



User Guide

300Mbps Wireless N Nano Router
TL-WR802N

Contents

About This Guide	1
 Chapter 1. Get to Know About Your Router	 2
1. 1. Product Overview	3
1. 2. Panel Layout	3
 Chapter 2. Connect the Hardware	 4
2. 1. Position Your Router	5
2. 2. Connect Your Router	5
 Chapter 3. Set Up Internet Connection Via Quick Setup Wizard	 8
3. 1. Log In to the Router	9
3. 2. Set Up Internet Connection	9
 Chapter 4. Configure the Router in Wireless Router Mode	 11
4. 1. Status	12
4. 2. Operation Mode	13
4. 3. Network	14
4. 4. Wireless	22
4. 5. Guest Network	30
4. 6. DHCP	31
4. 7. Forwarding	33
4. 8. Security	37
4. 9. Parental Controls	40
4. 10. Access Control	41
4. 11. Advanced Routing	44
4. 12. Bandwidth Control	45
4. 13. IP & MAC Binding	47
4. 14. Dynamic DNS	48
4. 15. IPv6	51
4. 16. System Tools	56
4. 17. Log out	64
 Chapter 5. Configure the Router in WISP Mode (Hotspot Mode)	 65
5. 1. Status	66
5. 2. Operation Mode	67

5.3.	Network	68
5.4.	Wireless	76
5.5.	Guest Network.....	85
5.6.	DHCP.....	86
5.7.	Forwarding	88
5.8.	Security	92
5.9.	Parental Controls	95
5.10.	Access Control	96
5.11.	Advanced Routing	99
5.12.	Bandwidth Control.....	100
5.13.	IP & MAC Binding	101
5.14.	Dynamic DNS.....	103
5.15.	IPv6	105
5.16.	System Tools	110
5.17.	Log out.....	119

Chapter 6. Configure the Router in Access Point Mode 120

6.1.	Status	121
6.2.	Operation Mode	122
6.3.	Network	122
6.4.	Wireless	123
6.5.	Guest Network.....	131
6.6.	DHCP.....	133
6.7.	System Tools	135
6.8.	Log out.....	143

Chapter 7. Configure the Router in Range Extender Mode 144

7.1.	Status	145
7.2.	Operation Mode	146
7.3.	Network	146
7.4.	Wireless	147
7.5.	DHCP.....	152
7.6.	System Tools	154
7.7.	Log out.....	160

Chapter 8. Configure the Router in Client Mode 161

8.1.	Status	162
8.2.	Operation Mode	163
8.3.	Network	163
8.4.	Wireless	164

8. 5.	DHCP.....	165
8. 6.	System Tools	167
8. 7.	Log out	174
	FAQ	175

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
<u>Underlined</u>	Underlined words or phrases are hyperlinks. You can click to redirect to a website or a specific section.
Teal	Contents to be emphasized and texts on the web page are in teal, including the menus, items, buttons 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.

*Maximum wireless signal rates are the physical rates derived from IEEE Standard 802.11 specifications. Actual wireless data throughput and wireless coverage are not guaranteed and will vary as a result of network conditions, client limitations, and environmental factors, including building materials, obstacles, volume and density of traffic, and client location.

More Info

The latest software, management app and utility are available from the [Download Center](https://www.tp-link.com/support) at <https://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 <https://www.tp-link.com>.

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

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

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

To meet the wireless needs of almost any situation you might encounter, the TP-Link portable router, with multiple operation modes, is designed for home and travel use. The portable size of the router means that you can put it in your pocket and take it with you wherever you go. The built-in adapter makes it perfect for travelers, students, and anyone else living a life on the go.

1.2. Panel Layout

1.2.1. Top View



LED Explanation

Status	Indication
Solid	The router is connected to the host Wi-Fi network or internet.
Blinking steadily	The router is disconnected from the host Wi-Fi network or internet.
Blinking irregularly	The router is booting or updating firmware.

Port and Button Description

Item	Description
LAN/WAN Port	This port functions as the WAN port in Wireless Router mode and as the LAN port in WISP, Range Extender and Client modes. This port is for connecting to the existing router in Access Point mode.
Power Port	Connect to a USB charger, power adapter or computer USB port via the USB cable for power supply.
Reset Button	Use a pin to press and hold the Reset button until the LED blinks.

Chapter 2

Connect the Hardware

This chapter contains the following sections:

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

2.1. Position Your Router

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

2.2. Connect Your Router

There are five operation modes supported by this router: Wireless Router, WISP, Access Point, Range Extender and Client. Please determine the operation mode you need and carry out the corresponding steps.

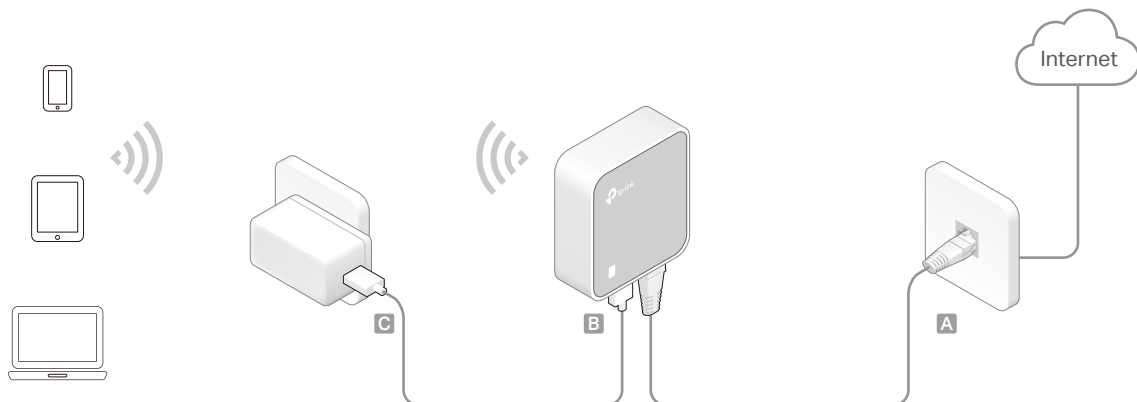
2.2.1. Wireless Router Mode

Create an instant private wireless network and share internet to multiple Wi-Fi devices. This mode is suitable for hotel rooms and home networks.

1. Connect the hardware according to Step A to C.
2. Use the default Wi-Fi Name and Wi-Fi Password printed on the Wi-Fi Info Card or on the product label at the bottom of your router to connect to the Wi-Fi.

Note:

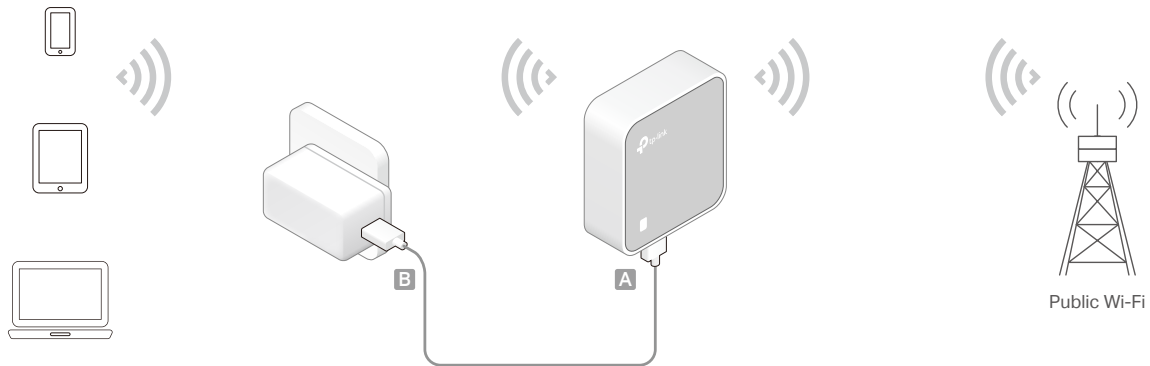
- If the hotel's internet has an authentication process, you will need to authenticate only once and only on one device.
- Check the internet connection on your laptop or smartphone, and please note that:
 - If you can access the internet without any restriction, no configuration is required.
 - If you're directed to an authentication page, please complete it to access the internet.



2. 2. 2. WISP Mode (Hotspot Mode)

In WISP mode, the router enables multiple users to share internet connection anywhere public Wi-Fi exists. For example: hotel room, trade show, ...

1. Connect the router according to Step A to B.
2. Use the default Wi-Fi Name and Wi-Fi Password printed on the Wi-Fi Info Card or on the product label at the bottom of your router to connect to the Wi-Fi.



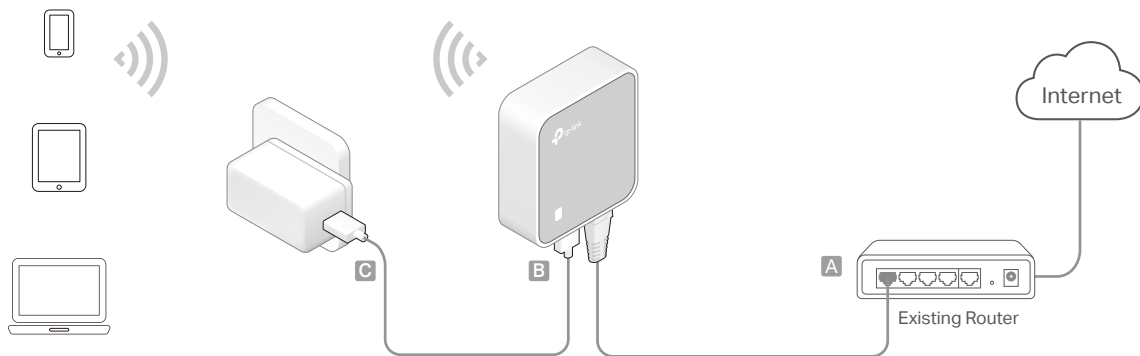
2. 2. 3. Access Point Mode

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

1. Connect the router according to Step A to C.
2. Use the default Wi-Fi Name and Wi-Fi Password printed on the Wi-Fi Info Card or on the product label at the bottom of your router to connect to the Wi-Fi.

Note:

If the hotel's internet has an authentication process, you will need to authenticate it on EACH device.

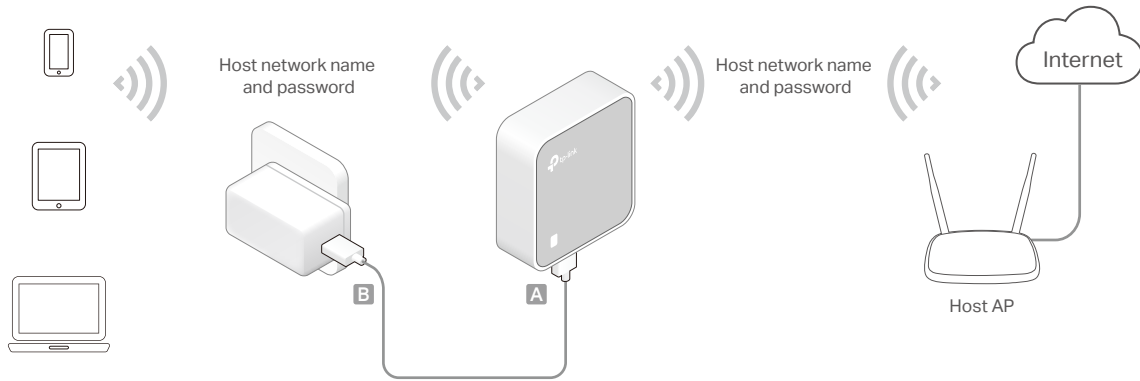


2. 2. 4. Range Extender Mode

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

router to maintain a stable wireless connection. The repeated signal will display the same network name and password as those of your existing wireless network.

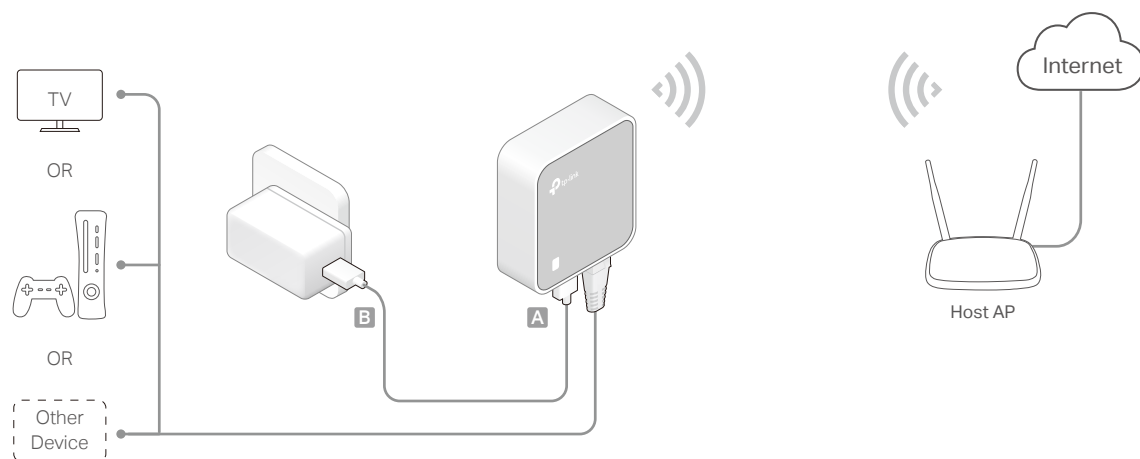
1. Connect the router according to Step A to B.
2. Use the default Wi-Fi Name and Wi-Fi Password printed on the Wi-Fi Info Card or on the product label at the bottom of your router to connect to the Wi-Fi.



2. 2. 5. Client Mode

In this mode, this device can be connected to another device via an Ethernet cable and act as an adapter to grant your wired devices access to a wireless network, especially for a smart TV, media player, or game console.

1. Connect the router according to Step A to B.
2. On your wireless device, use the default Wi-Fi Name and Wi-Fi Password printed on the Wi-Fi Info Card or on the product label at the bottom of your router to connect to the Wi-Fi.



Chapter 3

Set Up Internet Connection Via Quick Setup Wizard

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

It contains the following sections:

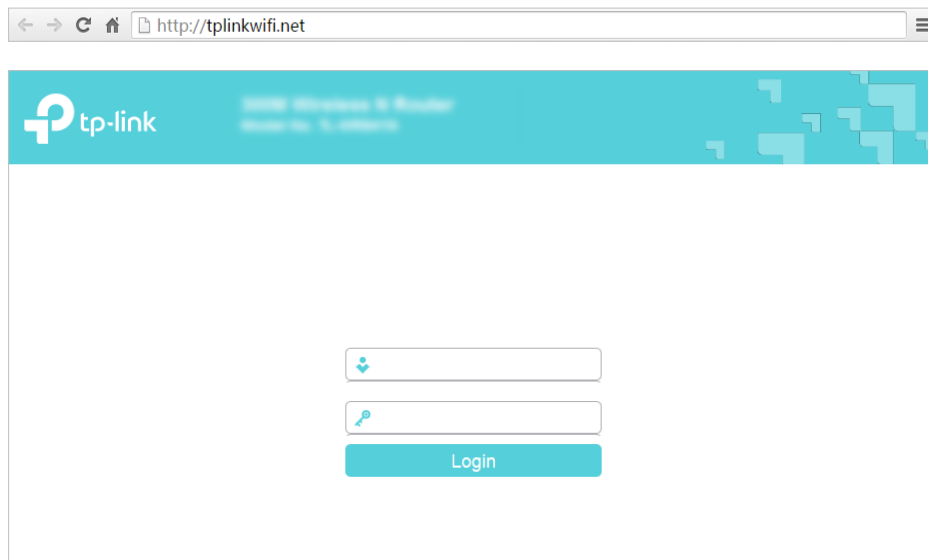
- [Log In to the Router](#)
- [Set Up Internet Connection](#)

3.1. Log In to the Router

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

Follow the steps below to log into your router.

1. Set up the TCP/IP Protocol in [Obtain an IP address automatically](#) mode on your computer.
2. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router. The default one is [admin](#) (all lowercase) for both username and password.



Note:

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

3.2. Set Up Internet Connection

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

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [Quick Setup](#) and click [Next](#) to start.
3. Choose the working mode you need and click [Next](#).

Quick Setup - Operation Mode

Choose Operation Mode:

☒ **Wireless Router**
Share Internet connection from an Ethernet cable. For example, hotel room, small office...

☐ WISP

☐ Access Point

☐ Range Extender

☐ Client

Back **Next**

4. Follow the corresponding steps to connect your router to the internet.

Note:

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

Chapter 4

Configure the Router in Wireless Router Mode

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

It contains the following sections:

- [Status](#)
- [Operation Mode](#)
- [Network](#)
- [Wireless](#)
- [Guest Network](#)
- [DHCP](#)
- [Forwarding](#)
- [Security](#)
- [Parental Controls](#)
- [Access Control](#)
- [Advanced Routing](#)
- [Bandwidth Control](#)
- [IP&MAC Binding](#)
- [Dynamic DNS](#)
- [IPv6](#)
- [System Tools](#)
- [Log out](#)

4.1. 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	
Firmware Version:	2.0.1.3 (2018-08-16) (Build 170811 Rel.170811)
Hardware Version:	V1.0 (2018-08-16) (Build 170811 Rel.170811)
LAN	
MAC Address:	00:0A:EB:13:09:69
IP Address:	192.168.0.1
Subnet Mask:	255.255.255.0
Wireless	
Operation Mode:	Router
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
WAN	
MAC Address:	00:0A:EB:13:09:6A
IP Address:	0.0.0.0 (Dynamic IP)
Subnet Mask:	0.0.0.0
Default Gateway:	0.0.0.0 Unplugged
DNS Server:	0.0.0.0 0.0.0.0
System Up Time: 1 day(s) 06:50:47 Refresh	

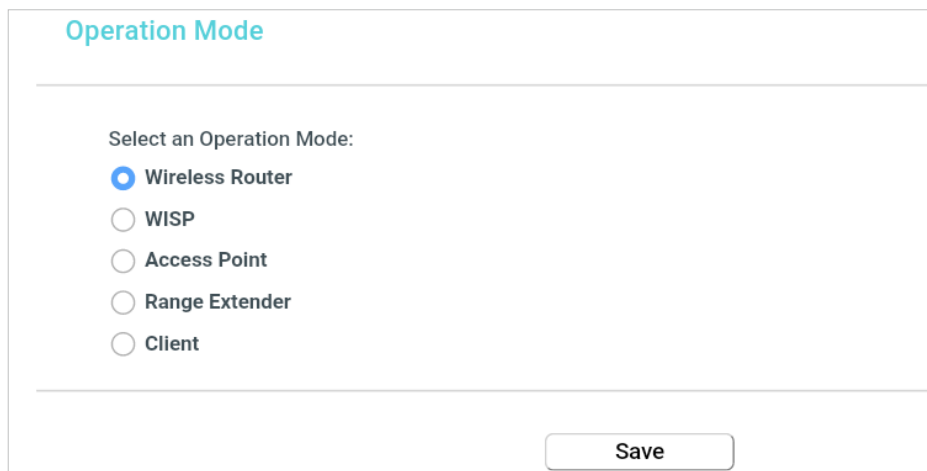
- [Firmware Version](#) - The version information of the router's firmware.
- [Hardware Version](#) - The version information of the router's hardware.
- [LAN](#) - This field displays the current settings of the LAN, and you can configure them on the [Network > LAN](#) page.
 - [MAC address](#) - The 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.
- **WAN** - This field displays the current settings of the WAN, and you can configure them on the **Network > WAN** 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.
- **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.

4.2. 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**.



The screenshot shows the 'Operation Mode' configuration page. At the top, the title 'Operation Mode' is in blue. Below it, a section titled 'Select an Operation Mode:' contains five radio button options: 'Wireless Router' (selected), 'WISP', 'Access Point', 'Range Extender', and 'Client'. A 'Save' button is located at the bottom right of the form.

4.3. Network

4.3.1. WAN

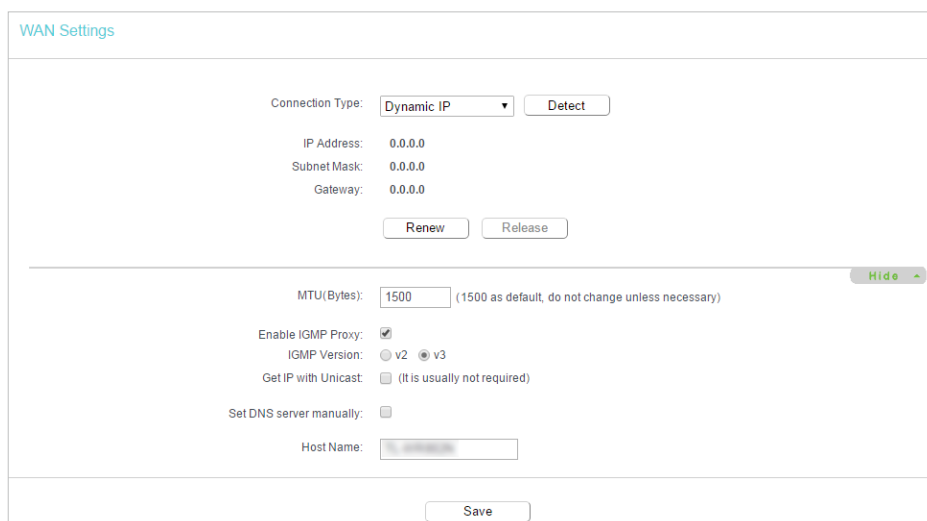
1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [Network](#) > [WAN](#).
3. Configure the IP parameters of the WAN and click [Save](#).

Dynamic IP

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

Click [Renew](#) to renew the IP parameters from your ISP.

Click [Release](#) to release the IP parameters.



The screenshot shows the 'WAN Settings' configuration page. The title 'WAN Settings' is in blue. The 'Connection Type' is set to 'Dynamic IP' with a dropdown arrow and a 'Detect' button. Below this, the IP Address, Subnet Mask, and Gateway are all set to '0.0.0.0'. There are 'Renew' and 'Release' buttons. A horizontal line separates the top section from the bottom section. In the bottom section, 'MTU(Bytes)' is set to '1500' with a note '(1500 as default, do not change unless necessary)' and a 'Hide' button. Below this, 'Enable IGMP Proxy' is checked. 'IGMP Version' has radio buttons for 'v2' and 'v3', with 'v3' selected. 'Get IP with Unicast' is unchecked with a note '(It is usually not required)'. 'Set DNS server manually' is unchecked. 'Host Name' is set to 'tplinkwifi.net'. A 'Save' button is at the bottom.

- **MTU(Bytes)** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU size unless required by your ISP.
- **Enable IGMP Proxy** - IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is enabled, and if you are not sure, please contact your ISP or just leave it.
- **Get IP with Unicast** - A few ISPs' DHCP servers do not support the broadcast applications. If you cannot get the IP address normally, you can choose this option. (It is rarely required.)
- **Set DNS server manually** - If your ISP gives you one or two DNS addresses, select Set DNS server manually and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned automatically from your ISP.
- **Host Name** - This option specifies the name of the router.

Static IP

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

The screenshot shows the 'WAN Settings' page. Under the 'Connection Type' dropdown, 'Static IP' is selected. Below this are input fields for 'IP Address', 'Subnet Mask', 'Gateway', 'Primary DNS Server', and 'Secondary DNS Server', all containing '0.0.0.0'. The 'Secondary DNS Server' field is marked as '(optional)'. Below these fields is a section for 'MTU(Bytes)' with a value of '1500' and a note '(1500 as default, do not change unless necessary)'. There is a 'Hide' button next to the MTU field. Below the MTU field is a checkbox for 'Enable IGMP Proxy' which is checked, and a radio button for 'IGMP Version' with 'v2' and 'v3' options, where 'v3' is selected. A 'Save' button is at the bottom of the form.

- **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.
- **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.
- **MTU (Bytes)** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU size unless required by your ISP.

- **Enable IGMP Proxy** - IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is enabled, and if you are not sure, please contact your ISP or just leave it.

PPPoE

If your ISP provides PPPoE connection, select **PPPoE**.

The screenshot shows the 'WAN Settings' page with the following fields and options:

- Connection Type:** A dropdown menu set to 'PPPoE' with a 'Detect' button next to it.
- PPP Username:** A text input field.
- PPP Password:** A text input field.
- Confirm password:** A text input field.
- Secondary Connection:** Radio buttons for 'Disabled' (selected), 'Dynamic IP', and 'Static IP (For Dual Access)'.
- Connection Mode:** Radio buttons for 'Always on' (selected), 'Connect on demand', and 'Connect manually'.
- Max Idle Time:** A text input field set to '15' with the unit 'minutes (0 meaning connection remains active at all times)'.
- Authentication Type:** A dropdown menu set to 'AUTO_AUTH'.
- Buttons:** 'Connect' and 'Disconnect' buttons.
- Service Name:** A text input field with a note '(do not change unless necessary)'.
- Server Name:** A text input field with a note '(do not change unless necessary)'.
- MTU(Bytes):** A text input field set to '1480' with a note '(1480 as default, do not change unless necessary)'.
- Enable IGMP Proxy:** A checked checkbox.
- IGMP Version:** Radio buttons for 'v2' and 'v3' (selected).
- Use IP address specified by ISP:** An unchecked checkbox.
- Echo request interval:** A text input field set to '0' with a note '(0-120 seconds, 0 meaning no request)'.
- Set DNS server manually:** An unchecked checkbox.
- Buttons:** A 'Save' button at the bottom.

- **PPP Username/Password** - Enter the user name and password provided by your ISP. These fields are case-sensitive.
- **Confirm Password** - Enter the Password provided by your ISP again to ensure the password you entered is correct.
- **Secondary Connection** - It's available only for PPPoE connection. If your ISP provides an extra connection type, select **Dynamic IP** or **Static IP** to activate the secondary connection.
- **Connection Mode**
 - **Always On** - In this mode, the internet connection will be active all the time.
 - **Connect on Demand** - In this mode, the internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the internet again. If you want to keep your internet connection active all the time, please enter 0 in the **Max Idle Time**

field. Otherwise, enter the number of minutes you want to have elapsed before your internet access disconnects.

- **Connect Manually** - You can click **Connect/Disconnect** to connect/disconnect immediately. This mode also supports the **Max Idle Time** function as **Connect on Demand** mode. The internet connection can be disconnected automatically after a specified inactivity period (Max Idle Time) and not be able to re-establish when you attempt to access the internet again.
- **Authentication Type** - Choose an authentication type.

Note:

Sometimes the connection cannot be terminated although you have specified the **Max Idle Time** because some applications are visiting the internet continually in the background.

- **Service Name/Server Name** - The service name and server name should not be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank will work.
- **MTU(Bytes)** - The default MTU size is 1480 bytes. It is not recommended that you change the default MTU size unless required by your ISP.
- **Enable IGMP Proxy** - IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is enabled, and if you are not sure, please contact your ISP or just leave it.
- **ISP Specified IP Address** - If your ISP does not automatically assign IP addresses to the router, please select **Use IP address specified by ISP** and enter the IP address provided by your ISP in dotted-decimal notation.
- **Echo Request Interval** - The router will detect Access Concentrator online at every interval. The default value is 0. You can input the value between 0 and 120. The value 0 means no detect.
- **DNS Server/Secondary DNS Server** - If your ISP does not automatically assign DNS addresses to the router, please select **Set DNS server manually** and enter the IP address in dotted-decimal notation of your ISP's primary DNS server. If a secondary DNS server address is available, enter it as well.

L2TP

If your ISP provides L2TP connection, please select **L2TP**.

- **Username/Password** - Enter the username and password provided by your ISP. These fields are case-sensitive.
- **Addressing Type** - Choose the addressing type given by your ISP, either Dynamic IP or Static IP. Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.
- **MTU(Bytes)** - The default MTU size is “1460” bytes, which is usually fine. It is not recommended that you change the default MTU Size unless required by your ISP.
- **Enable IGMP Proxy** - IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is enabled, and if you are not sure, please contact your ISP or just leave it.
- **Connection Mode**
 - **Always On** - In this mode, the internet connection will be active all the time.
 - **Connect on Demand** - In this mode, the internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the internet again. If you want to keep your internet connection active all the time, please enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your internet access disconnects.
 - **Connect Manually** - You can click **Connect/Disconnect** to connect/disconnect immediately. This mode also supports the **Max Idle Time** function as **Connect**

on Demand mode. The internet connection can be disconnected automatically after a specified inactivity period (Max Idle Time) and not be able to re-establish when you attempt to access the internet again.

Note:

Sometimes the connection cannot be terminated although you have specified the Max Idle Time because some applications are visiting the internet continually in the background.

PPTP

If your ISP provides PPTP connection, please select PPTP.

The screenshot shows the 'WAN Settings' configuration page. At the top, 'Connection Type' is set to 'PPTP' with a 'Detect' button. Below are fields for 'Username' and 'Password', followed by 'Connect' and 'Disconnect' buttons. The 'Addressing Type' section has 'Dynamic IP' selected. Below this are fields for 'Server IP Address/Name', 'IP Address', 'Subnet Mask', 'Gateway', and 'DNS Server', all with default values of 0.0.0.0. Further down are 'Internet IP Address' and 'Internet DNS' fields, also with 0.0.0.0. The 'MTU(Bytes)' field is set to 1420, with a note '(1420 as default, do not change unless necessary)'. The 'Enable IGMP Proxy' checkbox is checked. 'IGMP Version' has 'v2' selected. 'Connection Mode' has 'Always on' selected, with options for 'Connect on demand' and 'Connect manually'. The 'Max Idle Time' is set to 15 minutes, with a note '(0 meaning connection remains active at all times)'. A 'Save' button is at the bottom.

- **Username/Password** - Enter the username and password provided by your ISP. These fields are case-sensitive.
- **Addressing Type** - Choose the addressing type given by your ISP, either Dynamic IP or Static IP. Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.
- **MTU(Bytes)** - The default MTU size is "1420" bytes, which is usually fine. It is not recommended that you change the default MTU Size unless required by your ISP.
- **Enable IGMP Proxy** - IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is enabled, and if you are not sure, please contact your ISP or just leave it.
- **Connection Mode**

- **Always On** - In this mode, the internet connection will be active all the time.
- **Connect on Demand** - In this mode, the internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the internet again. If you want to keep your internet connection active all the time, please enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your internet access disconnects.
- **Connect Manually** - You can click **Connect/Disconnect** to connect/disconnect immediately. This mode also supports the **Max Idle Time** function as **Connect on Demand** mode. The internet connection can be disconnected automatically after a specified inactivity period (Max Idle Time) and not be able to re-establish when you attempt to access the internet again.

Note:

Sometimes the connection cannot be terminated although you have specified the **Max Idle Time** because some applications are visiting the internet continually in the background.

BigPond Cable

If your ISP provides BigPond cable connection, please select **BigPond Cable**.

The screenshot shows the 'WAN Settings' configuration page. At the top, 'WAN Settings' is written in blue. Below it, the 'Connection Type' is set to 'BigPond Cable' with a dropdown arrow and a 'Detect' button. There are input fields for 'Username:', 'Password:', 'Auth Server:', and 'Auth Domain:'. The 'MTU(Bytes):' is set to '1500' with a note '(1500 as default, do not change unless necessary)'. The 'Enable IGMP Proxy:' checkbox is checked. The 'IGMP Version:' has radio buttons for 'v2' and 'v3', with 'v3' selected. The 'Connection Mode:' has radio buttons for 'Always on', 'Connect on demand', and 'Connect manually', with 'Always on' selected. The 'Max Idle Time:' is set to '15' minutes with a note '(0 meaning connection remains active at all times)'. At the bottom, there are 'Connect' and 'Disconnect' buttons, and a 'Save' button at the very bottom.

- **Username/Password** - Enter the username and password provided by your ISP. These fields are case-sensitive.
- **Auth Server** - Enter the authenticating server IP address or host name.
- **Auth Domain** - Type in the domain suffix server name based on your location.
- **MTU(Bytes)** - The default MTU size is 1500 bytes. It is not recommended that you change the default MTU size unless required by your ISP.

- **Enable IGMP Proxy** - IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is enabled, and if you are not sure, please contact your ISP or just leave it.
- **Connection Mode**
 - **Always On** - In this mode, the internet connection will be active all the time.
 - **Connect on Demand** - In this mode, the internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the internet again. If you want to keep your internet connection active all the time, please enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your internet access disconnects.
 - **Connect Manually** - You can click **Connect/Disconnect** to connect/disconnect immediately. This mode also supports the **Max Idle Time** function as **Connect on Demand** mode. The internet connection can be disconnected automatically after a specified inactivity period (Max Idle Time) and not be able to re-establish when you attempt to access the internet again.

4.3.2. 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**.

LAN Settings

MAC Address: 30:B5:C2:E6:9F:CE

IP Address:

Subnet Mask:

Enable IGMP Snooping: ☒

- **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 of your router (the default one is 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.
- **Enable IGMP Snooping** - IGMP snooping is designed to prevent hosts on a local network from receiving traffic for a multicast group they have not explicitly joined.

IGMP snooping is especially useful for bandwidth-intensive IP multicast applications such as IPTV.

Note:

- If you have changed the IP address, you must use the new IP address to log in.
- 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 automatically, but the Virtual Server and DMZ Host will not take effect until they are re-configured.

4.3.3. MAC Clone

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Network > MAC Clone**.
3. Configure the WAN MAC address and click **Save**.

MAC Clone	
WAN MAC Address:	00:0A:EB:13:09:6A <button>Restore Factory MAC</button>
Your PC's MAC Address:	40:8D:5C:89:74:B5 <button>Clone MAC Address</button>
Save	

- **WAN MAC Address** - This field displays the current MAC address of the WAN port. If your ISP requires you to register the MAC address, please enter the correct MAC address in this field. Click **Restore Factory MAC** to restore the MAC address of WAN port to the factory default value.
- **Your PC's MAC Address** - This field displays the MAC address of the PC that is managing the router. If the MAC address is required, you can click **Clone MAC Address** and this MAC address will be filled in the **WAN MAC Address** field.

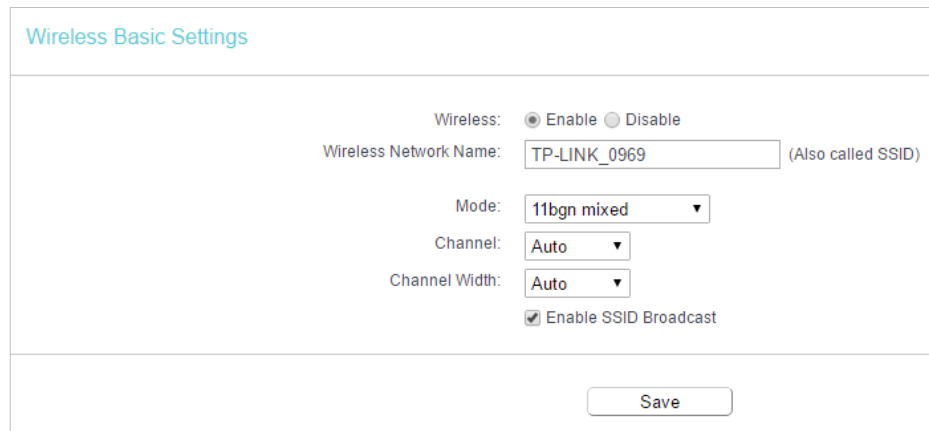
Note:

- You can only use the MAC Address Clone function for PCs on the LAN.
- If you have changed the WAN MAC address when the WAN connection is PPPoE, it will not take effect until the connection is re-established.

4.4. Wireless

4.4.1. 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**.

The image shows a web interface for configuring wireless settings. At the top, there's a title 'Wireless Basic Settings'. Below it, there are several configuration options: 'Wireless' with radio buttons for 'Enable' (selected) and 'Disable'; 'Wireless Network Name' with a text box containing 'TP-LINK_0969' and a note '(Also called SSID)'; 'Mode' with a dropdown menu showing '11bgn mixed'; 'Channel' with a dropdown menu showing 'Auto'; 'Channel Width' with a dropdown menu showing 'Auto'; and a checkbox for 'Enable SSID Broadcast' which is checked. At the bottom right, there is a 'Save' button.

Wireless Basic Settings

Wireless: ☒ Enable ☐ Disable

Wireless Network Name: (Also called SSID)

Mode:

Channel:

Channel Width:

☒ Enable SSID Broadcast

Save

- **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).

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.

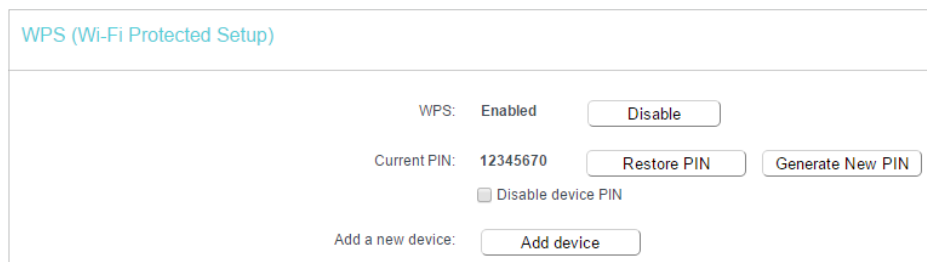
Note:

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 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)

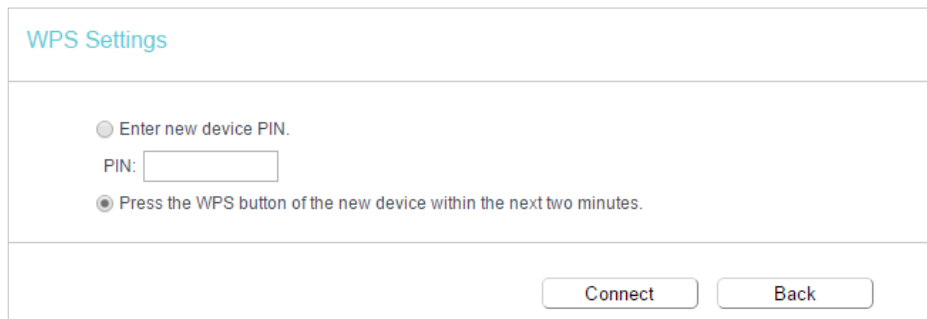
WPS: **Enabled** [Disable](#)

Current PIN: **12345670** [Restore PIN](#) [Generate New PIN](#)

☐ Disable device PIN

Add a new device: [Add device](#)

2. Select [Press the WPS button of the new device within the next two minutes](#) and click [Connect](#).



WPS Settings

☐ Enter new device PIN.

PIN:

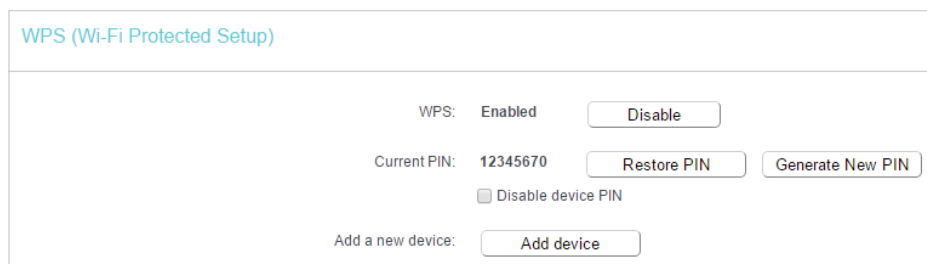
☒ Press the WPS button of the new device within the next two minutes.

[Connect](#) [Back](#)

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)

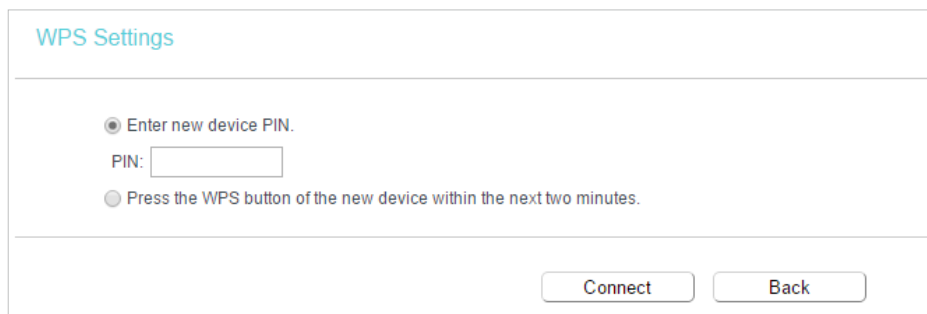
WPS: **Enabled** [Disable](#)

Current PIN: **12345670** [Restore PIN](#) [Generate New PIN](#)

☐ Disable device PIN

Add a new device: [Add device](#)

2. Select [Enter new device PIN](#), enter your client device's current PIN in the [PIN](#) field and click [Connect](#).



WPS Settings

☒ Enter new device PIN.

PIN:

☐ Press the WPS button of the new device within the next two minutes.

[Connect](#) [Back](#)

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** Disable

Current PIN: **12345670** Restore PIN Generate New PIN

☐ Disable device PIN

Add a new device: Add device

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

4. 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)

Version: **WPA2-PSK**

Encryption: **AES**

Wireless Password: **87338003**

Group Key Update Period: **0**

☐ WPA/WPA2 - Enterprise

Version: **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

Save

- **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.
 - **Version** - 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.
 - **Version** - 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** - 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.

4.4.4. Wireless MAC Filtering

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

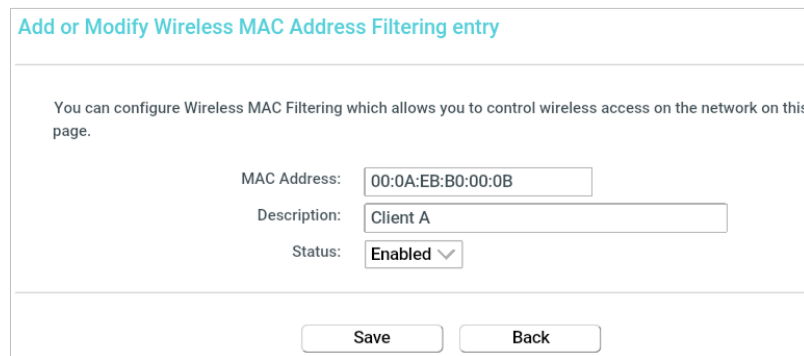
I want to:

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:

Description:

Status:

- 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 ☐ Disable

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:00:00:0B	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.

4. 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.

Wireless Advanced

Transmit Power:

Beacon Interval: (40-1000)

RTS Threshold: (1-2346)

Fragmentation Threshold: (256-2346)

DTIM Interval: (1-15)

☒ Enable Short GI
☐ Enable Client Isolation
☒ Enable WMM

- **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.

4. 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.

Wireless Stations Status					
Wireless Stations Currently Connected: 1 Refresh					
ID	MAC Address	Current Status	Received Packets	Sent Packets	SSID
1	44:00:10:BF:3B:A7	Associated	29	19	TP-LINK_XXXXXX

- **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.

4.5. Guest Network

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

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [Guest Network](#).
3. Enable the [Guest Network](#) function.
4. Create a network name for your guest network.
5. Select the [Security](#) type and create the [Password](#) of the guest network.
6. Select [Schedule](#) from the [Access Time](#) drop-down list and customize it for the guest network.
7. Click [Save](#).

Guest Network

Allow Guests To Access My Local Network: Disable

Guest Network Isolation: Disable

Guest Network Bandwidth Control: Disable

Guest Network: ☒ Enable ☐ Disable

Network Name:

Max Guests number:

Security: WPA/WPA2 - Personal

Authentication Type: Auto

Encryption: Auto

Wireless Password:
(Enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

Group Key Update Period: (seconds, minimum is 30, 0 means no update)

Access Time: Schedule

Click the schedule table or use the 'Add' button to choose the period on which you need the guest network off automatically!

The Schedule is based on the time of the Router. The time can be set in "System Tools -> Time Settings".

Wireless Schedule: ☐ Enable ☒ Disable

Apply To: Each Day

Start Time: 00:00

End Time: 24:00

Add

Time	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
Sun.															
Mon.															
Tues.															
Wed.															
Thur.															
Fri.															
Sat.															

Clear Schedule

Save

- [Allow Guest To Access My Local Network](#) - If enabled, guests can access the local network and manage it.
- [Guest Network Isolation](#) - If enabled, guests are isolated from each other.
- [Enable Guest Network Bandwidth Control](#) - If enabled, the Guest Network Bandwidth Control rules will take effect.

Note:

The range of bandwidth for guest network is calculated according to the setting of Bandwidth Control on the [Bandwidth Control](#) page.

4.6. DHCP

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

4.6.1. DHCP Settings

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [DHCP > DHCP Settings](#).
3. Specify DHCP server settings and click [Save](#).

DHCP Settings

DHCP Server: ☐ Disable ☒ Enable

Start IP Address:

End IP Address:

Lease Time: minutes (1~2880 minutes, the default value is 120)

Default Gateway: (optional)

Default Domain: (optional)

DNS Server: (optional)

Secondary DNS Server: (optional)

- [DHCP Server](#) - Enable or disable the DHCP server. If disabled, you must have another DHCP server within your network or else you must configure the computer manually.
- [Start IP Address](#) - Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.0.100 is the default start address.
- [End IP Address](#) - Specify an IP address for the DHCP Server to end with when assigning IP addresses. 192.168.0.199 is the default end address.

- **Address Lease Time** - The Address Lease Time is the amount of time a network user will be allowed to connect to the router with the current dynamic IP Address. When time is up, the user will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 2880 minutes. The default value is 120.
- **Default Gateway (Optional)** - It is suggested to input the IP address of the LAN port of the router. The default value is 192.168.0.1.
- **Default Domain (Optional)** - Input the domain name of your network.
- **DNS Server (Optional)** - Input the DNS IP address provided by your ISP.
- **Secondary DNS Server (Optional)** - Input the IP address of another DNS server if your ISP provides two DNS servers.

Note:

To use the DHCP server function of the router, you must configure all computers on the LAN as [Obtain an IP Address automatically](#).

4. 6. 2. DHCP Clients List

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **DHCP > DHCP Clients List** to view the information of the clients connected to the router.

DHCP Clients List				
This page displays information of all DHCP clients on the network.				
ID	Client Name	MAC Address	Assigned IP	Lease Time
1	Camille	40:8D:5C:89:74:B5	192.168.0.100	00:00:32
2	iPhone	34:E2:FD:14:1D:0D	192.168.0.101	00:00:55
Refresh				

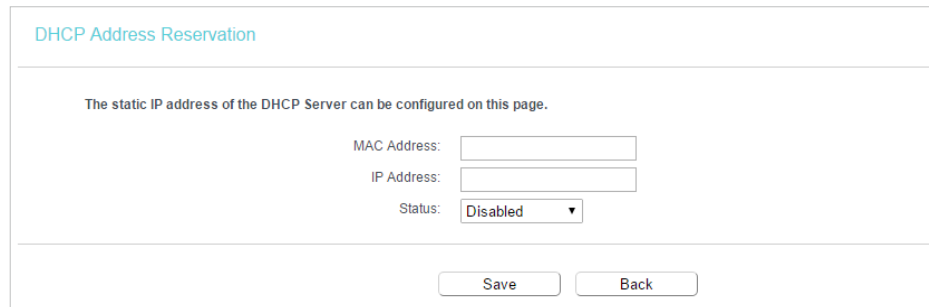
- **Client Name** - The name of the DHCP client.
- **MAC Address** - The MAC address of the DHCP client.
- **Assigned IP** - The IP address that the router has allocated to the DHCP client.
- **Lease Time** - The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic IP address will be automatically assigned to the user.

You cannot change any of the values on this page. To update this page and show the current attached devices, click [Refresh](#).

4. 6. 3. Address Reservation

You can reserve an IP address for a specific client. When you specify a reserved IP address for a PC on the LAN, this PC will always receive the same IP address each time when it accesses the DHCP server.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **DHCP > Address Reservation**.
3. Click **Add New** and fill in the blanks.



DHCP Address Reservation

The static IP address of the DHCP Server can be configured on this page.

MAC Address:

IP Address:

Status: Disabled ▼

Save Back

- 1) Enter the MAC address (in XX:XX:XX:XX:XX:XX format.) of the client for which you want to reserve an IP address.
- 2) Enter the IP address (in dotted-decimal notation) which you want to reserve for the client.
- 3) Leave the **Status** as **Enabled**.
- 4) Click **Save**.

4.7. 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.

4.7.1. Virtual Server

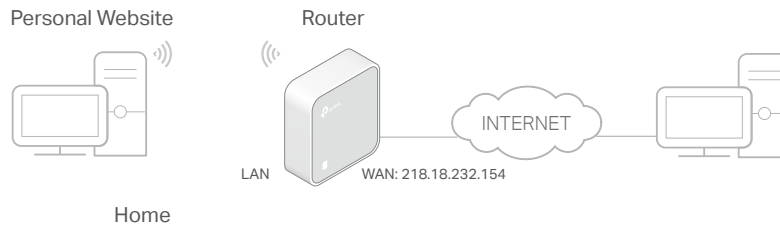
When you build up a server in the local network and want to share it on the internet, Virtual Servers can realize the service and provide it to internet users. At the same time virtual servers can keep the local network safe as other services are still invisible from the internet.

Virtual Servers can be used to set up public services in your local network, such as HTTP, FTP, DNS, POP3/SMTP and Telnet. Different service uses different service port. Port 80 is used in HTTP service, port 21 in FTP service, port 25 in SMTP service and port 110 in POP3 service. Please verify the service port number before 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 in my home PC (192.168.0.100). I hope that my friends on the internet can visit my website in some way. My PC is connected to the router with the WAN IP address 218.18.232.154.



1. Set your PC to a static IP address, for example 192.168.0.100.
2. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
3. Go to [Forwarding > Virtual Server](#).
4. Click [Add New](#). Select [HTTP](#) from the [Common Service Port](#) list. The service port, internal port and protocol will be automatically filled in. Enter the PC's IP address 192.168.0.100 in the [IP Address](#) field.

Virtual Server	
Service Port:	80 (XX-XX or XX)
IP Address:	192.168.0.100
Internal Port:	80 (XX or keep empty. If it's empty, Internal port equals to Service port)
Protocol:	TCP
Status:	Enabled
Common Service Port:	HTTP
Save Back	

5. Leave the status as [Enabled](#) and click [Save](#).

Note:

- 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 [Common Service Port](#) list, 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 [Service 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.

Note:

- If you have changed the default [Service Port](#), you should use [http:// WAN IP: Service Port](#) to visit the website.
- Some specific service ports are forbidden by the ISP, if you fail to visit the website, please use another service port.

4.7.2. 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 username and password you set for the router.
2. Go to [Forwarding > Port Triggering](#).
3. Click [Add New](#). Select the desired application from the [Common Service Port](#) list. The [Trigger Port](#) and [Open Port](#) will be automatically filled in. The following picture takes application [MSN Gaming Zone](#) as an example.

Port Trigger

Trigger Port: 47624 (XX)

Trigger Protocol: ALL

Open Port: 2300-2400,28800-29 (XX or XX-XX or XX-XX,XX)

Open Protocol: ALL

Status: Enabled

Common Service Port: MSN Gaming Zone

Save Back

4. Leave the status as [Enabled](#) and click [Save](#).

Note:

- You can add multiple port triggering rules as needed.
- The triggering ports can not be overlapped.
- If the application you need is not listed in the [Common Service Port](#) list, please enter the parameters manually. You should verify the open ports the application uses first and enter them in [Open Port](#) field. You can input at most 5 groups of ports (or port sections). Every group of ports must be set apart with ",". For example, 2000-2038, 2050-2051, 2085, 3010-3030.

4.7.3. 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.

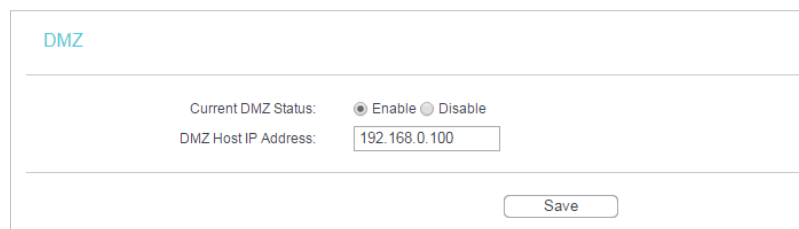
I want to:

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 username and 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** field.



DMZ	
Current DMZ Status:	☒ Enable ☐ Disable
DMZ Host IP Address:	192.168.0.100
Save	

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.

4.7.4. UPnP

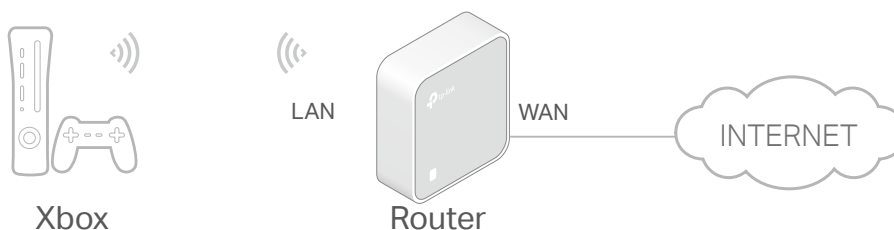
The UPnP (Universal Plug and Play) protocol allows the applications or host devices to automatically find the front-end NAT device and send request to it to open the

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 username and password you set for the router.
2. Go to **Forwarding > UPnP**.
3. Click **Disable** or **Enable** according to your needs.

UPnP						
Current UPnP Status: Enabled Disable						
Current UPnP Settings List						
ID	App Description	External Port	Protocol	Internal Port	IP Address	Status
Refresh						

4.8. Security

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

4.8.1. Basic Security

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

2. Go to [Security > Basic Security](#), and you can enable or disable the security functions.

Basic Security

Firewall

Enable SPI Firewall: ☒

VPN

PPTP Pass-through: ☒ Enable ☐ Disable

L2TP Pass-through: ☒ Enable ☐ Disable

IPSec Pass-through: ☒ Enable ☐ Disable

ALG

FTP ALG: ☒ Enable ☐ Disable

TFTP ALG: ☒ Enable ☐ Disable

H323 ALG: ☒ Enable ☐ Disable

SIP ALG: ☒ Enable ☐ Disable

RTSP ALG: ☒ Enable ☐ Disable

Save

- **Firewall** - A firewall protects your network from internet attacks.
 - **Enable SPI Firewall** - SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol. SPI Firewall is enabled by default.
- **VPN** - VPN Passthrough must be enabled if you want to allow VPN tunnels using IPSec, PPTP or L2TP protocols to pass through the router's firewall.
 - **PPTP Pass-through** - Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. If you want to allow PPTP tunnels to pass through the router, you can keep the default (Enabled).
 - **L2TP Pass-through** - Layer 2 Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the internet on the Layer 2 level. If you want to allow L2TP tunnels to pass through the router, you can keep the default (Enabled).
 - **IPSec Pass-through** - Internet Protocol Security (IPSec) is a suite of protocols for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. If you want to allow IPSec tunnels to pass through the router, you can keep the default (Enabled).
- **ALG** - It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged

into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc.

- **FTP ALG** - To allow FTP clients and servers to transfer data across NAT, keep the default **Enable**.
- **TFTP ALG** - To allow TFTP clients and servers to transfer data across NAT, keep the default **Enable**.
- **H323 ALG** - To allow Microsoft NetMeeting clients to communicate across NAT, keep the default **Enable**.
- **SIP ALG** - To allow some multimedia clients to communicate across NAT, click **Enable**.
- **RTSP ALG** - To allow some media player clients to communicate with some streaming media servers across NAT, click **Enable**.

3. Click **Save**.

4. 8. 2. Advanced Security

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Security** > **Advanced Security**, and you can protect the router from being attacked by ICMP-Flood, UDP Flood and TCP-SYN Flood.

Advanced Security

DoS Protection: ☐ Enable ☒ Disable

☐ Enable ICMP-Flood Attack Filtering
ICMP-Flood Packets Threshold (5~3600): packets/second

☐ Enable UDP-Flood Attack Filtering
UDP-Flood Packets Threshold (5~3600): packets/second

☐ Enable TCP-SYN-Flood Attack Filtering
TCP-SYN-Flood Packets Threshold (5~3600): packets/second

☒ Forbid Ping Packet From WAN Port
☐ Forbid Ping Packet From LAN Port

- **DoS Protection** - Denial of Service protection. Select Enable or Disable to enable or disable the DoS protection function. Only when it is enabled, will the flood filters be enabled.

Note:

Dos Protection will take effect only when the Statistics in **System Tools** > **Statistics** is enabled.

- [Enable ICMP-FLOOD Attack Filtering](#) - Tick the checkbox to enable or disable this function.
 - [ICMP-FLOOD Packets Threshold \(5~3600\)](#) - The default value is 50. Enter a value between 5 ~ 3600. When the number of the current ICMP-FLOOD packets is beyond the set value, the router will startup the blocking function immediately.
 - [Enable UDP-FLOOD Filtering](#) - Tick the checkbox to enable this function.
 - [UDP-FLOOD Packets Threshold \(5~3600\)](#) - The default value is 500. Enter a value between 5 ~ 3600. When the number of the current UPD-FLOOD packets is beyond the set value, the router will startup the blocking function immediately.
 - [Enable TCP-SYN-FLOOD Attack Filtering](#) -Tick the checkbox to enable or disable this function.
 - [TCP-SYN-FLOOD Packets Threshold \(5~3600\)](#) - The default value is 50. Enter a value between 5 ~ 3600. When the number of the current TCP-SYN-FLOOD packets is beyond the set value, the router will startup the blocking function immediately.
 - [Ignore Ping Packet From WAN Port](#) - The default setting is disabled. If enabled, the ping packet from the internet cannot access the router.
 - [Forbid Ping Packet From LAN Port](#) - The default setting is disabled. If enabled, the ping packet from LAN cannot access the router. This function can be used to defend against some viruses.
3. Click [Save](#).
 4. Click [Blocked DoS Host List](#) to display the DoS host table by blocking.

4.9. 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.

For example, you want the children's PC with the MAC address 00:11:22:33:44:AA can access www.tp-link.com on Saturday only while the parent PC with the MAC address 00:11:22:33:44:BB is without any restriction.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [Parental Controls](#).
3. Tick the [Enable Parental Controls](#) checkbox, enter the MAC address 00:11:22:33:44:BB in the [MAC Address of Parental PC](#) field and then click [Save](#).

Parental Controls

Parental Controls can be used to administer all Internet activity including limiting usage and/or access to specific websites to all clients on the network for a specified period of time. The Schedule is based on the time of the Router. The time can be set in "System Tools -> [Time Settings](#)".

☒ Enable Parental Controls

MAC Address Of Parental PC:

MAC Address of Current PC: [Copy to Above](#)

[Save](#)

4. Enter 00:11:22:33:44:AA in the **MAC Address 1** field.

MAC Address - 1:

MAC Address - 2:

MAC Address - 3:

MAC Address - 4:

MAC Address in current LAN: [Copy to](#)

5. Select **Each Week** from the **Apply To** drop-down list, and select **Sat.** Select **00:00** as the **Start Time** and Select **24:00** as the **End Time**. And then click **Add**.

Apply To: **Start Time:** **End Time:** [Add](#)

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

Time	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
Sun.															
Mon.															
Tues.															
Wed.															
Thur.															
Fri.															
Sat.															

[Clear Schedule](#)

6. Enter **www.tp-link.com** in the **Add URL** field. Click **Add**.

Add URL: [Add](#)

☐ [Details](#)

[Delete Selected](#) (Will not take effect until you save these changes)

7. Click **Save**.

4. 10. Access Control

Access Control is used to deny or allow specific client devices to access your network with access time and content restrictions.

I want to:

Deny or allow specific client devices to access my network with access time and

content restrictions.

For example, If you want to restrict the internet activities of host with MAC address 00:11:22:33:44:AA on the LAN to access www.tp-link.com only, please follow the steps below:

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 [Access Control](#) > [Host](#) and configure the host settings:
 - 1) Click [Add New](#).
 - 2) Select [MAC Address](#) as the mode type. Create a unique description (e.g. [host_1](#)) for the host in the [Description](#) field and enter 00:11:22:33:44:AA in the [MAC Address](#) field.

- 3) Click [Save](#).
3. Go to [Access Control](#) > [Target](#) and configure the target settings:
 - 1) Click [Add New](#).
 - 2) Select [URL Address](#) as the mode type. Create a unique description (e.g. [target_1](#)) for the target in the [Target Description](#) field and enter the domain name, either the full name or the keywords (for example TP-Link) in the [Add URL Address](#) field. And then Click [Add](#).

Note:

Any URL address with keywords in it (e.g. www.tp-link.com) will be blocked or allowed.

- 3) Click [Save](#).
4. Go to [Access Control](#) > [Schedule](#) and configure the schedule settings:

- 1) Click [Add New](#).
- 2) Create a unique description (e.g. [schedule_1](#)) for the schedule in the [Schedule Description](#) field and set the day(s) and time period. And then click [Add](#).

[Add or Edit A Schedule Entry](#)

The Schedule is based on the time of the Router. The time can be set in "System Tools -> [Time Settings](#)".

Description:

Apply To: Start Time: End Time: [Add](#)

Time	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
Sun.															
Mon.															
Tues.															
Wed.															
Thur.															
Fri.															
Sat.															

[Clear Schedule](#)

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

- 3) Click [Save](#).
5. Go to [Access Control](#) > [Rule](#) and add a new access control rule.
 - 1) Click [Add New](#).
 - 2) Give a name for the rule in the [Description](#) field. Select [host_1](#) from the LAN host drop-down list; select [target_1](#) from the target drop-down list; select [schedule_1](#) from the schedule drop-down list.

[Add Internet Access Control Entry](#)

Description:

LAN Host: [Add LAN Host](#)

Target: [Add Target](#)

Schedule: [Add Schedule](#)

Rule:

Status:

Direction:

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

- 3) Leave the status as [Enabled](#) as click [Save](#).

Note:

When [Target](#) is set to be [URL Address](#) mode, the [Direction](#) field is [OUT](#) and not editable, which means the host can only visit or is not allowed to visit the URL address you set.

6. Select **Enable Internet Access Control** to enable Access Control function.
7. Select **Allow the packets specified by any enabled access control policy to pass through the Router** as the default filter policy and click **Save**.

Access Control Rule Management

This device can restrict Internet activity for specified LAN hosts. You can set and combine access control rules to effectively manage your network.

☒ Enable Internet access control

Default Filtering Rules:

☒ Allow the packets not specified by any filtering rules to passthrough this device.

☐ Deny the packets not specified by any filtering rules to passthrough this device.

Save

Done!

Now only the specific host(s) can visit the target(s) within the scheduled time period.

Note:

When **LAN Host** and **Target** are both set to be the MAC Address mode, you need to set **Protocol**: ALL, TCP, UDP, ICMP. The default setting is **ALL** and it is recommended to keep the default setting.

4. 11. Advanced Routing

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

4. 11. 1. Static Route List

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Advanced Routing > Static Route List**.

- **To add static routing entries:**

1. Click **Add New**.
2. Enter the following information.

Static Route

Destination IP Address:

Subnet Mask:

Gateway:

Interface: (optional)

Status: Enabled

Save Back

- **Destination IP Address** - The Destination Network is the address of the network or host that you want to assign to a static route.
- **Subnet Mask** - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.
- **Gateway** - This is the IP address of the default gateway device that allows the contact between the router and the network or host.

3. Select **Enabled** or **Disabled** for this entry on the **Status** drop-down list.

4. Click **Save**.

4. 11. 2. System Routing Table

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

2. Go to **Advanced Routing > System Routing Table**, and you can view all the valid route entries in use.

System Routing Table				
ID	Destination Network	Subnet Mask	Gateway	Interface
1	192.168.0.0	255.255.255.0	0.0.0.0	LAN & WLAN
Refresh				

- **Destination Network** - The Destination Network is the address of the network or host to which the static route is assigned.
- **Subnet Mask** - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.
- **Gateway** - This is the IP address of the gateway device that allows for contact between the Router and the network or host.
- **Interface** - This interface tells you whether the Destination IP Address is on the LAN & WLAN (internal wired and wireless networks), or the WAN (Internet).

Click **Refresh** to refresh the data displayed.

4. 12. Bandwidth Control

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

2. Go to **Bandwidth Control**.

3. Tick the **Enable Bandwidth Control** checkbox, and configure the **Egress Bandwidth** and **Ingress Bandwidth**, and then click **Save**. The **Egress/Ingress Bandwidth** is the

upload/download speed through the WAN port. The value should be less than 100,000Kbps.

The screenshot shows a 'Bandwidth Control' configuration window. It has a title bar 'Bandwidth Control'. Below the title bar, there is a checkbox labeled 'Enable Bandwidth Control' which is checked. To the right of the checkbox, there are two input fields: 'Egress Bandwidth:' with the value '512' and 'Kbps', and 'Ingress Bandwidth:' with the value '2048' and 'Kbps'. At the bottom left, there is a 'Save' button.

4. Click [Add New](#), fill in the blanks and click [Save](#).

The screenshot shows a 'Bandwidth Control' configuration window for adding a new rule. It has a title bar 'Bandwidth Control'. Below the title bar, there is a checkbox labeled 'Enable:' which is checked. Below this, there are four input fields: 'IP Range:' with two empty boxes separated by '--', 'Port Range:' with two empty boxes separated by '--', 'Protocol:' with a dropdown menu showing 'ALL', and 'Priority:' with a dropdown menu showing '5' and a note '(1 meaning highest priority)'. Below these, there are two columns of input fields: 'Min Bandwidth(Kbps)' and 'Max Bandwidth(Kbps)'. Under 'Min Bandwidth(Kbps)', there are 'Egress Bandwidth:' and 'Ingress Bandwidth:' fields, both empty. Under 'Max Bandwidth(Kbps)', there are 'Egress Bandwidth:' and 'Ingress Bandwidth:' fields, both empty. At the bottom, there are 'Save' and 'Back' buttons.

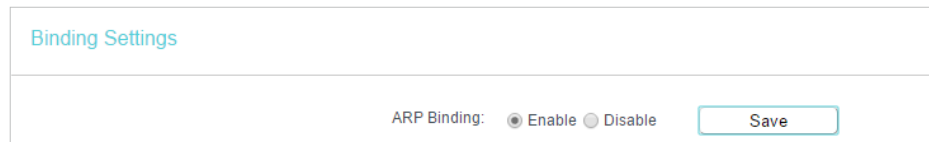
- **IP Range** - Interior PC address range. If both are blank or 0.0.0.0, the domain is noneffective.
- **Port Range** - The port range which the Interior PC access the outside PC. If all are blank or 0, the domain is noneffective.
- **Protocol** - Transport layer protocol, here there are ALL, TCP, UDP.
- **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.
- **Egress Bandwidth** - The max and the min upload speed which through the WAN port.
- **Ingress Bandwidth** - The max and the min download speed through the WAN port.

4.13. IP & MAC Binding

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

4.13.1. Binding Settings

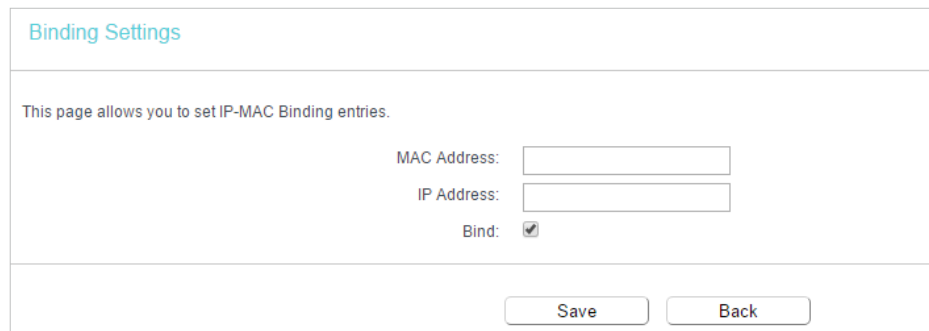
1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [IP & MAC Binding](#) > [Binding Settings](#).
3. Select [Enable](#) for ARP Binding and click [Save](#).



The screenshot shows the 'Binding Settings' page. At the top, there is a header 'Binding Settings'. Below it, there is a section for 'ARP Binding' with two radio buttons: 'Enable' (selected) and 'Disable'. To the right of these buttons is a 'Save' button.

- **To add IP & MAC Binding entries:**

1. Click [Add New](#).
2. Enter the MAC address and IP address.
3. Tick the [Bind](#) checkbox and click [Save](#).



The screenshot shows the 'Binding Settings' page with the instruction 'This page allows you to set IP-MAC Binding entries.' Below this, there are two input fields: 'MAC Address:' and 'IP Address:'. Below these fields is a 'Bind:' checkbox, which is checked. At the bottom of the page, there are two buttons: 'Save' and 'Back'.

- **To modify or delete an existing entry:**

1. Select the desired entry in the table.
2. Click [Edit](#) or [Delete Selected](#).

4.13.2. ARP List

To manage a device, you can observe the device on the LAN by checking its MAC address and IP address on the ARP list, and you can also configure the items. This page displays the ARP list which shows all the existing IP & MAC Binding entries.

ARP List

☐	MAC Address	IP Address	Status
☐	00:E0:4C:00:07:BE	192.168.0.4	Bound
☐	40:8D:5C:89:74:B5	192.168.0.100	Unloaded

- **MAC Address** - The MAC address of the listed computer on the LAN.
- **IP Address** - The assigned IP address of the listed computer on the LAN.
- **Status** - Indicates whether or not the MAC and IP addresses are bound.
- Click the **Load Selected** button to load the selected items to the IP & MAC Binding list.
- Click the **Delete Selected** button to delete the selected items to the IP & MAC Binding list.
- Click the **Refresh** button to refresh all items.

Note:

An item can not be loaded to the IP & MAC Binding list if the IP address of the item has been loaded before.

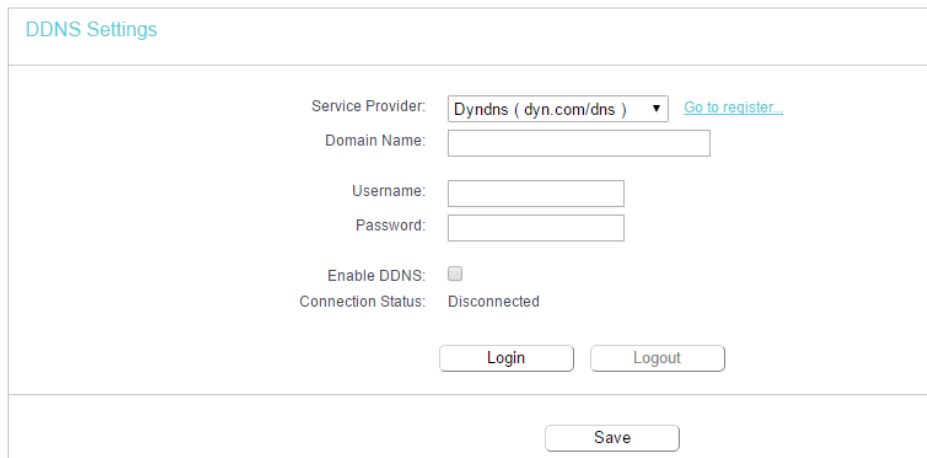
4. 14. Dynamic DNS

The router offers the DDNS (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address. Thus your friends can connect to your server by entering your domain name no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers such as www.comexe.cn, www.dyndns.org, or www.noip.com. The Dynamic DNS client service provider will give you a password or key.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **Dynamic DNS**.

Dyndns DDNS

If the dynamic DNS Service Provider you select is dyn.com/dns, the following page will appear.



The screenshot shows the 'DDNS Settings' page. At the top, the title 'DDNS Settings' is in blue. Below it, the 'Service Provider' dropdown is set to 'DynDNS (dyn.com/dns)' with a 'Go to register...' link. The 'Domain Name' field is empty. The 'Username' and 'Password' fields are also empty. The 'Enable DDNS' checkbox is unchecked. The 'Connection Status' is 'Disconnected'. There are 'Login' and 'Logout' buttons, and a 'Save' button at the bottom.

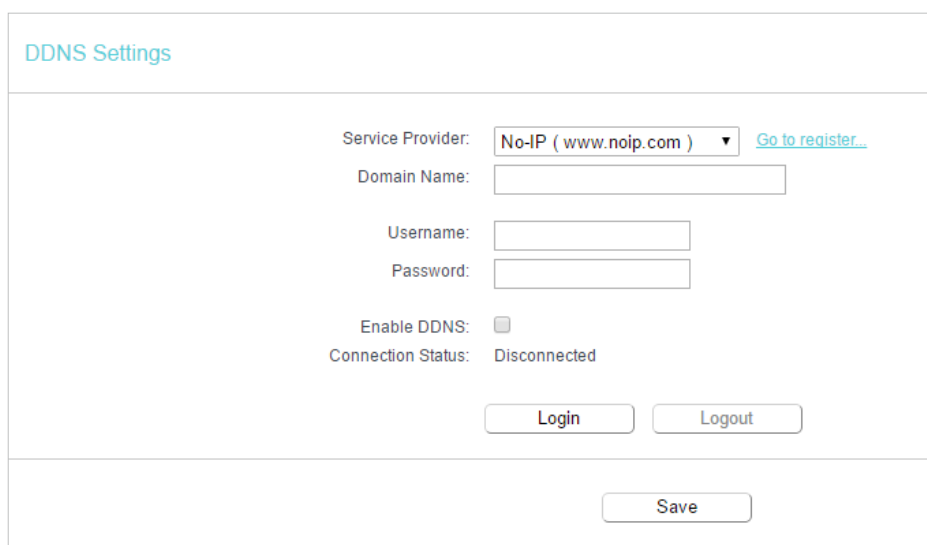
To set up for DDNS, follow these instructions:

1. Enter the [Domain Name](#) you received from dynamic DNS service provider here.
2. Enter the [Username](#) for your DDNS account.
3. Enter the [Password](#) for your DDNS account.
4. Click [Login](#).
5. Click [Save](#).

- [Connection Status](#) - The status of the DDNS service connection is displayed here.
- [Logout](#) - Click [Logout](#) to log out of the DDNS service.

No-IP DDNS

If the dynamic DNS Service Provider you select is www.noip.com, the following page will appear.



The screenshot shows the 'DDNS Settings' page with 'No-IP (www.noip.com)' selected in the 'Service Provider' dropdown. The 'Domain Name' field is empty. The 'Username' and 'Password' fields are also empty. The 'Enable DDNS' checkbox is unchecked. The 'Connection Status' is 'Disconnected'. There are 'Login' and 'Logout' buttons, and a 'Save' button at the bottom.

To set up for DDNS, follow these instructions:

1. Enter the [Domain Name](#) you received from dynamic DNS service provider.

2. Enter the [Username](#) for your DDNS account.
3. Enter the [Password](#) for your DDNS account.
4. Click [Login](#).
5. Click [Save](#).

- [Connection Status](#) - The status of the DDNS service connection is displayed here.
- [Logout](#) - Click [Logout](#) to log out of the DDNS service.

Comexe DDNS

If the dynamic DNS Service Provider you select is www.comexe.cn, the following page will appear.

DDNS Settings

Service Provider: Comexe (www.comexe.cn) [Go to register...](#)

Domain Name1:

Domain Name2:

Domain Name3:

Domain Name4:

Domain Name5:

Username:

Password:

Enable DDNS: ☐

Connection Status: Disconnected

Login Logout

Save

To set up for DDNS, follow these instructions:

1. Enter the [Domain Name](#) received from your dynamic DNS service provider.
 2. Enter the [Username](#) for your DDNS account.
 3. Enter the [Password](#) for your DDNS account.
 4. Click [Login](#).
 5. Click [Save](#).
- [Connection Status](#) - The status of the DDNS service connection is displayed here.
 - [Logout](#) - Click [Logout](#) to log out of the DDNS service.

4. 15. IPv6

This function allows you to enable IPv6 function and set up the parameters of the router's Wide Area Network (WAN) and Local Area Network (LAN).

4. 15. 1. IPv6 Status

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **IPv6 > IPv6 Status**, and you can view the current IPv6 status information of the router.

IPv6 Status	
WAN	
Connection Type:	Disabled
IPv6 LAN	
IPv6 Address Type:	RADVD
Prefix Length:	64
IPv6 Address:	N/A

- **WAN** - This section shows the current IPv6 **Connection Type**.
- **IPv6 LAN** - This section shows the current IPv6 information of the router's LAN port, including **IPv6 Address Type**, **Prefix Length** and **IPv6 Address**.

4. 15. 2. IPv6 WAN

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **IPv6 > IPv6 WAN**. Select **Enable IPv6**.

IPv6 WAN

Enable IPv6: ☒

Connection Type: **Dynamic IPv6**

IPv6 Address: ::

Prefix Length: 0

IPv6 Gateway: ::

Addressing Type: **DHCPv6**

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

Enable MLD Proxy: ☐

Set IPv6 DNS Server manually: ☐

Host Name: **TL-WR802N**

Save

3. Select the **WAN Connection Type** and fill in the blanks according to your ISP, and then click **Save**.

- **Dynamic IPv6** - Connections which use dynamic IPv6 address assignment.
- **Static IPv6** - Connections which use static IPv6 address assignment.
- **PPPoEv6** - Connections which use PPPoEv6 that requires a username and password.
- **Tunnel 6to4** - Connections which use 6to4 address assignment.

Dynamic IPv6

IPv6 WAN

Enable IPv6: ☒

Connection Type: **Dynamic IPv6**

IPv6 Address: ::

Prefix Length: 0

IPv6 Gateway: ::

Addressing Type: **DHCPv6**

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

Enable MLD Proxy: ☐

Set IPv6 DNS Server manually: ☐

Host Name: **TL-WR802N**

Save

- **IPv6 Address** - The IPv6 address assigned by your ISP dynamically.
- **Prefix Length** - The length of IPv6 address prefix.
- **IPv6 Gateway** - Enter the default gateway provided by your ISP.
- **Addressing Type** - There are two types of assignment for IPv6 address: SLAAC (Stateless address auto-configuration) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.
- **MTU(Bytes)** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs, you may need to modify the

MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

- [Enable MLD Proxy](#) - Enable the Multicast Listener Discovery (MLD) Proxy function if you need.
- [Set IPv6 DNS Server manually](#) - If your ISP gives you one or two DNS IPv6 addresses, select [Set IPv6 DNS Server manually](#) and enter the [IPv6 DNS Server](#) and [Secondary IPv6 DNS Server](#) into the correct fields. Otherwise, the DNS servers will be assigned from ISP dynamically.

Note:

If you get Address not found error when you access a Web site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

Static IPv6

IPv6 WAN

Enable IPv6: ☒

Connection Type: [Static IPv6](#)

IPv6 Address:

Prefix Length:

IPv6 Gateway: (optional)

IPv6 DNS Server: (optional)

Secondary IPv6 DNS Server: (optional)

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

Enable MLD Proxy: ☐

Save

- [IPv6 Address](#) - Enter the IPv6 address provided by your ISP.
- [Prefix Length](#) - The length of IPv6 address prefix.
- [IPv6 Gateway](#) - Enter the default gateway provided by your ISP.
- [IPv6 DNS Server](#) - Enter the DNS IPv6 address provided by your ISP.
- [Secondary IPv6 DNS Server](#) - Enter another DNS IPv6 address provided by your ISP.
- [MTU\(Bytes\)](#) - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs, you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- [Enable MLD Proxy](#) - Enable the Multicast Listener Discovery (MLD) Proxy function if you need.

PPPoEv6

The screenshot shows the 'IPv6 WAN' configuration page. At the top, 'Enable IPv6:' is checked. 'Connection Type:' is set to 'PPPoEv6'. There is an unchecked checkbox for 'PPPoE same session with IPv4 connection'. Below are input fields for 'PPP Username:', 'PPP Password:', and 'Confirm password:'. 'Authentication Type:' is set to 'AUTO_AUTH' and 'Addressing Type:' is set to 'DHCPv6'. A horizontal line separates the top section from the bottom section. In the bottom section, there are input fields for 'Service Name:' and 'Server Name:', both with a note '(do not change unless necessary)'. Below these is 'MTU(Bytes):' set to '1480' with a note '(1480 as default, do not change unless necessary)'. At the bottom, there are three unchecked checkboxes: 'Enable MLD Proxy:', 'Use IPv6 address specified by ISP:', and 'Set IPv6 DNS Server manually:'. A 'Save' button is at the very bottom.

- **PPP Username/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Authentication Type** – Choose one authentication type from AUTO-AUTH, PAP, CHAP and MS-CHAP.
- **Addressing Type** - There are two types of assignation for IPv6 address: SLAAC (Stateless address auto-configuration) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.
- **MTU(Bytes)** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs, you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- **Enable MLD Proxy** - Enable the Multicast Listener Discovery (MLD) Proxy function if you need.
- **Use IPv6 address specified by ISP** - Input a static IPv6 address from the ISP.
- **Set IPv6 DNS Server manually** - Enter the IP address of the IPv6 DNS server and secondary IPv6 DNS server.