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.

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 and so on.
>	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.

More Info

The latest software, management app and utility are 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 About Your Router

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

It contains the following sections:

- Product Overview
- Panel Layout

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 and the powerful Tether app.

1. 2. Panel Layout

1. 2. 1. Top View

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

LED Explanation

Name	Status	Indication
⏻ (Power)	On	System initialization completes.
	Flashing	System initialization or firmware upgrade is in progress. Do not disconnect or power off the router.
	Off	Power is off.
📶 (Wireless)	On	The wireless function is working properly.
	Off	The wireless function is disabled.
🖥 (Ethernet)	On	One of LAN ports is connected.
	Off	No LAN port is connected.
🌐 (Internet)	On	The Internet is available.
	Off	The router's WAN port is not connected or the Internet is unavailable.
🔒 (WPS)	On/Off	Turns on when 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. The Back Panel

The following parts (view from left to right) are located on the rear panel.

Item	Description
Power Port	For connecting the router to a power socket via the provided power adapter.
WAN Port	For connecting to a DSL/Cable modem, or an Ethernet port.
LAN Ports (1/2/3/4)	For connecting your PCs or other wired network devices to the router.
WPS/RESET Button	To enable the WPS function, press this button for 1 second. If you have a WPS-supported device, you can press this button to quickly establish connection between the router and the client device and automatically configure wireless security for your wireless network.
	Press and hold this button for more than 5 seconds until the LED blinks 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 to the Internet

This chapter contains the following sections:

- Position Your Router
- Connect to the Internet

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.

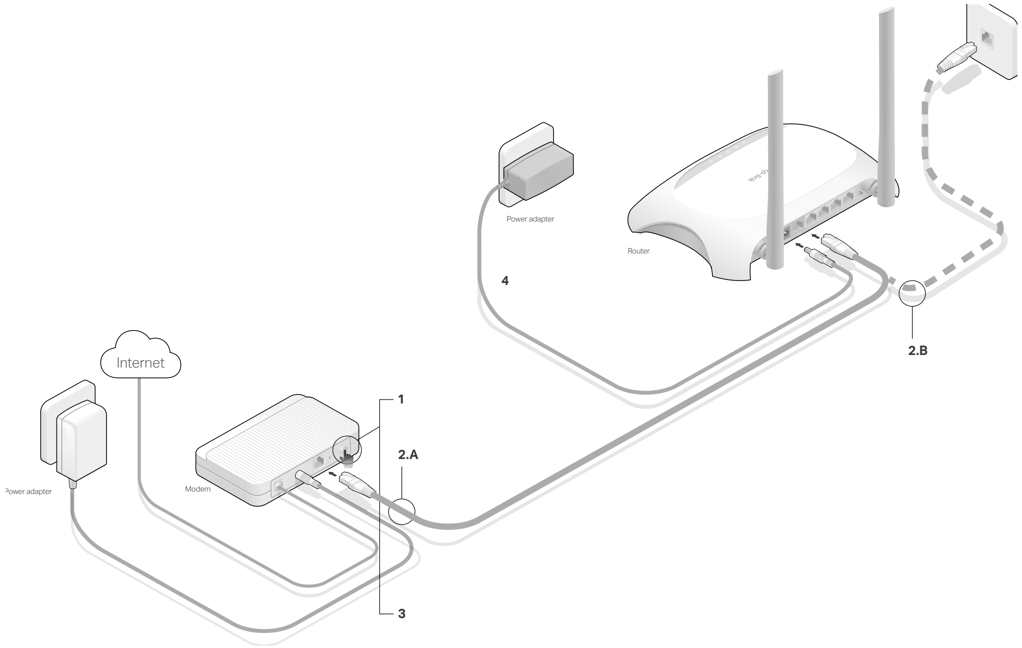
2. 2. Connect to the Internet

The Router provides two working modes: Wireless Router and Access Point. You can choose the mode to better suit your network needs and follow the guide to complete the configuration.

2. 2. 1. Wireless Router Mode

1. 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 Step2B, 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.

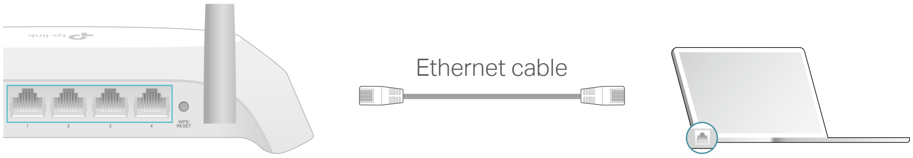
3) Turn on the modem, and then wait about **2 minutes** for it to restart.

4) Connect the power adapter to the router.

2. Connect your computer to the router.

- **Method 1: Wired**

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

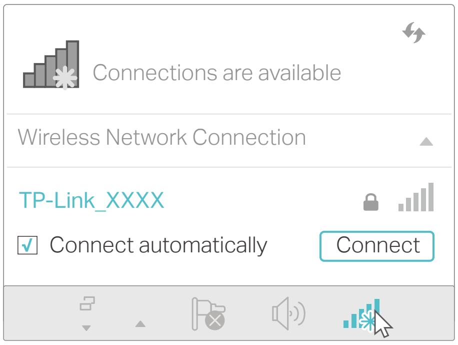


- **Method 2: Wirelessly**

1) Find the SSID (Network Name) and Wireless Password printed on the label at the bottom of the router.

2) Click the network icon of your computer or go to Wi-Fi Settings of your smart device, and then select the SSID to join the network.

Computer



Connections are available

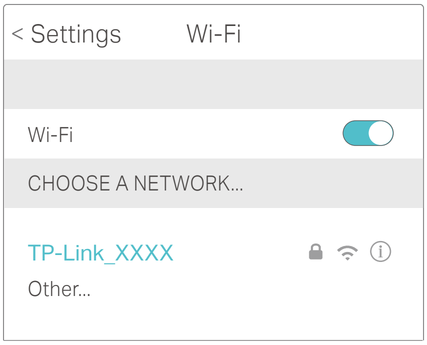
Wireless Network Connection

TP-Link_XXXX

☑ Connect automatically Connect

OR

Smart Device



< Settings Wi-Fi

Wi-Fi

CHOOSE A NETWORK...

TP-Link_XXXX

Other...

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

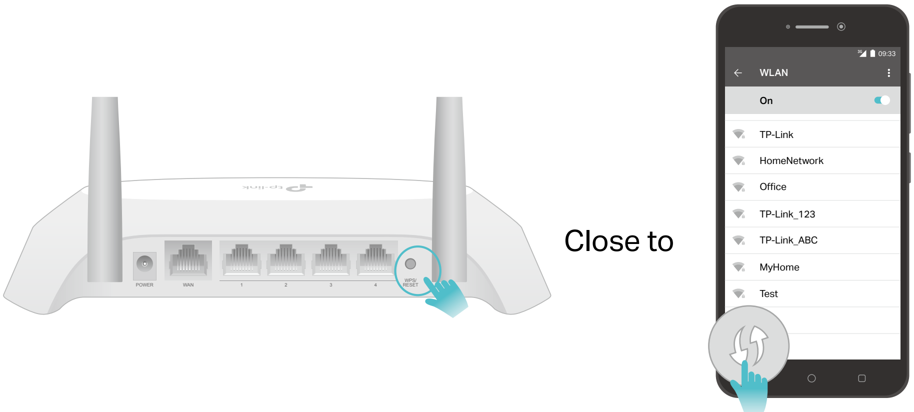
Wireless devices that support WPS, including Android phones, tablets, most USB network cards, can be connected to your router through this method.

Note:

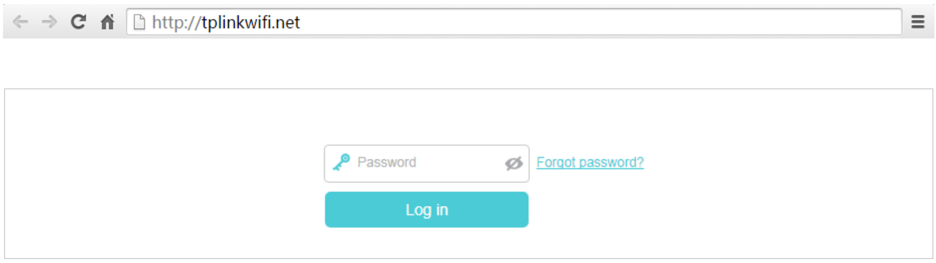
- WPS is not supported by iOS devices.
- The WPS function cannot be configured if the wireless function of the router is disabled. Also, the WPS function will be disabled if your wireless encryption is WEP. Please make sure the wireless function is enabled and is configured with the appropriate encryption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



3. Enter http://tplinkwifi.net in the address bar of a web browser. Use admin for password, and then click Login.



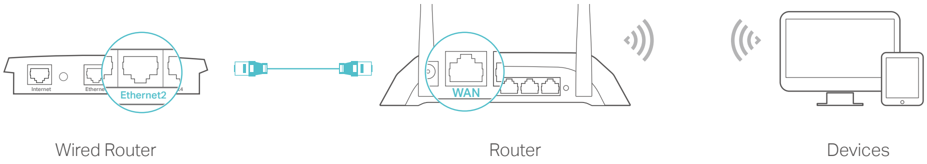
Note:

If the above screen does not pop-up, it means that your IE Web-browser has been set to a proxy. Go to menu Tools > Internet Options > Connections > LAN Settings, in the screen that appears, untick the Using Proxy checkbox, and click OK.

4. Enjoy! For wireless devices, you may have to reconnect to the wireless network if you have customized the SSID (wireless name) and password during the configuration.

2. 2. 2. Access Point Mode

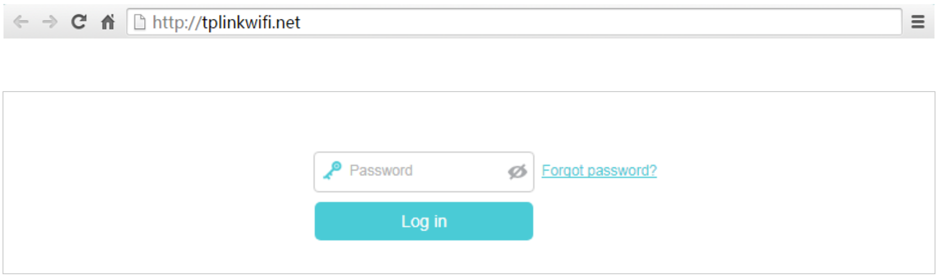
This mode transforms your existing wired network to a wireless network.



1. Connect the power adapter to the router.
2. Connect the router to your wired host router's Ethernet port via an Ethernet cable as shown above.

3. Connect a computer to the router via an Ethernet cable or wirelessly by using the SSID (network name) and password printed on the bottom label of the router.

4. Enter http://tplinkwifi.net in the address bar of a web browser. Use admin for password, and then click Login.



Note:

If the above screen does not pop-up, it means that your IE Web-browser has been set to a proxy. Go to menu Tools > Internet Options > Connections > LAN Settings, in the screen that appears, untick the Using Proxy checkbox, and click OK.

5. After successfully login, go to Advanced > Operation Mode and select Access Point mode, then click Save.

6. Enjoy! Connect to the wireless network by using the SSID (network name) and password of the router.

Chapter 3

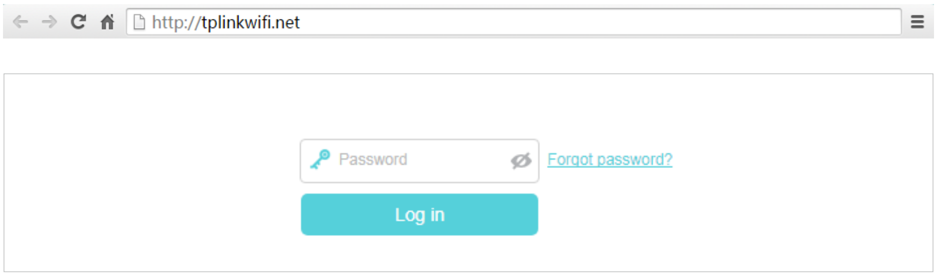
Log In to the Router

This chapter introduces how to log in to the web management page of 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 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 log in with the password you set for the router. The default password is admin (all lowercase).



Note:

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

Chapter 4

Configure the Router in Wireless Router Mode

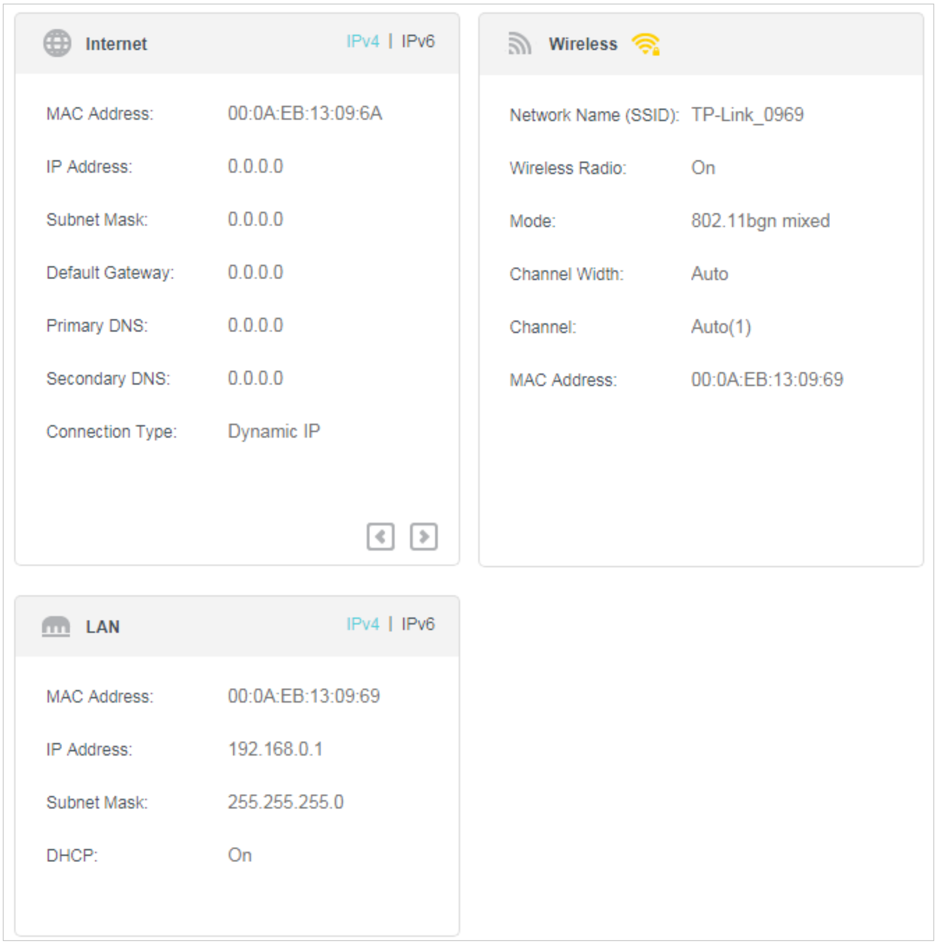
This chapter presents how to configure the various features of the router working as a wireless router.

It contains the following sections:

4. 1. Status

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

2. Go to Status. You can view the current status information of the router.



MAC Address: 00:0A:EB:13:09:6A

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0

Connection Type: Dynamic IP

Network Name (SSID): TP-Link_0969

Wireless Radio: On

Mode: 802.11bgn mixed

Channel Width: Auto

Channel: Auto(1)

MAC Address: 00:0A:EB:13:09:69

MAC Address: 00:0A:EB:13:09:69

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

DHCP: On

- LAN - This field displays the current settings of the LAN, and you can configure them on the Network > LAN Settings page.
    - MAC address - The physical address of the router.
    - IP address - The LAN IP address of the router.
    - Subnet Mask - The subnet mask associated with the LAN IP address.
- Wireless - This field displays the basic information or status of the wireless function, and you can configure them on the Wireless > Wireless Settings page.
    - Wireless Radio - Indicates whether the wireless radio feature of the router is enabled or disabled.
    - Network Name(SSID) - The SSID of the router.
    - Mode - The current wireless mode which the router works on.
    - Channel - The current wireless channel in use.

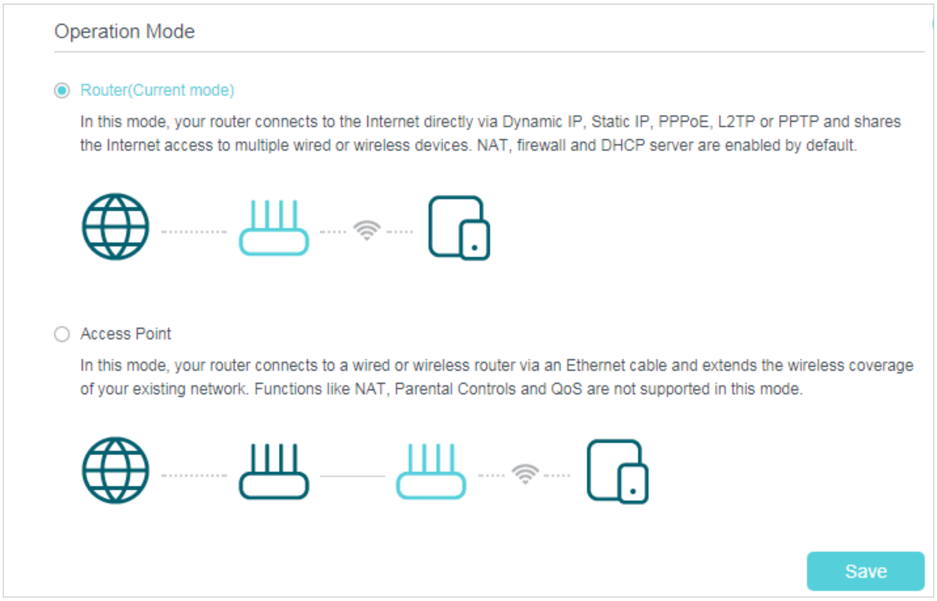
  - Channel Width - The current wireless channel width in use.
  - MAC Address - The physical address of the router.
- Internet - This field displays the current settings of the Internet, and you can configure them on the Network > Internet page.
  - MAC Address - The physical address of the WAN port.
  - IP Address - The current WAN (Internet) IP Address. This field will be blank or 0.0.0.0 if the IP Address is assigned dynamically and there is no internet connection.
  - Subnet Mask - The subnet mask associated with the WAN IP Address.
  - Default Gateway - The Gateway currently used is shown here. When you use Dynamic IP as the internet connection type, click Renew or Release here to obtain new IP parameters dynamically from the ISP or release them.
  - DNS Server - The IP addresses of DNS (Domain Name System) server.

4. 2. Operation Mode

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

2. Go to Operation Mode.

3. Select the working mode as needed and click Save.



Operation Mode

● Router(Current mode)

In this mode, your router connects to the Internet directly via Dynamic IP, Static IP, PPPoE, L2TP or PPTP and shares the Internet access to multiple wired or wireless devices. NAT, firewall and DHCP server are enabled by default.

○ Access Point

In this mode, your router connects to a wired or wireless router via an Ethernet cable and extends the wireless coverage of your existing network. Functions like NAT, Parental Controls and QoS are not supported in this mode.

4. 3. Network

4. 3. 1. Internet

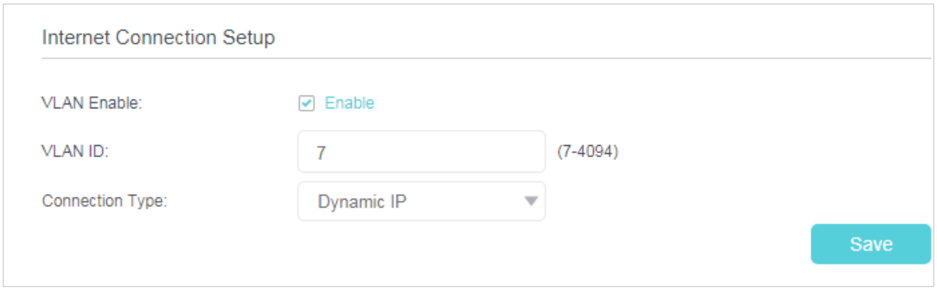
1. Visit http://tplinkwifi.net, and log in with the password you set for the router.

2. Go to Basic > Internet.

3. Configure the IP parameters of the Internet and click Save.

Dynamic IP

If your ISP provides the DHCP service, please select Dynamic IP, and the router will automatically get IP parameters from your ISP.



Internet Connection Setup

VLAN Enable: ☑ Enable

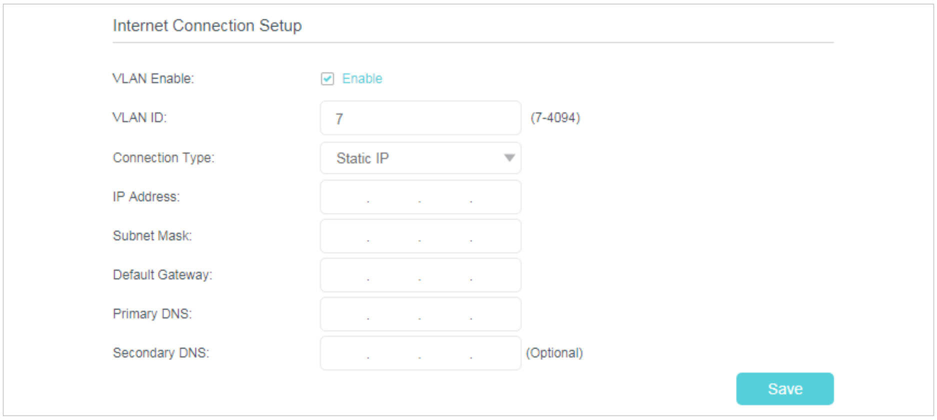
VLAN ID: 7 (7-4094)

Connection Type: Dynamic IP

- VLAN Enable - Select the checkbox to enable VLAN ID.
- VLAN ID - Enter the VLAN ID provided by your ISP.

Static IP

If your ISP provides a static or fixed IP address, subnet mask, default gateway and DNS setting, please select Static IP.



Internet Connection Setup

VLAN Enable: ☑ Enable

VLAN ID: 7 (7-4094)

Connection Type: Static IP

IP Address: . . .

Subnet Mask: . . .

Default Gateway: . . .

Primary DNS: . . .

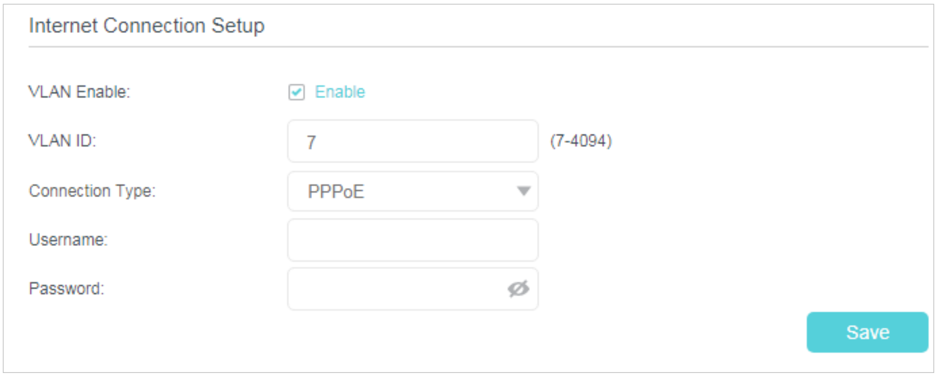
Secondary DNS: . . . (Optional)

- IP Address - Enter the IP address in dotted-decimal notation provided by your ISP.
- Subnet Mask - Enter the subnet mask in dotted-decimal notation provided by your ISP. Normally 255.255.255.0 is used as the subnet mask.

- Default Gateway - Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- Primary/Secondary DNS Server - (Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.

PPPoE

If your ISP provides PPPoE connection, select PPPoE.



Internet Connection Setup

VLAN Enable: ☑ Enable

VLAN ID: 7 (7-4094)

Connection Type: PPPoE

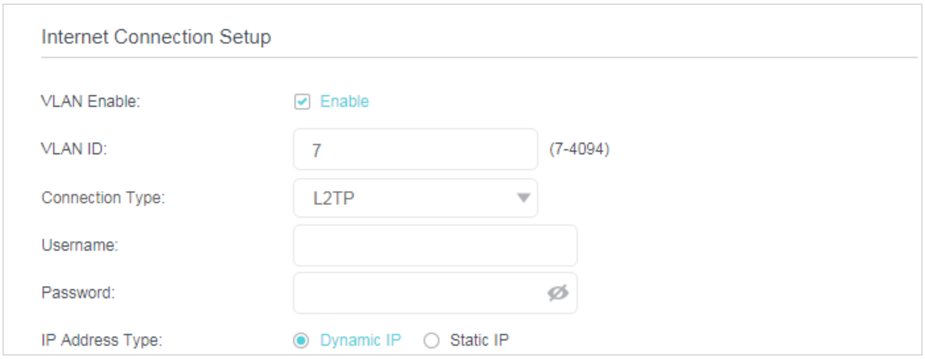
Username:

Password:

- User Name/Password - Enter the user name and password provided by your ISP. These fields are case-sensitive.

L2TP

If your ISP provides L2TP connection, please select L2TP. Enter the Username and Password and choose the IP Address Type provided by your ISP. Different parameters are needed according to the IP Address Type you have chosen.



Internet Connection Setup

VLAN Enable: ☑ Enable

VLAN ID: 7 (7-4094)

Connection Type: L2TP

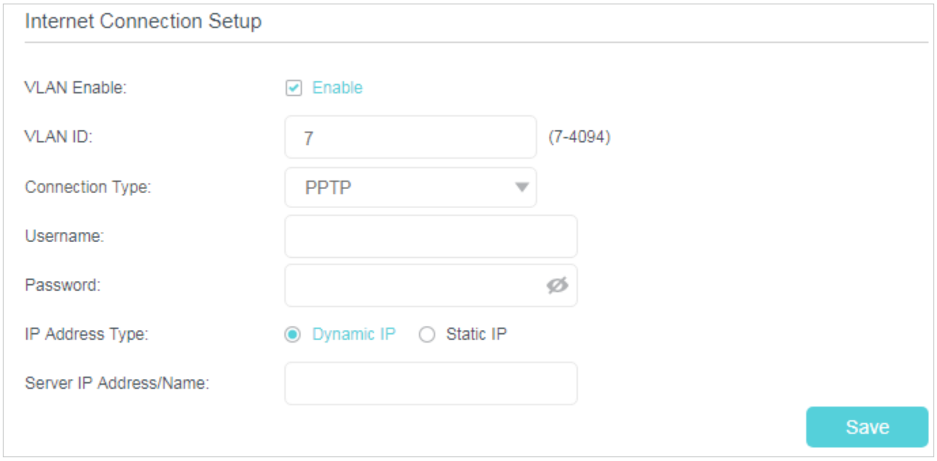
Username:

Password:

IP Address Type: ● Dynamic IP ○ Static IP

PPTP

If your ISP provides PPTP connection, please select PPTP. Enter the Username and Password, and choose the IP Address Type provided by your ISP. Different parameters are needed according to the IP Address Type you have chosen.



Internet Connection Setup

VLAN Enable: ☑ Enable

VLAN ID: 7 (7-4094)

Connection Type: PPTP

Username:

Password:

IP Address Type: ● Dynamic IP ○ Static IP

Server IP Address/Name:

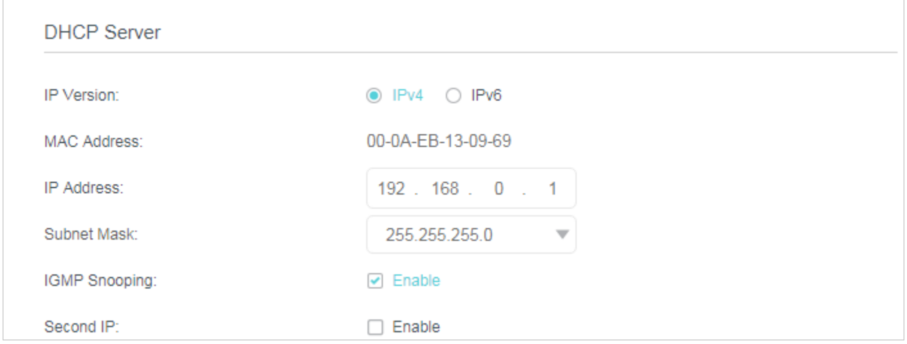
4. 3. 2. LAN Settings

4.3.2.1. 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.



DHCP Server

IP Version: ● IPv4 ○ IPv6

MAC Address: 00-0A-EB-13-09-69

IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255.255.255.0

IGMP Snooping: ☑ Enable

Second IP: □ Enable

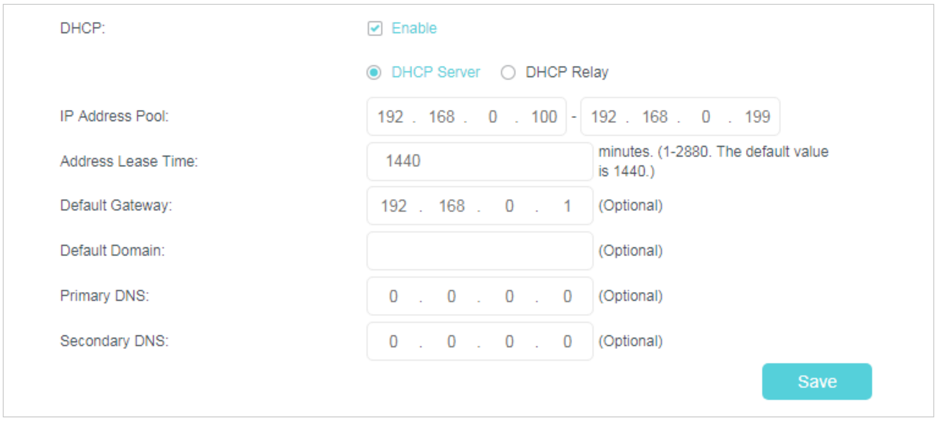
3. Type in a new IP Address appropriate to your needs.
4. Select the Subnet Mask from the drop-down list. The subnet mask together with the IP address identifies the local IP subnet.
5. Keep IGMP Snooping as enabled by default. IGMP snooping is the process of listening to IGMP (Internet Group Management 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 modem router's Second IP and Subnet Mask for LAN interface through which you can also access the web management page.
7. Leave the rest of the default settings as they are.
8. Click Save to make the settings effective.

4.3.2.2. 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.



DHCP: ☑ Enable

● DHCP Server ○ DHCP Relay

IP Address Pool: 192 . 168 . 0 . 100 - 192 . 168 . 0 . 199

Address Lease Time: 1440 minutes. (1-2880. The default value is 1440.)

Default Gateway: 192 . 168 . 0 . 1 (Optional)

Default Domain: (Optional)

Primary DNS: 0 . 0 . 0 . 0 (Optional)

Secondary DNS: 0 . 0 . 0 . 0 (Optional)

3. Select DHCP to enable the 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 value for the Address Lease Time. The Address Lease Time is the amount of time in which a DHCP client can lease its current dynamic IP address assigned by the modem router. After the dynamic IP address expires, the user will be automatically assigned a new dynamic IP address. The default is 1440 minutes.
6. Keep the rest of the settings as default and click Save.

Note:

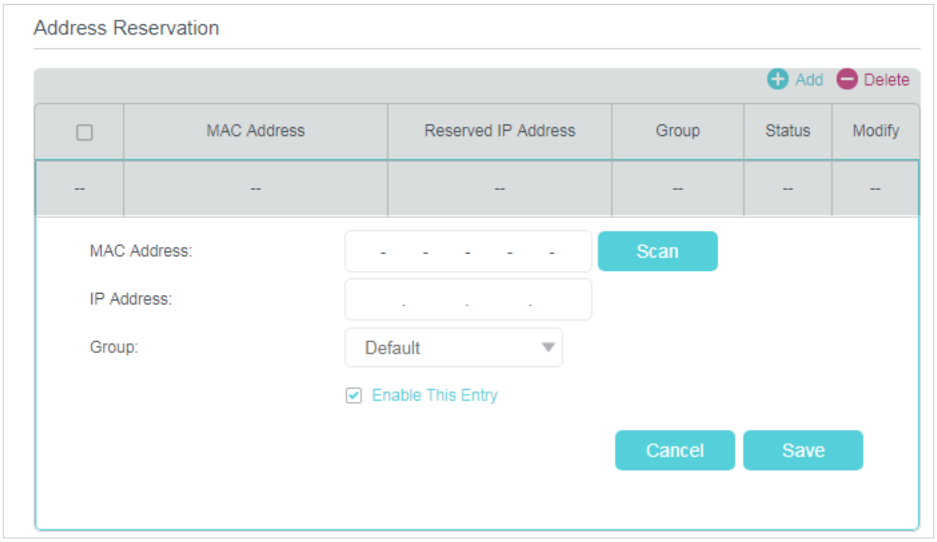
1. The router can be configured to work as a DHCP Relay. A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. If it is enabled, the DHCP requests 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 actual situation on Advanced > Network > LAN Settings page.

4.3.2.3. 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 device.

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 locate the Address Reservation table and click Add to add an address reservation entry for your device.


Address Reservation

□	MAC Address	Reserved IP Address	Group	Status	Modify
--	--	--	--	--	--

MAC Address: - - - - -

IP Address: . . .

Group: Default

☑ Enable This Entry

4. Enter the MAC address of the device for which you want to reserve IP address.

5. Specify the IP address which will be reserved by the router.

6. Check to Enable this entry and click Save to make the settings effective.

4. 3. 3. IPv6 LAN Settings

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

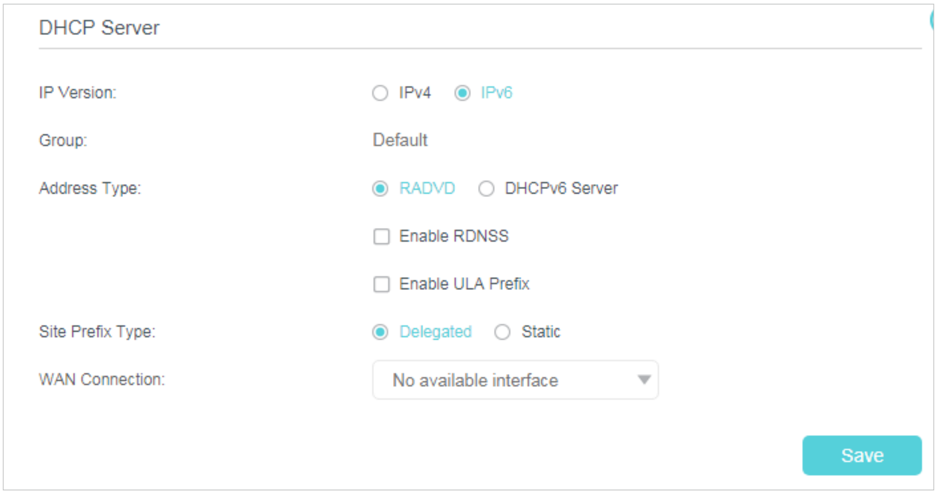
- Configure the RADVD (Router Advertisement Daemon) address type
- Configure the DHCPv6 Server address type

4.3.3.1. 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 page.

3. Select IPv6 to configure IPv6 LAN parameters.


DHCP Server

IP Version: ○ IPv4 ● IPv6

Group: Default

Address Type: ● RADVD ○ DHCPv6 Server

□ Enable RDNSS

□ Enable ULA Prefix

Site Prefix Type: ● Delegated ○ Static

WAN Connection: No available interface

1) Select the RADVD 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 value Delegated. If your ISP has provided a specific IPv6 site prefix, select Static and enter the prefix.

3) Keep WAN Connection as the default value.

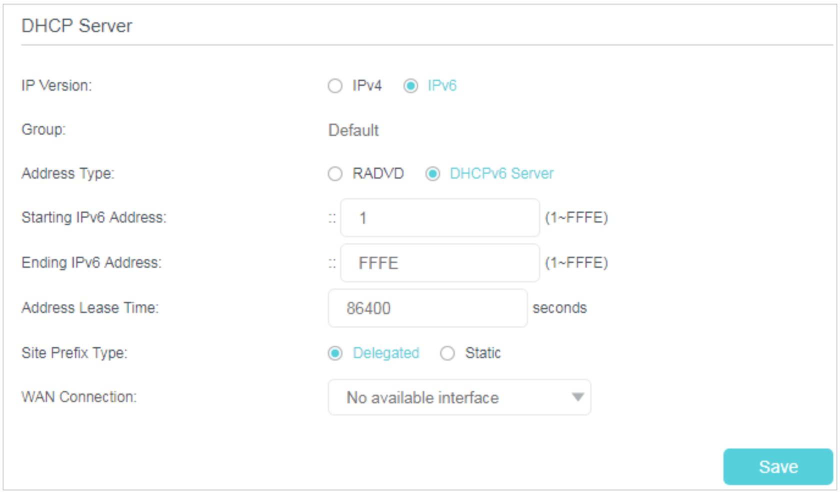
4. Click Save to make the settings effective.

4.3.3.2. 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 page.

3. Select IPv6 to configure IPv6 LAN parameters.



DHCP Server

IP Version:	○ IPv4 ● IPv6
Group:	Default
Address Type:	○ RADVD ● DHCPv6 Server
Starting IPv6 Address:	:: 1 (1~FFFE)
Ending IPv6 Address:	:: FFFE (1~FFFE)
Address Lease Time:	86400 seconds
Site Prefix Type:	● Delegated ○ Static
WAN Connection:	No available interface

1) Select the DHCPv6 Server address type to make the router assign IPv6 addresses to hosts.

2) Specify the Start/End IPv6 Address for the IPv6 suffixes. The router will generate IPv6 addresses within the specified range.

3) Keep Leased Time as the default value.

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.

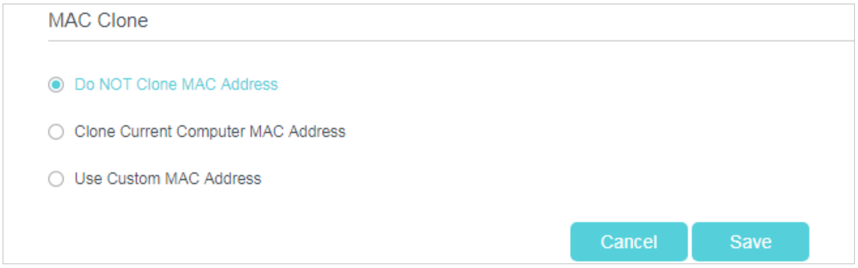
5) Keep WAN Connection as the default value.

4. 3. 4. MAC Clone

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

2. Go to Network > Internet page.

3. Click the Add icon, and scroll down to get the MAC Clone section..



MAC Clone

● Do NOT Clone MAC Address

○ Clone Current Computer MAC Address

○ Use Custom MAC Address

- If you are using the computer with the authenticated MAC address to access the modem router, please select Clone Current Computer MAC Address.
- If you know the authenticated MAC address, please select Use Custom MAC Address and then enter the address.

4. Click Save to make the settings effective.

4. 3. 5. Interface Grouping

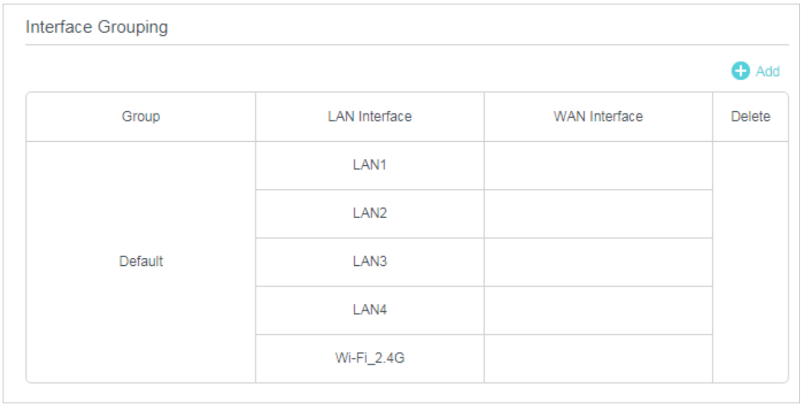
I want to:

Divide my devices connected to the modem 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?

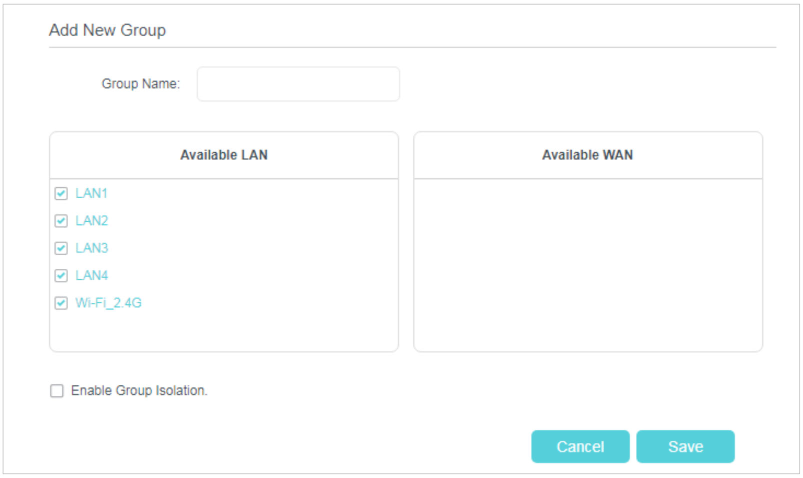
1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Network > Interface Grouping page to open the configuration page where some interfaces can be grouped together.



Interface Grouping

Group	LAN Interface	WAN Interface	Delete
Default	LAN1		
	LAN2		
	LAN3		
	LAN4		
	Wi-Fi_2.4G		

3. Click to Add a new group.



Add New Group

Group Name:

Available LAN
☑ LAN1
☑ LAN2
☑ LAN3
☑ LAN4
☑ Wi-Fi_2.4G

Available WAN

□ Enable Group Isolation.

4. Name the group.
5. Check the boxes of LAN1 and LAN3 in Available LAN. Here Wi-Fi 2.4G network network is viewed as a LAN interface respectively.
6. Click Enable Group Isolation to isolate working devices and disallow other devices from communicating with them.
7. Click Save to save the settings.

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

4. 3. 6. 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 192.168.0.x) to the router.

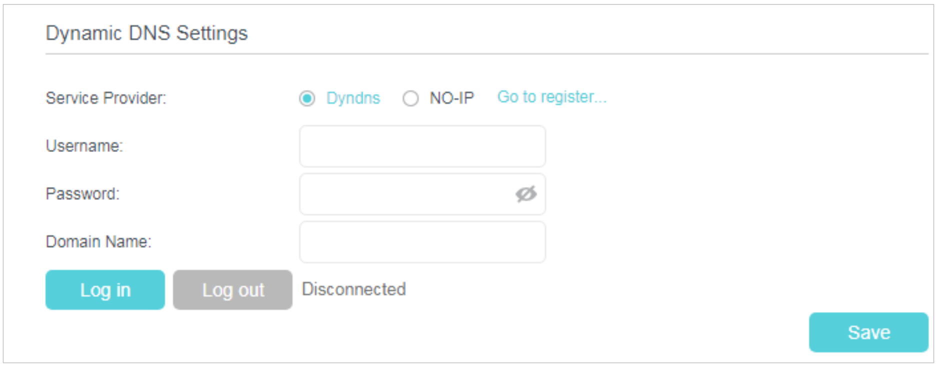
To set up DDNS, please follow the instructions below:

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

2. Go to Network > Internet > Dynamic DNS page.

3. Select the DDNS service provider (Dyndns and 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).



Dynamic DNS Settings

Service Provider: ● Dyndns ○ NO-IP Go to register...

Username:

Password:

Domain Name:

Disconnected

5. Click Log in and Save.

Tips:

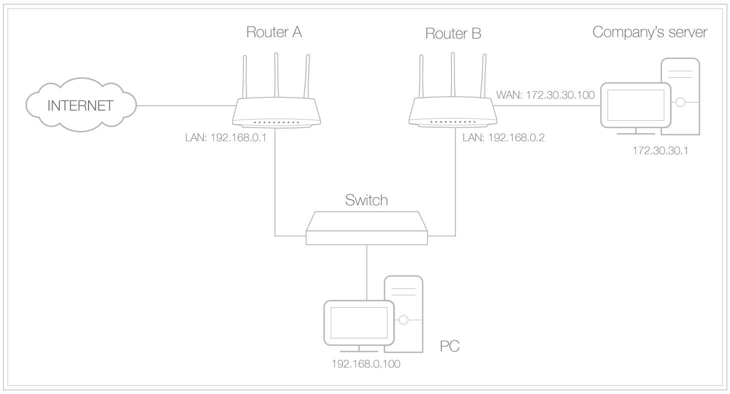
If you want to use a new DDNS account, please Logout first, then login with the new account.

4. 3. 7. 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.

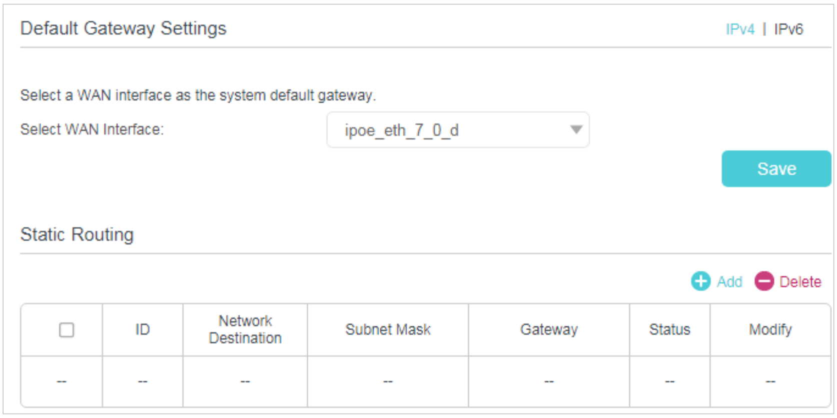
I want to: Visit multiple networks and multiple servers at the same time.

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 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. 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.
3. Go to Advanced > Network > Static Routing. Select your current WAN Interface and click Save.



Default Gateway Settings

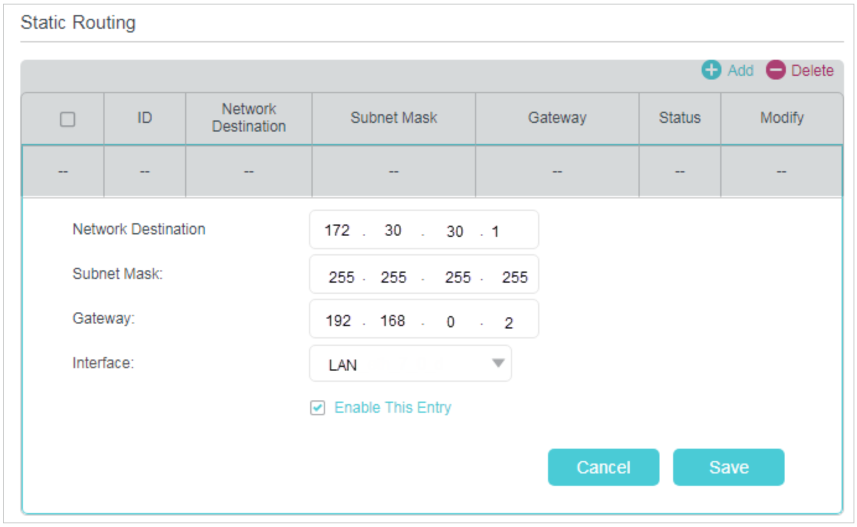
Select a WAN interface as the system default gateway.

Select WAN Interface: ipoe_eth_7_0_d

Static Routing

□	ID	Network Destination	Subnet Mask	Gateway	Status	Modify
--	--	--	--	--	--	--

4. Click Add to add a new static routing entry. Finish the settings according to the following explanations:



Static Routing

□	ID	Network Destination	Subnet Mask	Gateway	Status	Modify
--	--	--	--	--	--	--

Network Destination: 172 . 30 . 30 . 1

Subnet Mask: 255 . 255 . 255 . 255

Gateway: 192 . 168 . 0 . 2

Interface: LAN

☑ Enable This Entry

- 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.

- 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 2 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, so LAN should be selected.

5. Select the check box to enable this entry.
6. Click Save to save the settings.

Done!

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

4. 3. 8. 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 way to set up 6rd and DS-Lite tunnel are similar.

4.3.8.1. Use the Public IPv6 Tunnel Service-6to4

The 6to4 tunnel is a kind of public service. If there is any 6to4 server in 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.

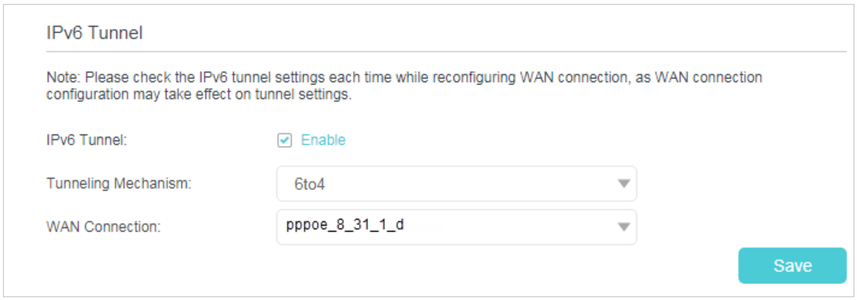
I want to:

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 Advaced > Network > IPv6 Tunnel.

3. Tick the check box, select 6to4 as the tunneling mechanism and select a WAN connection from the drop-down list, then click Save.



IPv6 Tunnel

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

IPv6 Tunnel: ☑ Enable

Tunneling Mechanism: 6to4

WAN Connection: pppoe_8_31_1_d

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.

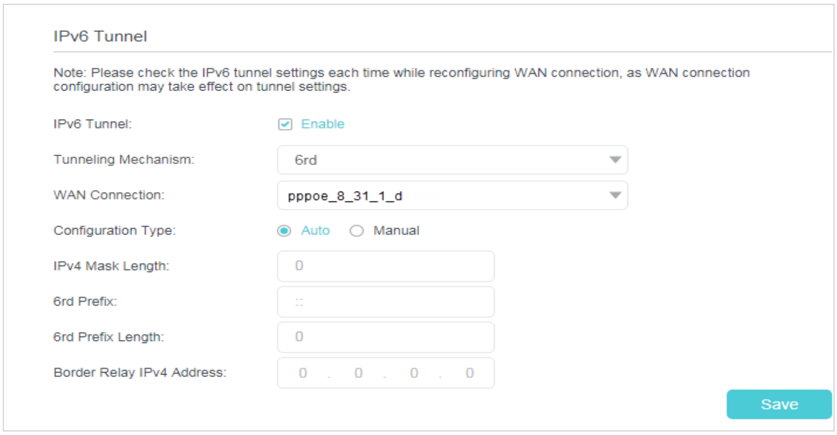
Note:

Still not being able to access IPv6 resources means that not any 6to4 public server was found in your network. You can contact your ISP to sign up for IPv6 connection service.

4.3.8.2. 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.

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advaced > Network > IPv6 Tunnel.
3. Tick the check box, 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.



IPv6 Tunnel

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

IPv6 Tunnel: ☑ Enable

Tunneling Mechanism: 6rd

WAN Connection: pppoe_8_31_1_d

Configuration Type: ● Auto ○ Manual

IPv4 Mask Length: 0

6rd Prefix: ::

6rd Prefix Length: 0

Border Relay IPv4 Address: 0 . 0 . 0 . 0

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.

Note:

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.

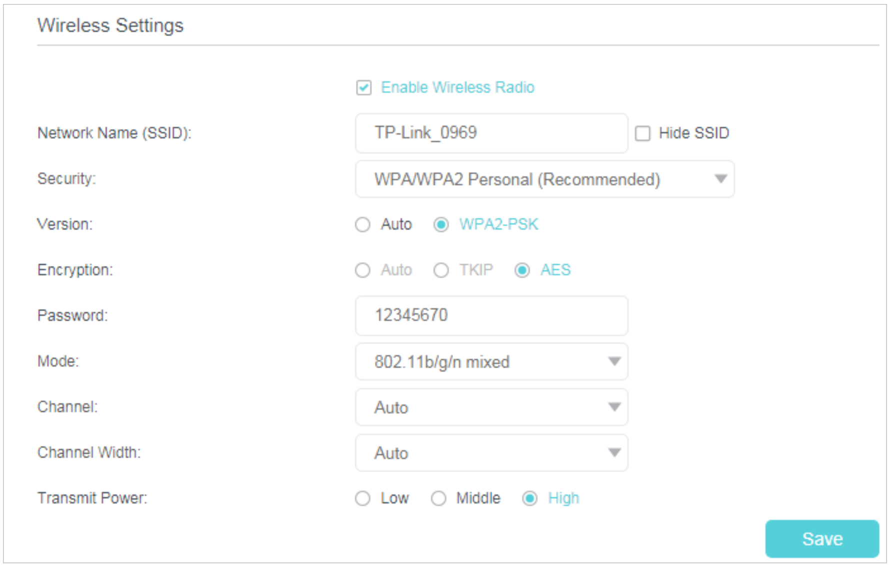
4. 4. Wireless

4. 4. 1. Wireless Settings

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

2. Go to Wireless > Wireless Settings.

3. Configure the basic settings for the wireless network and click Save.



Wireless Settings

☑ Enable Wireless Radio

Network Name (SSID): TP-Link_0969 □ Hide SSID

Security: WPA/WPA2 Personal (Recommended)

Version: ○ Auto ● WPA2-PSK

Encryption: ○ Auto ○ TKIP ● AES

Password: 12345670

Mode: 802.11b/g/n mixed

Channel: Auto

Channel Width: Auto

Transmit Power: ○ Low ○ Middle ● High

- Network Name - Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network.
- Security- Select an option from the Security drop-down list. 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.
- Version - Select Auto or WPA2-PSK.
- Encryption - Select Auto, TKIP or AES.
- Mode - Select the desired mode.
  - 802.11n only: Select only if all of your wireless clients are 802.11n devices.
  - 802.11gn mixed: Select if you are using both 802.11g and 802.11n wireless clients.
  - 802.11bgn 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 modem router. It is strongly recommended that you select 802.11bgn mixed, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the modem router.

  - 802.11ac/n mixed (5GHz): Select if you are using both 802.11ac and 802.11n wireless clients.
  - 802.11a/n/ac mixed (5GHz): Select if you are using a mix of 802.11a, 802.11n and 802.11ac wireless clients. It is strongly recommended that you select 11a/n/ac mixed.
- Channel - This field determines which operating frequency will be used. The default channel is set to Auto. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- Channel Width - 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. If you select auto, then AP will choose the best channel automatically.

4. 4. 2. WPS

WPS (Wi-Fi Protected Setup) can help you to quickly and securely connect to a network. This section will guide you to add a new wireless device to your router's network quickly via WPS.

Note:

The WPS function cannot be configured if the wireless function of the router is disabled. Please make sure the wireless function is enabled before configuration.

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

3. Follow one of the following methods to connect your client device to the router's Wi-Fi network.

Method ONE: Use the WPS Button

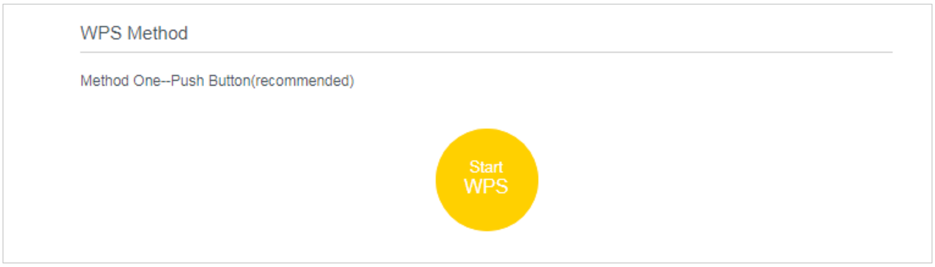
Use this method if your client device has a WPS button.

1. Press the WPS button of the modem router for 1 second.
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 modem router.

Method TWO: 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 Wireless > WPS.

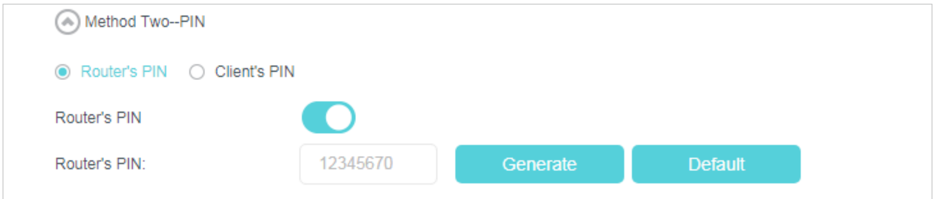


3. Click Start WPS on the page.
4. Press the WPS button of the client device directly.
5. The WPS LED of the router flashes for about 2 minutes during the WPS process.
6. When the WPS LED is on, the client device has successfully connected to the router.

Method Three: 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 page. Click Method Two--PIN.



● Router's PIN ○ Client's PIN

Router's PIN: on

Router's PIN: 12345670

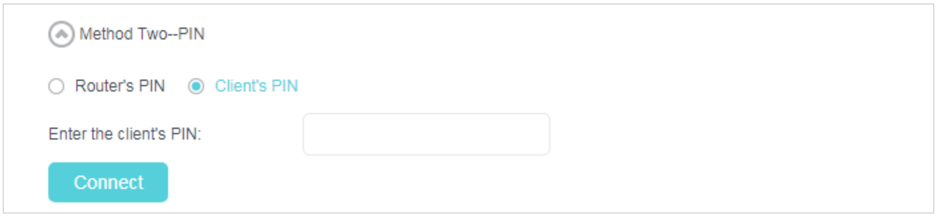
3. Take a note of the Current PIN of the router. You can also click the Generate button to get a new PIN.
4. On the client device, enter the router's PIN. (The default PIN is also printed on the label of the router.)
5. The WPS LED flashes for about two minutes during the WPS process.
6. When the WPS 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 modem router is disabled. Please make sure the wireless function is enabled before configuring the WPS.

Method Four: 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 page. Click Method Two--PIN.



Method Two--PIN

○ Router's PIN ● Client's PIN

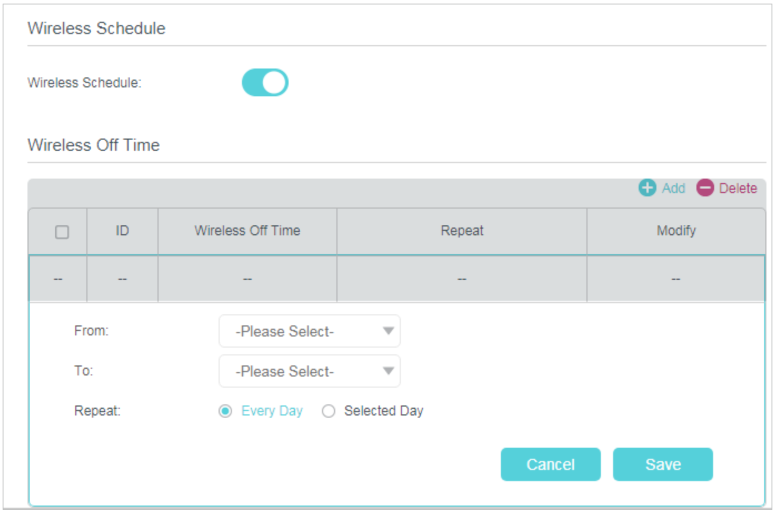
Enter the client's PIN:

3. Select Client's PIN.
4. Enter the client device's PIN in the field. Then click the Connect button.
5. Connect successfully will appear on the above screen, which means the client device has successfully connected to the router.

4. 4. 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 page.
3. Toggle on the button to enable the Wireless Schedule feature.



Wireless Schedule

Wireless Schedule: ●

Wireless Off Time

□	ID	Wireless Off Time	Repeat	Modify
--	--	--	--	--

From: -Please Select-

To: -Please Select-

Repeat: ● Every Day ○ Selected Day

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

5. Repeat steps 3 and 4 to set another entry.

Note:

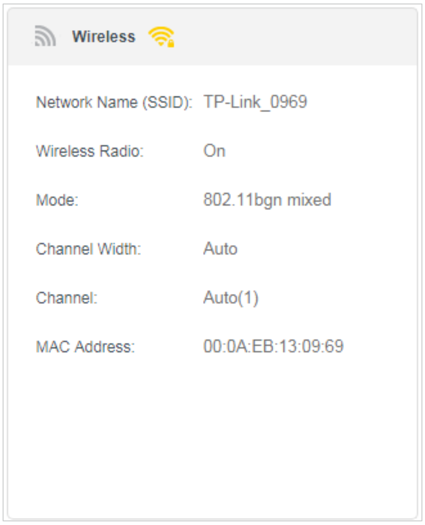
1. Make sure that the time of the router is correct before using this function.
2. If you just set time for one wireless band, the other wireless band is still always on, so set time for both of the two bands to schedule your whole wireless network.
3. The wireless LED (2.4GHz , 5GHz) will turn off if the corresponding wireless network is disabled.
4. The wireless network will be automatically turned on after the time period you set.

4. 4. 4. View Wireless Information

► **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 > Status page.



Wireless

Network Name (SSID): TP-Link_0969

Wireless Radio: On

Mode: 802.11bgn mixed

Channel Width: Auto

Channel: Auto(1)

MAC Address: 00:0A:EB:13:09:69

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:**

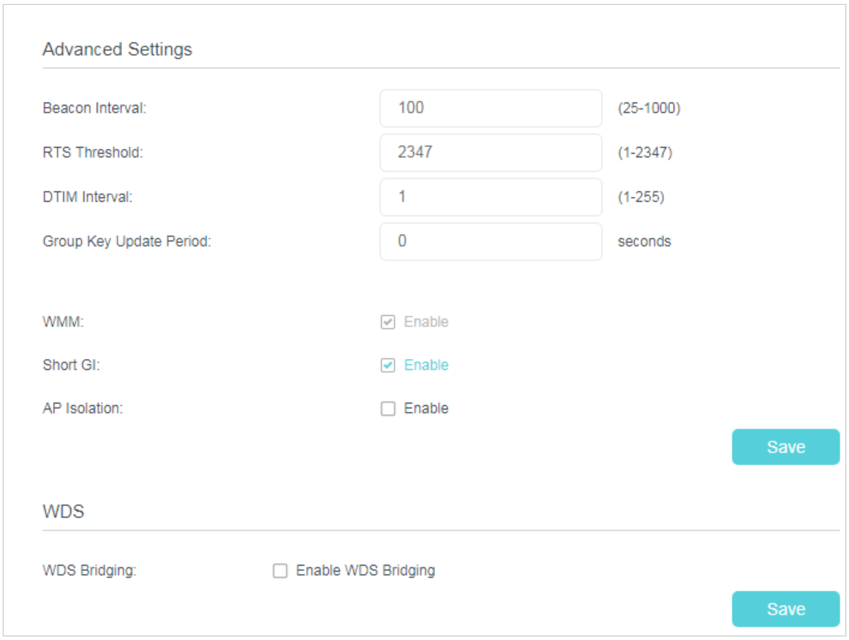
1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Wireless > Statistics page.
3. You can view the detailed information of the wireless clients, including its connected wireless band and security option as well as the packets transmitted.

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

4. 4. 5. Advanced Wireless Settings

Advanced wireless settings are for those who have a network concept. 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.

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



Advanced Settings

Beacon Interval: 100 (25-1000)
RTS Threshold: 2347 (1-2347)
DTIM Interval: 1 (1-255)
Group Key Update Period: 0 seconds

WMM: ☑ Enable
Short GI: ☑ Enable
AP Isolation: □ Enable

WDS

WDS Bridging: □ Enable WDS Bridging

- Beacon Interval: Enter a value between 25 and 1000 in milliseconds to determine the duration between which beacon packets are broadcasted 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. It is strongly recommended to enable WMM.
- Short GI: This feature is enabled by default and recommended to increase the data capacity by reducing the Guard Interval (GI) time.
- AP Isolation: Select this check box to enable the AP Isolation feature that allows you to confine and restrict all wireless devices on your network from interacting with each other, but still able to access the Internet. AP isolation is disabled by default.
- WDS Bridging: Select this check box to enable the WDS (Wireless Distribution System) Bridging feature to allow the router to bridge with another access point (AP) in a wireless local area network (WLAN).

4. 5. NAT Forwarding

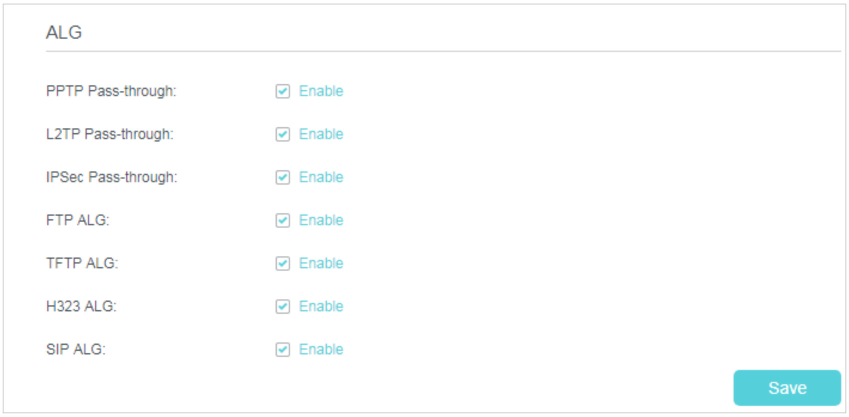
The router's NAT (Network Address Translation) feature makes the devices on the LAN use the same public IP address to communicate on the internet, which protects the local network by hiding IP addresses of the devices. However, it also brings about the problem that external hosts cannot initiatively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

With the forwarding feature, the router can traverse the isolation of NAT so that clients on the internet can reach devices on the LAN and realize some specific functions.

The 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.

4. 5. 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, H323 etc. Enabling ALG is recommended.



ALG

PPTP Pass-through: ☑ Enable

L2TP Pass-through: ☑ Enable

IPSec Pass-through: ☑ Enable

FTP ALG: ☑ Enable

TFTP ALG: ☑ Enable

H323 ALG: ☑ Enable

SIP ALG: ☑ Enable

- 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.
- 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.

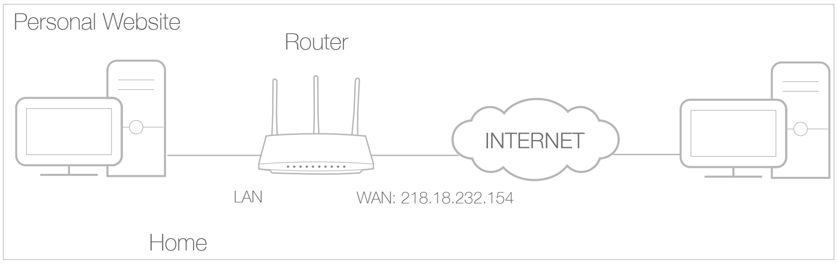
4. 5. 2. Share Local Resources on the Internet by Virtual Servers

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.

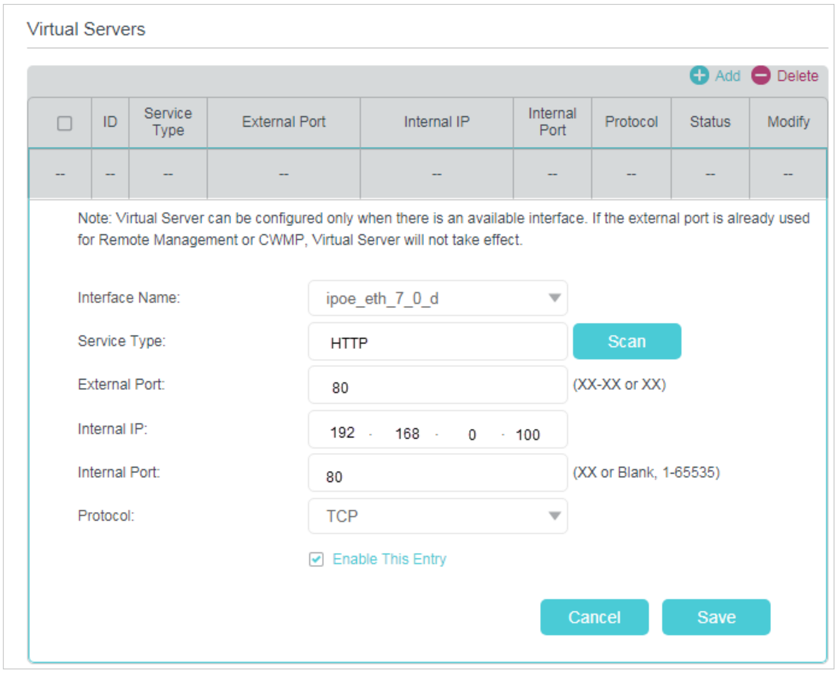
I want to: Share my personal website I've built in local network with my friends through the internet.

For example, the personal website has been built on my home PC (192.168.0.100). I hope that my friends 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 192.168.0.100.
2. Visit http://tplinkwifi.net, and log in with the password you set for the router.
3. Go to Advaced > NAT Fowarding > Virtual Servers.
4. Click Add. Click Scan and choose 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.



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

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

Interface Name: ipoe_eth_7_0_d

Service Type: HTTP Scan

External Port: 80 (XX-XX or XX)

Internal IP: 192 . 168 . 0 . 100

Internal Port: 80 (XX or Blank, 1-65535)

Protocol: TCP

☑ Enable This Entry

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:

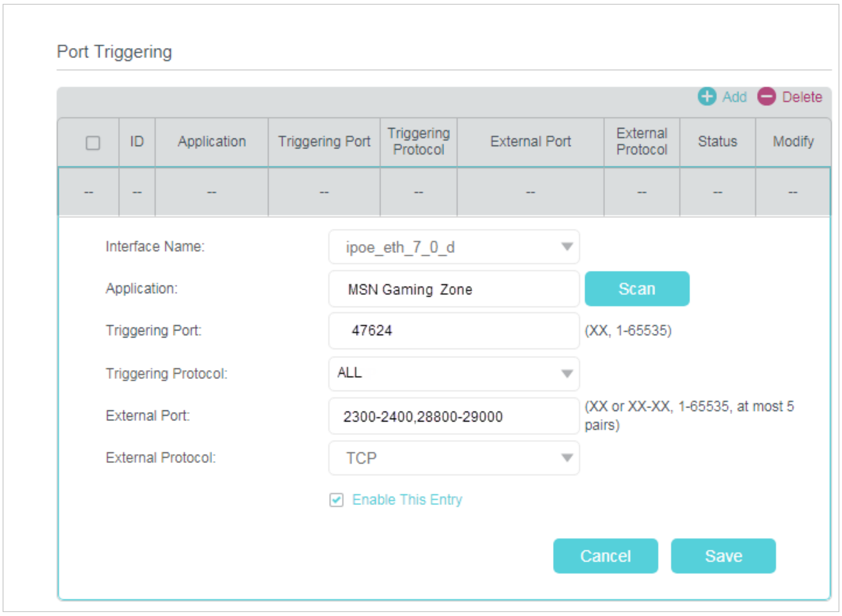
- The WAN IP should be a public IP address. For the WAN IP is assigned dynamically by the ISP, it is recommended to apply and register a domain name for the WAN . Then users on the internet can use http:// domain name to visit the website.
- If you have changed the default External Port, you should use http:// WAN IP: External Port or http:// domain name: External Port to visit the website.

4. 5. 3. 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 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, Quick Time 4 players and more.

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 > 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 with contents . The following picture takes application MSN Gaming Zone as an example.
4. Click Save.



Port Triggering

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

Interface Name:	ipoe_eth_7_0_d	
Application:	MSN Gaming Zone	Scan
Triggering Port:	47624	(XX, 1-65535)
Triggering Protocol:	ALL	
External Port:	2300-2400,28800-29000	(XX or XX-XX, 1-65535, at most 5 pairs)
External Protocol:	TCP	

☑ Enable This Entry

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.

4. 5. 4. 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, such as IP camera and database software, you can set the PC to be a DMZ host.

Note:

DMZ is more applicable in the situation that users are not clear about 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:

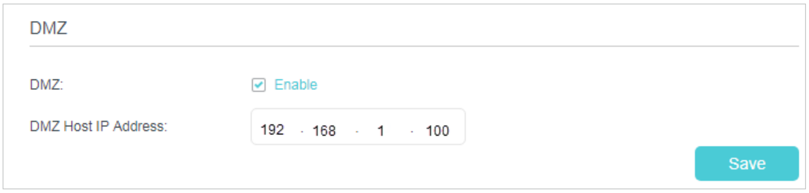
Make the home PC join the internet online game without port restriction.

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 host 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 the router.
3. Go to Forwarding > DMZ.
4. Select Enable and enter the IP address 192.168.0.100 in the DMZ Host IP Address filed.



DMZ

DMZ: ☑ Enable

DMZ Host IP Address: 192 . 168 . 1 . 100

5. Click Save.

Done! You've set your PC to a DMZ host and now you can make a team to game with other players.

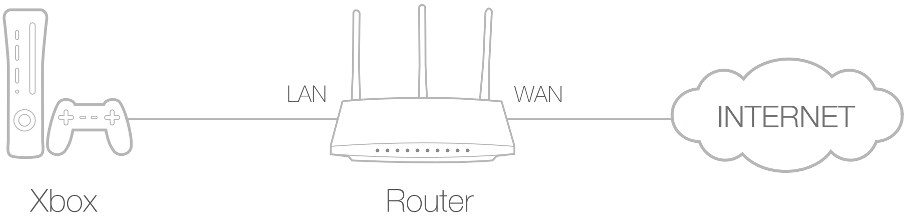
4. 5. 5. UPnP

The 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 on the local network and the internet can freely communicate with each other 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 is 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.

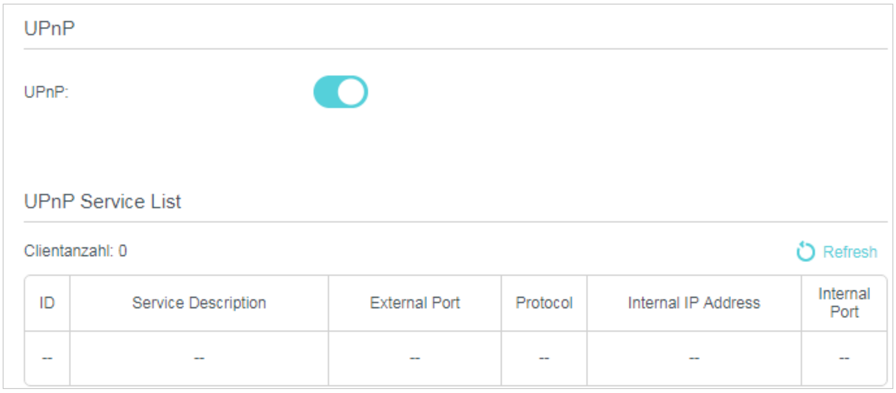


If necessary, you can follow the steps to change the status of UPnP.

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

2. Go to Forwarding > UPnP.

3. Go to Advanced > NAT Forwarding > UPnP and toggle on or off according to your needs..



UPnP

UPnP: ●

UPnP Service List

Clientanzahl: 0

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

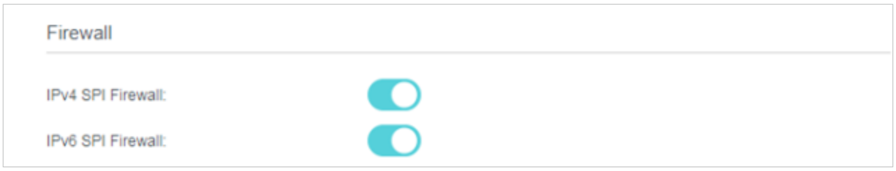
4. 6. Security

This function allows you to protect your home network from cyber attacks and unauthorized users by implementing these network security functions.

4. 6. 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's recommended to keep the default settings.



Firewall

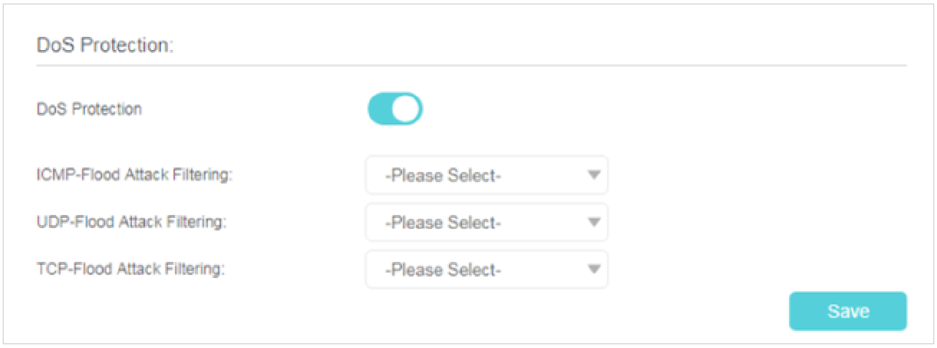
IPv4 SPI Firewall: ●

IPv6 SPI Firewall: ●

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.



DoS Protection:

DoS Protection	●
ICMP-Flood Attack Filtering:	-Please Select-
UDP-Flood Attack Filtering:	-Please Select-
TCP-Flood Attack Filtering:	-Please Select-

3. Enable DoS Protection.

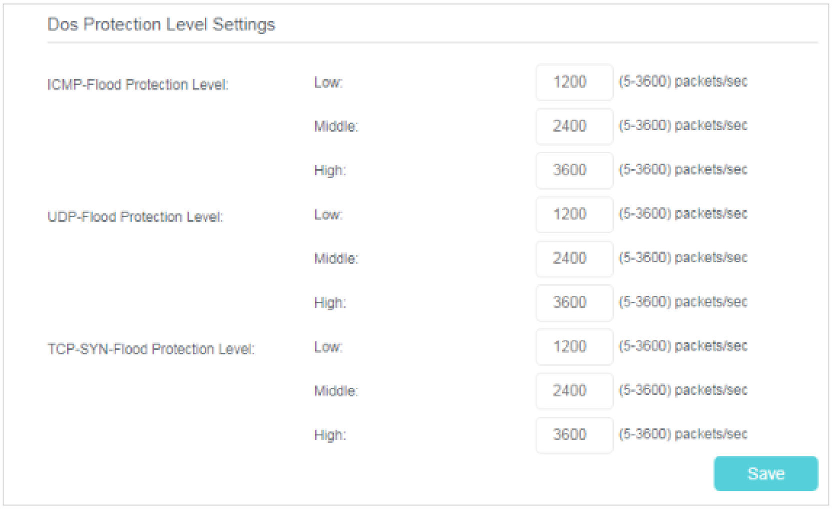
4. Set the level (Low, Middle or High) of protection for ICMP-FLOOD Attack Filtering, UDP-FlOOD Attack Filtering and TCP-FLOOD Attack Filtering.

   - 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:

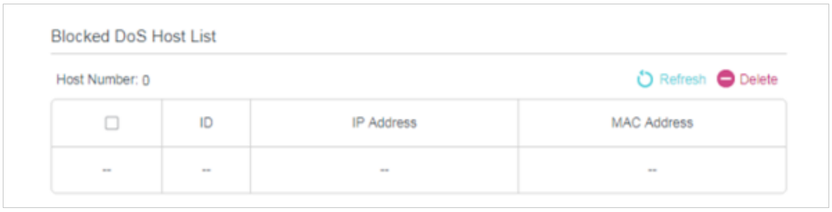
1. The level of protection is based on the number of traffic packets. Specify the level at DoS Protection Level Settings.



Dos Protection Level Settings

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

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



Blocked DoS Host List

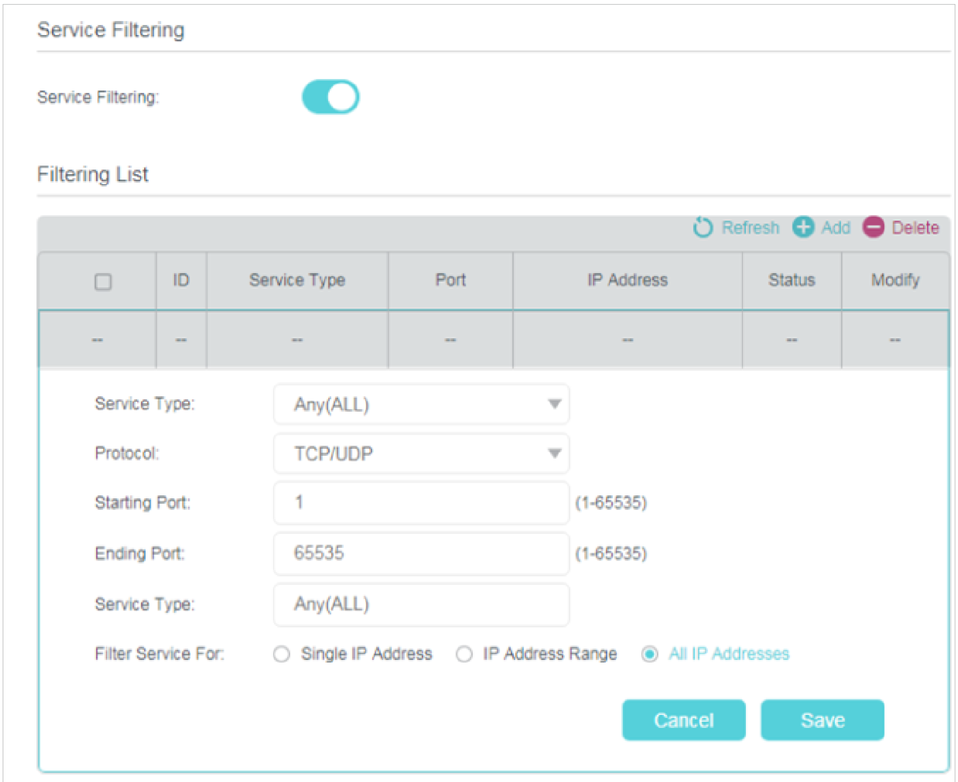
Host Number: 0

□	ID	IP Address	MAC Address
--	--	--	--

4. 6. 2. Service Filtering

With Service Filtering, you can prevent certain users from accessing the specified service, 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.
3. Toggle On Service Filtering.
4. Click Add.



Service Filtering

Service Filtering: On

Filtering List

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

Service Type:	Any(ALL)	
Protocol:	TCP/UDP	
Starting Port:	1	(1-65535)
Ending Port:	65535	(1-65535)
Service Type:	Any(ALL)	
Filter Service For:	○ Single IP Address ○ IP Address Range ● All IP Addresses	

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

Note:

If you want to disable this entry, click the Bulb icon .

4. 6. 3. Access Control

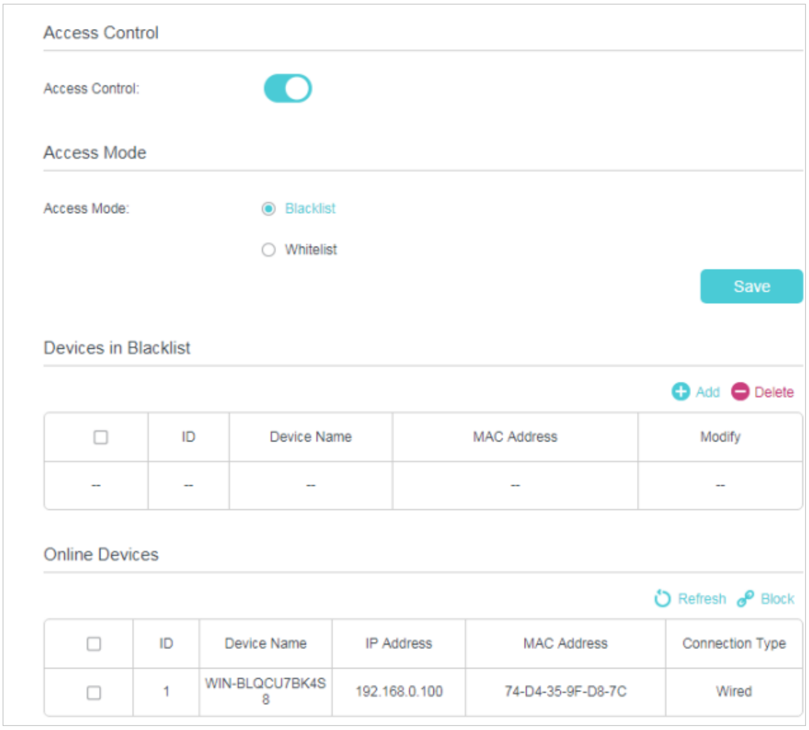
Access Control is used to block or allow specific client devices to access your network (via wired or wireless) based on a list of blocked devices (Blacklist) or a list of allowed devices (Whitelist).

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.



Access Control

Access Control: ●

Access Mode

Access Mode: ● Blacklist
○ Whitelist

Devices in Blacklist

□	ID	Device Name	MAC Address	Modify
--	--	--	--	--

Online Devices

□	ID	Device Name	IP Address	MAC Address	Connection Type
□	1	WIN-BLQCU7BK4S8	192.168.0.100	74-D4-35-9F-D8-7C	Wired

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

   To block specific device(s)

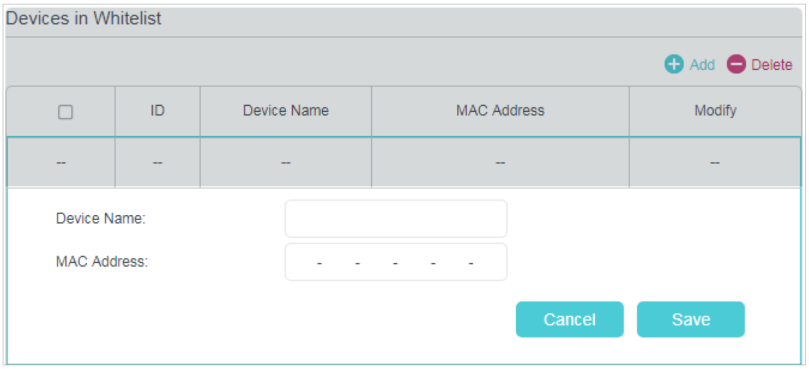
1) Select Blacklist and click Save.
2) Select the device(s) to be blocked in the Online Devices table.

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.



Devices in Whitelist

□	ID	Device Name	MAC Address	Modify
--	--	--	--	--

Device Name:

MAC Address: - - - - -

3) Enter the Device Name and MAC Address (You can copy and paste the information from Devices Online 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) using the Blacklist or Whitelist.

4. 6. 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.

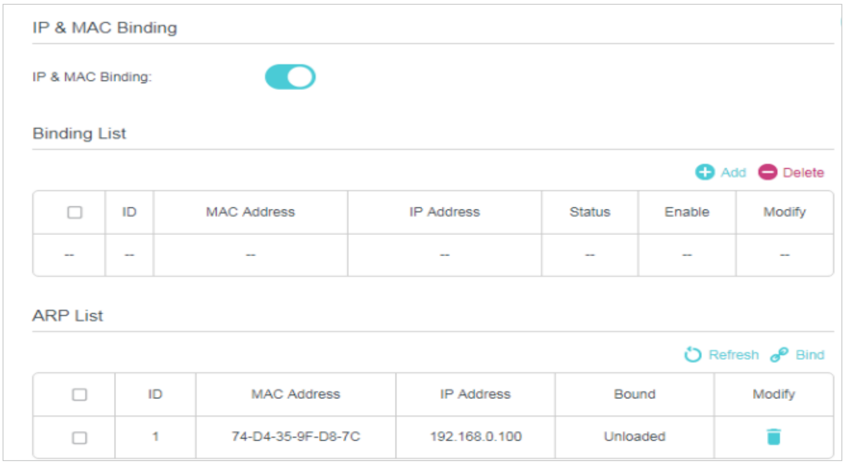
I want to:

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 and enable IP & MAC Binding.



IP & MAC Binding

IP & MAC Binding: ●

Binding List

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

ARP List

□	ID	MAC Address	IP Address	Bound	Modify
□	1	74-D4-35-9F-D8-7C	192.168.0.100	Unloaded	🗑

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

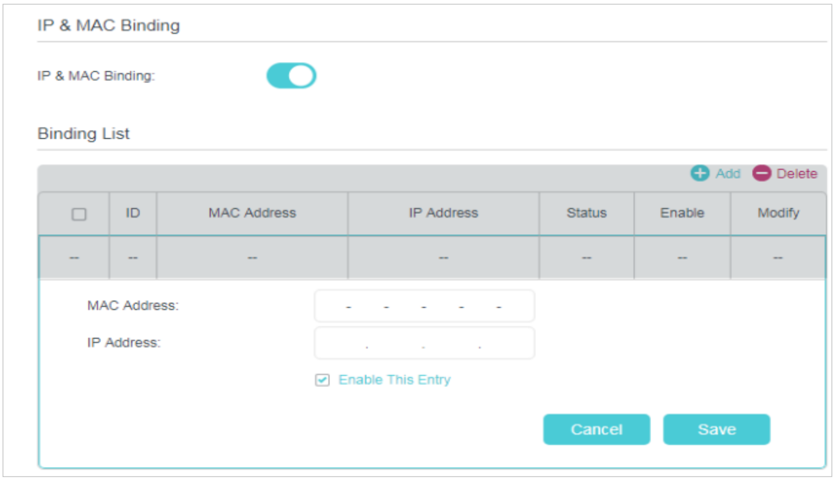
To bind the connected device(s)

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

2) Click Bind to add to the Binding List.

To bind the unconnected device

1) Click Add.



IP & MAC Binding

IP & MAC Binding: ●

Binding List

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

MAC Address: - - - - -

IP Address: . . .

☑ Enable This Entry

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

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

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

4. 7. Parental Controls

Parental Controls allows you to block inappropriate and malicious websites, and control access to specific websites at specific time for your children's devices.

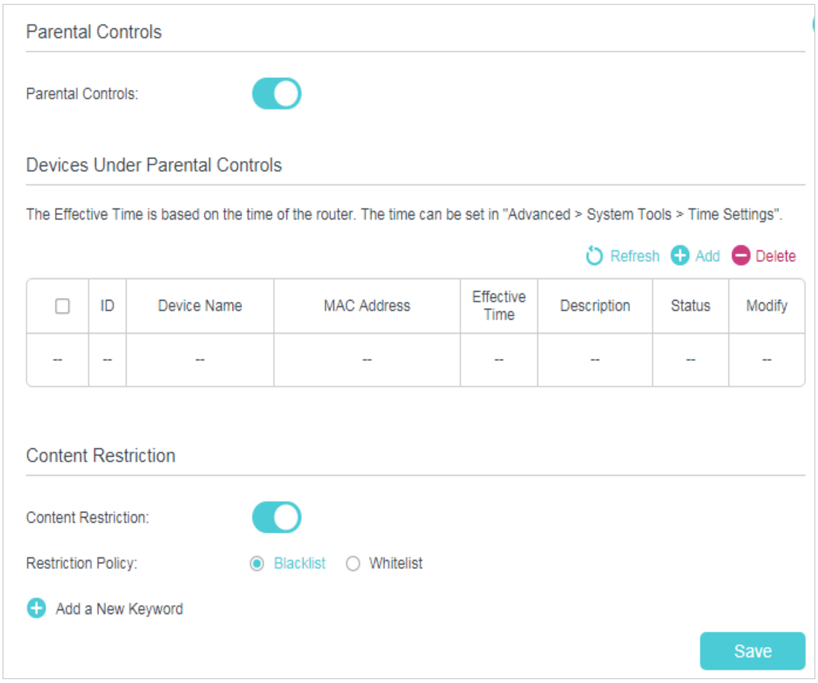
I want to:

Control what types of websites my children or other home network users can visit and even 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 (6PM) to 22:00 (10PM) on 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 orAdvanced > Parental Controls and enable Parental Controls.



Parental Controls

Parental Controls: ●

Devices Under Parental Controls

The Effective Time is based on the time of the router. The time can be set in "Advanced > System Tools > Time Settings".

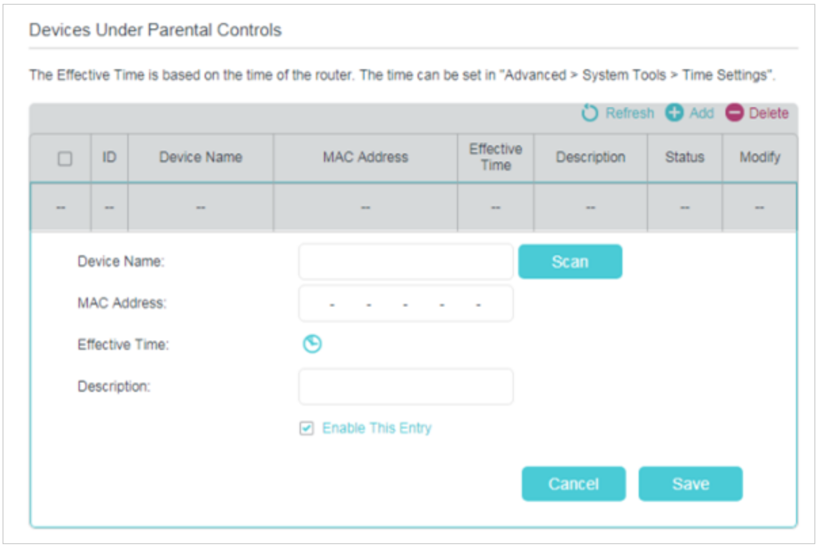
□	ID	Device Name	MAC Address	Effective Time	Description	Status	Modify
--	--	--	--	--	--	--	--

Content Restriction

Content Restriction: ●

Restriction Policy: ● Blacklist ○ Whitelist

3. Click Add.



Devices Under Parental Controls

The Effective Time is based on the time of the router. The time can be set in "Advanced > System Tools > Time Settings".

☐	ID	Device Name	MAC Address	Effective Time	Description	Status	Modify
--	--	--	--	--	--	--	--

Device Name:

MAC Address: - - - - -

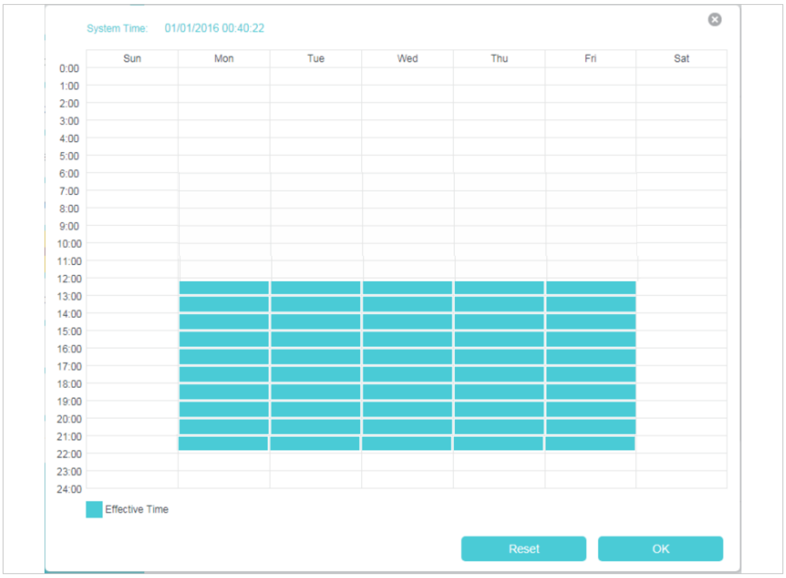
Effective Time:

Description:

☑ Enable This Entry

4. Click Scan, and add the device to be controlled. Or, enter the Device Name and MAC Address manually.

5. Click the icon to set the Effctive Time. Drag the cursor over the appropriate cell(s) and click Save.



System Time: 01/01/2016 00:40:22

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
0:00							
1:00							
2:00							
3:00							
4:00							
5:00							
6:00							
7:00							
8:00							
9:00							
10:00							
11:00							
12:00		🟦	🟦	🟦	🟦	🟦	
13:00		🟦	🟦	🟦	🟦	🟦	
14:00		🟦	🟦	🟦	🟦	🟦	
15:00		🟦	🟦	🟦	🟦	🟦	
16:00		🟦	🟦	🟦	🟦	🟦	
17:00		🟦	🟦	🟦	🟦	🟦	
18:00		🟦	🟦	🟦	🟦	🟦	
19:00		🟦	🟦	🟦	🟦	🟦	
20:00		🟦	🟦	🟦	🟦	🟦	
21:00		🟦	🟦	🟦	🟦	🟦	
22:00							
23:00							
24:00							

🟦 Effective Time

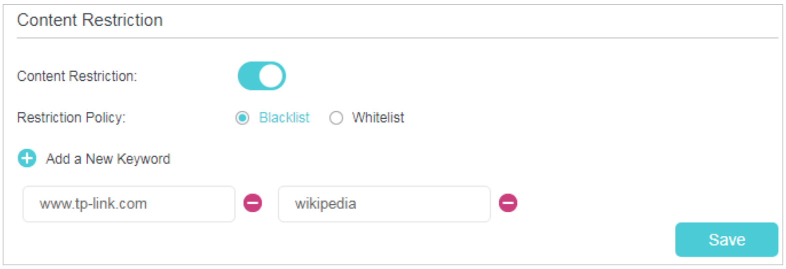
6. Enter a Description for the entry.

7. Select the checkbox to enable this entry and click Save.

8. Enable Content Restriction and select the restriction mode.

1) In Blacklist mode, the controlled devices cannot access any websites containing the specified keywords during the Internet Access Time period.

2) In Whitelist mode, the controlled devices can only access websites containing the specified keywords during the Effective Time period.



Content Restriction

Content Restriction: ●

Restriction Policy: ● Blacklist ○ Whitelist

Add a New Keyword

www.tp-link.com

wikipedia

9. Click Add a New Keyword. You can add many keywords for both Blacklist and Whitelist. Below are some sample entries to allow access.

1) Enter a web address (e.g. www.tp-link.com) or a web address keyword (e.g. wikipedia) to only allow or block access to the websites containing that keyword.

2) Specify the domain suffix (eg. .edu or .org) to allow access only to the websites with that suffix.

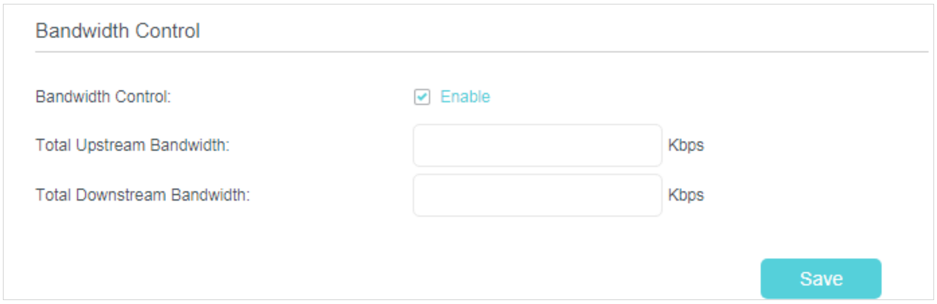
10. Enter the keywords or websites you want to add and click Save.

Done! Now you can control your children's Internet access according to your needs.

4. 8. Bandwidth Control

4. 8. 1. Configure the Bandwidth Control

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.



Bandwidth Control

Bandwidth Control: ☑ Enable

Total Upstream Bandwidth: Kbps

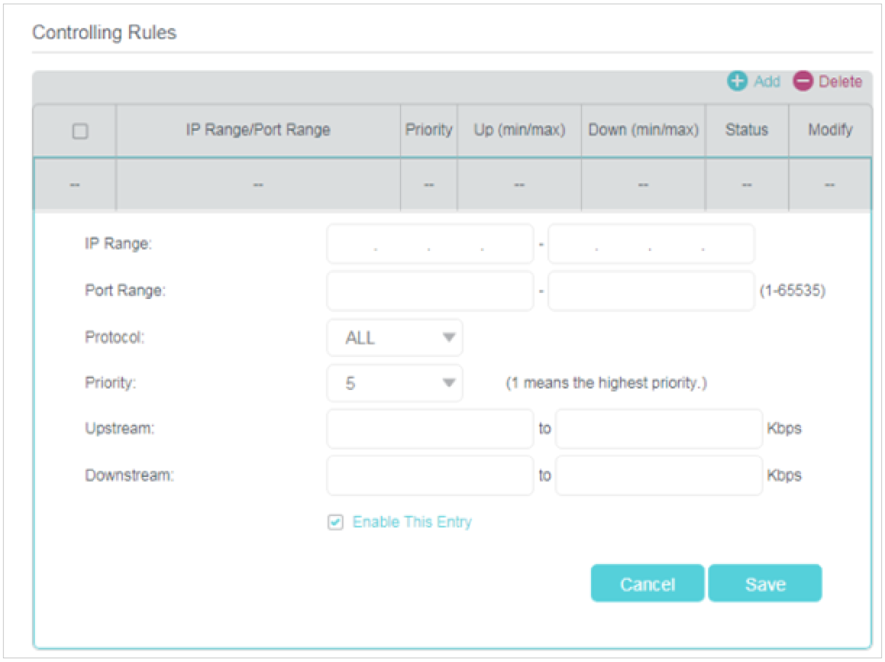
Total Downstream Bandwidth: Kbps

4. Click Save.

4. 8. 2. Controlling rules

1. Click Add to add a new rule for the Bandwidth Control.

2. Enter the information as the figure shown below.



Controlling Rules

□	IP Range/Port Range	Priority	Up (min/max)	Down (min/max)	Status	Modify
--	--	--	--	--	--	--

IP Range: . . . - . . .

Port Range: - (1-65535)

Protocol: ALL

Priority: 5 (1 means the highest priority.)

Upstream: to Kbps

Downstream: to Kbps

☑ Enable This Entry

- IP Range - Interior PC address range. If both are blank or 0.0.0.0, the domain is noneffective.
- Port Range - The port range which the Interior PC access the outside PC. If all are blank or 0, the domain is noneffective.
- Protocol - Transport layer protocol, here there are ALL, TCP, UDP.
- Priority - Priority of Bandwidth Control rules. ‘1’ stands for the highest priority while ‘8’ stands for the lowest priority. The total Upstream/ Downstream Bandwidth is first allocated to guarantee all the Min Rate of Bandwidth Control rules. If there is any bandwidth left, it is first allocated to the rule with the highest priority, then to the rule with the second highest priority, and so on.

- Upstream - The max and the min upload speed which through the WAN port.
- Downstream - The max and the min download speed through the WAN port.

3. Select Enable This Entry.
4. Click Save.

4. 9. VPN Server

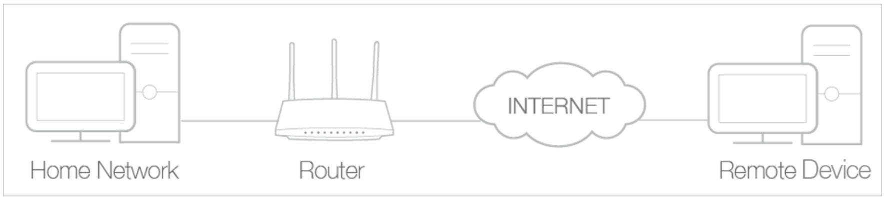
The VPN (Virtual Private Networking) Server allows you to access your home network in a secured way through internet when you are out of home. The router offers two ways to set up VPN connection: OpenVPN and PPTP (Point to Point Tunneling Protocol) VPN.

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.

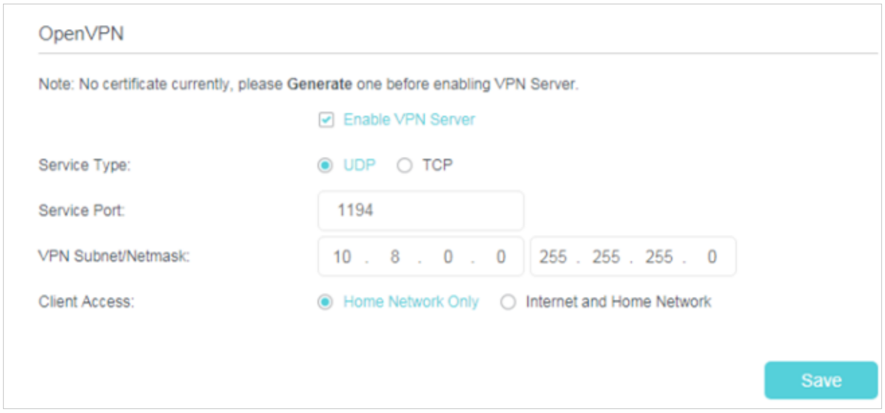
4. 9. 1. Use Open VPN to Access Your Home Network

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.



OpenVPN

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

☑ Enable VPN Server

Service Type: ● UDP ○ TCP

Service Port: 1194

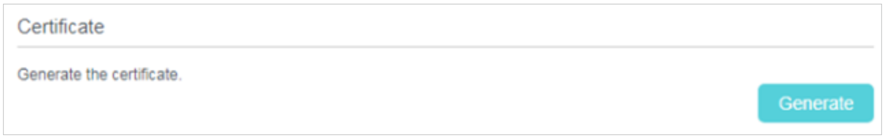
VPN Subnet/Netmask: 10 . 8 . 0 . 0 255 . 255 . 255 . 0

Client Access: ● Home Network Only ○ Internet and Home Network

Note:

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

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



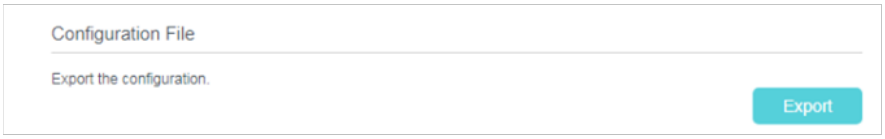
Certificate

Generate the certificate.

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.



Configuration File

Export the configuration.

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 funxtion to access your router. Mobile devices should download a third-party app from Google Play or Apple App Store.

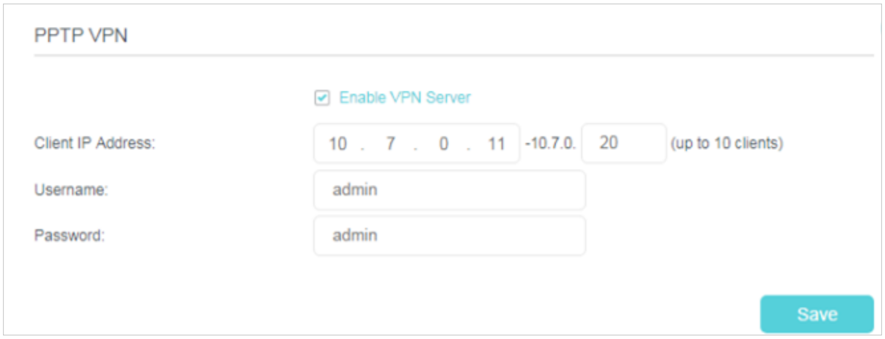
2. After the installation, copy the file exported from your router to the OpenVPN client utility's "config" folder (for example, C:\Program Files\OpenVPN\config on Windows). The path depends on where the OpenVPN client utility is installed.
3. Run the OpenVPN client utility and connect it to OpenVPN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

4. 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 > PPTP VPN, and select Enable VPN Server.



PPTP VPN

☑ Enable VPN Server

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

Username: admin

Password: admin

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.

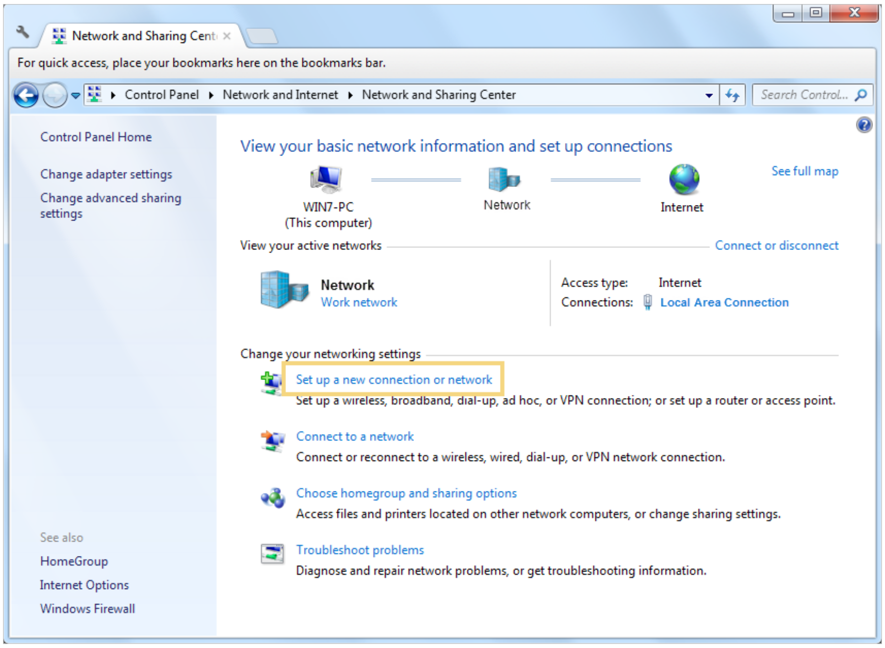
3. In the Client IP Address filed, enter the range of IP addresses (up to 10) that can be leased to the devices by the PPTP VPN server.
4. Enter Username and Password to authenticate clients to the PPTP VPN server.
5. Click Save.

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.



Network and Sharing Cent ×
For quick access, place your bookmarks here on the bookmarks bar.
Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search Control...
Control Panel Home
Change adapter settings
Change advanced sharing settings
See also
HomeGroup
Internet Options
Windows Firewall
WIN7-PC
(This computer)
Network
Internet
See full map
Connect or disconnect

View your basic network information and set up connections

View your active networks

Network
Work network

Access type: Internet
Connections: Local Area Connection

Change your networking settings

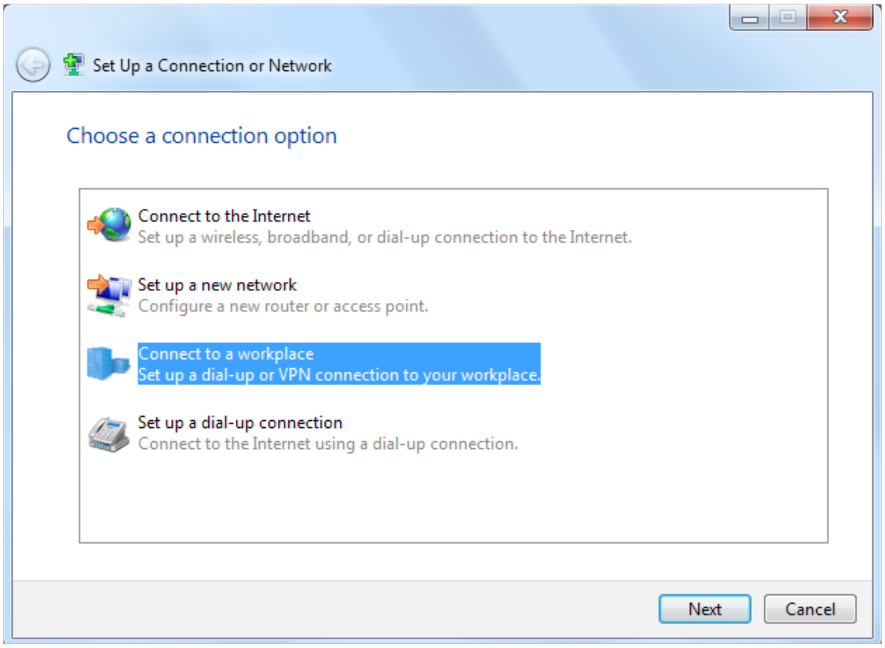
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

3. Select Connect to a workplace and click Next.



Set Up a Connection or Network

Choose a connection option

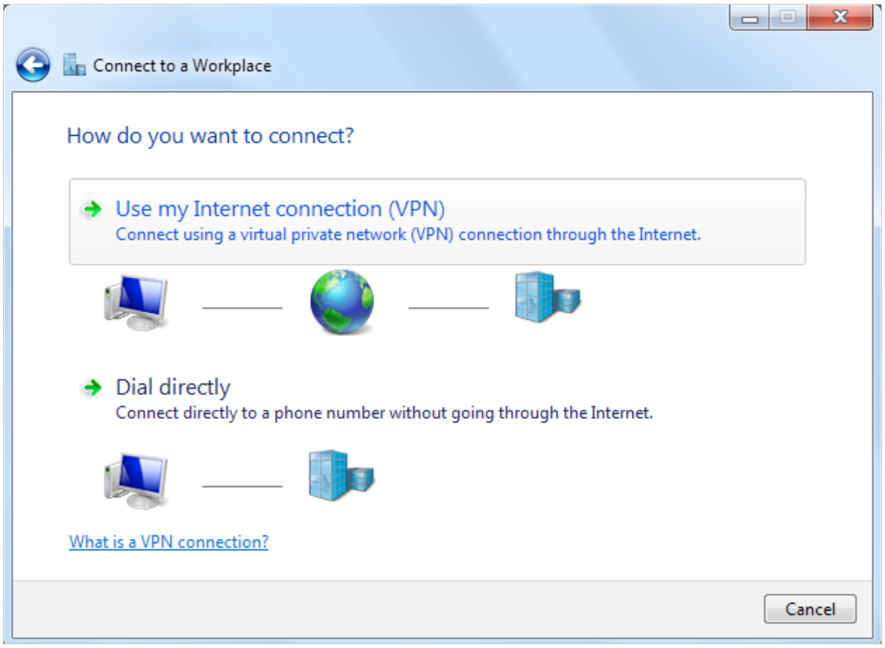
Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.

Set up a new network
Configure a new router or access point.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Set up a dial-up connection
Connect to the Internet using a dial-up connection.

4. Select Use my Internet connection (VPN).



Connect to a Workplace

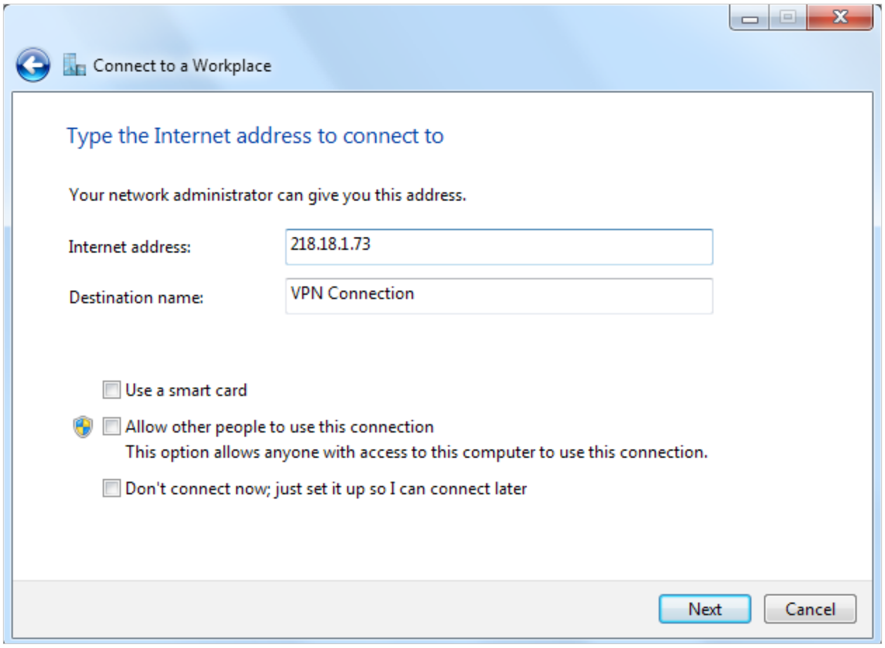
How do you want to connect?

→ Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

→ Dial directly
Connect directly to a phone number without going through the Internet.

What is a VPN connection?

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



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 218.18.1.73

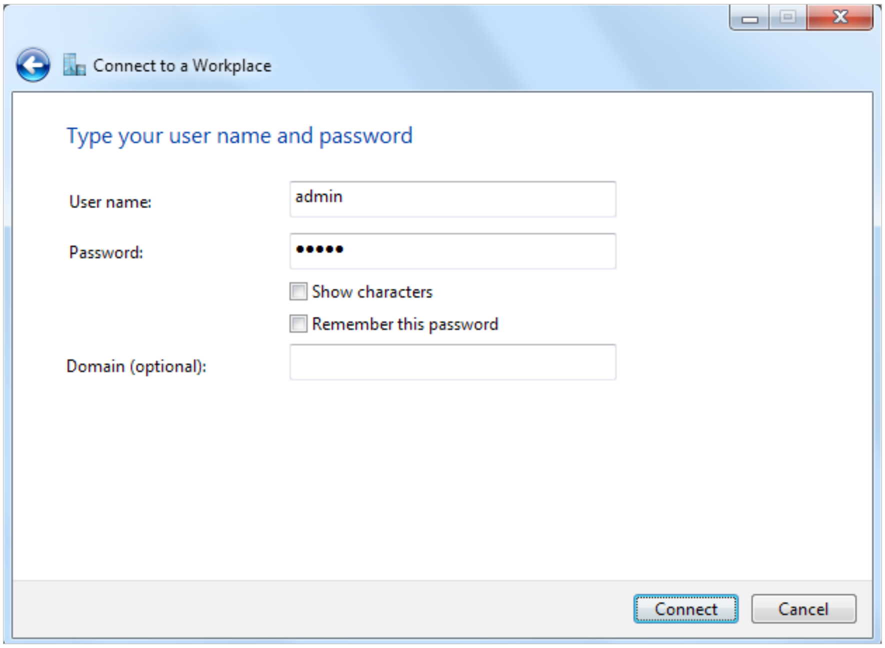
Destination name: VPN Connection

□ Use a smart card

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

□ Don't connect now; just set it up so I can connect later

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



Type your user name and password

User name: admin

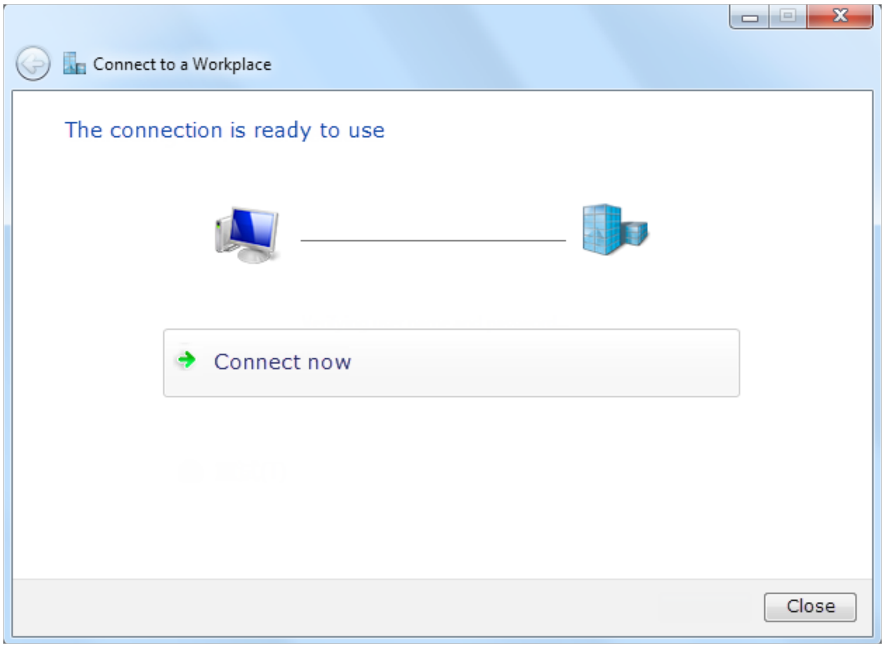
Password: •••••

□ Show characters

□ Remember this password

Domain (optional):

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



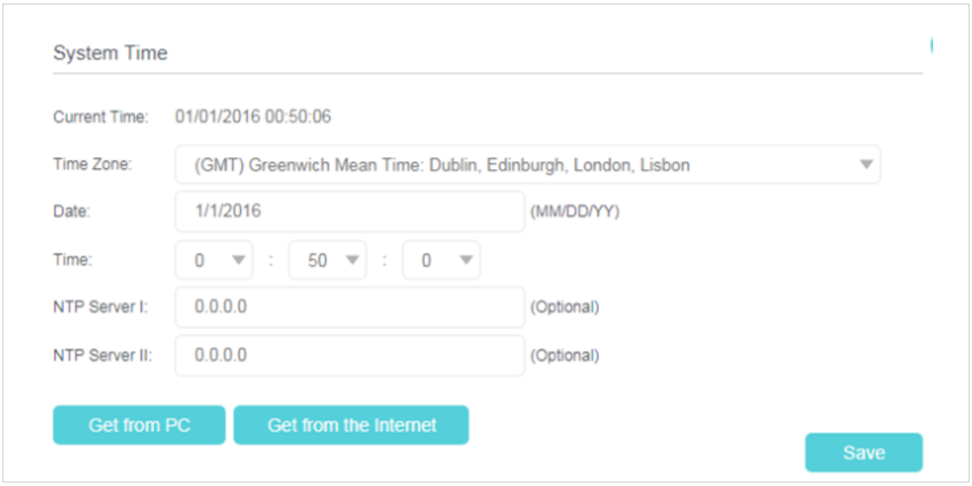
The connection is ready to use

4. 10. System Tools

4. 10. 1. Time Settings

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. You can choose the way to obtain the system time as needed.

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



System Time

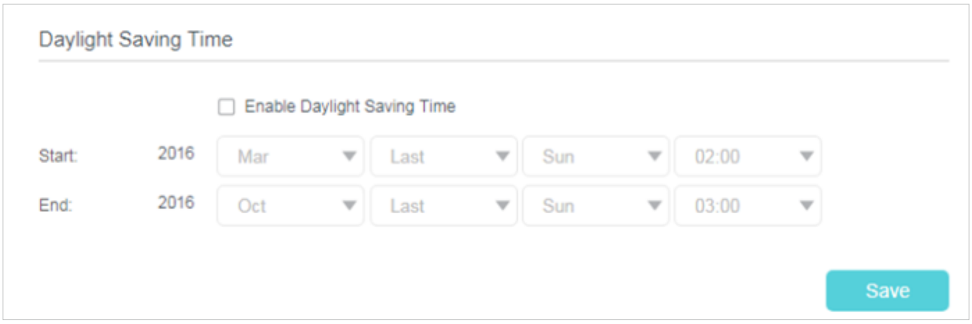
Current Time:	01/01/2016 00:50:06	
Time Zone:	(GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon	
Date:	1/1/2016	(MM/DD/YY)
Time:	0 : 50 : 0	
NTP Server I:	0.0.0.0	(Optional)
NTP Server II:	0.0.0.0	(Optional)

3. Configure the system time using the following methods:

   Manually: Select your time zone and enter your local time.

   Get from PC: Click this button if you want to use the current managing PC's time.

   Get from the Internet: Click this button if you want to get time from the Internet. Make sure your modem 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. Tick the checkbox to enable Daylight Saving Time, set the start and end time and then click Save to make the settings effective.



Daylight Saving Time

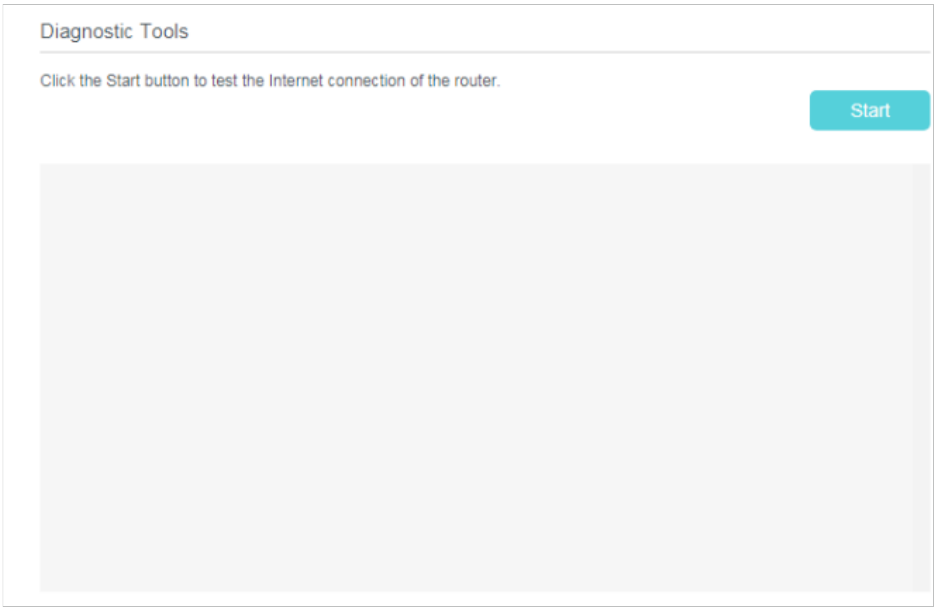
□ Enable Daylight Saving Time

Start:	2016	Mar	Last	Sun	02:00
End:	2016	Oct	Last	Sun	03:00

4. 10. 2. Diagnostic

Diagnostic 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 System Tools > Diagnostic.



Diagnostic Tools

Click the Start button to test the Internet connection of the router.

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

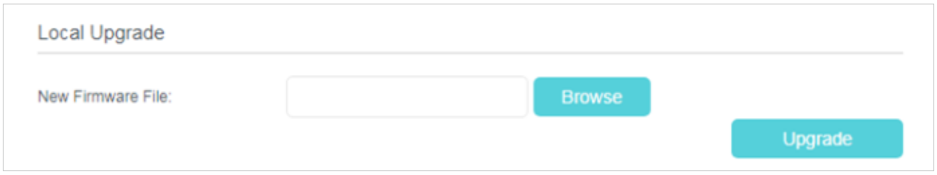
4. 10. 3. Firmware Upgrade

TP-Link is dedicated to improving and richening the product features, giving users a better network experience. We will release the latest firmware at TP-Link official website www.tp-link.com. You can download the lastest firmware file from the Support page of our website and upgrade the firmware to the latest version.

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. Make sure you remove any USB storage device connected to the router before the firmware upgrade to prevent data loss.
3. Back up your router configuration before upgrading the firmware.
4. Do NOT turn off the router during the firmware upgrade.

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.



Local Upgrade

New Firmware File:

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

4. 10. 4. Back up and Restore Configuration Settings

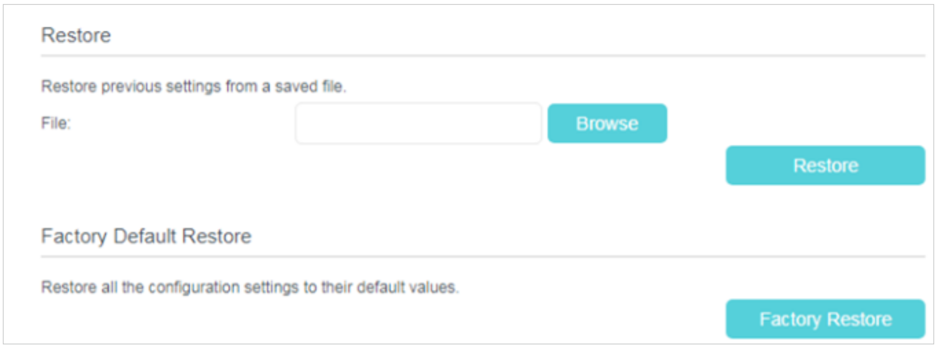
The configuration settings are stored as a configuration file in the router. You can back up the configuration file to your computer for future use and restore the router to a previous settings from the backup file when needed. Moreover, if needed you can erase the current settings and reset the modem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

▶ **To back up configuration settings**

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Click Advanced > System Tools > Backup & Restore page.
3. 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. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Click Advanced > System Tools > Backup & Restore page.



Restore

Restore previous settings from a saved file.

File:

Factory Default Restore

Restore all the configuration settings to their default values.

▶ **To reset the router to factory default settings**

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Click Advanced > System Tools > Backup & Restore page.
3. Click Restore to restore all configuration settings to default values, except your login. Click Factory Restore to reset the router.
4. Wait for the resetting and then the router will automatically reboot.

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.

4. 10. 5. Reboot

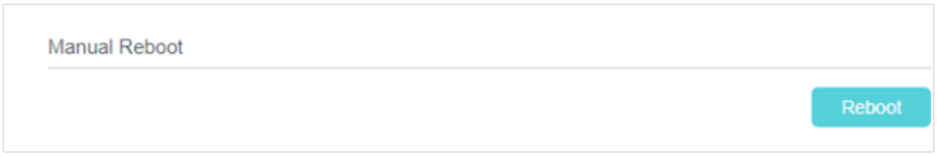
Some settings of the router will take effect only after rebooting, including:

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Working Modes.
- 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).

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

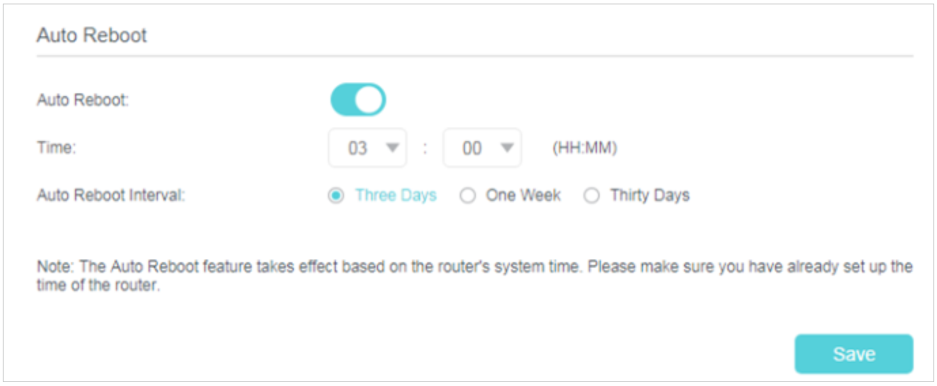
➢ **To reboot the router manually:**

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


Manual Reboot

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

1. Select Schedule from the Auto Reboot Time drop-down list.
2. Specify the Day(s) and Time for the router to reboot.
3. Click Save.


Auto Reboot

Auto Reboot: ●

Time: 03 : 00 (HH:MM)

Auto Reboot Interval: ● Three Days ○ One Week ○ Thirty Days

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.

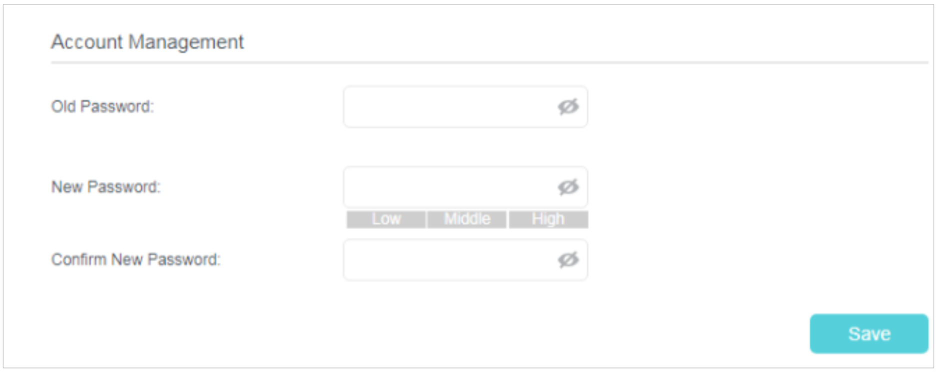
4. 10. 6. Administrator

4.10.6.1 Change the Administrator Account

Admin account is used to log in to the router's web management page. You are required to set the admin account at first login. You can also change it on the web page.

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

2. Go to Advanced > System Tools> Administration page. Locate the Account Management section.



Account Management

Old Password:

New Password:

Confirm New Password:

It is strongly recommended that you change the default password of the router, for all users that try to access the router's web-based utility or Quick Setup will be prompted for the router's password.

3. Enter the old password. Enter the new password and enter again to confirm.

4. Click Save to make the settings effective.

4.10.6.2 Local Management

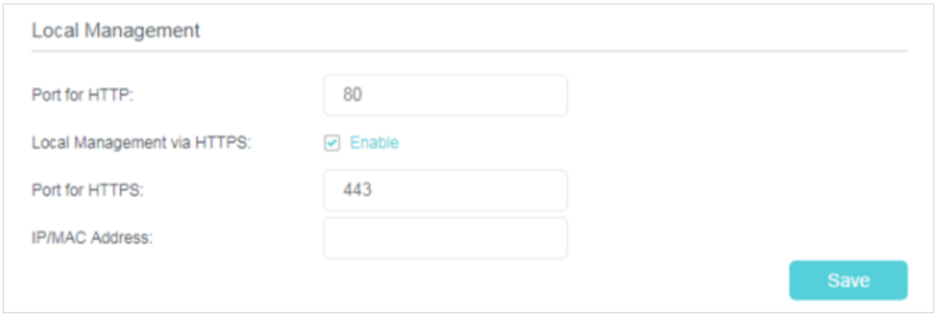
You can control the local devices' authority to manage the router via Local Management feature. By default all local connected devices are allowed to manage therouter. You can also allow only one device to manage the router and enable local management over a more secure way, HTTPS.

➢ **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 page. Locate the Local Management section.

3. Keep the Port as the default setting. Enable Management over HTTPS and keep the Port for HTTPS as the default setting. Enter the IP address or MAC address of the local device to manage the router.



Local Management

Port for HTTP: 80

Local Management via HTTPS: ☑ Enable

Port for HTTPS: 443

IP/MAC Address:

4. Click Save.

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

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

4.10.6.3 Remote Management

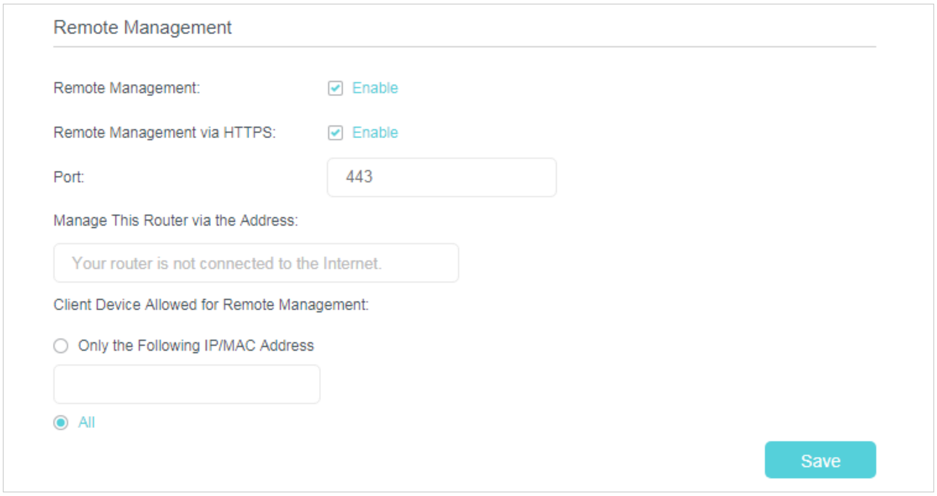
By default, the remote devices are not allowed to manage the router from the internet. You can enable remote management over HTTP and/or HTTPS if needed. HTTPS is a more secure way to access the router.

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 mange 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 page. Locate the Remote Management section.



Remote Management

Remote Management: ☑ Enable

Remote Management via HTTPS: ☑ Enable

Port: 443

Manage This Router via the Address:

Your router is not connected to the Internet.

Client Device Allowed for Remote Management:

○ Only the Following IP/MAC Address

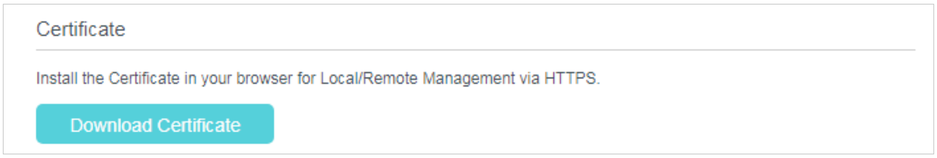
● All

3. Tick the checkbox to enable Remote Management. Enable 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.



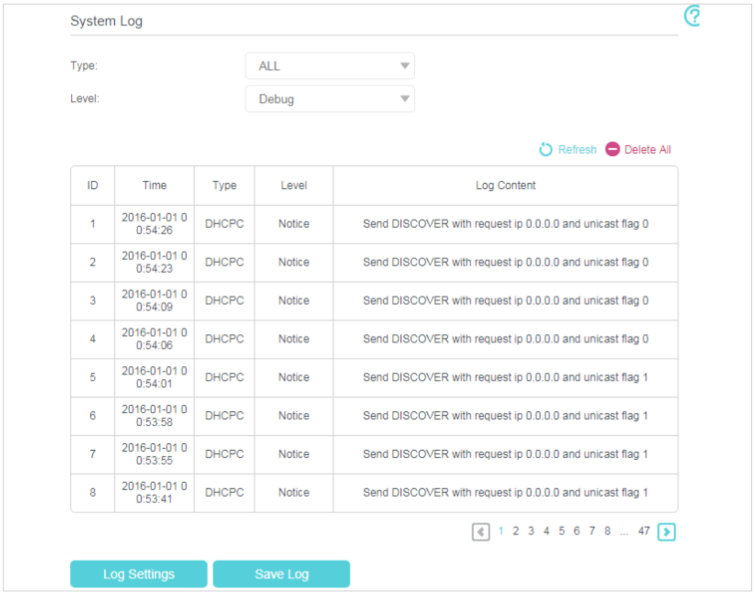
Certificate

Install the Certificate in your browser for Local/Remote Management via HTTPS.

4. 10. 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 will 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 System Tools > System Log.



System Log

Type: ALL

Level: Debug

ID	Time	Type	Level	Log Content
1	2016-01-01 00:54:26	DHCPC	Notice	Send DISCOVER with request ip 0.0.0.0 and unicast flag 0
2	2016-01-01 00:54:23	DHCPC	Notice	Send DISCOVER with request ip 0.0.0.0 and unicast flag 0
3	2016-01-01 00:54:09	DHCPC	Notice	Send DISCOVER with request ip 0.0.0.0 and unicast flag 0
4	2016-01-01 00:54:06	DHCPC	Notice	Send DISCOVER with request ip 0.0.0.0 and unicast flag 0
5	2016-01-01 00:54:01	DHCPC	Notice	Send DISCOVER with request ip 0.0.0.0 and unicast flag 1
6	2016-01-01 00:53:58	DHCPC	Notice	Send DISCOVER with request ip 0.0.0.0 and unicast flag 1
7	2016-01-01 00:53:55	DHCPC	Notice	Send DISCOVER with request ip 0.0.0.0 and unicast flag 1
8	2016-01-01 00:53:41	DHCPC	Notice	Send DISCOVER with request ip 0.0.0.0 and unicast flag 1

- **To view the system logs:**

You can view specific system logs by selecting the log Type and Level.

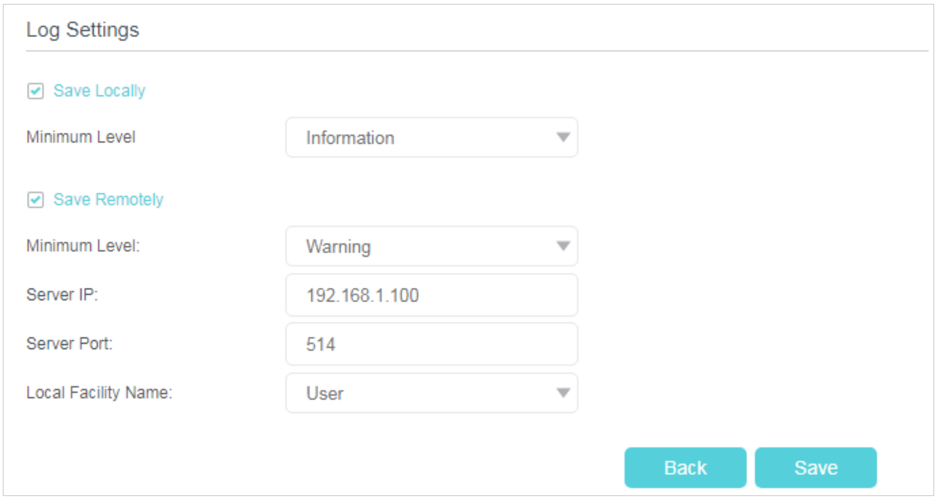
Click Refresh to refresh the log list.

- **To save the system logs:**

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

Click Save Log to save the logs in a txt file to your computer.

Click Log Settings to set the storage path of logs.



Log Settings

☑ Save Locally

Minimum Level: Information

☑ Save Remotely

Minimum Level: Warning

Server IP: 192.168.1.100

Server Port: 514

Local Facility Name: User

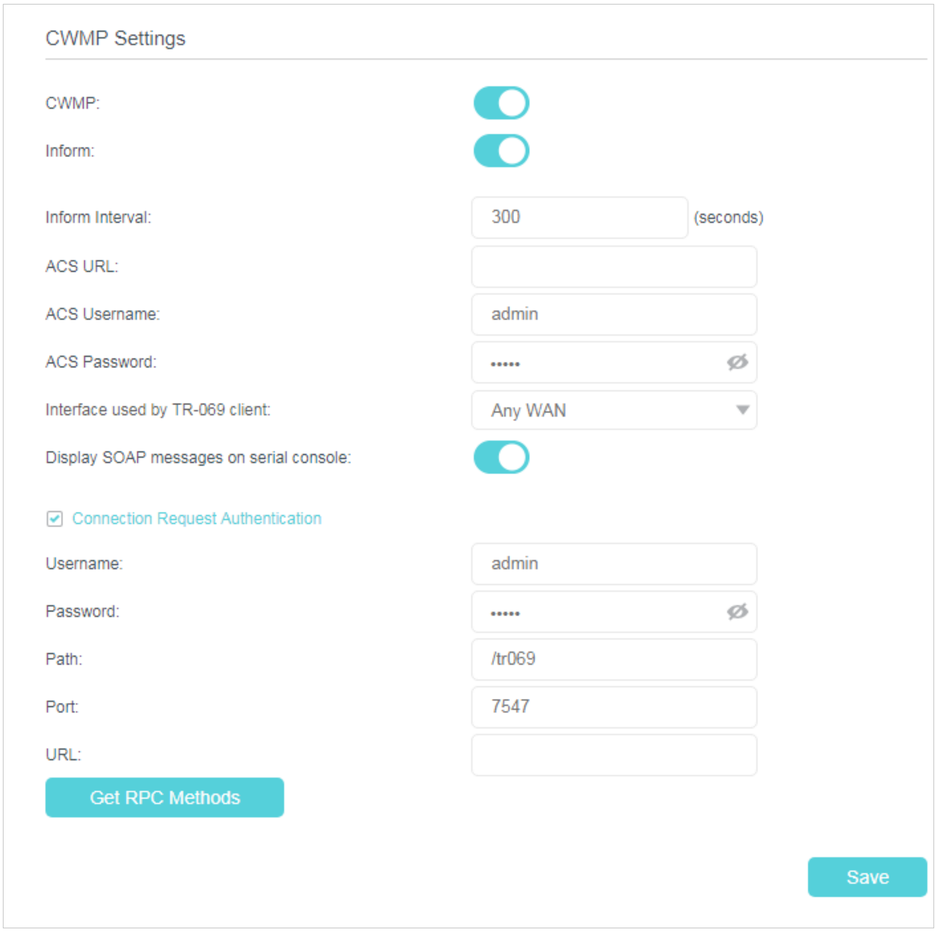
- Save Locally: Select this option to cache the system log to the router's local memory, select the minimum level of system log to be saved from the drop-down list. The logs will be shown in the table in descending order on the System Log page.
- Save Remotely: Select this option to send the system log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

4. 10. 8. CWMP Settings

The router offers CWMP feature. The function supports TR-069 protocol which collects information, diagnoses the devices 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 System Tools > CWMP Settings page.



CWMP Settings

CWMP: On

Inform: On

Inform Interval: 300 (seconds)

ACS URL:

ACS Username: admin

ACS Password: •••••

Interface used by TR-069 client: Any WAN

Display SOAP messages on serial console: On

☑ Connection Request Authentication

Username: admin

Password: •••••

Path: /tr069

Port: 7547

URL:

- CWMP: Toggle On to enable the CWMP (CPE WAN Management Protocol) feature.
- Inform: Enable this feature to send an Inform message to the ACS (Auto Configuration Server) periodically.
- Inform Interval: Enter 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: Toggle to enable or disable this feature.
- Connection Request Authentication: Select this checkbox 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.
- Get RPC methods: Click to get the methods to support CWMP.

Click Save to make the settings effective.

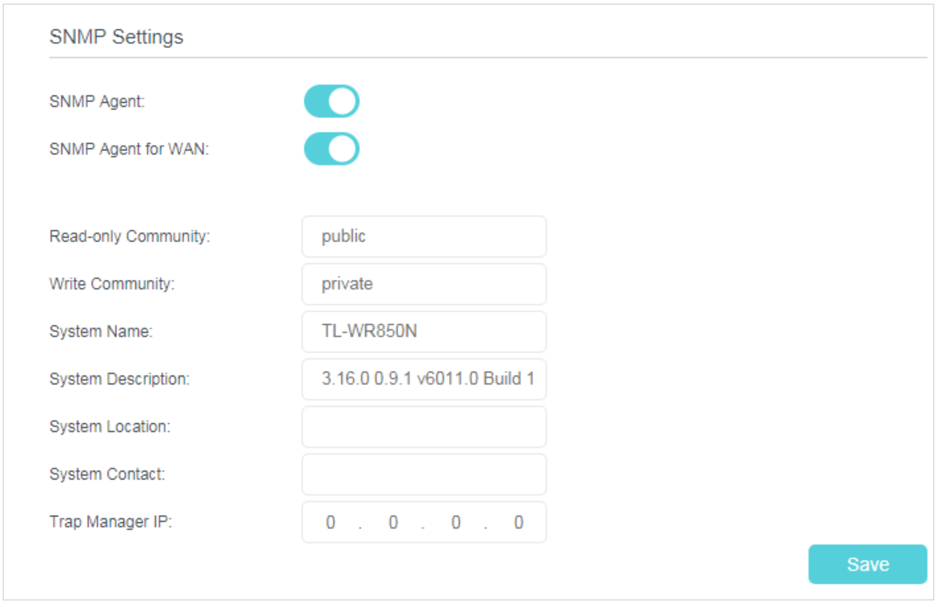
4. 10. 9. SNMP Settings

SNMP (Simple Network Management Protocol) has been widely applied in the computer networks currently, which is used for ensuring the transmission of the management information between two nodes. 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.

An 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 System Tools > SNMP Settings page.



SNMP Settings

SNMP Agent: ●

SNMP Agent for WAN: ●

Read-only Community: public

Write Community: private

System Name: TL-WR850N

System Description: 3.16.0 0.9.1 v6011.0 Build 1

System Location:

System Contact:

Trap Manager IP: 0 . 0 . 0 . 0

- SNMP Agent: Toggle 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.

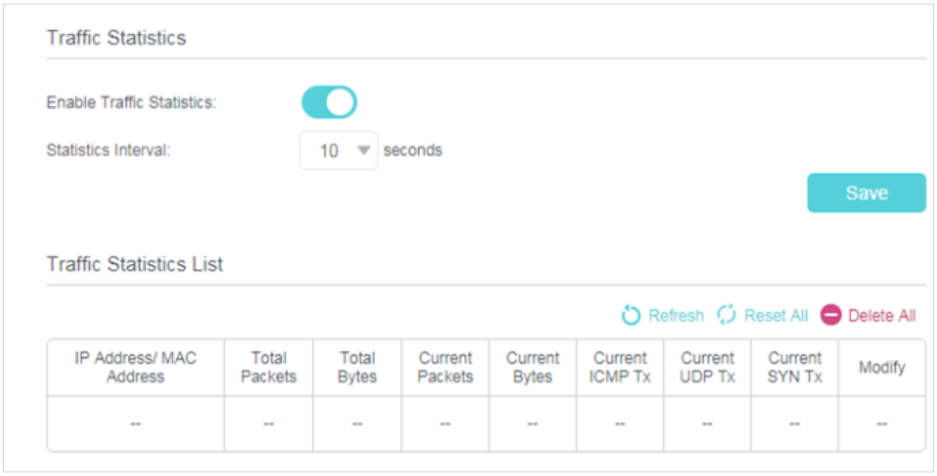
- Write Community: Displays the default write community string that protects the router from unauthorized changes.
- System Name: Displays the administratively-assigned name for this managed device.
- System Description: Displays the textual description of the managed device. This value should include 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 (e.g., 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.

4. 10. 10. Statistics

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to System Tools > Statistics.
3. Toggle on Traffic Statistics, and then you can monitor the traffic statistics in Traffic Statistics List section.



Traffic Statistics

Enable Traffic Statistics: ●

Statistics Interval: 10 seconds

Traffic Statistics List

IP Address/ MAC Address	Total Packets	Total Bytes	Current Packets	Current Bytes	Current ICMP Tx	Current UDP Tx	Current SYN Tx	Modify
--	--	--	--	--	--	--	--	--

Click Refresh to update the statistic information on the page.

Click Reset All to reset all statistic values in the list to zero.

Click Delete All to delete all statistic information in the list.

4. 11. Logout

Click Logout at the bottom of the main menu, and you will log out of the web management page and return to the login window.

Chapter 5

Configure the Router in Access Point Mode

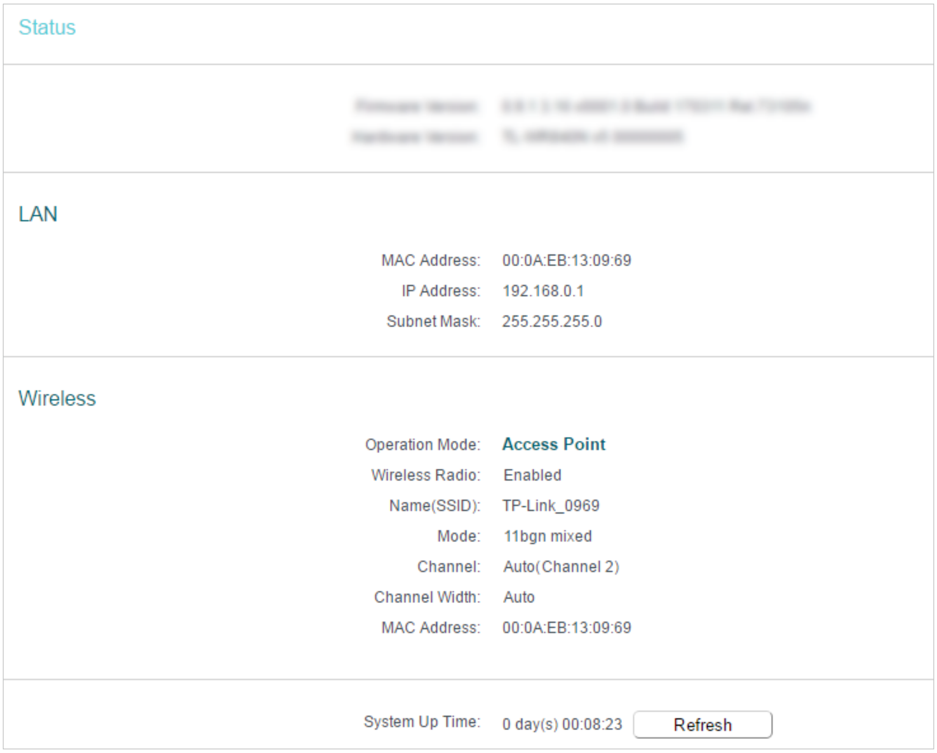
This chapter presents how to configure the various features of the router working as an access point.

It contains the following sections:

5. 1. Status

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

2. Go to Status. You can view the current status information of the router.



Status

[redacted]

LAN

MAC Address: 00:0A:EB:13:09:69
IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0

Wireless

Operation Mode: Access Point
Wireless Radio: Enabled
Name(SSID): TP-Link_0969
Mode: 11bgn mixed
Channel: Auto(Channel 2)
Channel Width: Auto
MAC Address: 00:0A:EB:13:09:69

System Up Time: 0 day(s) 00:08:23

- Firmware Version - The version information of the router's firmware.
- Hardware Version - The version information of the router's hardware.
- LAN - This field displays the current settings of the LAN, and you can configure them on the Network > LAN page.
    - MAC address - The physical address of the router.
    - IP address - The LAN IP address of the router.
    - Subnet Mask - The subnet mask associated with the LAN IP address.
- Wireless - This field displays the basic information or status of the wireless function, and you can configure them on the Wireless > Basic Settings page.
    - Operation Mode - The current wireless working mode in use.
    - Wireless Radio - Indicates whether the wireless radio feature of the router is enabled or disabled.
    - Name(SSID) - The SSID of the router.
    - Mode - The current wireless mode which the router works on.
    - Channel - The current wireless channel in use.
    - Channel Width - The current wireless channel width in use.

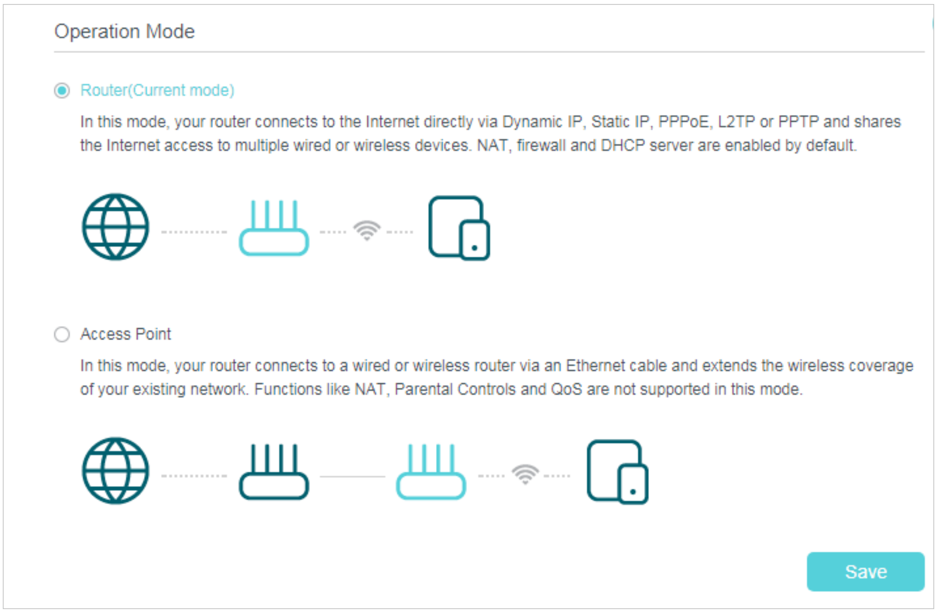
- MAC Address - The physical address of the router.

- System Up Time - The length of the time since the router was last powered on or reset.

Click Refresh to get the latest status and settings of the router.

5. 2. Operation Mode

1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Operation Mode.
3. Select the working mode as needed and click Save.



Operation Mode

● Router(Current mode)

In this mode, your router connects to the Internet directly via Dynamic IP, Static IP, PPPoE, L2TP or PPTP and shares the Internet access to multiple wired or wireless devices. NAT, firewall and DHCP server are enabled by default.

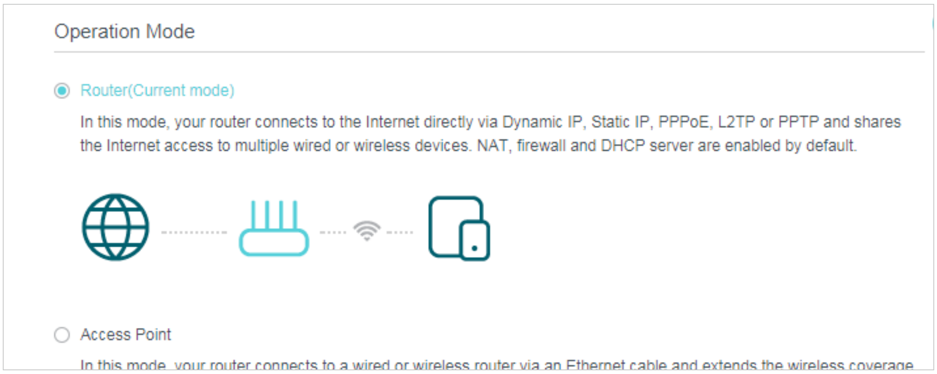
○ Access Point

In this mode, your router connects to a wired or wireless router via an Ethernet cable and extends the wireless coverage of your existing network. Functions like NAT, Parental Controls and QoS are not supported in this mode.

5. 3. Network

5. 3. 1. LAN

1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Network > LAN.
3. Configure the IP parameters of the LAN and click Save.



Operation Mode

● Router(Current mode)

In this mode, your router connects to the Internet directly via Dynamic IP, Static IP, PPPoE, L2TP or PPTP and shares the Internet access to multiple wired or wireless devices. NAT, firewall and DHCP server are enabled by default.

○ Access Point

In this mode, your router connects to a wired or wireless router via an Ethernet cable and extends the wireless coverage

- Type - Either select Smart IP(DHCP) to get IP address from DHCP server, or Static IP to configure IP address manually.
- MAC Address - The physical address of the LAN ports. The value can not be changed.
- IP Address - Enter the IP address in dotted-decimal notation if your select Static IP (factory default - 192.168.0.1).
- Subnet Mask - An address code that determines the size of the network. Normally 255.255.255.0 is used as the subnet mask.

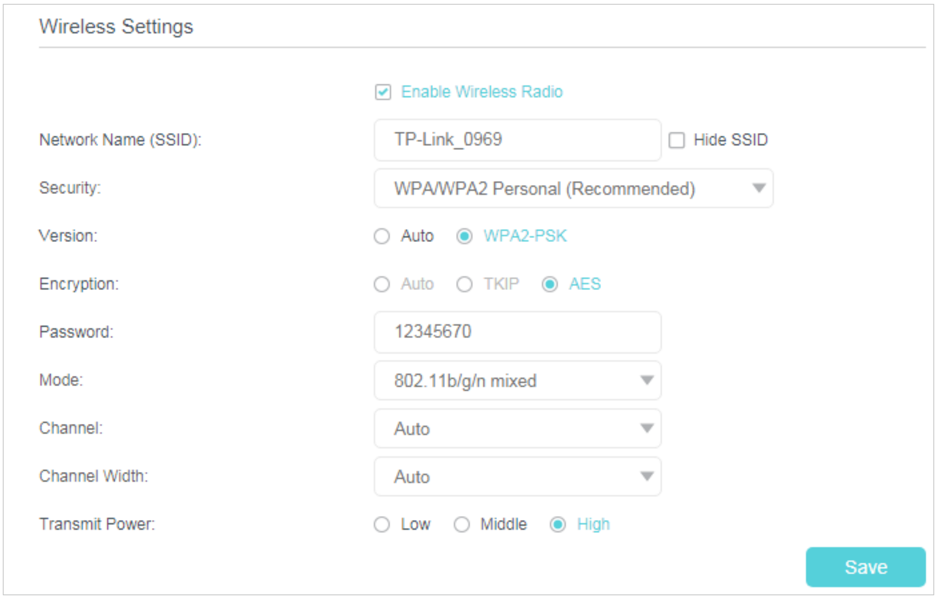
Note:

- If you have changed the IP address, you must use the new IP address to login.
- If you select Smart IP(DHCP), the DHCP server of the router will not start up.
- If the new IP address you set is not in the same subnet as the old one, the IP Address pool in the DHCP Server will be configured.

5. 4. Wireless

5. 4. 1. Basic Settings

1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Wireless > Basic Settings.
3. Configure the basic settings for the wireless network and click Save.



Wireless Settings

☑ Enable Wireless Radio

Network Name (SSID): TP-Link_0969 □ Hide SSID

Security: WPA/WPA2 Personal (Recommended)

Version: ○ Auto ● WPA2-PSK

Encryption: ○ Auto ○ TKIP ● AES

Password: 12345670

Mode: 802.11b/g/n mixed

Channel: Auto

Channel Width: Auto

Transmit Power: ○ Low ○ Middle ● High

- Wireless - Enable or disable wireless network.
- Wireless Network Name - Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network.
- Mode - You can choose the appropriate “Mixed” mode.
- Channel - This field determines which operating frequency will be used. The default channel is set to Auto. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- Channel Width - 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. If you select auto, then AP will choose the best channel automatically.
- Enable SSID Broadcast - If enabled, the router will broadcast the wireless network name (SSID).

5. 4. 2. WPS

WPS (Wi-Fi Protected Setup) can help you to quickly and securely connect to a network. This section will guide you to add a new wireless device to your router’s network quickly via WPS.

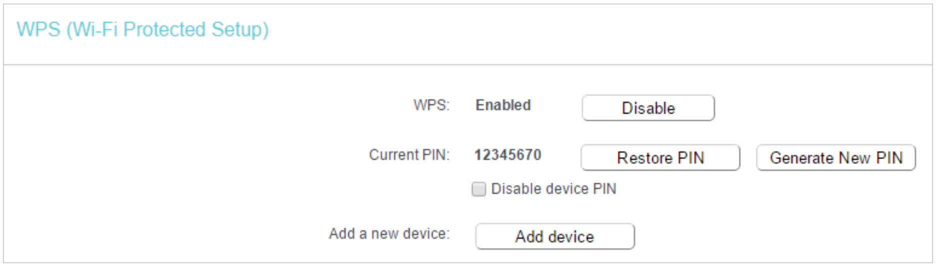
Note:

The WPS function cannot be configured if the wireless function of the router is disabled. Please make sure the wireless function is enabled before configuration.

1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Wireless > WPS.
3. Follow one of the following three methods to connect your client device to the router's Wi-Fi network.

Method ONE: Press the WPS Button on Your Client Device

1. Keep the WPS Status as Enabled and click Add Device.



WPS (Wi-Fi Protected Setup)

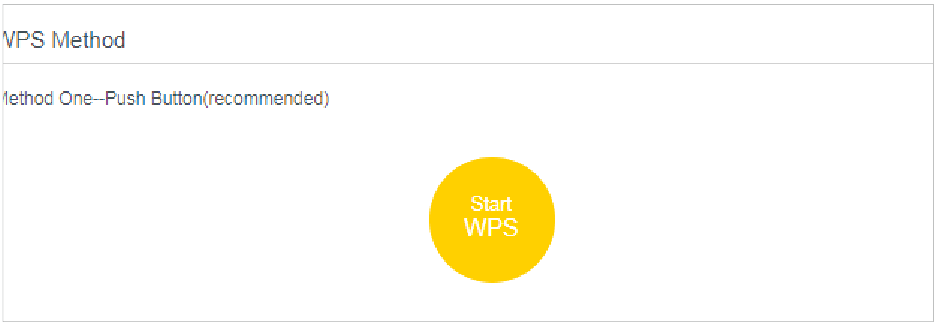
WPS: Enabled

Current PIN: 12345670

□ Disable device PIN

Add a new device:

2. Select Press the WPS button of the new device within the next two minutes and click Connect.



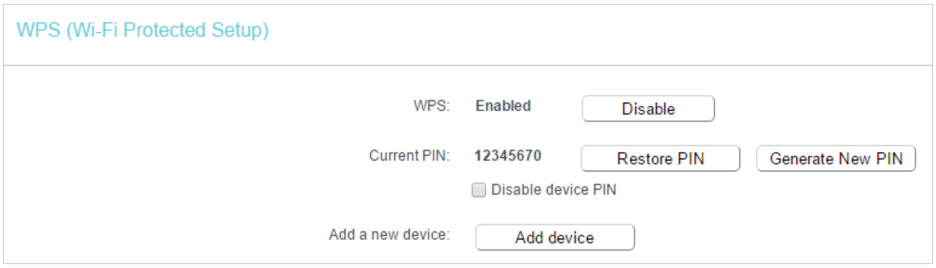
VPS Method

lethod One--Push Button(recommended)

3. Within two minutes, press the WPS button on your client device.
4. A success message will appear on the WPS page if the client device has been successfully added to the router's network.

Method TWO: Enter the Client's PIN

1. Keep the WPS Status as Enabled and click Add Device.



WPS (Wi-Fi Protected Setup)

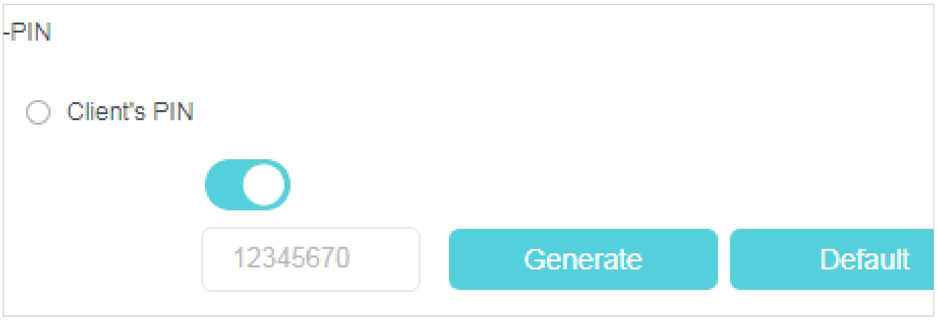
WPS: Enabled

Current PIN: 12345670

□ Disable device PIN

Add a new device:

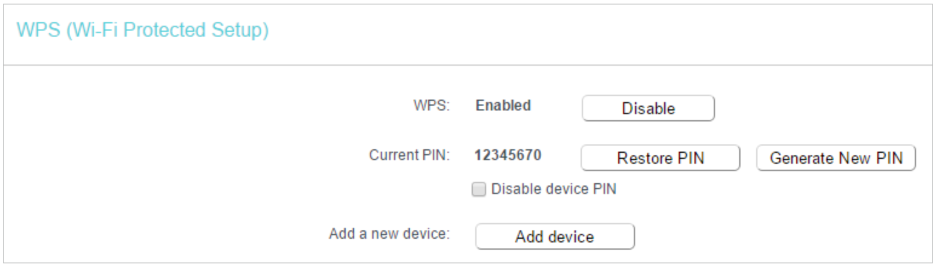
2. Select Enter new device PIN, enter your client device's current PIN in the PIN filed and click Connect.



3. A success message will appear on the WPS page if the client device has been successfully added to the router's network.

Method Three: Enter the Router's PIN

1. Keep the WPS Status as Enabled and get the Current PIN of the router.

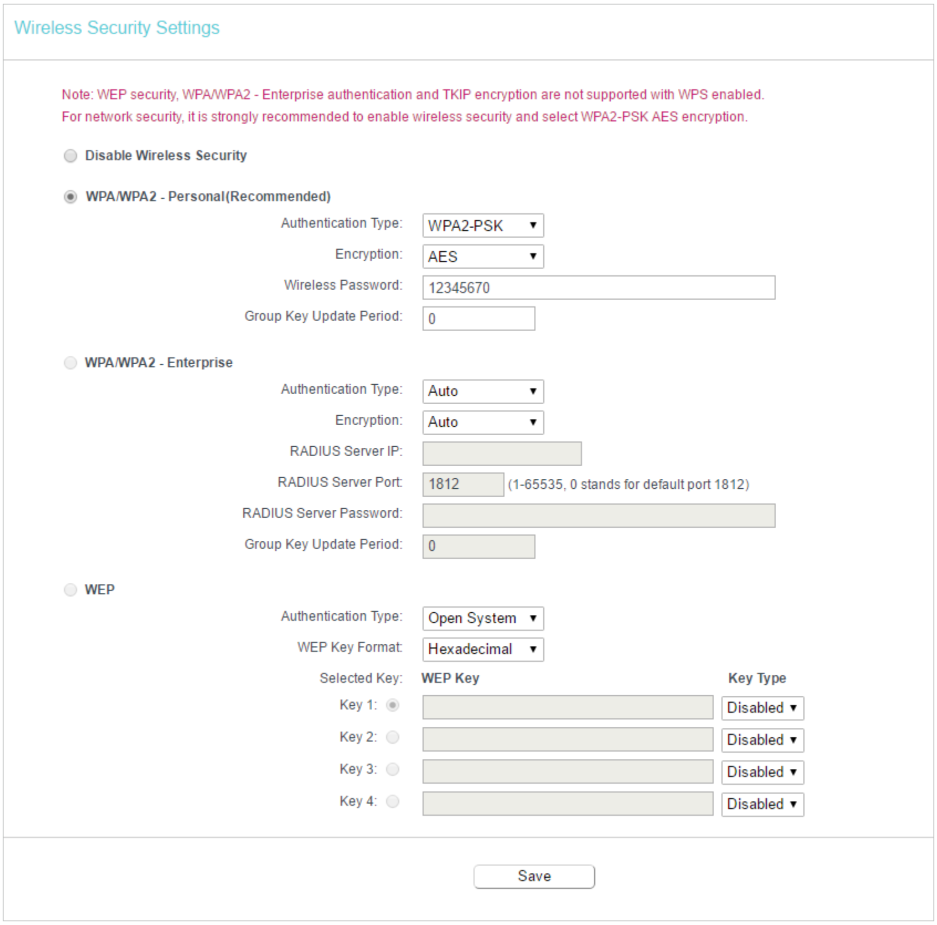

WPS (Wi-Fi Protected Setup)

WPS: Enabled
Current PIN: 12345670
□ Disable device PIN
Add a new device:

2. Enter the router's current PIN on your client device to join the router's Wi-Fi network.

5. 4. 3. Wireless Security

1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Wireless > Wireless Security.
3. Configure the security settings of your wireless network and click Save.



Wireless Security Settings

Note: WEP security, WPA/WPA2 - Enterprise authentication and TKIP encryption are not supported with WPS enabled.
For network security, it is strongly recommended to enable wireless security and select WPA2-PSK AES encryption.

○ Disable Wireless Security

● WPA/WPA2 - Personal(Recommended)

Authentication Type: WPA2-PSK
Encryption: AES
Wireless Password: 12345670
Group Key Update Period: 0

○ WPA/WPA2 - Enterprise

Authentication Type: Auto
Encryption: Auto
RADIUS Server IP:
RADIUS Server Port: 1812 (1-65535, 0 stands for default port 1812)
RADIUS Server Password:
Group Key Update Period: 0

○ WEP

Authentication Type: Open System
WEP Key Format: Hexadecimal

Selected Key:	WEP Key	Key Type
Key 1: ●		Disabled
Key 2: ○		Disabled
Key 3: ○		Disabled
Key 4: ○		Disabled

- Disable Wireless Security - The wireless security function can be enabled or disabled. If disabled, wireless clients can connect to the router without a password. It's strongly recommended to choose one of the following modes to enable security.
- WPA-PSK/WPA2-Personal - It's the WPA/WPA2 authentication type based on pre-shared passphrase.
    - Authentication Type - Select Auto, WPA-PSK or WPA2-PSK.
    - Encryption - Select Auto, TKIP or AES.
    - Wireless Password - Enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters.
    - Group Key Update Period - Specify the group key update interval in seconds. The value can be 0 or at least 30. Enter 0 to disable the update.
- WPA /WPA2-Enterprise - It's based on Radius Server.
    - Authentication Type - Select Auto, WPA or WPA2.
    - Encryption - Select Auto, TKIP or AES.
    - Radius Server IP - Enter the IP address of the Radius server.
    - Radius Server Port - Enter the port that Radius server used.

  - Radius Server Password - Enter the password for the Radius server.
  - Group Key Update Period - Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.
- WEP - It is based on the IEEE 802.11 standard.
  - Authentication Type - The default setting is Auto, which can select Shared Key or Open System authentication type automatically based on the wireless client's capability and request.
  - WEP Key Format - Hexadecimal and ASCII formats are provided here. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. ASCII format stands for any combination of keyboard characters in the specified length.
  - WEP Key (Password) - Select which of the four keys will be used and enter the matching WEP key. Make sure these values are identical on all wireless clients in your network.
  - Key Type - Select the WEP key length (64-bit, 128-bit or 152-bit) for encryption. Disabled means this WEP key entry is invalid.
  - 64-bit - Enter 10 hexadecimal digits (any combination of 0-9, a-f and A-F. Null key is not permitted) or 5 ASCII characters.
  - 128-bit - Enter 26 hexadecimal digits (any combination of 0-9, a-f and A-F. Null key is not permitted) or 13 ASCII characters.

5. 4. 4. Wireless MAC Filtering

Wireless MAC Filtering is used to deny or allow specific wireless client devices to access your network by their MAC addresses.

I want to:

Deny or allow specific wireless client devices to access my network by their MAC addresses.

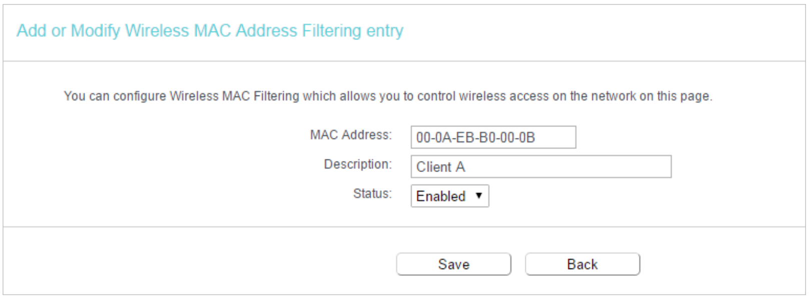
For example, you want the wireless client A with the MAC address 00-0A-EB-B0-00-0B and the wireless client B with the MAC address 00-0A-EB-00-07-5F to access the router, but other wireless clients cannot access the router

How can I do that?

1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Wireless > Wireless MAC Filtering.
3. Click Enable to enable the Wireless MAC Filtering function.
4. Select Allow the stations specified by any enabled entries in the list to access as the filtering rule.

5. Delete all or disable all entries if there are any entries already.

6. Click Add New and fill in the blank.



Add or Modify Wireless MAC Address Filtering entry

You can configure Wireless MAC Filtering which allows you to control wireless access on the network on this page.

MAC Address: 00-0A-EB-B0-00-0B

Description: Client A

Status: Enabled ▾

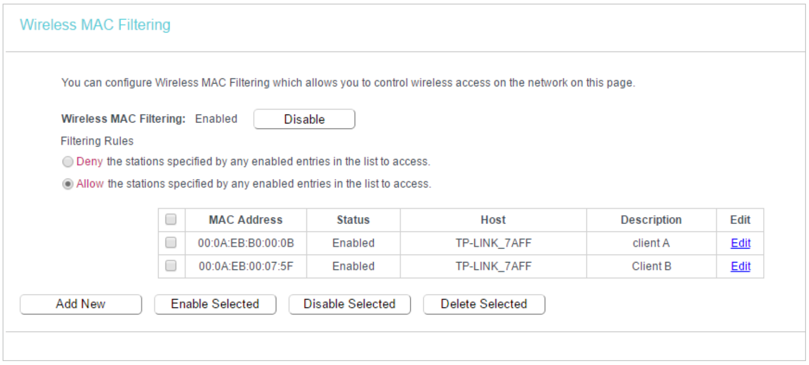
1) Enter the MAC address 00-0A-EB-B0-00-0B / 00-0A-EB-00-07-5F in the MAC Address field.

2) Enter wireless client A/B in the Description field.

3) Select Enabled in the Status drop-down list.

4) Click Save and click Back.

7. The configured filtering rules should be listed as the picture shows below.



Wireless MAC Filtering

You can configure Wireless MAC Filtering which allows you to control wireless access on the network on this page.

Wireless MAC Filtering: Enabled

Filtering Rules

○ Deny the stations specified by any enabled entries in the list to access.

● Allow the stations specified by any enabled entries in the list to access.

□	MAC Address	Status	Host	Description	Edit
□	00:0A:EB:B0:00:0B	Enabled	TP-LINK_7AFF	client A	Edit
□	00:0A:EB:00:07:5F	Enabled	TP-LINK_7AFF	Client B	Edit

Done!

Now only client A and client B can access your network.

5. 4. 5. Wireless Advanced

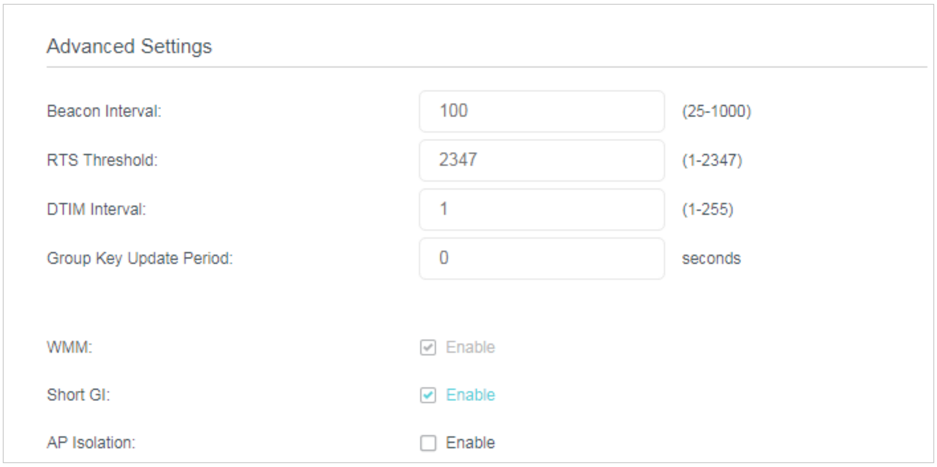
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.

2. Go to Wireless > Wireless Advanced.

3. Configure the advanced settings of your wireless network and click Save.

Note:

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



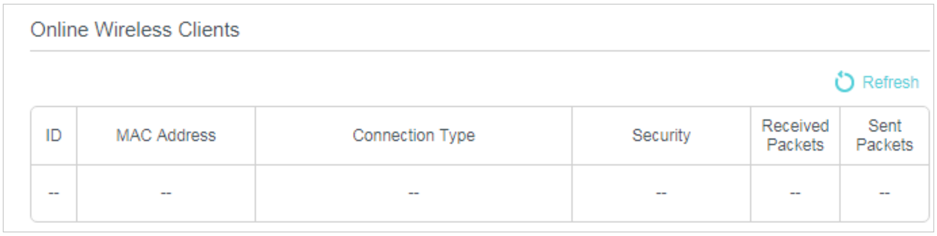
Advanced Settings

Beacon Interval:	100	(25-1000)
RTS Threshold:	2347	(1-2347)
DTIM Interval:	1	(1-255)
Group Key Update Period:	0	seconds
WMM:	☑ Enable	
Short GI:	☑ Enable	
AP Isolation:	□ Enable	

- Transmit Power - Select High, Middle or Low which you would like to specify for the router. High is the default setting and recommended.
- Beacon Interval - Enter a value between 40-1000 milliseconds for Beacon Interval here. Beacon Interval value determines the time interval of the beacons. The beacons are the packets sent by the router to synchronize a wireless network. The default value is 100.
- RTS Threshold - Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- Fragmentation Threshold - This value is the maximum size determining whether packets will be fragmented. Setting a low value for the Fragmentation Threshold may result in poor network performance because of excessive packets. 2346 is the default setting and is recommended.
- DTIM Interval - This value determines the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- Enable Short GI - It is recommended to enable this function, for it will increase the data capacity by reducing the guard interval time.
- Enable Client Isolation - This function isolates all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.
- Enable WMM - WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended to enable this function.

5. 4. 6. Wireless Statistics

1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Wireless > Wireless Statistics to check the data packets sent and received by each client device connected to the router.



Online Wireless Clients

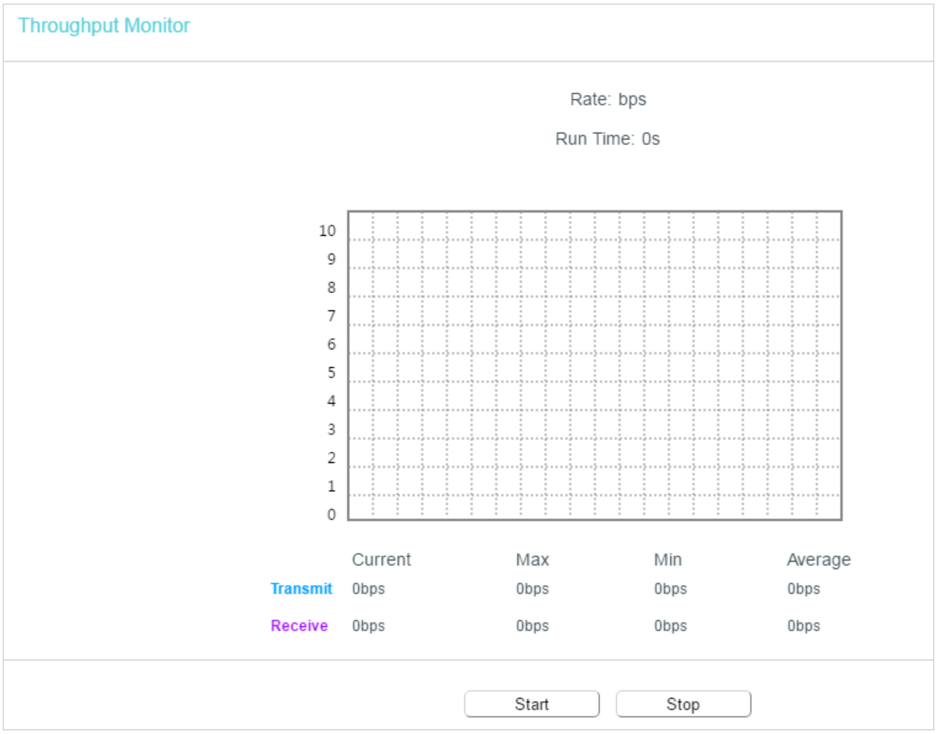
Refresh

ID	MAC Address	Connection Type	Security	Received Packets	Sent Packets
--	--	--	--	--	--

- MAC Address - The MAC address of the connected wireless client.
- Current Status - The running status of the connected wireless client.
- Received Packets - Packets received by the wireless client.
- Sent Packets - Packets sent by the wireless client.
- SSID - SSID that the station associates with.

5. 4. 7. Throughput Monitor

1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Wireless > Throughput Monitor to view the wireless throughput information.



Throughput Monitor

Rate: bps

Run Time: 0s

	Current	Max	Min	Average
Transmit	0bps	0bps	0bps	0bps
Receive	0bps	0bps	0bps	0bps

- Rate - The Throughput unit.
- Run Time - How long this function is running.
- Transmit - Wireless transmit rate information.
- Receive - Wireless receive rate information.

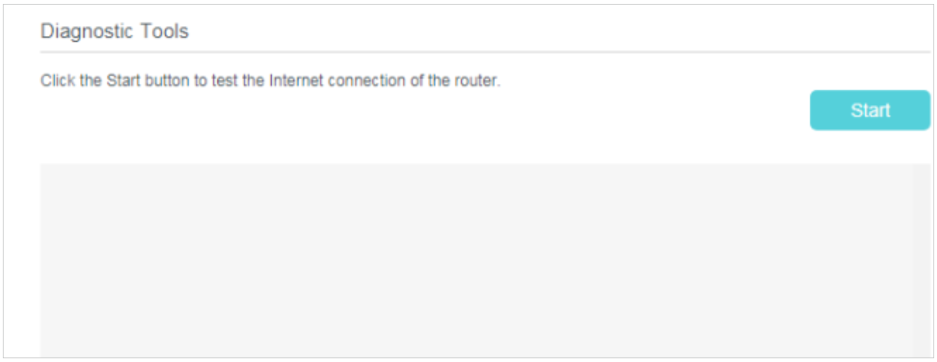
Click Start/Stop to start or stop wireless throughput monitor.

5. 5. System Tools

5. 5. 1. Diagnostic

Diagnostic 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 username and password you set for the router.
2. Go to System Tools > Diagnostic.



Diagnostic Tools

Click the Start button to test the Internet connection of the router.

- Diagnostic Tool - Select one diagnostic tool.
- Ping - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
- Tracerouter - This diagnostic tool tests the performance of a connection.

Note:

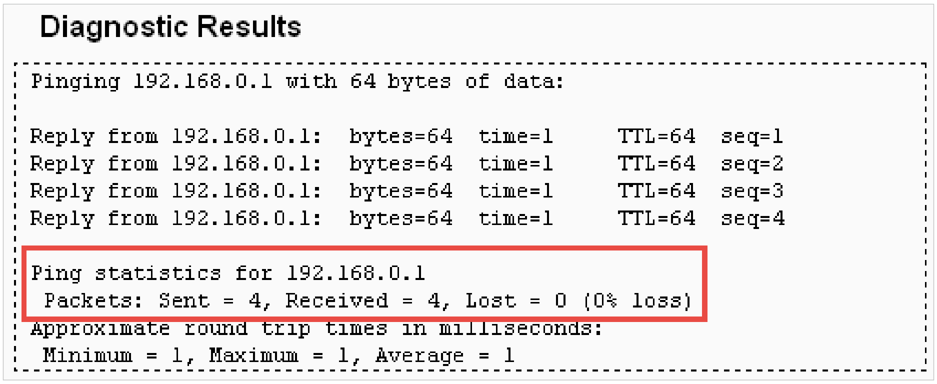
You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting the domain name is not, you might have a name resolution problem. In this case, ensure that the domain name you are specifying can be resolved by using Domain Name System (DNS) queries.

- IP Address/Domain Name - Enter the destination IP address (such as 192.168.0.1) or Domain name (such as www.tp-link.com).
- Pings Count - The number of Ping packets for a Ping connection.
- Ping Packet Size - The size of Ping packet.
- Ping Timeout - Set the waiting time for the reply of each Ping packet. If there is no reply in the specified time, the connection is overtime.

- Traceroute Max TTL - The max number of hops for a Traceroute connection.

3. Click Start to check the connectivity of the internet.

4. The Diagnostic Results page displays the diagnosis result. If the result is similar to the following figure, the connectivity of the internet is fine.



Diagnostic Results

```
Pinging 192.168.0.1 with 64 bytes of data:

Reply from 192.168.0.1:  bytes=64  time=1     TTL=64  seq=1
Reply from 192.168.0.1:  bytes=64  time=1     TTL=64  seq=2
Reply from 192.168.0.1:  bytes=64  time=1     TTL=64  seq=3
Reply from 192.168.0.1:  bytes=64  time=1     TTL=64  seq=4

Ping statistics for 192.168.0.1
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milliseconds:
 Minimum = 1, Maximum = 1, Average = 1
```

5. 5. 2. Firmware Upgrade

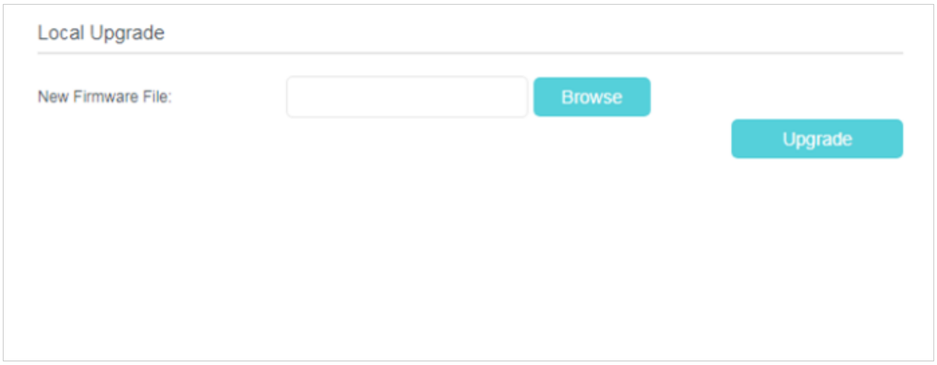
TP-Link is dedicated to improving and richening the product features, giving users a better network experience. We will release the latest firmware at TP-Link official website www.tp-link.com. You can download the lastest firmware file from the Support page of our website and upgrade the firmware to the latest version.

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 username and password you set for the router.

3. Go to System Tools > Firmware Upgrade.

4. Click Choose File to locate the downloaded firmware file, and click Upgrade.



5. 5. 3. Factory Defaults

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

2. Go to System Tools > Factory Defaults. Click Restore to reset all settings to the default values.

Restore

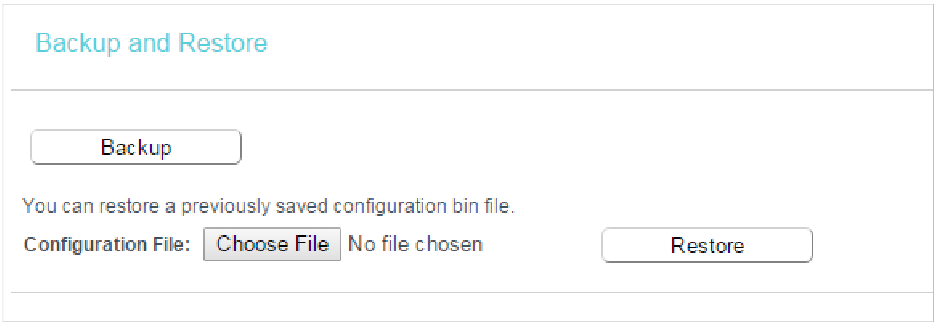
Restore previous settings from a saved file.

- Default Username: admin
- Default Password: admin
- Default IP Address: 192.168.0.1
- Default Subnet Mask: 255.255.255.0

5. 5. 4. Backup & Restore

The configuration settings are stored as a configuration file in the router. You can backup the configuration file in your computer for future use and restore the router to the previous settings from the backup file when needed.

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



Backup and Restore

You can restore a previously saved configuration bin file.

Configuration File: Choose File No file chosen

➢ **To backup configuration settings:**

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

➢ **To restore configuration settings:**

1. Click Choose File to locate the backup configuration file stored in your computer, and click Restore.
2. Wait a few minutes for the restoring and rebooting.

Note:

During the restoring process, do not power off or reset the router.

5. 5. 5. Reboot

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

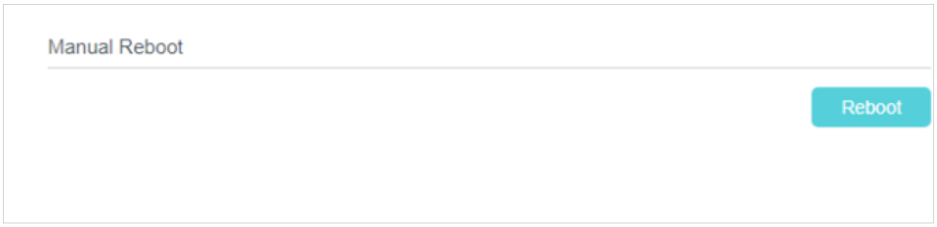
- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Working Modes.

- 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).

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

➢ **To reboot the router manually:**

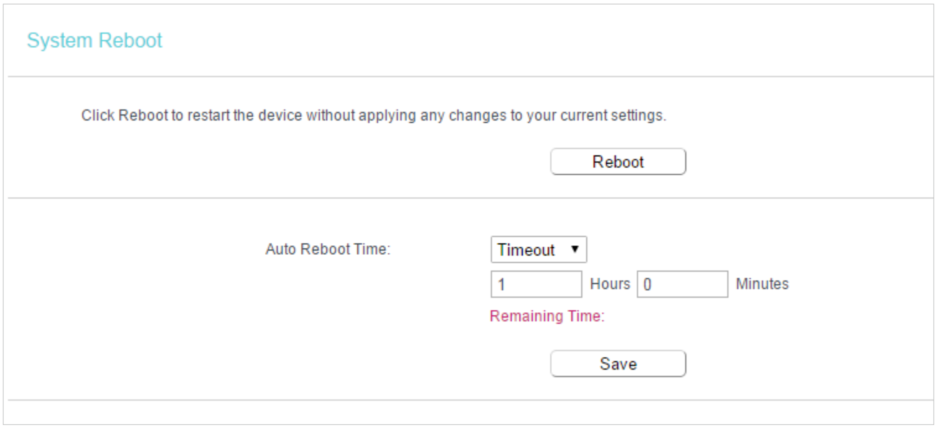
Click Reboot, and wait a few minutes for the router to rebooting.



Manual Reboot

➢ **To set the router reboot every a couple of hours:**

1. Select Timeout from the Auto Reboot Time drop-down list.
2. Specify a time interval. The router will reboot automatically after every this interval.
3. Click Save.



System Reboot

Click Reboot to restart the device without applying any changes to your current settings.

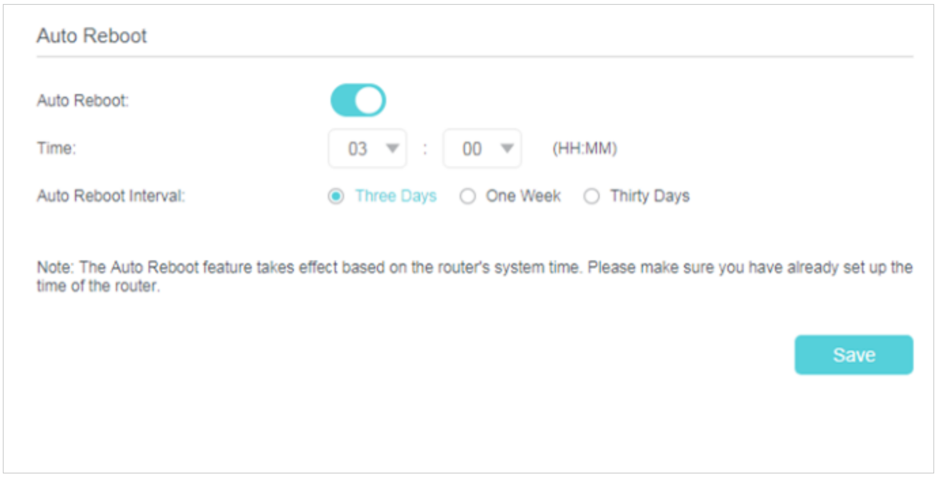
Auto Reboot Time: Timeout

1 Hours 0 Minutes

Remaining Time:

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

1. Select Schedule from the Auto Reboot Time drop-down list.
2. Specify the Day(s) and Time for the router to reboot.
3. Click Save.



Auto Reboot

Auto Reboot: On

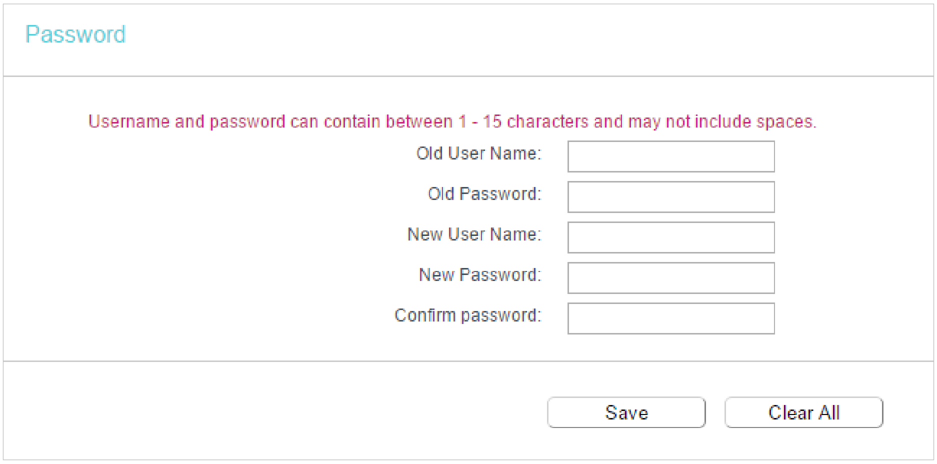
Time: 03 : 00 (HH:MM)

Auto Reboot Interval: ● Three Days ○ One Week ○ Thirty Days

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.

5. 5. 6. Password

1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to System Tools > Password, and you can change the factory default username and password of the router.



It is strongly recommended that you change the default username and password of the router, for all users that try to access the router's web-based utility or Quick Setup will be prompted for the router's username and password.

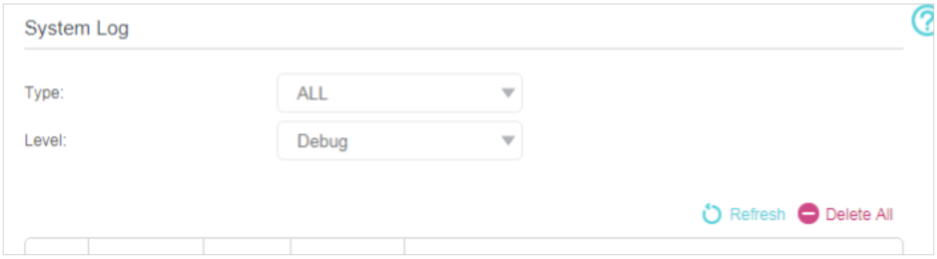
Note:

The new username and password must not exceed 15 characters and not include any spacing.

3. Click Save.

5. 5. 7. System Log

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



- Loge Type -By selecting the log type, only logs of this type will be shown.
- Log Level - By selecting the log level, only logs of this level will be shown.
- Refresh - Refresh the page to show the latest log list.
- Clear Log - All the logs will be deleted from the router permanently, not just from the page.

5. 6. Logout

Click Logout at the bottom of the main menu, and you will log out of the web management page and return to the login window.

FAQ

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

The default wireless password is printed on the label of the router. If the password has been altered, please connect your computer to the router using an Ethernet cable and follow the steps below:

1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Wireless > Wireless Security to retrieve or reset your wireless password.

Q2. What should I do if I forget my login password of the web management page?

The default username and password of the web management page are admin (in lowercase).

If you have altered the username and password:

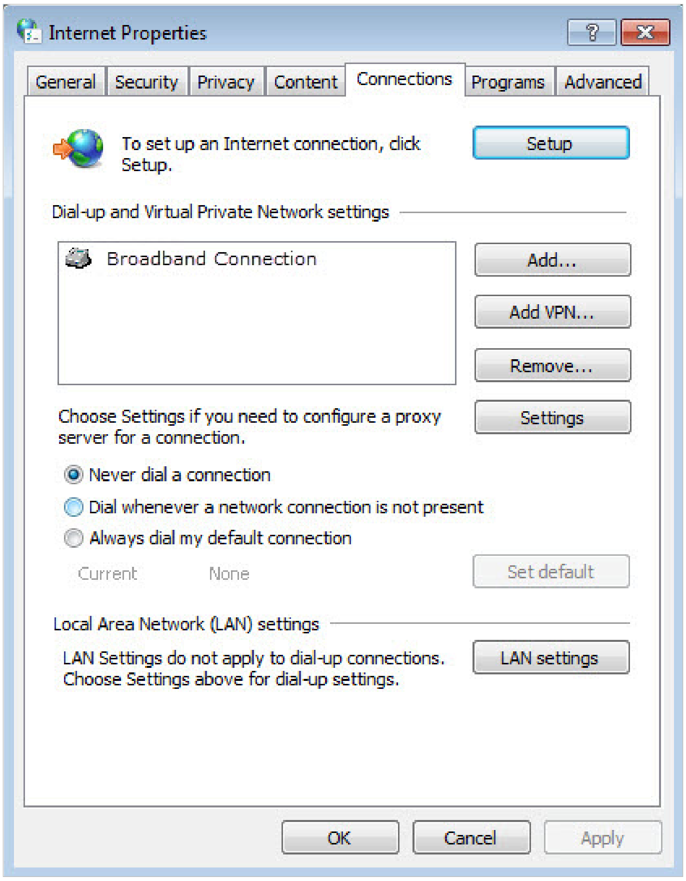
1. Reset the router to its factory default settings.
2. Visit http://tplinkwifi.net, and enter admin (in lowercase) as both username and password to log in.

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 computerthe has connected to the router correctly and the corresponding LED 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 you enter the correct IP address to log in: http://tplinkwifi.net or 192.168.0.1.
- 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.



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Broadband Connection

Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection

○ Dial whenever a network connection is not present

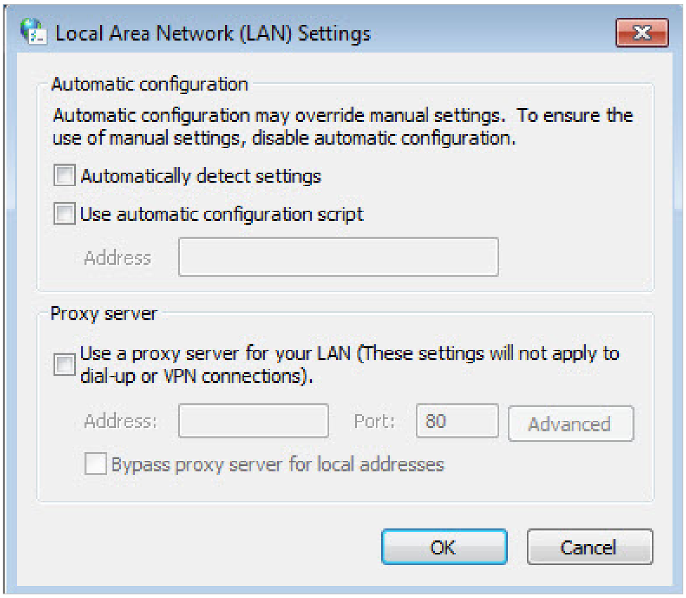
○ Always dial my default connection

Current None

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

4) Click LAN settings and deselect the following three options, and click OK.



Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address

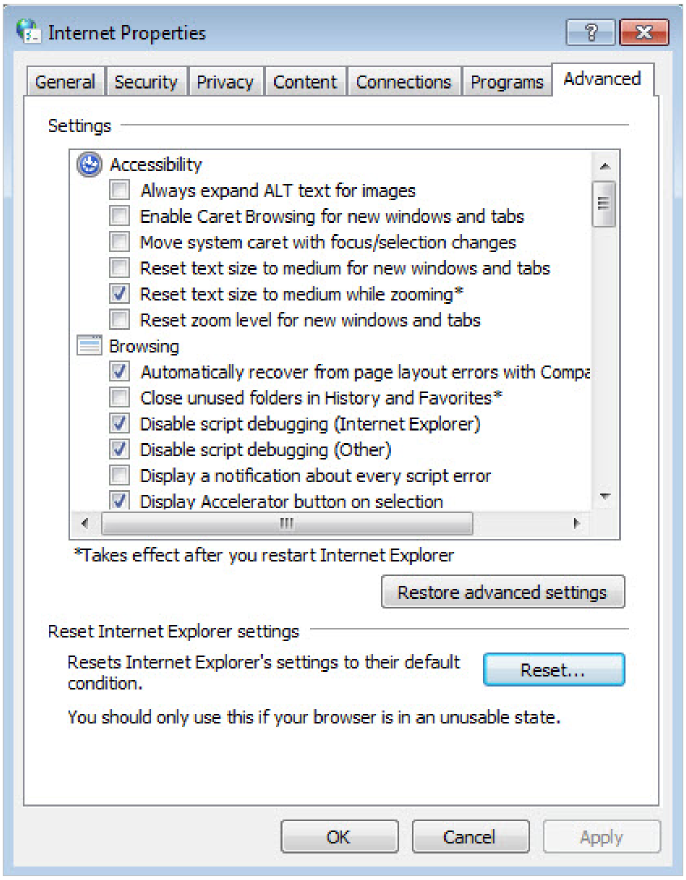
Proxy server

□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port: 80

□ Bypass proxy server for local addresses

5) Go to Advanced > Restore advanced settings, and click OK.



Settings

Accessibility

- □ Always expand ALT text for images
- □ Enable Caret Browsing for new windows and tabs
- □ Move system caret with focus/selection changes
- □ Reset text size to medium for new windows and tabs
- ☑ Reset text size to medium while zooming*
- □ Reset zoom level for new windows and tabs

Browsing

- ☑ Automatically recover from page layout errors with Compa
- □ Close unused folders in History and Favorites*
- ☑ Disable script debugging (Internet Explorer)
- ☑ Disable script debugging (Other)
- □ Display a notification about every script error
- ☑ Display Accelerator button on selection

*Takes effect after you restart Internet Explorer

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

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

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

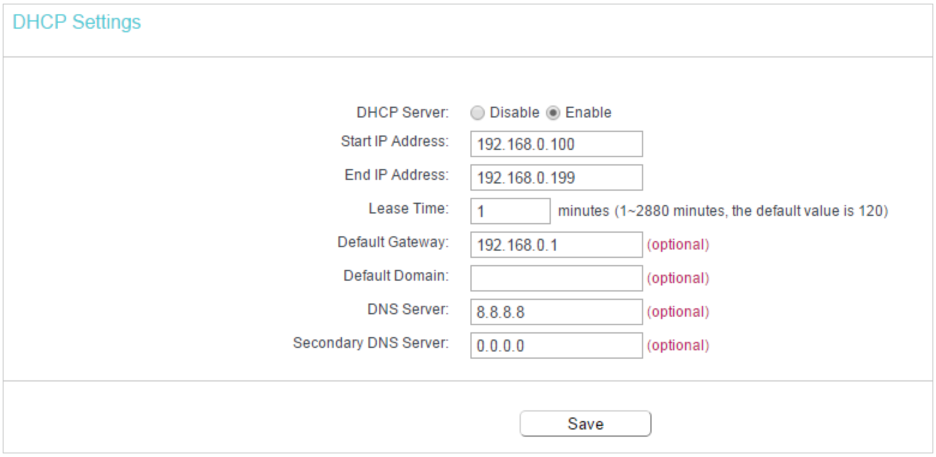
Q4. What should I do if I cannot access the internet even though the configuration is finished?

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

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

- Your computer might not recognize any DNS server addresses, please manually configure DNS server.
  1) Go to DHCP.
  2) Enter 8.8.8.8 as Primary DNS, and click Save.

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



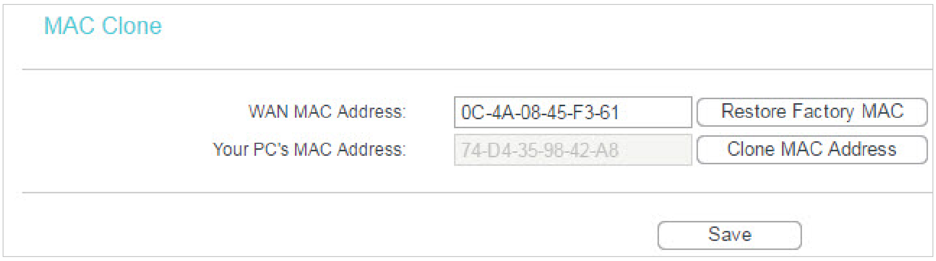
DHCP Settings

DHCP Server:	○ Disable ● Enable
Start IP Address:	192.168.0.100
End IP Address:	192.168.0.199
Lease Time:	1 minutes (1~2880 minutes, the default value is 120)
Default Gateway:	192.168.0.1 (optional)
Default Domain:	(optional)
DNS Server:	8.8.8.8 (optional)
Secondary DNS Server:	0.0.0.0 (optional)

- Restart the modem and the router.
  1) Power off your modem and the router, and leave them off for 1 minute.
  2) Power on your modem first, and wait about 2 minutes.
  3) Power on the router, and 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.

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 username and password you set for the router.
  2) Go to Network > MAC Clone, select Clone MAC Address and click Save.



MAC Clone

WAN MAC Address:	0C-4A-08-45-F3-61
Your PC's MAC Address:	74-D4-35-98-42-A8

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:

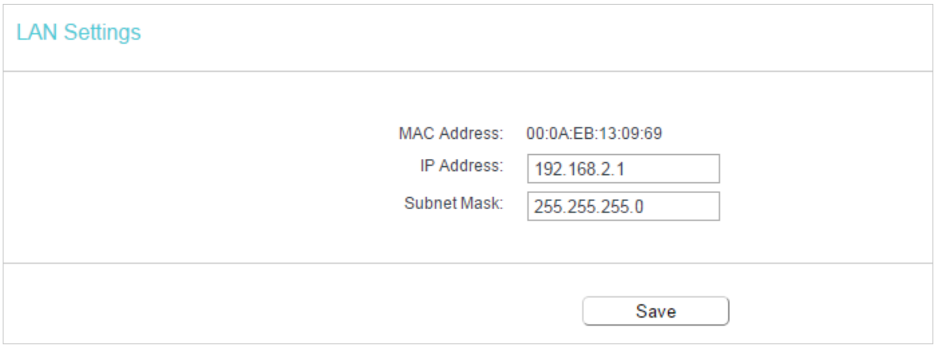
  Most TP-Link routers use 192.168.0.1/192.168.1.1 as their default LAN IP address, it may conflict with the IP range of your existent ADSL modem/router. If so, the router is not able to communicate with your modem and cause you can't access the Internet. To resolve this problem, we need to change the 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 username and password you set for the router.

  2) Go to Network > LAN.

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

  4) Click Save.



LAN Settings

MAC Address: 00:0A:EB:13:09:69

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

- Restart the modem and the router.

  1) Power off your modem and the router, and leave them off for 1 minute.

  2) Power on your modem first, and wait about 2 minutes.

  3) Power on the router, and wait another 1 or 2 minutes and check the internet access.

- Double check the Internet Connection Type.

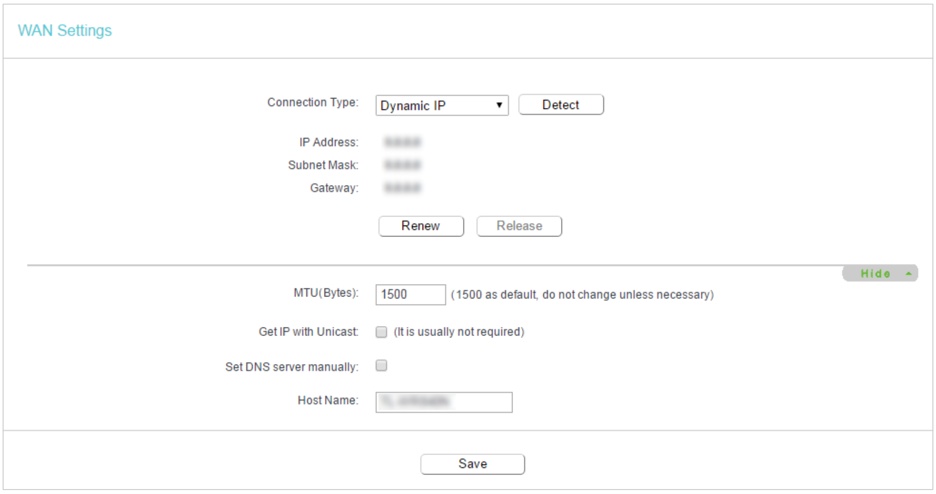
  1) Confirm your Internet Connection Type, which can be learned from the ISP.

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

  3) Go to Network > WAN.

  4) Select your WAN Connection Type and fill in other parameters.

  5) Click Save.



WAN Settings

Connection Type: Dynamic IP ▾ Detect

IP Address: [redacted]

Subnet Mask: [redacted]

Gateway: [redacted]

Renew Release

Hide ▴

MTU(Bytes): 1500 (1500 as default, do not change unless necessary)

Get IP with Unicast: □ (It is usually not required)

Set DNS server manually: □

Host Name: [redacted]

Save

6) Restart the modem and the router.

- Please upgrade the firmware of the router.

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

Q5. What should I do if I cannot find my wireless network or I cannot connect to 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 a 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) Clicking 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 My Computer on Desktop, and select Manage to open Computer Management window.

4) Expand Services and Applications > Services, and 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 Start and make sure the Service status is Started. And then click OK.

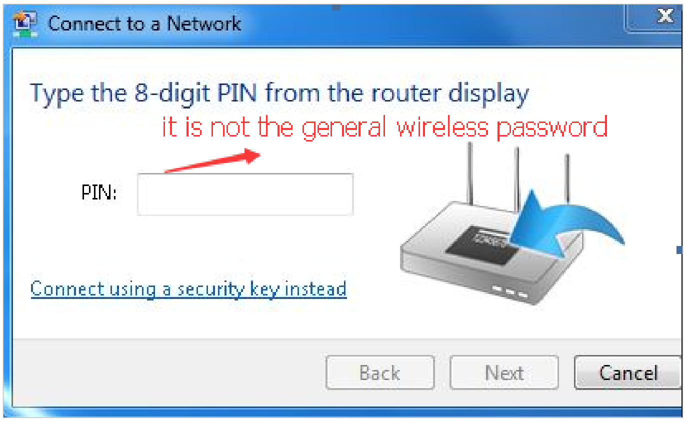
If you can find other wireless network except your own, please follow the steps below:

- 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 closer if it is currently too far away.

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.



Connect to a Network

Type the 8-digit PIN from the router display

it is not the general wireless password

PIN:

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

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:

This device may not cause harmful interference.

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)

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 RSSs. 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.

Antenna	2 fixed Omni Directional Antennas

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.

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

Safety Information

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