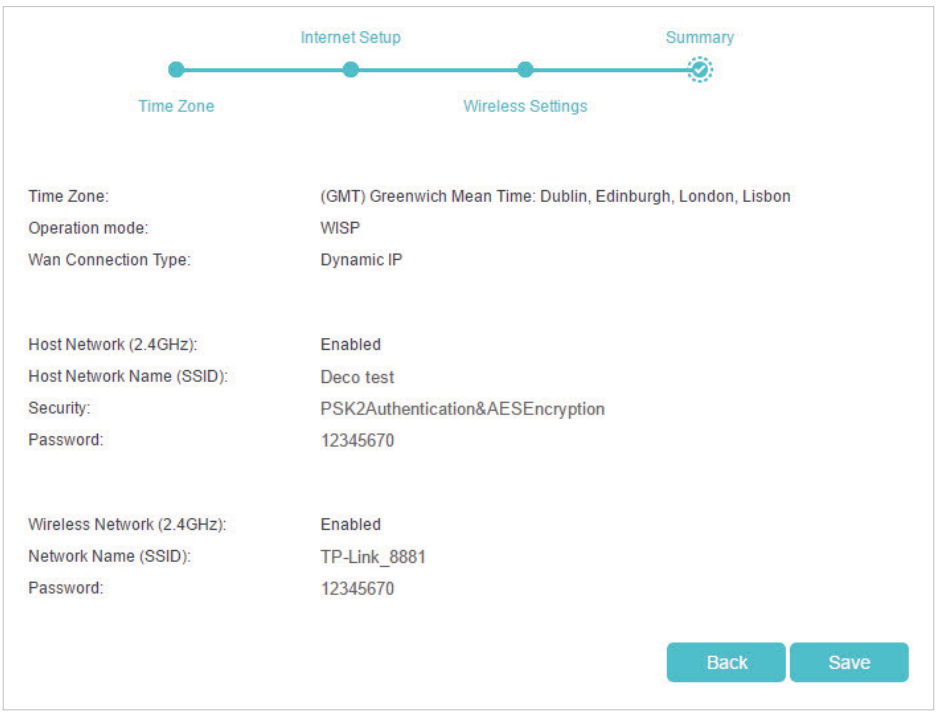
3. Select Internet Connection Type. Then click Next and enter corresponding parameters.



4. Either customize your Network Name (SSID) and Password or keep the default ones, and then click Next.

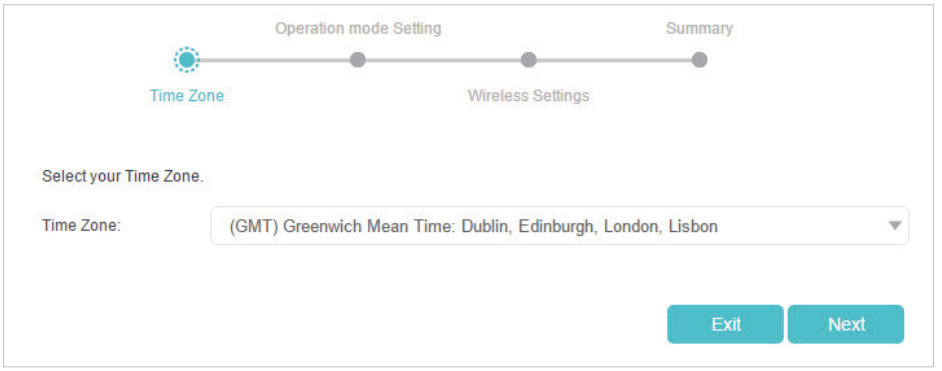


5. Click Save to complete the configuration.

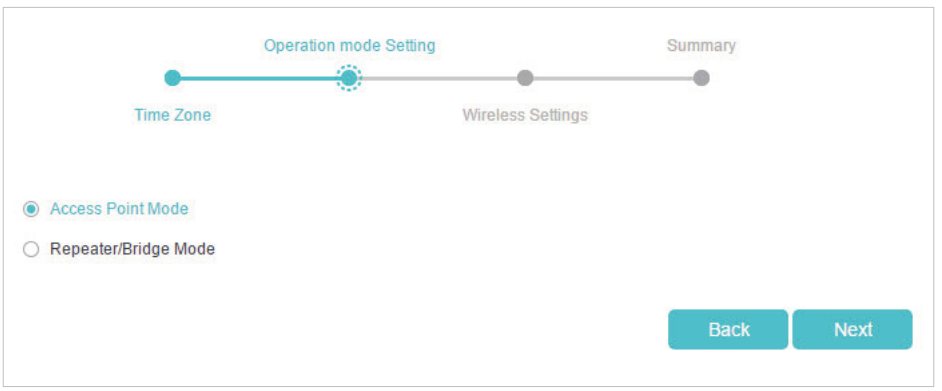


3. 2. 4. Access Point Mode

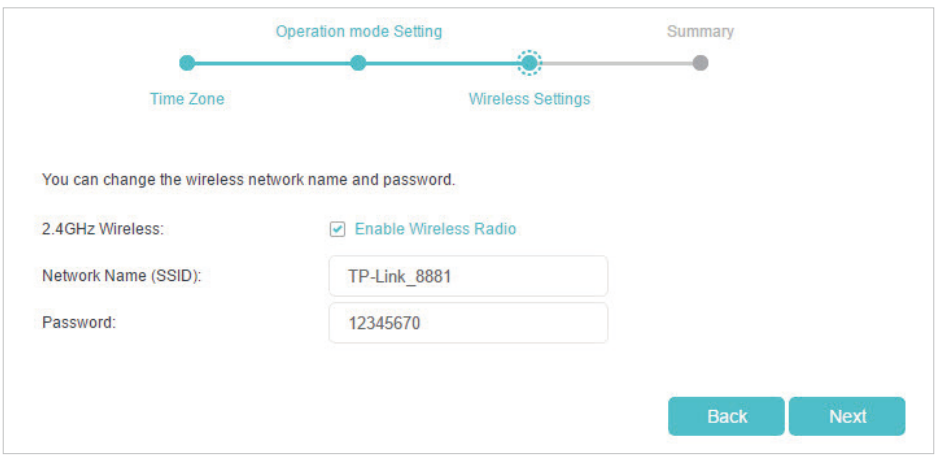
1. Select your Time Zone and click Next.



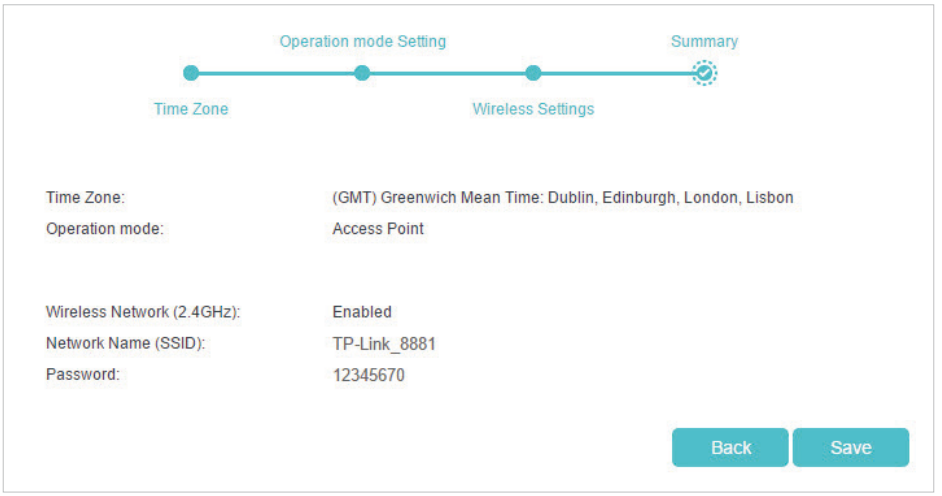
2. Select Access Point Mode and click Next.



3. Either customize your Network Name (SSID) and Password or keep the default ones, and then click Next.

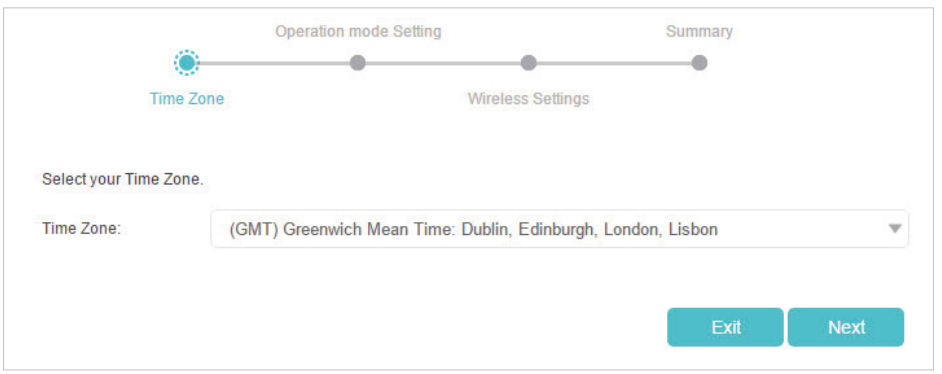


4. Click Save to complete the configuration.



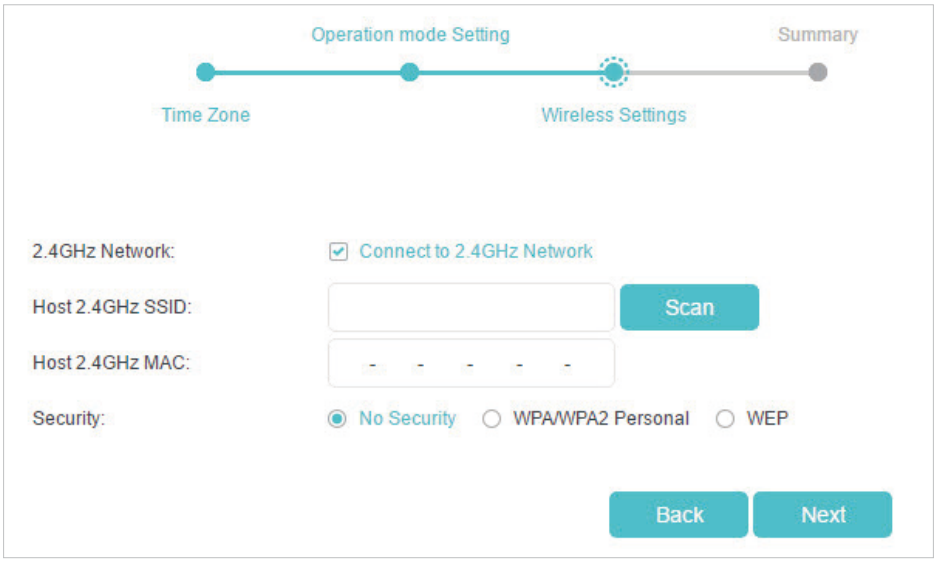
3. 2. 5. Repeater/Bridge Mode

1. Select your Time Zone and click Next.

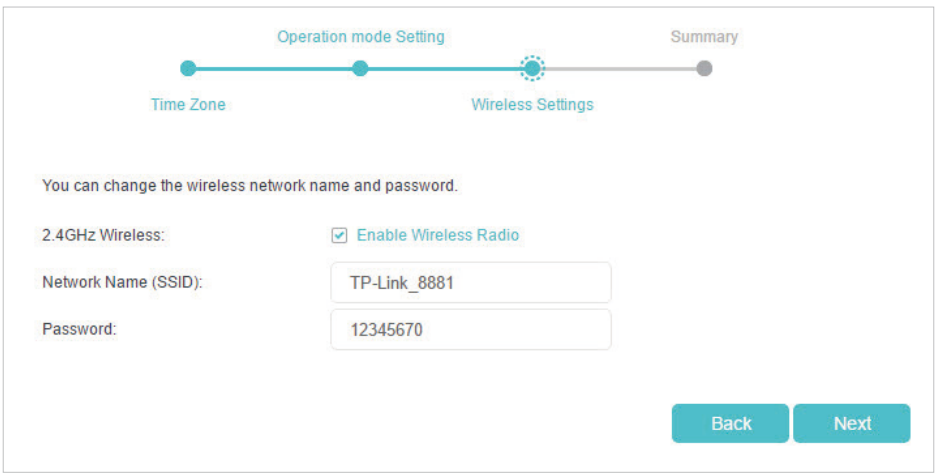


2. Select Repeater/Bridge Mode and click Next.

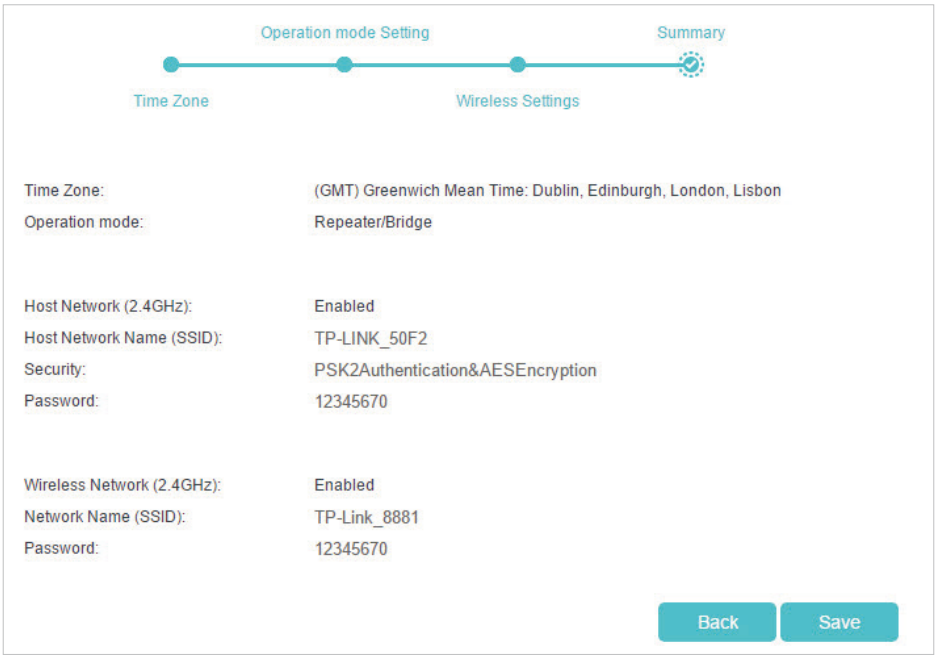
3. Click Scan to find the network you want to extend. Enter the Password for the selected wireless network if it is encrypted. Then click Next.



4. Either customize your Network Name (SSID) and Password or keep the default ones, and then click Next.



5. Click Save to complete the configuration.



6. Relocate the router about halfway between your host router and the Wi-Fi dead zone.

Chapter 4

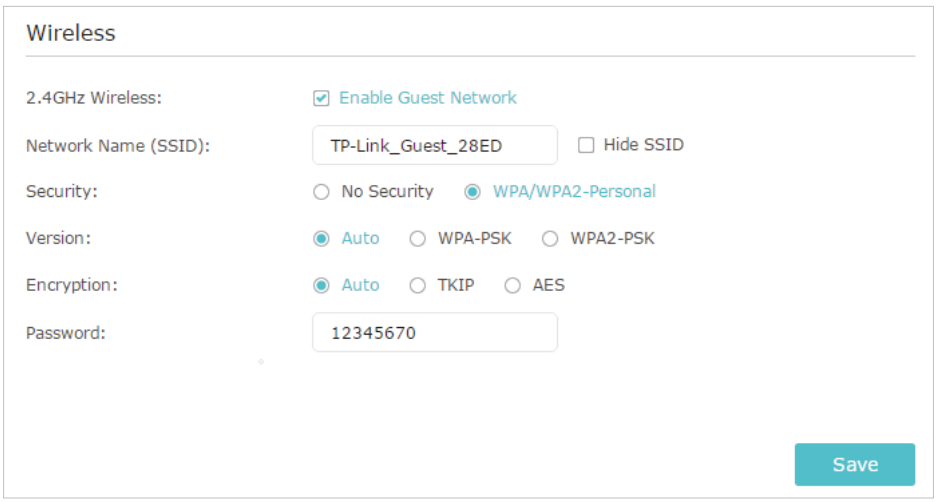
Guest Network

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

It contains the following sections:

4. 1. Create a Network for Guests

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Guest Network. Locate the Wireless section.
3. Create a guest network as needed.
   1) Tick the Enable Guest Network checkbox.
   2) Customize the SSID. Don't select Hide SSID unless you want your guests to manually input the SSID for guest network access.
   3) Set Security to WPA/WPA2 Personal, keep the default Version and Encryption values, and customize your own password.

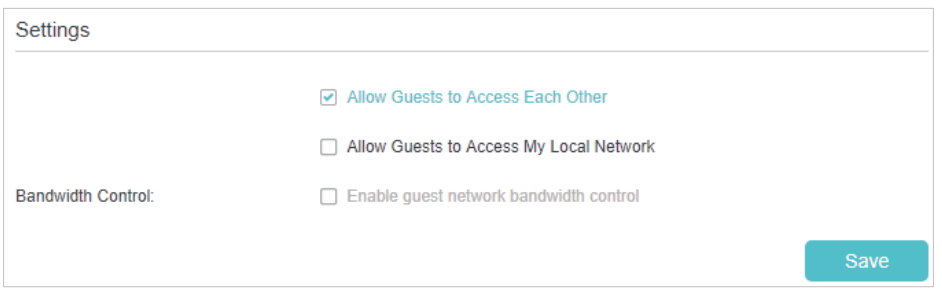


4. Click Save. Now your guests can access your guest network using the SSID and password you set!

Tips: To view guest network information, go to Advanced > Status and locate the Guest Network section.

4. 2. Customize Guest Network Options

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Guest Network. Locate the Settings section.
3. Customize guest network options as needed.



- Allow Guests to Access Each Other

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

- Allow Guests to Access My Local Network (in Router mode)

Tick this checkbox if you want to allow the wireless clients on your guest network to communicate with the devices connected to your router's LAN ports or main network via methods such as network neighbors and Ping.

- Enable guest network bandwidth control

Tick this checkbox if you want to apply the Bandwidth Control settings to the wireless devices on your guest network .

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

Tips: To view guest network information, go to Advanced > Status and locate the Guest Network section.

Chapter 5

Parental Controls

This function allows you to block inappropriate, explicit and malicious websites, and control access to specified websites at specified time. Parental Controls are only supported by the Router mode.

I want to:

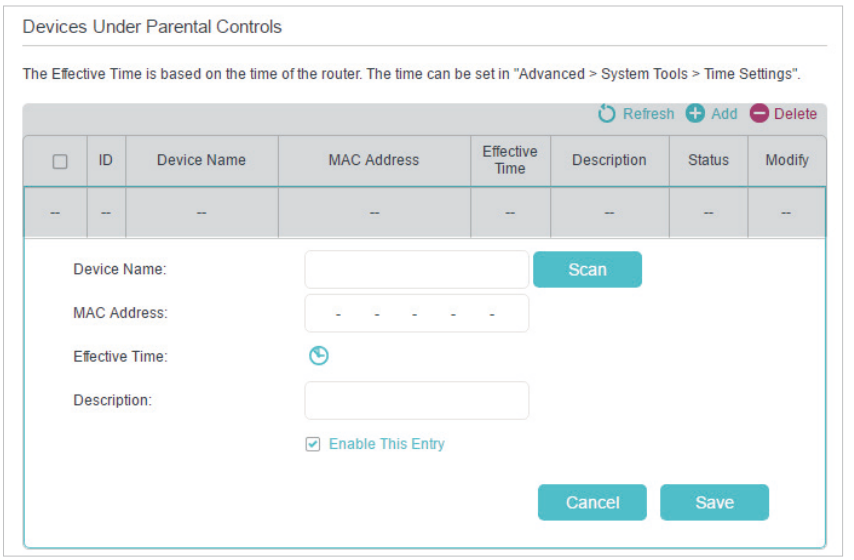
Control the times of day my children or other home network users are allowed to access the Internet and even types of websites they can visit.

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 (6PM) to 22:00 (10PM) at the weekend and not other times.

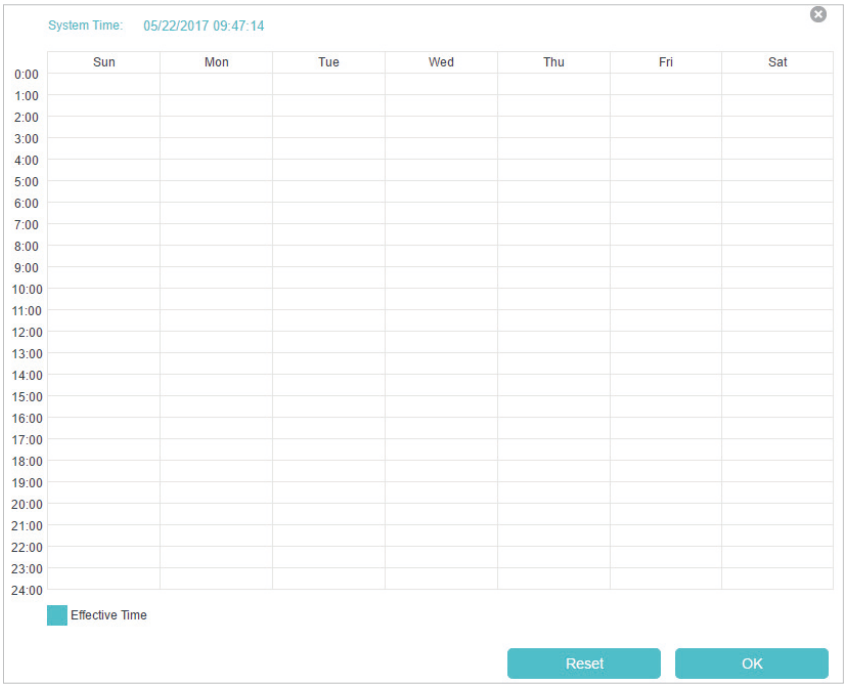
How can I do that?

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

3. Click Add. And then Click Scan, and select the access device. Or, input the Device Name and MAC Address manually.

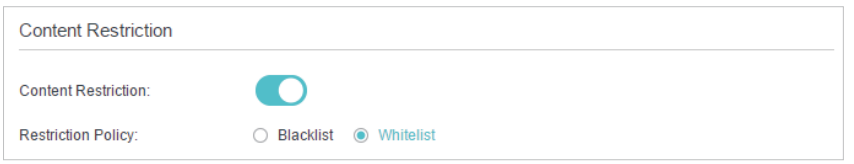


4. Click the icon to set the Internet Access Time. Drag the cursor over the appropriate cell(s) and click OK.



5. Enter a Description for the entry, tick the Enable This Entry checkbox, and then click OK.

6. Select Whitelist as the restriction policy.



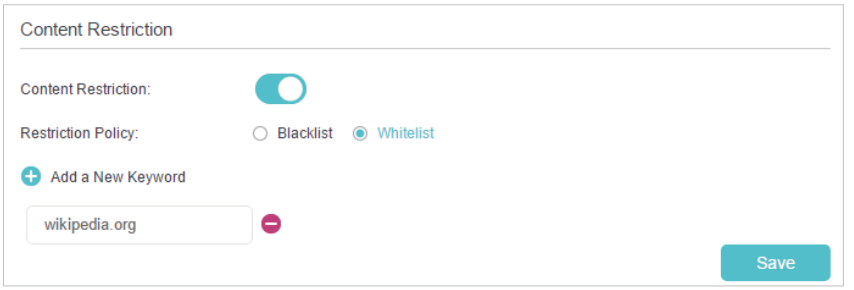
Tips:

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

7. Click Add a New Keyword. Enter a website and click Save.

   You can add up to 32 keywords for either Blacklist or Whitelist. Below are some sample entries to allow access.

   - 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 (eg. .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

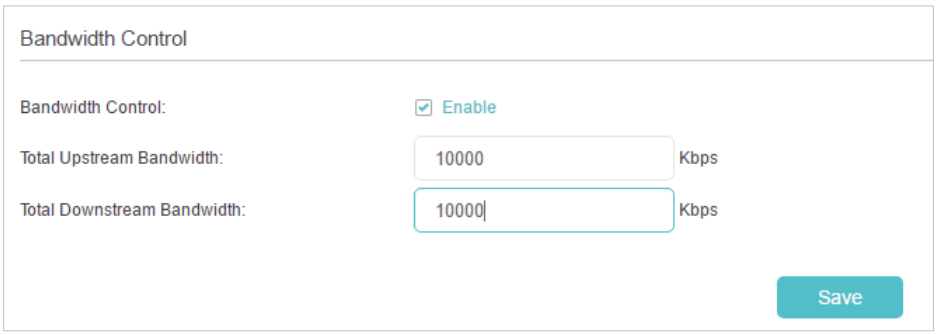
Bandwidth Control

This chapter introduces how to set bandwidth limits minimize the impact caused when the connection is under heavy load. Bandwidth Control is only supported by the Router mode.

It contains the following sections:

6. 1. Set Upstream and Downstream Bandwidth

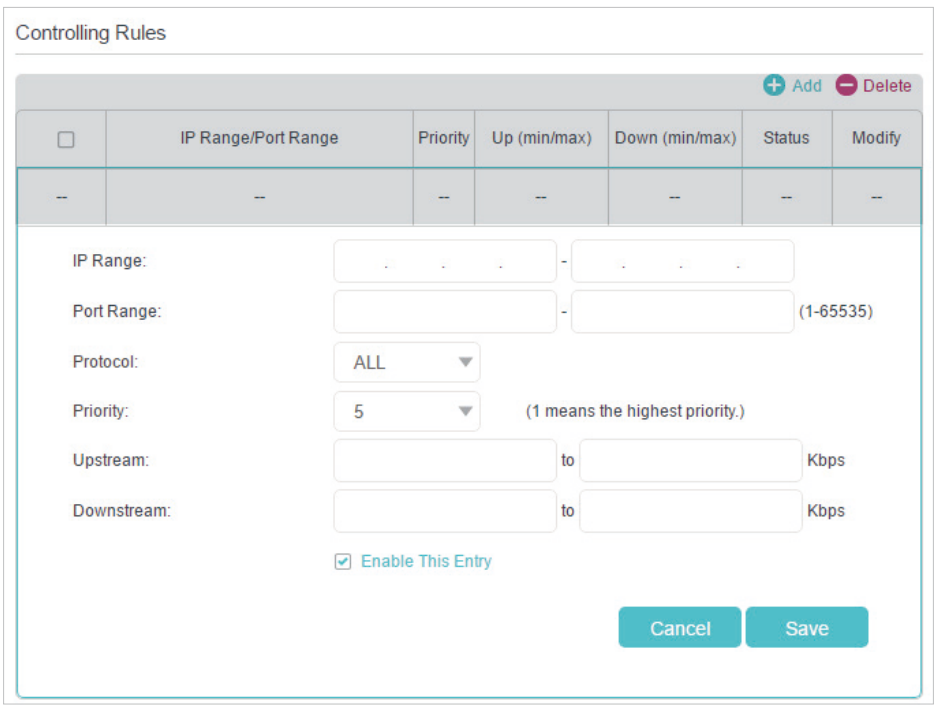
1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Bandwidth Control.
3. Enable Bandwidth Control and enter the Total Upstream Bandwidth and Total Downstream Bandwidth.



4. Click Save.

6. 2. Controlling Rules

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Bandwidth Control.
3. Click Add and fill in the blanks.



- IP Range: Enter the IP range of your devices that you want to apply Bandwidth Control to.
- Port Range: Enter the Port range of the protocols.
- Protocal: Select the protocols of services that you want to control.
- Priority: Select priority from 1 to 5. 1 means the highest priority.
- Upstream/Downstream: Enter the minimun and maxmium upstream/downstream bandwidth you want to allocate.

4. Click Save.

Chapter 7

Network Security

This chapter guides you on how to protect your home network from cyber attacks and unauthorized users by implementing these three network security functions. You can protect your home network against DoS (Denial of Service) attacks from flooding your network with server requests using DoS Protection, block or allow specific client devices to access your network using Access Control, or you can prevent ARP spoofing and ARP attacks using IP & MAC Binding. Some features are only supported by a certain mode.

It contains the following sections:

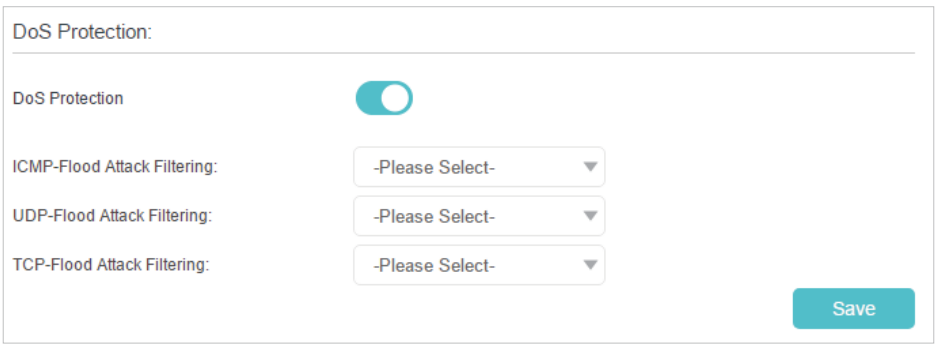
7. 1. Protect the Network from Cyber Attacks

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's recommended to keep the default settings.

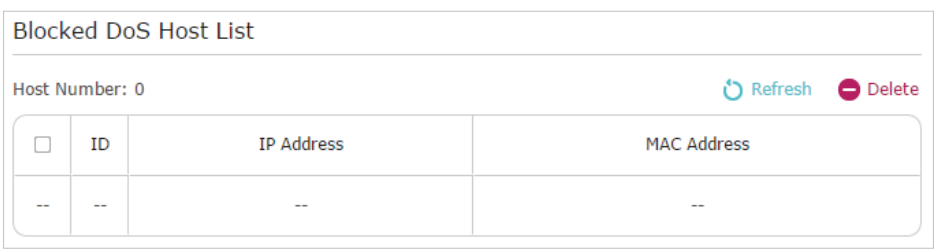
DoS Protection can protect your home network against DoS attacks from flooding your network with server requests. Follow the steps below to configure DoS Protection.

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 level (Low, Middle or High) of protection for ICMP-FLOOD Attack Filtering, UDP-FlOOD Attack Filtering and TCP-SYN-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-SYN-FLOOD Attack Filtering - Enable to prevent the TCP-SYN (Transmission Control Protocol-Synchronize) flood attack.

   Tips: The level of protection is based on the number of traffic packets. The protection will be triggered immediately when the number of packets exceeds the preset threshold value (the value can be set on DoS Protection Level Settings), and the vicious host will be displayed in the Blocked DoS Host List.



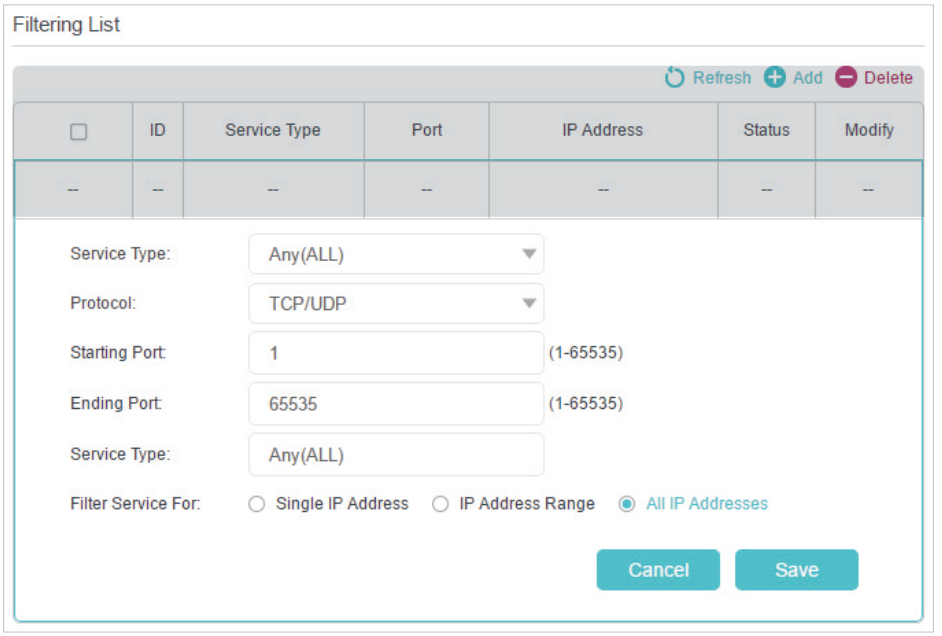
5. Click Save.

7. 2. Service Filtering

Service Filtering is used to prevent certain users from accessing a specific service. It can even block a user from accessing the internet.

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

4. Click Add.



5. Select a service type from the drop-down list and the corresponding parameters will be automatically filled in. Select Custom if your desired service type is not listed and enter the corresponding parameters.
6. Specify the IP address(es) this filtering rule will be applied to.
7. Click Save.

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).

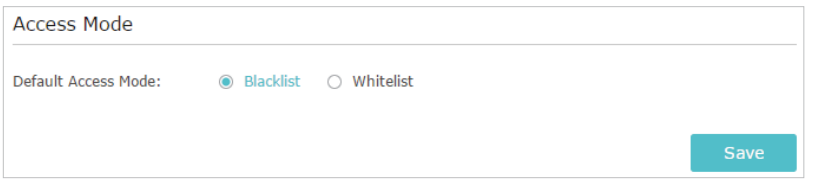
How can I do that?

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

4. Select the access mode to either block (recommended) or allow the device(s) in the list.

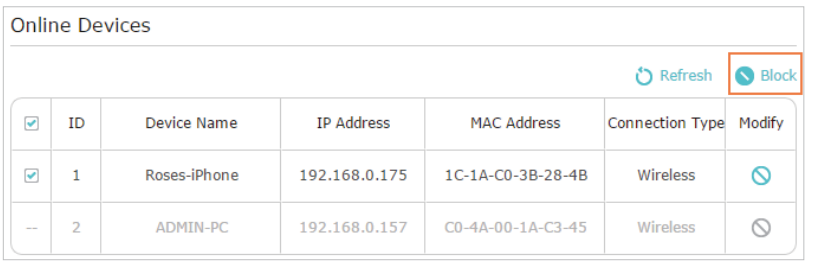
To block specific device(s):

1) Select Blacklist and click Save.



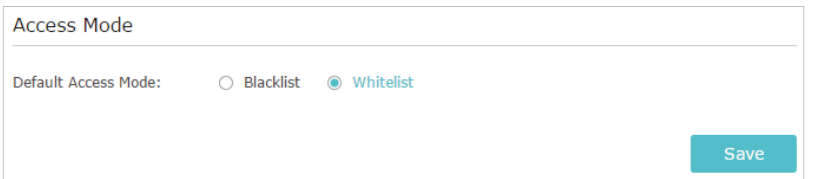
2) Select the device(s) to be blocked in the Online Devices table by ticking the checkbox(es).

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



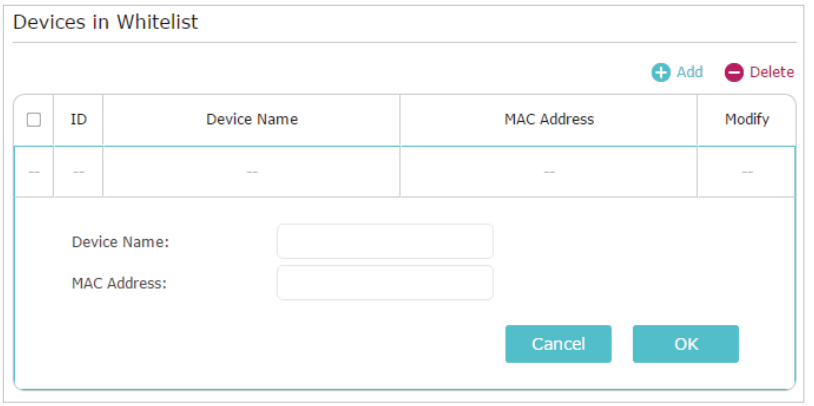
To allow specific device(s):

1) Select Whitelist and click Save.



2) Click Add in the Devices in Whitelist section. Enter the Device Name and MAC Address (You can copy and paste

the information from the Online Devices list if the device is connected to your network).



3) Click OK.

Done!

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

7. 4. IP & MAC Binding

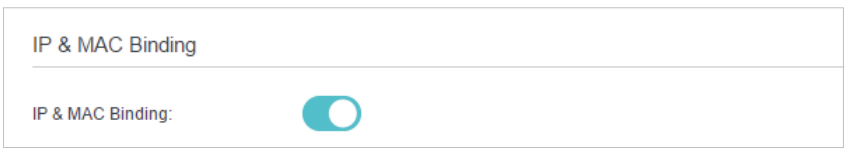
IP & MAC Binding, namely, ARP (Address Resolution Protocol) Binding, is used to bind network device's IP address to its MAC address. This will prevent ARP Spoofing and other ARP attacks by denying network access to a device with matching IP address in the Binding list, but unrecognized MAC address.

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.
3. Enable IP & MAC Binding.



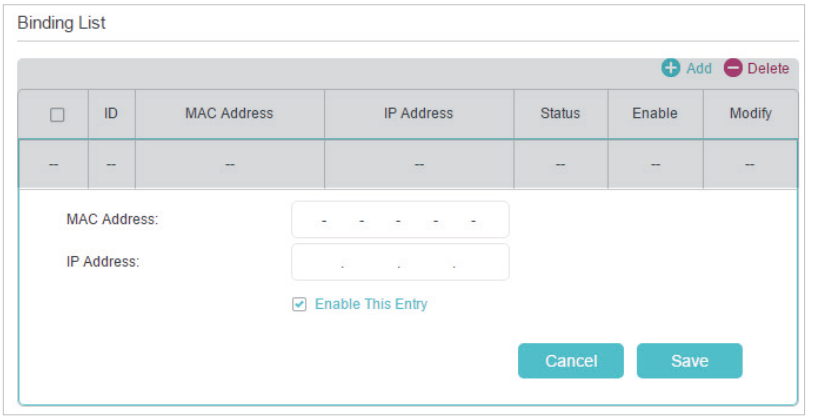
4. Bind your device(s) according to your need.

   To bind the connected device(s):

   Click to add the corresponding device 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) Tick the Enable This Entry checkbox and click Save.

Done!

Now you don't need to worry about ARP spoofing and ARP attacks!

Chapter 8

NAT Forwarding

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

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

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

NAT Forwarding is only supported by the Router mode.

It contains the following sections:

8. 1. Share Local Resources on the Internet by Virtual Servers

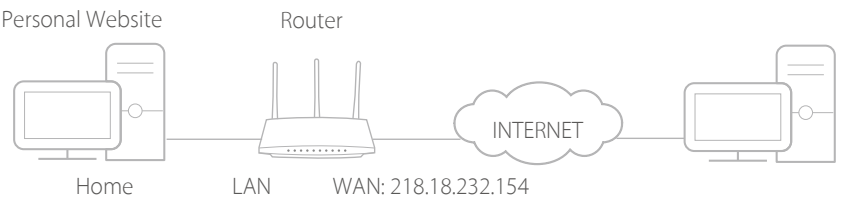
When you build up a server on the local network and want to share it on the internet, Virtual Servers can realize the service and provide it to internet users. At the same time Virtual Servers can keep the local network safe as other services are still invisible from the internet.

Virtual Servers can be used for setting up public services on your local network, such as HTTP, FTP, DNS, POP3/SMTP and Telnet. Different services use different service ports. 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 the configuration.

I want to:

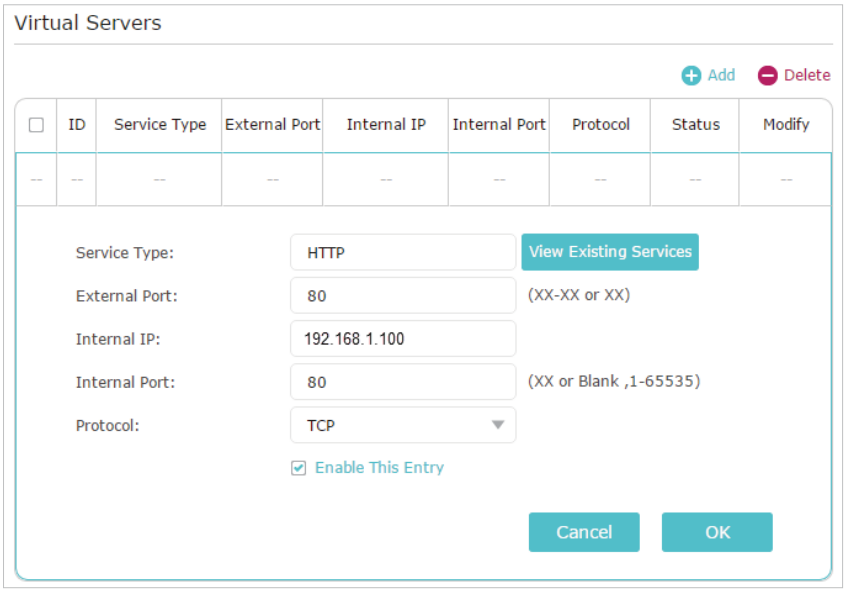
Share my personal website I've built on my local network with my friends through the internet.

For example, the personal website has been built on my home PC (192.168.1.100). I hope that my friends on the internet can visit my website in some way. 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 192.168.1.100.
2. Visit http://tplinkwifi.net, and log in with the password you set for the router.
3. Go to Advanced > NAT Forwarding > Virtual Servers.
4. Click Add. Click View Existing Services 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 OK.



Tips:

- 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.
- 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.
- You can add multiple virtual server rules if you want to provide several services in a router. Please note that the External Port should not be overlapped.

Done!

Users on the internet can enter http:// WAN IP (in this example: http:// 218.18.232.154) to visit your personal website.

Tips:

- The WAN IP should be a public IP address. For the WAN IP is assigned dynamically by the ISP, it is recommended to apply and register a domain name for the WAN referring to Set Up a Dynamic DNS Service Account. Then users on the internet can use http:// domain name to visit the website.
- 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.

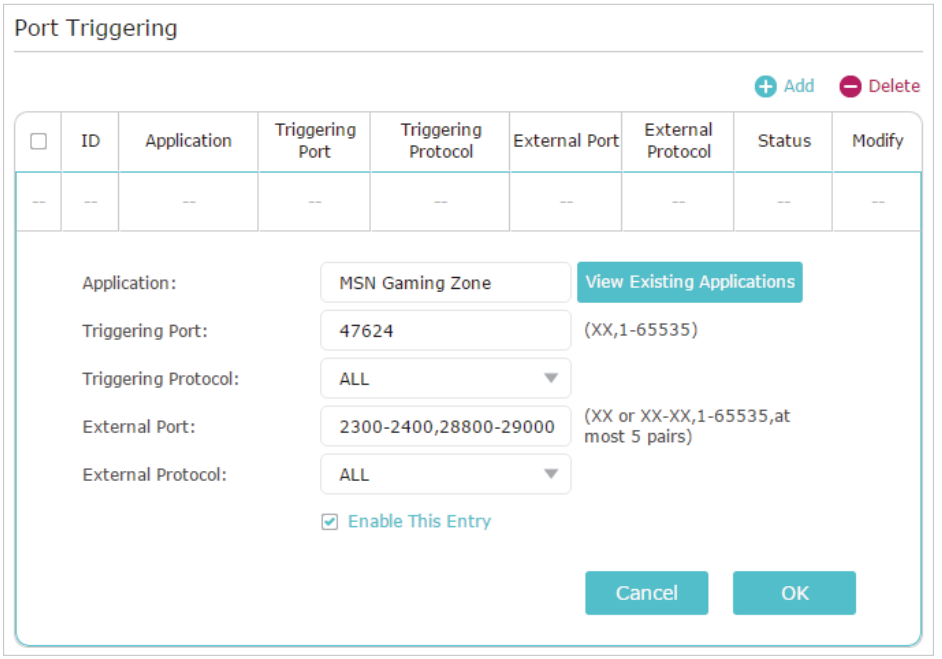
8. 2. Open Ports Dynamically by Port Triggering

Port Triggering can specify a triggering port and its corresponding external ports. When a host on the local network initiates a connection to the triggering port, all the external ports will be opened for subsequent connections. The router can record the IP address of the host. When the data from the internet return to the external ports, the router can forward them to the corresponding host. Port Triggering is mainly applied to online games, VoIPs, video players and common applications including MSN Gaming Zone, Dialpad and Quick Time 4 players, etc.

Follow the steps below to configure the Port Triggering rules:

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

3. Click View Existing Applications, and select the desired application. The Triggering Port, External Port and Protocol will be automatically filled in. The following picture takes application MSN Gaming Zone as an example.
4. Click OK.



Tips:

- You can add multiple port triggering rules according to your network need.
- The triggering ports can not be overlapped.
- If the application you need is not listed in the Existing Applications list, please enter the parameters manually. You should verify the external ports the application uses first and enter them into External Port field according to the format the page displays.

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

When a PC is set to be a DMZ (Demilitarized Zone) host on the local network, it is totally exposed to the internet, which can realize the unlimited bidirectional communication between internal hosts and external hosts. The DMZ host becomes a virtual server with all ports opened. When you are not clear about which ports to open in some special applications, such as IP camera and database software, you can set the PC to be a DMZ host.

Note: When DMZ is enabled, the DMZ host is totally exposed to the internet, which may bring some potential safety hazards. If DMZ is not in use, please disable it in time.

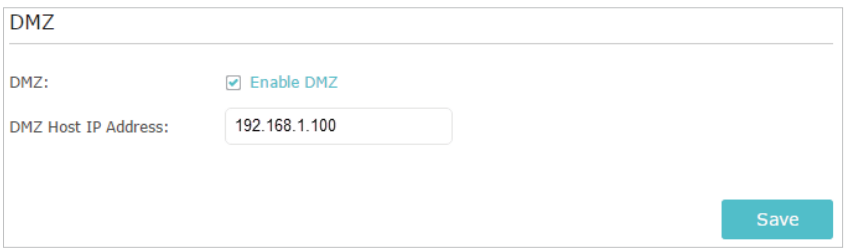
I want to:

Make the home PC join the internet online game without port restriction.

For example, due to some port restriction, when playing the online games, you can login normally but cannot join a team with other players. To solve this problem, set your PC as a DMZ host with all ports open.

How can I do that?

1. Assign a static IP address to your PC, for example 192.168.1.100.
2. Visit http://tplinkwifi.net, and log in with the password you set for the router.
3. Go to Advanced > NAT Forwarding > DMZ and select Enable DMZ.
4. Enter the IP address 192.168.1.100 in the DMZ Host IP Address filed.



5. Click Save.

Done!

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

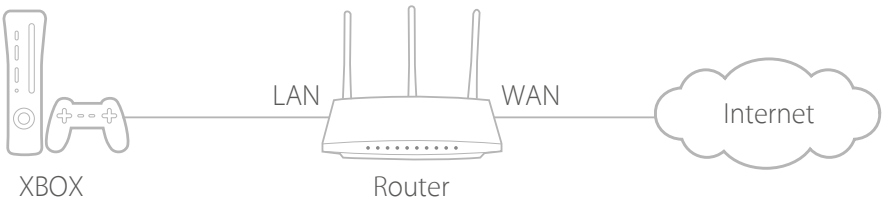
8. 4. Make Xbox Online Games Run Smoothly by UPnP

The UPnP (Universal Plug and Play) protocol allows applications or host devices to automatically find the front-end NAT device and send request to it to open the corresponding ports. With UPnP enabled, the applications or host devices on the local network and the internet can freely communicate with each other thus realizing the seamless connection of the network. You may need to enable the UPnP if you want to use applications for multiplayer gaming, peer-to-peer connections, real-time communication (such as VoIP or telephone conference) or remote assistance, etc.

Tips:

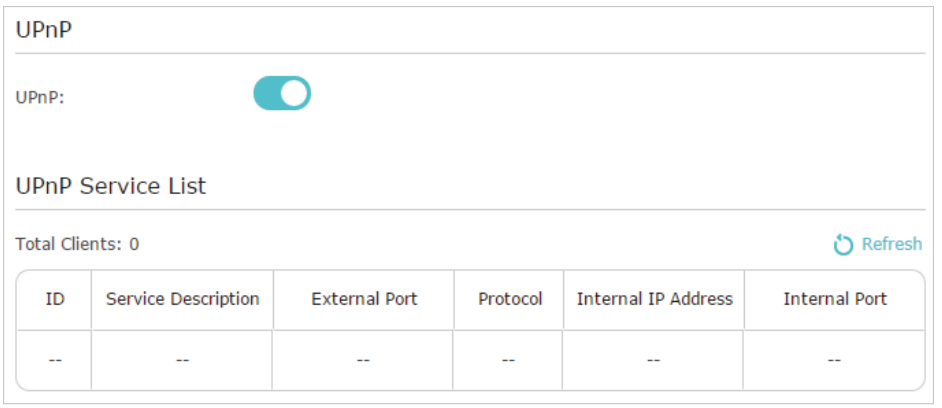
- UPnP is enabled by default in this router.
- Only the application supporting UPnP protocol can use this feature.
- UPnP feature needs the support of operating system (e.g. Windows Vista/ Windows 7/ Windows 8, etc. Some of operating system need to install the UPnP components).

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



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

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



Chapter 9

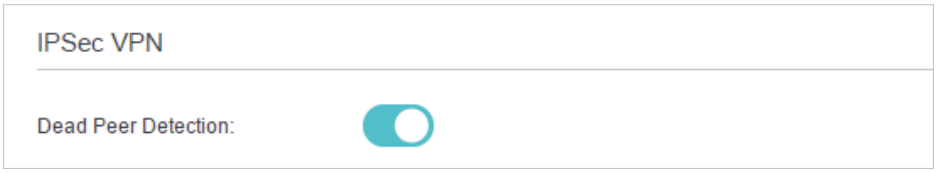
VPN

The VPN (Virtual Private Networking) feature allows you to access your home network in a secured way through internet when you are out of home.

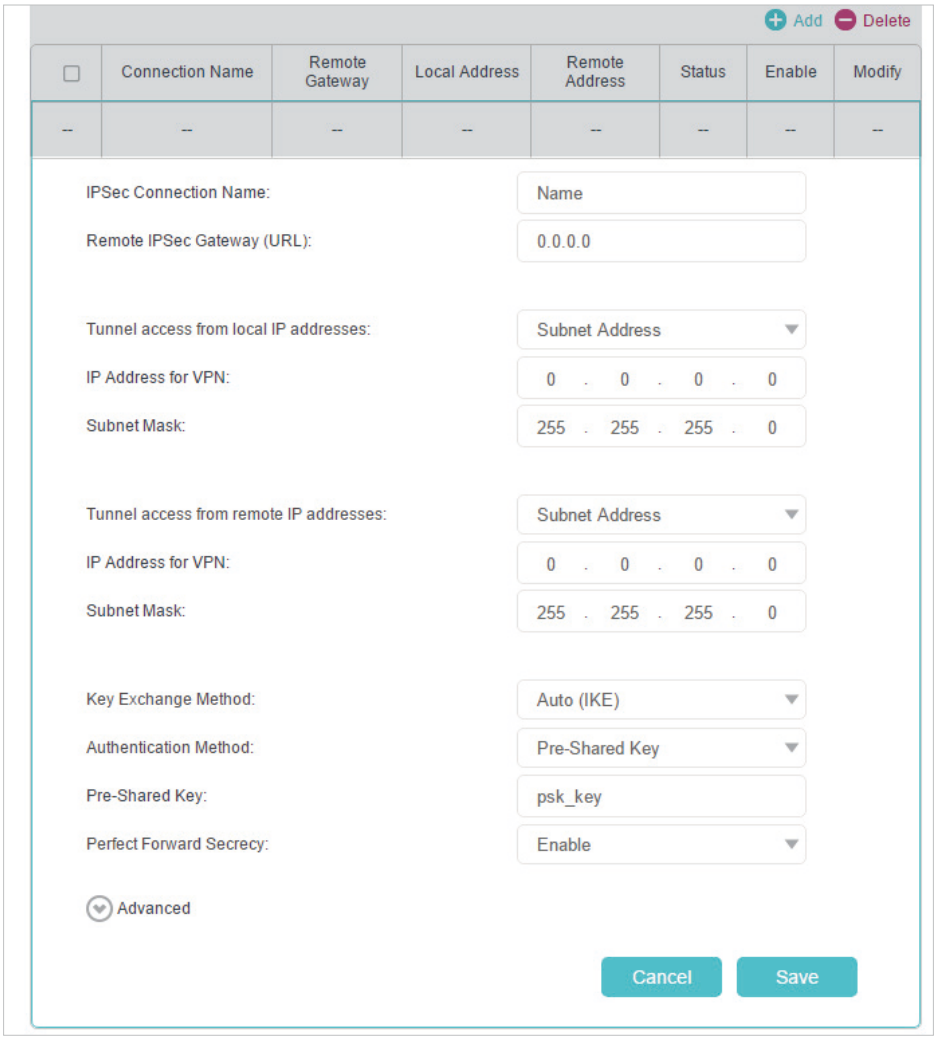
VPN is only supported by the Router mode.

With IPSec VPN, you can access the network securely when out of home. To use the VPN Service, you need to configure Dynamic DNS Service or assign a static IP address for the router's WAN port. And the System Time should be synchronized with the internet.

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > VPN > IPSec VPN.
3. Enable Dead Peer Detection.



4. Click Add and enter correspond parameters.



- IPSec Connection Name: Enter a name for the IPSec VPN connection.
- Remote IPSec Gateway (URL): Enter the destination gateway IP address which is the public WAN IP or domain name of the remote VPN server endpoint.

- Tunnel access from local IP addresses: Select Subnet Address if you want the whole LAN to join the VPN network, or select Single Address if you want a single IP to join the VPN network.
- IP Address for VPN: Enter the IP address of your LAN.
- Subnet Mask: Enter the subnet mask of your LAN.
- Tunnel access from remote IP addresses: Select Subnet Address if you want the whole remote LAN to join the VPN network, or select Single Address if you want a single IP to join the VPN network.
- IP Address for VPN: Enter the IP address of the remote LAN.
- IP Subnet Mask: Enter the subnet mask of the remote LAN.
- Key Exchange Method: Select Auto (IKE) or Manual to be used to authenticate IPSec peers.
- Authentication Method: Select Pre-Shared Key (recommended).
- Pre-Shared Key: Create a pre-shared key to be used for authentication.
- Perfect Forward Secrecy: Select Enable or Disable as an additional security protocol for the pre-shared key.

You can configure the advanced settings as needed. It's recommended to keep the default values. If you want to change these settings, make sure that both VPN server endpoints use the same Encryption Algorithm, Integrity Algorithm, Diffie-Hellman Group and Key Lifetime in both phase1 and phase2.

5. Click Save.

Chapter 10

Customize Your Network Settings

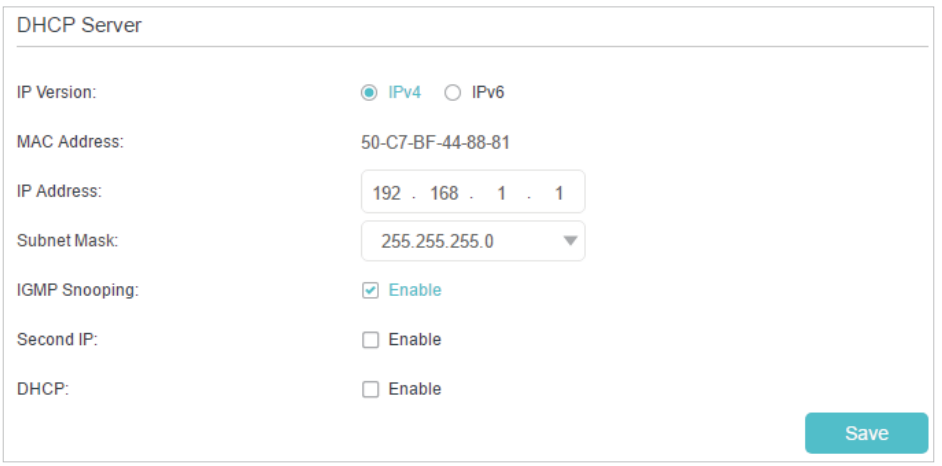
This chapter guides you on how to configure advanced network features. Some features are only supported by a certain mode.

It contains the following sections:

10. 1. Change the LAN Settings

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

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Network > LAN Settings.
3. Type in a new IP Address appropriate to your needs. And leave the Subnet Mask as the default settings.



4. Click Save.

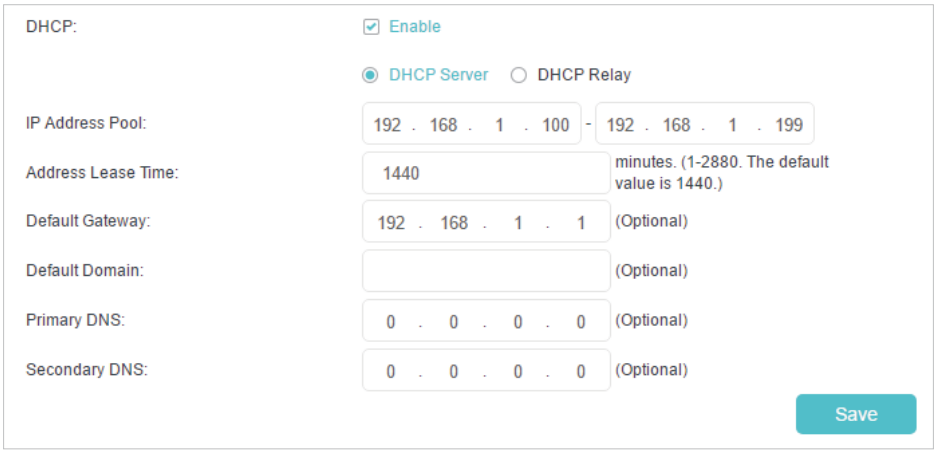
Note: If you have set the Virtual Server, DMZ or DHCP address reservation, and the new LAN IP address is not in the same subnet with the old one, then you should reconfigure these features.

10. 2. Specify DHCP Server Settings

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

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

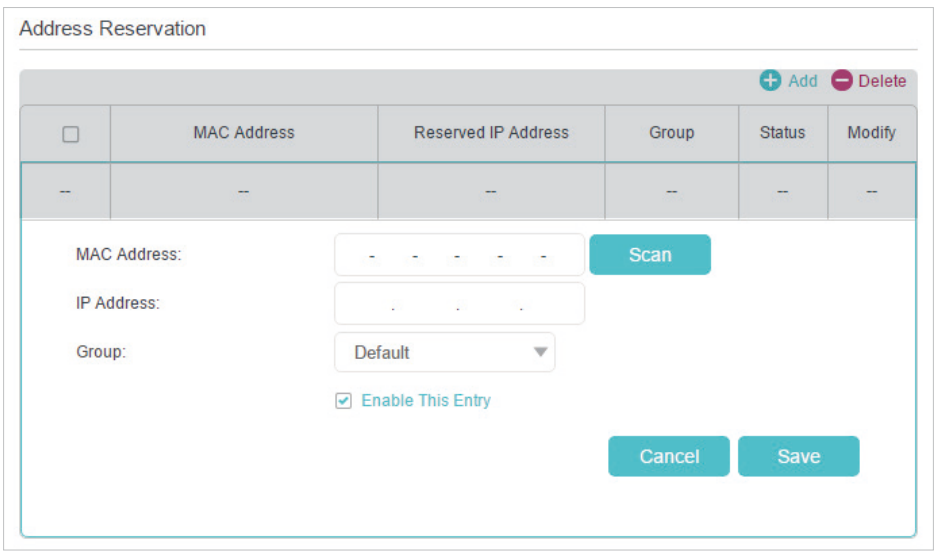
➢ **To specify the IP address that the router assigns:**



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

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

1. Click Add in the Address Reservation section.



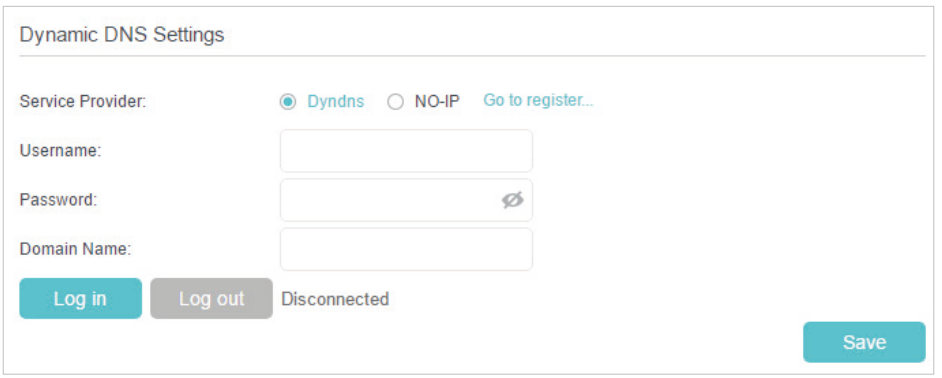
2. Click Scan to find a connected device you want to apply this rule to. You can also maunally enter the MAC address of the device if it's currently disconnected from the router.
3. Enter the IP address to reserve for the client device.
4. Tick the Enable This Entry checkbox and click Save.

10. 3. Set Up a Dynamic DNS Service Account

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

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

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Network > Dynamic DNS.
3. Select the DDNS Service Provider: NO-IP or DynDNS. If you don't have a DDNS account, you have to register first by clicking Go to register. Then enter the username, password and domain name of your account.



4. Click Log In and Save.

Tips: If you want to use a new DDNS account, please click Log out first, and then log in with a new account.

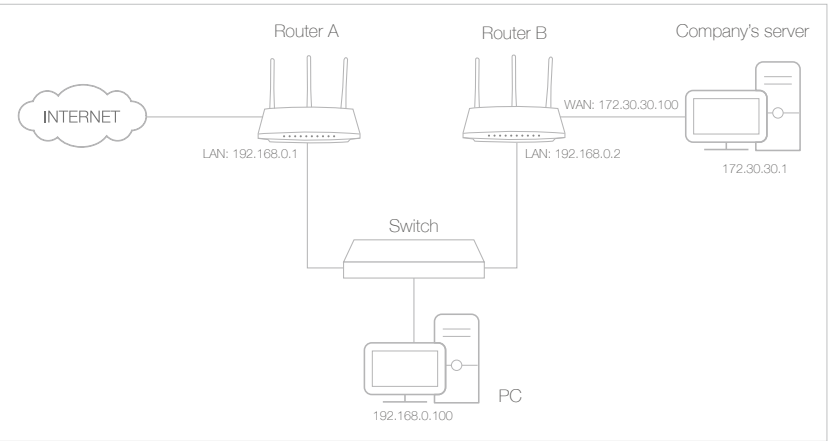
10. 4. Create Static Routes

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

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

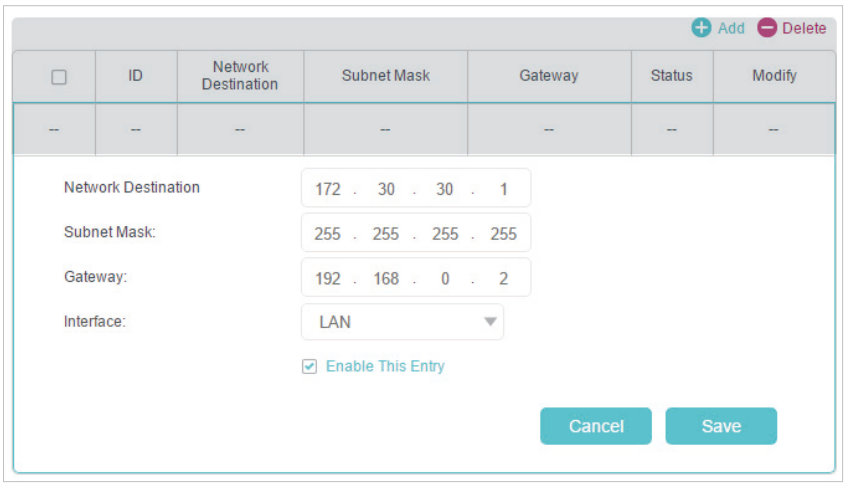
For example, in a small office, my PC can surf the internet through Router A, but I also want to visit my company's network. Now I have a switch and Router B. I connect the devices as shown in the following figure so that the physical connection between my PC and my company's server is established. To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

configure the static routing.



How can I do that?

1. Change the routers' LAN IP addresses to two different IP addresses on the same subnet. Disable Router B's DHCP function.
2. Visit http://tplinkwifi.net, and log in with the password you set for Router A.
3. Go to Advanced > Network > Advanced Routing.
4. Click Add and 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 Router A. In the example, the IP address of the company network is the destination IP address, so here enter 172.30.30.1.

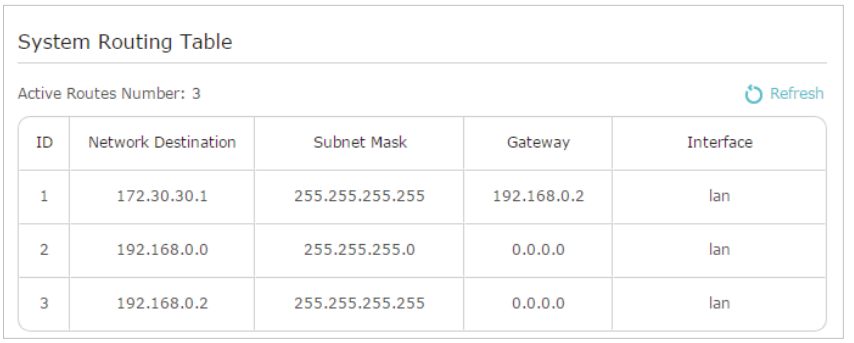
Subnet Mask: Determines the destination network with the destination IP address. If the destination is a single IP address,

enter 255.255.255.255; otherwise, enter the subnet mask of the corresponding network IP. In the example, the destination network is a single IP, so here enter 255.255.255.255.

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

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

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


System Routing Table

Active Routes Number: 3 Refresh

ID	Network Destination	Subnet Mask	Gateway	Interface
1	172.30.30.1	255.255.255.255	192.168.0.2	lan
2	192.168.0.0	255.255.255.0	0.0.0.0	lan
3	192.168.0.2	255.255.255.255	0.0.0.0	lan

Done!

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

10. 5. Specify 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 label of the router. 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, Settings > Wireless > Wireless Settings or Settings > Wireless > Extended Network.
2. The wireless radio is enabled by default. If you want to disable the wireless function of the router, just untick the Enable checkbox. 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, Settings > Wireless > Wireless Settings or Settings > Wireless > Extended Network.
2. Create a new SSID in Network Name (SSID) and customize the password for the network in Password. The value is case-sensitive.

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

➢ **To hide SSID:**

1. Go to Basic > Wireless, Settings > Wireless > Wireless Settings or Settings > Wireless > Extended Network.
2. Select Hide SSID, and your SSID won't display when you scan for local wireless networks on your wireless device and you need to manually join the network.

➢ **To change the security option:**

1. Go to Advanced > Wireless > Wireless Settings, Settings > Wireless > Wireless Settings or Settings > Wireless > Extended Network.
2. Select an option from the Security drop-down list. We recommend you don't change the default settings unless necessary. If you select other options, configure the related parameters according to the help page.

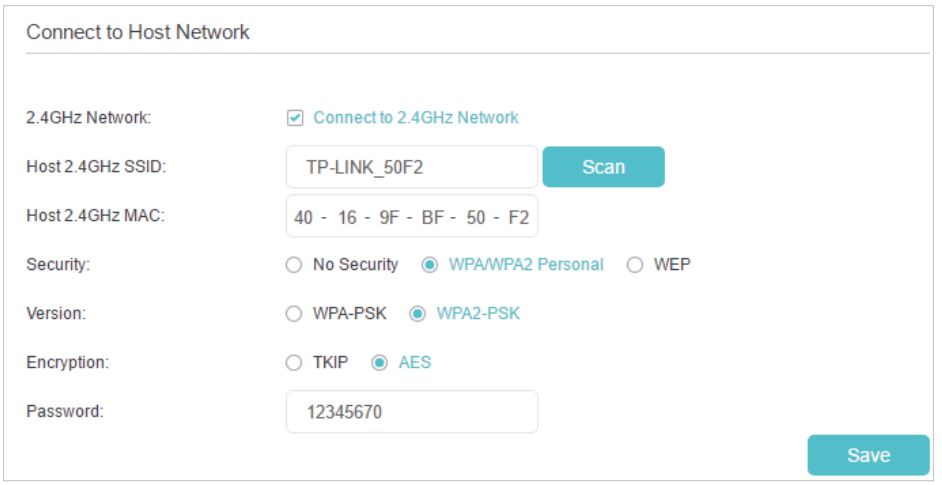
In addition

- Mode - Select a transmission mode according to your wireless client devices. It is recommended to just leave it as default.
- Channel Width - Select a channel width (bandwidth) for the wireless network.
- Channel - Select an operating channel for the wireless network. It is recommended to leave the channel to Auto, if you are not experiencing the intermittent wireless connection issue.

10. 6. Extend Host Nework

If you want to extend another host network after Quick Setup when the router works as a range extender, you can refer to this section.

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Settings > Wireless > Connect to Network.
3. Enable Connect to 2.4GHz Network and click Scan to find all available networks.



4. Select the host network you want to extend.

Note:

If the network you want to extend is on but not listed, please try the following steps.

- Move the router closer to your host router, and click Refresh in the top-right corner of the list.
- You can manually enter the SSID (network name) and password of the network you want to extend, and click Save.

5. Once a host network is selected, its SSID, MAC address and security type will be automatically filled in. If it's encrypted, enter the password in the Password field.

6. Click Save.

10. 7. Use WPS for Wireless Connection

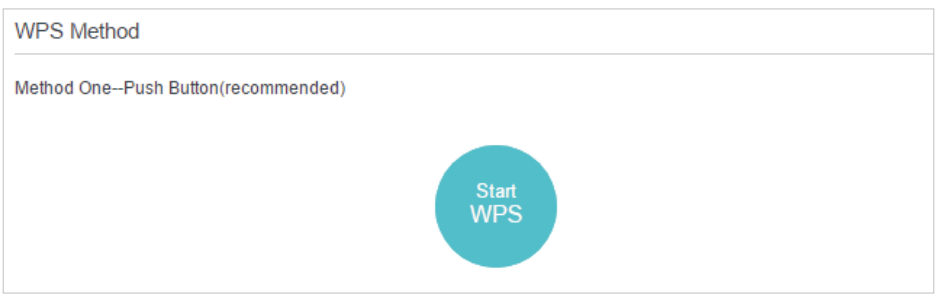
Wi-Fi Protected Setup (WPS) provides an easier approach to set up a security-protected Wi-Fi connection.

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

2. Go to Advanced > Wireless > WPS or Settings > Wireless > WPS.

10. 7. 1. Use the WPS Wizard for Wi-Fi Connections

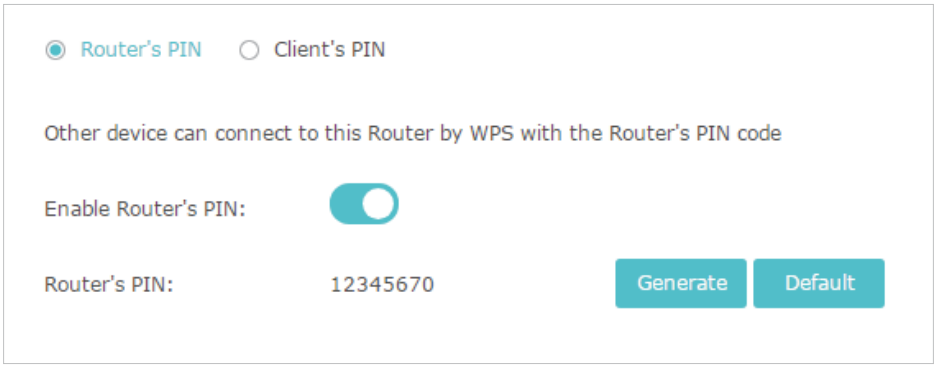
1. Click the Start WPS button on the screen. Within two minutes, press the WPS button on the client device.



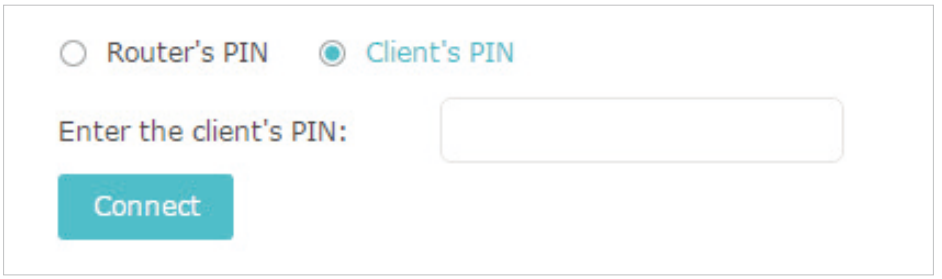
2. Success will appear on the above screen and the WPS LED on the router will keep on for five minutes if the client has been successfully added to the network.

10. 7. 2. Use the PIN for Wi-Fi connections

Router's PIN is enabled by default to allow wireless devices to connect to the router using the PIN. You can use the default one or generate a new one.



You can also enter the PIN of the device you want to connect to the Wi-Fi.



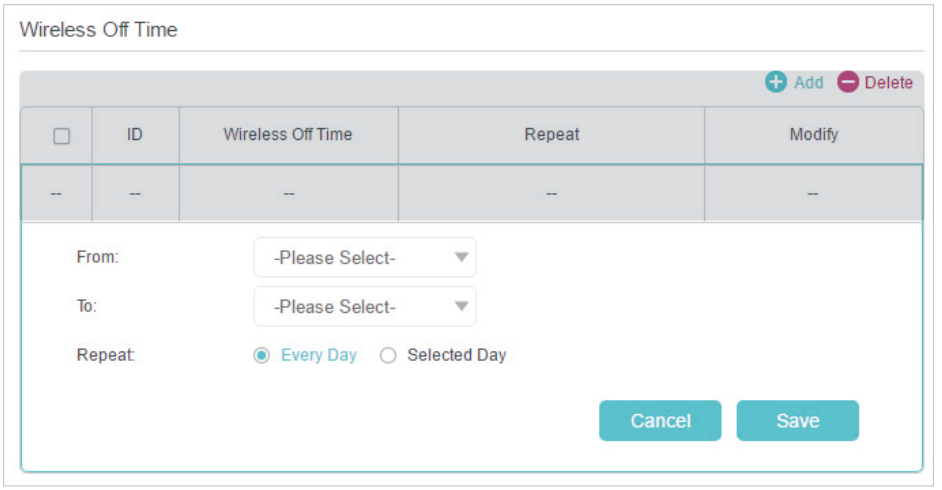
Note:

- If you want to enable/disable the WPS feature, go to Advanced > Wireless > Advanced Settings. Locate the WPS section and tick or untick the Enable checkbox.
- PIN (Personal Identification Number) is an eight-character identification number preset to each router. WPS supported devices can connect to your router with the PIN. The default PIN is printed on the label of the router.

10. 8. Schedule Your Wireless Function

The wireless network can be automatically off at a specific time 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 Wireless Schedule.
4. Click Add to set the wireless off time. Specfiy the time period and days whenthe wireless network will be off.


Wireless Off Time
Add
Delete
ID
Wireless Off Time
Repeat
Modify
From:
-Please Select-
To:
-Please Select-
Repeat:
Every Day
Selected Day
Cancel
Save

5. Click Save.

Chapter 11

Manage the Router

This chapter will show you the configuration for managing and maintaining your router. Some features are only supported by a certain mode.

It contains the following sections:

11. 1. Set Up 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.

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

➢ **To get time from the PC :**

1. Click Get from PC.
2. Click Save.

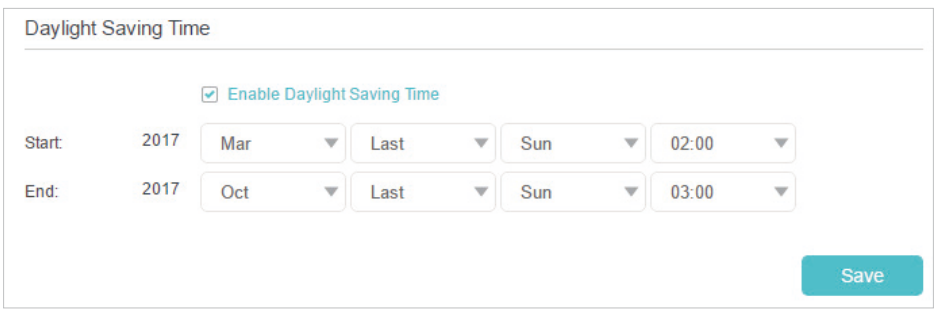
➢ **To get time from the internet :**

1. Select your local Time Zone from the drop-down list.

2. In the NTP Server I field, enter the IP address or domain name of your desired NTP Server.
3. (Optional) In the NTP Server II field, enter the IP address or domain name of the second NTP Server.
4. Click Get from the Internet and click Save.

➢ **To set up Daylight Saving Time:**

1. Select Enable Daylight Saving Time.



2. Select the correct Start date and time when daylight saving time starts at your local time zone.
3. Select the correct End date and time when daylight saving time ends at your local time zone.
4. Click Save.

11. 2. Test the Network Connectivity

Diagnostics 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 the router.
2. Go to Advanced > System Tools > Diagnostics.

3. Click Start to begin the diagnostics.

11. 3. Upgrade the Firmware

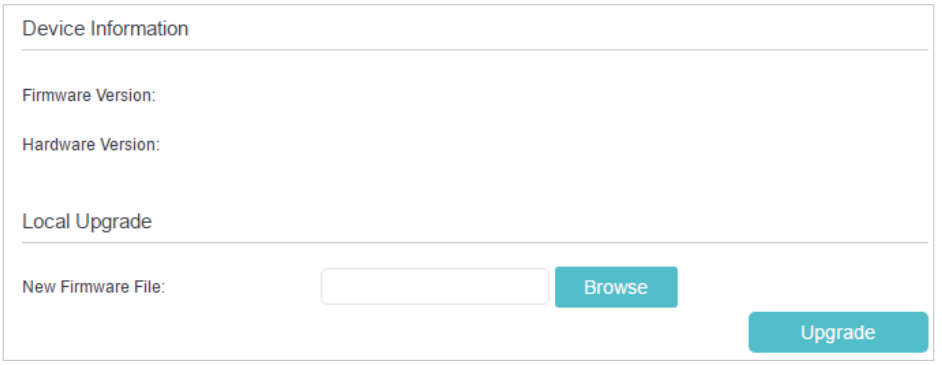
TP-Link aims at providing better network experience for users.

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

Note:

- Make sure you remove all attached USB devices from the router before the firmware upgrade to prevent data loss.
- Backup your router configuration before firmware upgrade.
- Do NOT turn off the router during the firmware upgrade.

1. Download the latest firmware file for the router from www.tp-link.com.
2. Visit http://tplinkwifi.net, and log in with the password you set for the router.
3. Go to System Tools > Firmware Upgrade.
4. Click Browse to locate the downloaded new firmware file, and click Upgrade.



5. Wait a few minutes for the upgrade and reboot to complete.

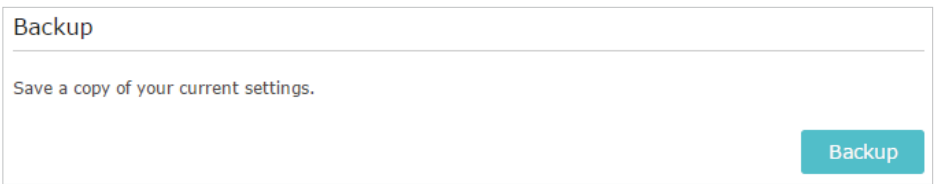
11. 4. Backup and Restore Configuration Settings

The configuration settings are stored as a configuration file in the router. You can backup 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 necessary you can erase the current settings and reset the router to the default factory settings.

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

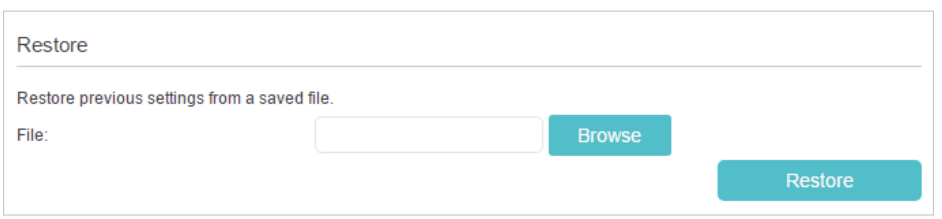
➢ **To backup configuration settings:**

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



➢ **To restore configuration settings:**

1. Click Browse to locate the backup configuration file stored on your computer, and click Restore.

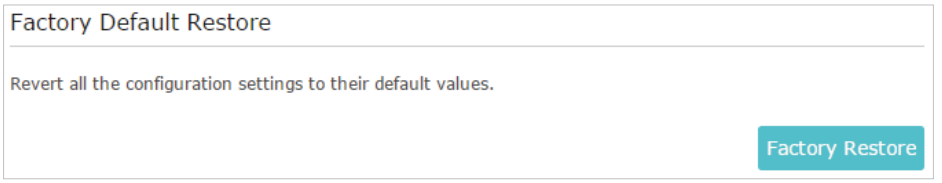


2. Wait a few minutes for the restoring and rebooting.

Note: During the restoring process, do not turn off or reset the router.

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

1. Click Factory Restore to reset the router.



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

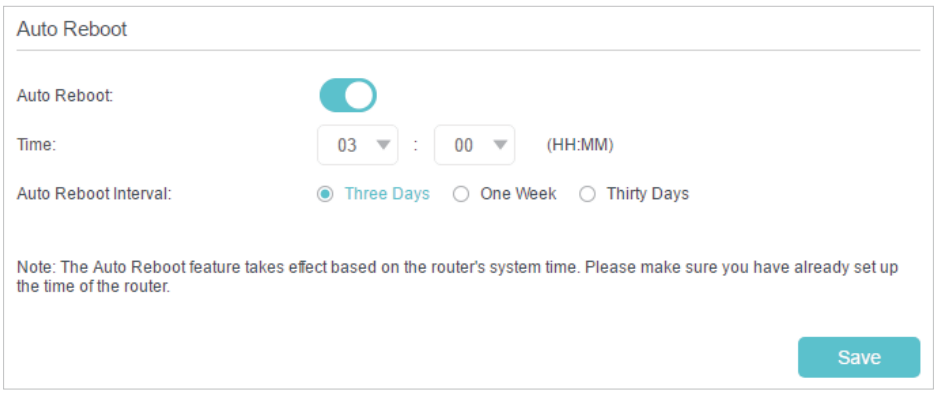
Note:

- During the resetting process, do not turn off or reset the router.
- We strongly recommend you backup the current configuration settings before resetting the router.

11. 5. Auto Reboot

Auto Reboot allows you to specify a time when the router will reboot automatically.

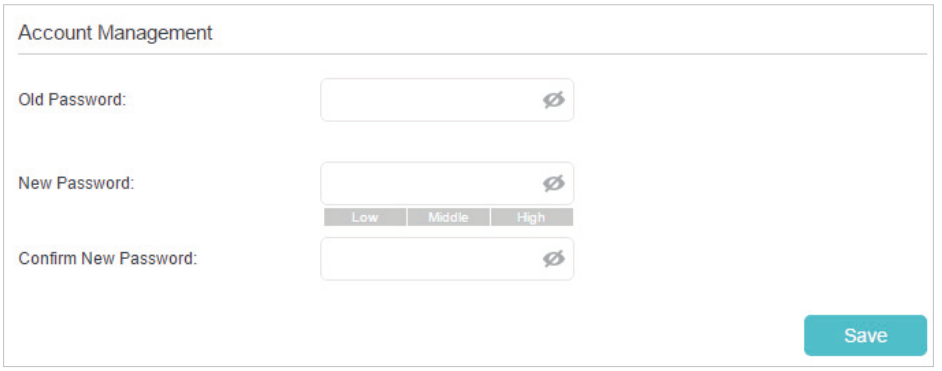
1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to System Tools > Reboot.
3. Enable Auto Reboot.
4. Specify the time at which your router will reboot and the Auto Reboot Interval.
5. Click Save.



11. 6. Change the Login Password

The account management feature allows you to change your login password of the web management page.

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to System Tools > Administration and focus on the Account Management section.

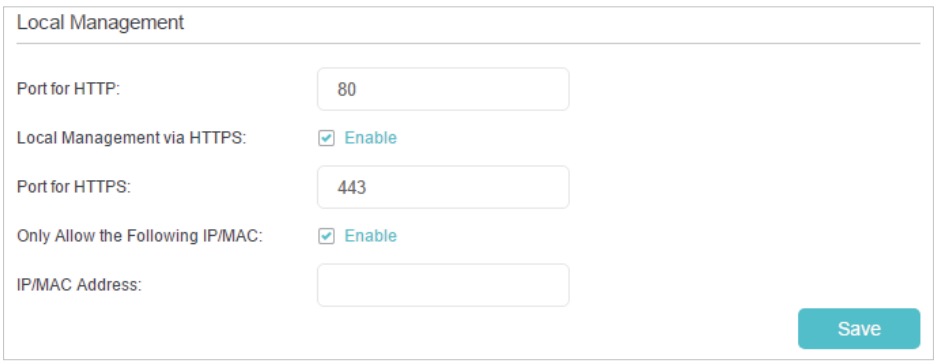


3. Enter the old password, then a new password twice (both case-sensitive). Click Save.
4. Use the new password for future logins.

11. 7. Local Management

Local Management allows local devices to access and manage the router. By default, all local devices can access and manage the router via HTTP.

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to System Tools > Administration and complete the settings In Local Management section as needed.



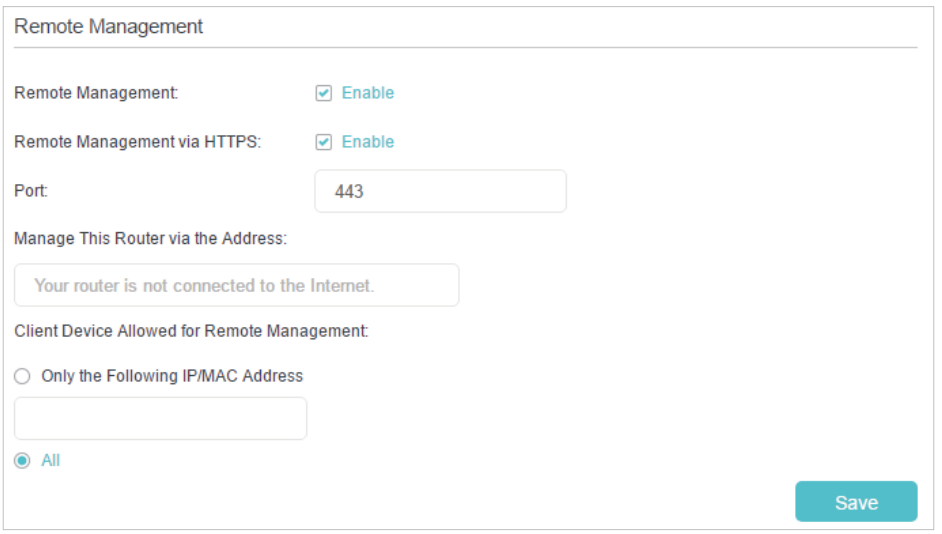
3. Enable Local Management via HTTPS if you want to access the router via both HTTPS and HTTP, or keep it disabled if you only want to access the router via HTTP.
4. Keep the Port for HTTP and Port for HTTPS as the default settings.
5. If you only want to allow one specific device to manage the router, enter the IP Address or MAC Address of the device in the IP/MAC Address field.
6. Click Save.

Note: If a warning pops up when you visit https://tplinkwifi.net, click Trust (or a similar option) to continue.

11. 8. Remote Management

Remote Management allows remote devices to access and manage the router. By default, all remote devices cannot access and manage the router.

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to System Tools > Administration and complete the settings in Remote Management section as needed.



3. Enable Remote Management if you want to allow Remote Management via HTTPS, or enable Remote Management and then disable Remote Management via HTTPS if you want to allow Remote Management via HTTP.
4. Keep the Port as the default setting.
5. Decide which remote device can access the router remotely:
   - Only the Following IP/MAC Address - Enter the IP Address or MAC Address of the remote device to access the router.
   - All - All remote devices can access the router.
6. Click Save.

Note: If a warning pops up when you visit the above address remotely, click Trust (or a similar option) to continue.

11. 9. System Log

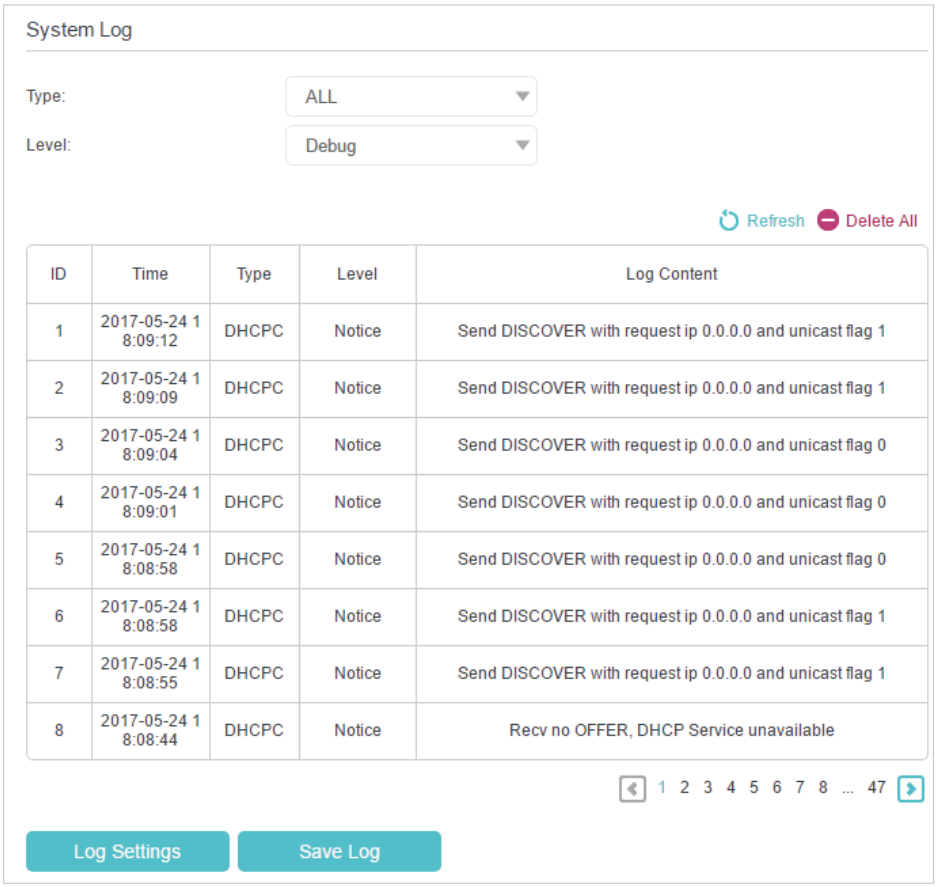
When the router does not work normally, you can save the system log and send it to the technical support for troubleshooting.

➢ **To save the system log locally:**

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

3. Choose the type and level of the system logs as needed.

4. Click Save Log to save the system logs to a local disk.

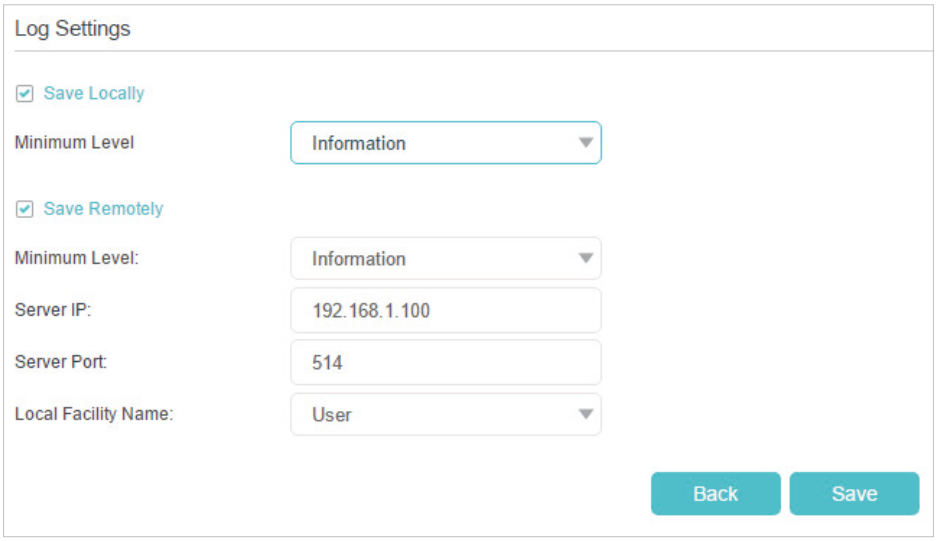


➢ **To send the system log to a remote server:**

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

2. Go to System Tools > System Log.

3. Click Log Settings.

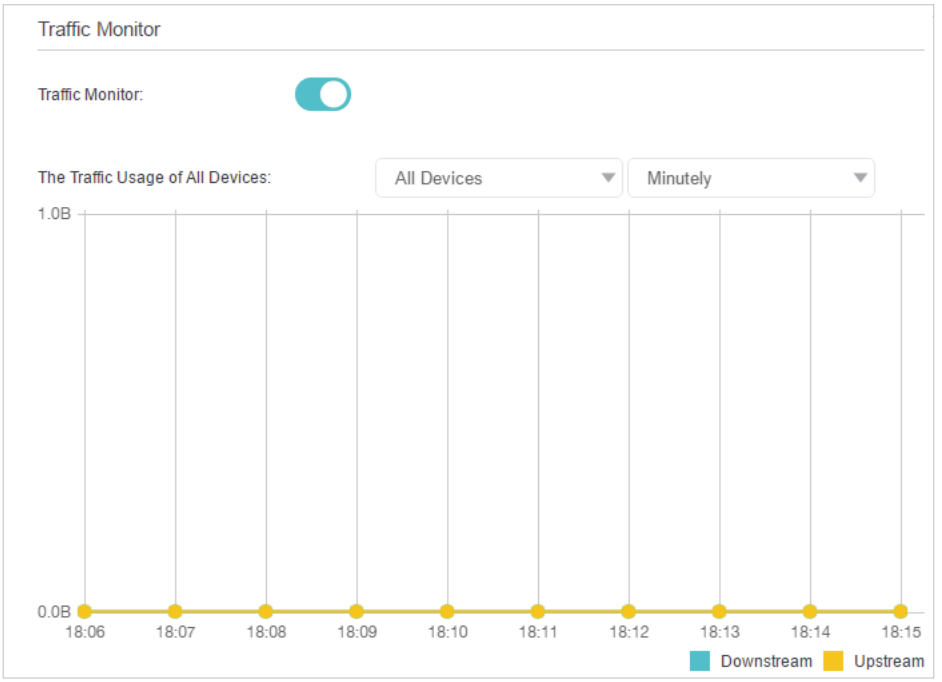


4. Select Save Remotely. If the remote server has a log viewer client or a sniffer tool implemented, you can view and analyze the system log remotely in real-time.
5. Select the minimum level of system logs to be saved from the drop-down list. The list is in descending order, with the lowest level listed last.
6. Specify the IP address of the remote system log server in the Server IP field.
7. Specify the port number of the remote system log server in the Server Port field.
8. Select the local facility name of the remote server from the drop-down list.
9. Click Save.

11. 10. Monitor the Internet Traffic Statistics

The Traffic Statistics page displays the traffic usage of a device in the past 10 minutes or that of all devices in the past 10 minutes/24 hours/7 days, allowing you to monitor the volume of internet traffic statistics.

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to System Tools > Traffic Monitor.
3. Toggle on Traffic Monitor. You can monitor the traffic usage of a device in the past 10 minutes or that of all devices in the past 10 minutes/24 hours/7 days.


Traffic Monitor
Traffic Monitor:
The Traffic Usage of All Devices:
All Devices
Minutely
1.0B
0.0B
18:06
18:07
18:08
18:09
18:10
18:11
18:12
18:13
18:14
18:15
Downstream
Upstream

FAQ

Q1. What should I do if I can't access the Internet?

- If using a cable modem, unplug the Ethernet cable and reboot the modem. Wait until its Online LED is on and stable, and then reconnect the Ethernet cable to the modem.
- If you're in a hotel room or on a trade show, the internet may be limited and requires that you authenticate for the service or purchase the Internet access.
- If your Internet access is still not available, contact TP-Link Technical Support.

Q2. How do I restore the router to its factory default settings?

With the router powered on, press and hold the WPS/RESET button until all the LEDs turn on and then release the button.

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

Q3. What should I do if I forget my wireless password?

- If you have not changed the default wireless password, it can be found on the label of the router.
- If you have changed the default wireless password, please refer to FAQ > Q2 to reset the router and go through the Quick Setup again.

Q4. What should I do if I forget my login password of the web management page?

1. Refer to FAQ > Q2 to reset the router to factory default settings.

2. Visit http://tplinkwifi.net, and create a new password for future logins.

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.

Q5. What should I do if my wireless signal is unstable or weak?

It may be caused by too much interference.

- Set your wireless channel to a different one.
- Choose a location with less obstacles that may block the signal between the router and the host router. An open corridor or a spacious location is ideal.
- Move the router to a new location away from Bluetooth devices and other household electronics, such as cordless phone, microwave, and baby monitor, etc., to minimize signal interference.
- When in Repeater/Bridge mode, the ideal location to place the router is halfway between your host router and the Wi-Fi dead zone. If that is not possible, place the router closer to your host router to ensure stable performance.

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

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."

CE Mark Warning

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)

2412MHz—2472MHz(20dBm)

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.

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.

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 20cm 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 & BSMI 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信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，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。

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。

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

Safety Information

- When product has power button, the power button is one of the way to shut off the product; when there is no power button, the only way to completely shut off power is to disconnect the product or the power adapter from the power source.
- Don't disassemble the product, or make repairs yourself. You run the risk of electric shock and voiding the limited warranty. If you need service, please contact us.
- Avoid water and wet locations.
- Adapter shall be installed near the equipment and shall be easily accessible.
- The plug considered as disconnect device of adapter.
- 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.

Explanations of the symbols on the product label

Symbol	Explanation
⎓	DC voltage
	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.