



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](#) 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](#) 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.

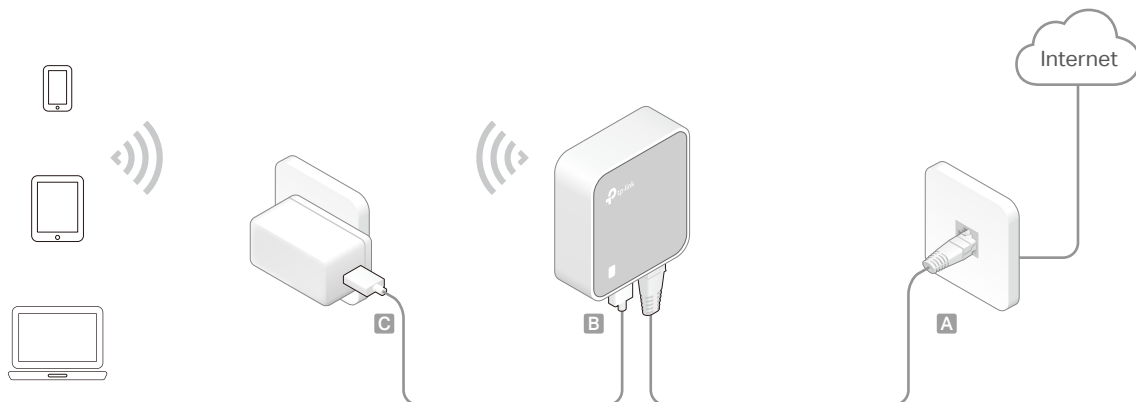
2.2.1. Wireless Router Mode

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:

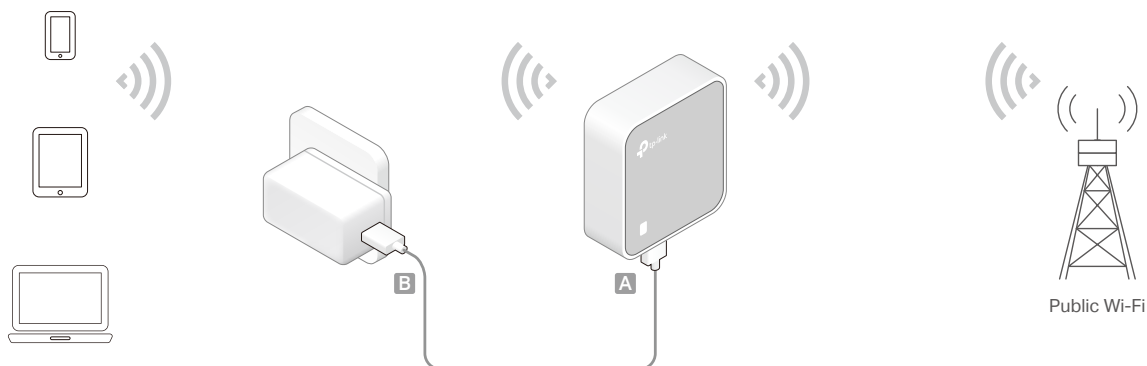
- If the hotel's internet has an authentication process, you will need to authenticate only once and only on one device.
- Check the internet connection on your laptop or smartphone, and please note that:
 - If you can access the internet without any restriction, no configuration is required.
 - If you're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



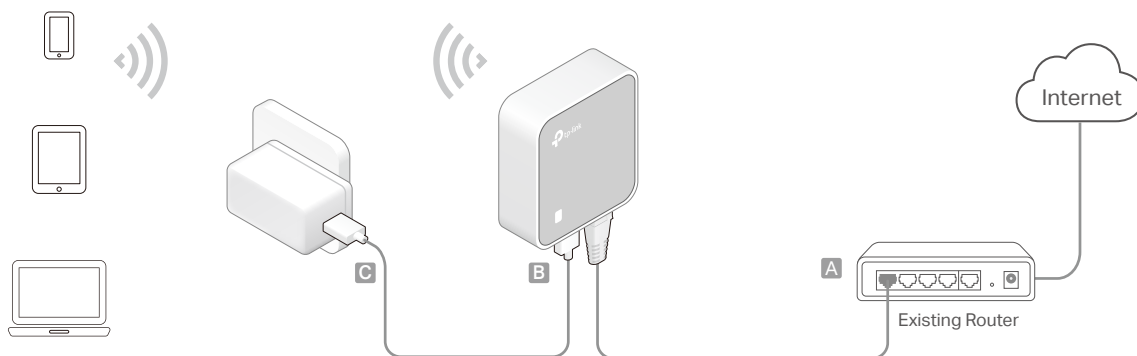
2. 2. 3. Access Point Mode

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.

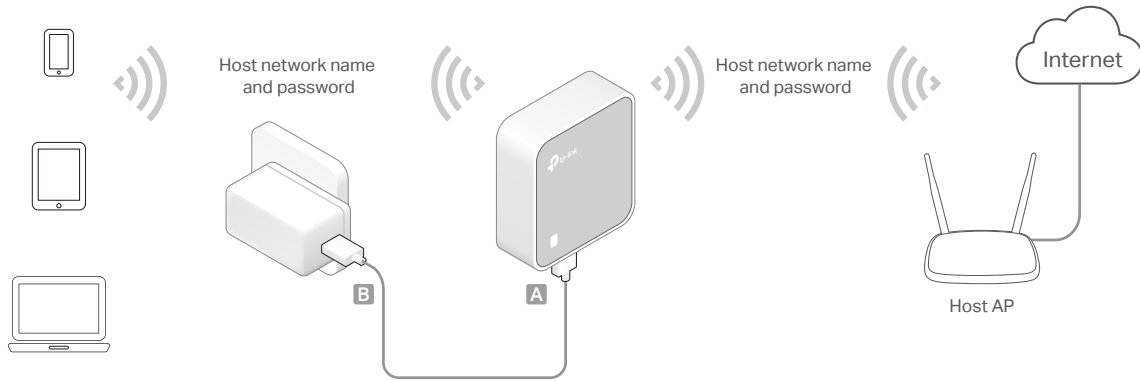


2. 2. 4. Range Extender Mode

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.

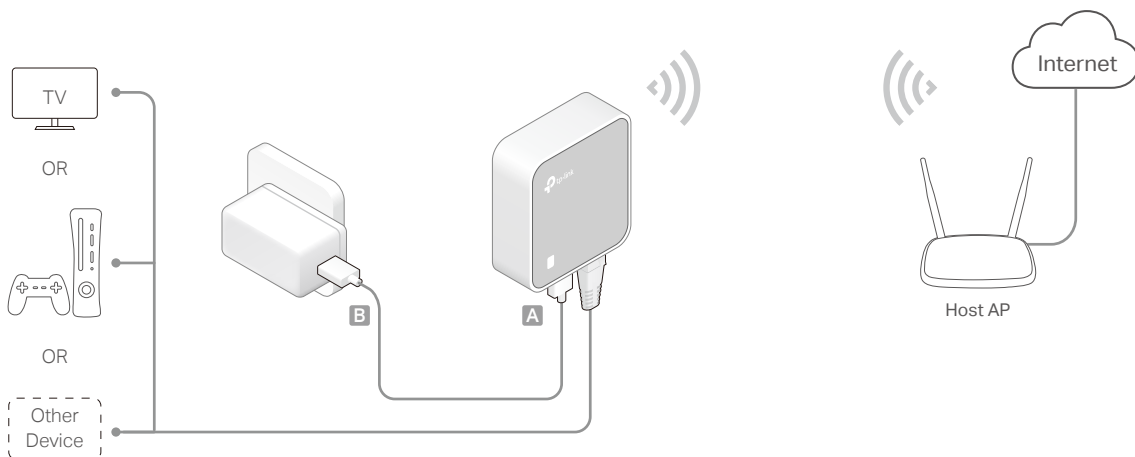
1. Connect the router according to Step A to B.
2. Use the default Wi-Fi Name and Wi-Fi Password printed on the Wi-Fi Info Card or on the product label at the bottom of your router to connect to the Wi-Fi.



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:

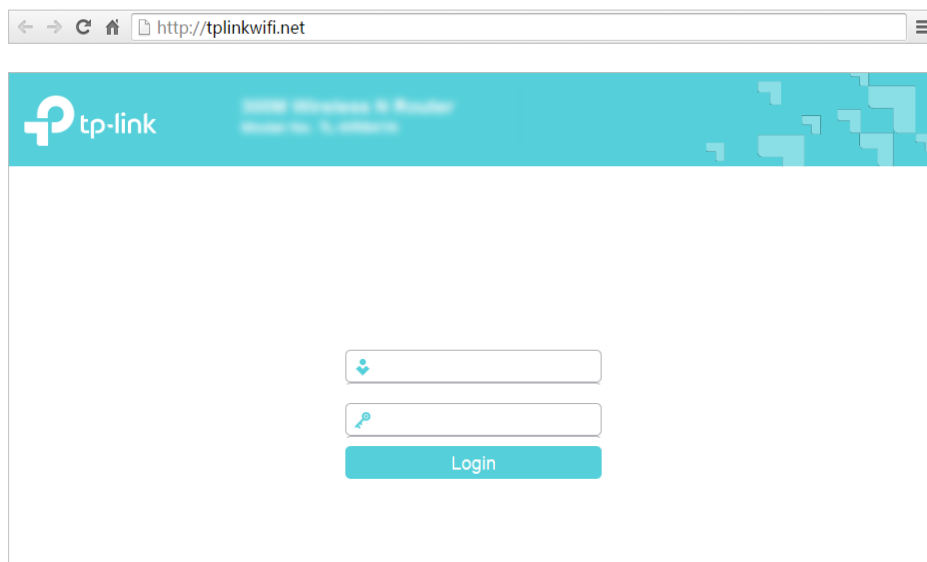
- [Log In to the Router](#)
- [Set Up Internet Connection](#)

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

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:	2.1.1.0 (2018.08.08)
Hardware Version:	V1.0 (2018.08.08)
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 <input type="button" value="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](#).

Operation Mode

Select an Operation Mode:

Wireless Router

WISP

Access Point

Range Extender

Client

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.

WAN Settings

Connection Type:

IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Gateway: 0.0.0.0

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

Enable IGMP Proxy:

IGMP Version: v2 v3

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

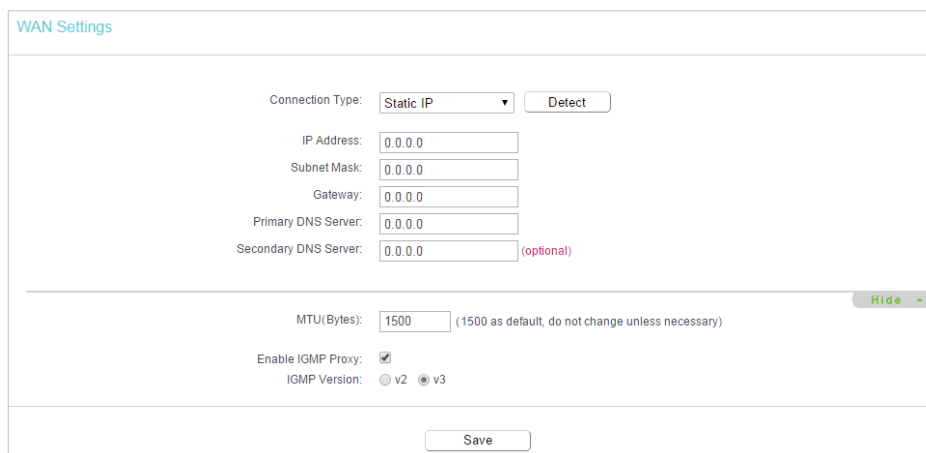
Set DNS server manually:

Host Name:

- **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 with the following configuration:

- Connection Type: Static IP (selected in a dropdown menu) with a Detect button.
- IP Address: 0.0.0.0
- Subnet Mask: 0.0.0.0
- Gateway: 0.0.0.0
- Primary DNS Server: 0.0.0.0
- Secondary DNS Server: 0.0.0.0 (optional)
- MTU(Bytes): 1500 (1500 as default, do not change unless necessary) with a Hide button.
- Enable IGMP Proxy:
- IGMP Version: v2 v3
- Save button at the bottom.

- **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 for a PPPoE connection. The 'Connection Type' is set to 'PPPoE' with a 'Detect' button. Below are input fields for 'PPP Username', 'PPP Password', and 'Confirm password'. The 'Secondary Connection' options are 'Disabled' (selected), 'Dynamic IP', and 'Static IP (For Dual Access)'. 'Connection Mode' has three radio buttons: 'Always on' (selected), 'Connect on demand', and 'Connect manually'. The 'Max Idle Time' is set to '15' minutes. The 'Authentication Type' is 'AUTO_AUTH', with 'Connect' and 'Disconnect' buttons. A 'Hide' button is on the right. Below a horizontal line, there are fields for 'Service Name', 'Server Name', and 'MTU(Bytes)' (set to 1480). The 'Enable IGMP Proxy' checkbox is checked, and 'IGMP Version' is set to 'v3'. There are also checkboxes for 'Use IP address specified by ISP', 'Set DNS server manually', and an 'Echo request interval' field set to '0'. A 'Save' button is 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**.

WAN Settings

Connection Type:

Username:

Password:

Addressing Type: Dynamic IP Static IP

Server IP Address/Name:

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

DNS Server: 0.0.0.0, 0.0.0.0

Internet IP Address: 0.0.0.0

Internet DNS: 0.0.0.0, 0.0.0.0

MTU(Bytes): (1460 as default, do not change unless necessary)

Enable IGMP Proxy:

IGMP Version: v2 v3

Connection Mode: Always on

Connect on demand

Connect manually

Max Idle Time: minutes (0 meaning connection remains active at all times)

- **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. The 'Connection Type' is set to 'PPTP'. There are input fields for 'Username' and 'Password', and buttons for 'Detect', 'Connect', and 'Disconnect'. The 'Addressing Type' is set to 'Dynamic IP'. Below this are fields for 'Server IP Address/Name', 'IP Address', 'Subnet Mask', 'Gateway', and 'DNS Server'. There are also fields for 'Internet IP Address' and 'Internet DNS'. The 'MTU(Bytes)' is set to 1420. The 'Enable IGMP Proxy' checkbox is checked. The 'IGMP Version' is set to 'v2'. The 'Connection Mode' is set to 'Always on'. The 'Max Idle Time' is set to 15 minutes. 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 page for a BigPond Cable connection. The page is titled "WAN Settings" and contains the following fields and options:

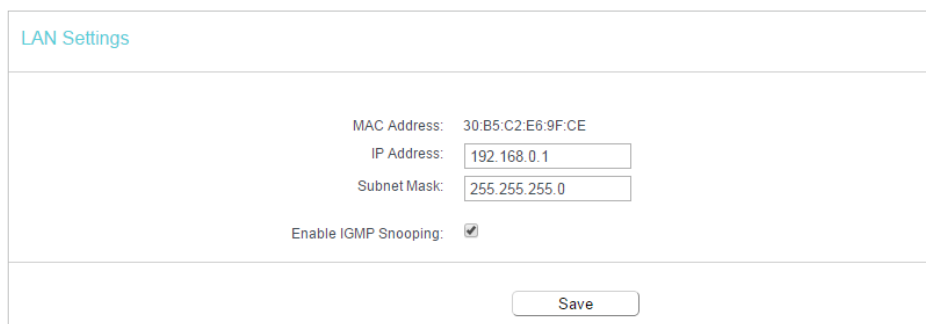
- Connection Type:** A dropdown menu set to "BigPond Cable" and a "Detect" button.
- Username:** A text input field.
- Password:** A text input field.
- Auth Server:** A text input field.
- Auth Domain:** A text input field.
- MTU(Bytes):** A text input field set to "1500" with a note "(1500 as default, do not change unless necessary)".
- Enable IGMP Proxy:** A checked checkbox.
- IGMP Version:** Radio buttons for "v2" and "v3", with "v3" selected.
- Connection Mode:** Radio buttons for "Always on", "Connect on demand", and "Connect manually", with "Always on" selected.
- Max Idle Time:** A text input field set to "15" with a note "minutes (0 meaning connection remains active at all times)".
- Buttons:** "Connect" and "Disconnect" buttons are located below the Max Idle Time field. A "Save" button is located at the bottom of the form.

- **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:	<input type="text" value="00:0A:EB:13:09:6A"/> <input type="button" value="Restore Factory MAC"/>
Your PC's MAC Address:	<input type="text" value="40:8D:5C:89:74:B5"/> <input type="button" value="Clone MAC Address"/>
<input type="button" value="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**.

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

Current PIN: 12345670

Disable device PIN

Add a new device:

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

WPS Settings

Enter new device PIN.
PIN:

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

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

Method TWO: Enter the Client's PIN

1. Keep the WPS Status as [Enabled](#) and click [Add Device](#).

WPS (Wi-Fi Protected Setup)

WPS: Enabled

Current PIN: 12345670

Disable device PIN

Add a new device:

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

WPS Settings

Enter new device PIN.
PIN:

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

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

Method Three: Enter the Router's PIN

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

WPS (Wi-Fi Protected Setup)

WPS: **Enabled**

Current PIN: **12345670**

Disable device PIN

Add a new device:

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

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:

Encryption:

Wireless Password:

Group Key Update Period:

WPA/WPA2 - Enterprise

Version:

Encryption:

RADIUS Server IP:

RADIUS Server Port: (1-65535, 0 stands for default port 1812)

RADIUS Server Password:

Group Key Update Period:

WEP

Authentication Type:

WEP Key Format:

Selected Key: Key Type

Key 1:

Key 2:

Key 3:

Key 4:

- **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.

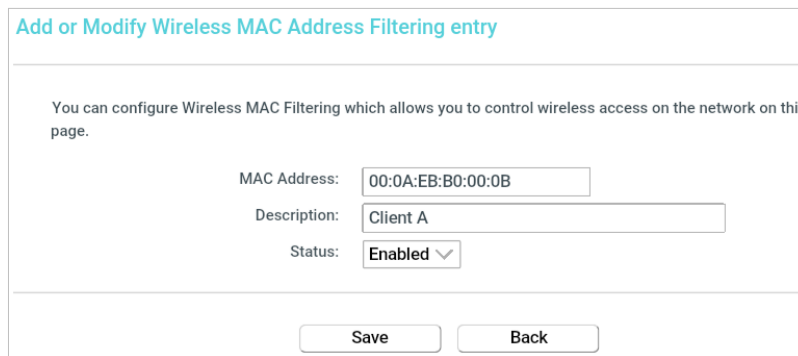
I want to:

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.

<input type="checkbox"/>	MAC Address	Status	Host	Description	Edit
<input type="checkbox"/>	00:0A:EB:00:00:0B	Enabled	TP-LINK_7AFF	client A	Edit
<input type="checkbox"/>	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 <input type="button" value="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 [Guset 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:

Guest Network Isolation:

Guest Network Bandwidth Control:

Guest Network: Enable Disable

Network Name:

Max Guests number:

Security:

Authentication Type:

Encryption:

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:

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:

Start Time:

End Time:

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.															

- [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
<input type="button" value="Refresh"/>				

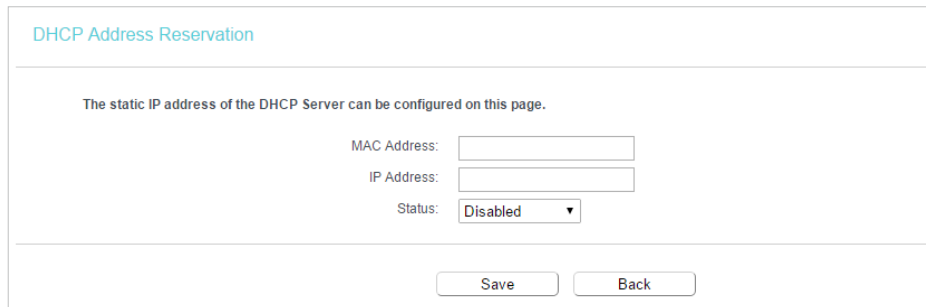
- **Client Name** - The name of the DHCP client.
- **MAC Address** - The MAC address of the DHCP client.
- **Assigned IP** - The IP address that the outer has allocated to the DHCP client.
- **Lease Time** - The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic IP 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:

- 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

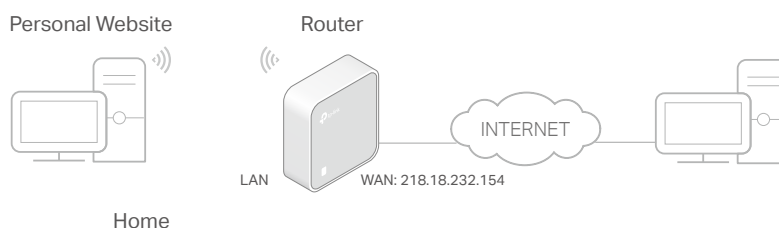
When you build up a server in the local network and want to share it on the internet, Virtual Servers can realize the service and provide it to internet users. At the same time virtual servers can keep the local network safe as other services are still invisible from the internet.

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:	<input type="text" value="80"/> (XX-XX or XX)
IP Address:	<input type="text" value="192.168.0.100"/>
Internal Port:	<input type="text" value="80"/> (XX or keep empty, if it's empty, Internal port equals to Service port)
Protocol:	<input type="text" value="TCP"/>
Status:	<input type="text" value="Enabled"/>
Common Service Port:	<input type="text" value="HTTP"/>
<input type="button" value="Save"/> <input type="button" value="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](http://WAN_IP) (in this example: [http:// 218.18.232.154](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: (XX)

Trigger Protocol:

Open Port: (XX or XX-XX or XX-XX,XX)

Open Protocol:

Status:

Common Service Port:

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.

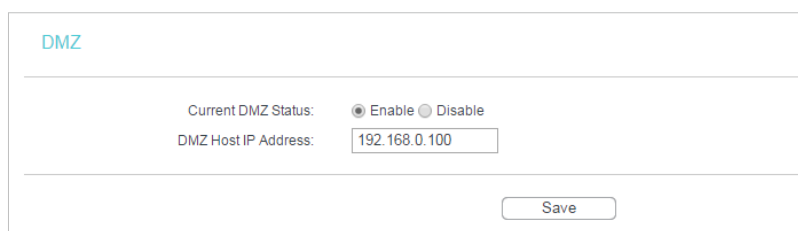
I want to:

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** filed.



DMZ

Current DMZ Status: Enable Disable

DMZ Host IP Address:

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

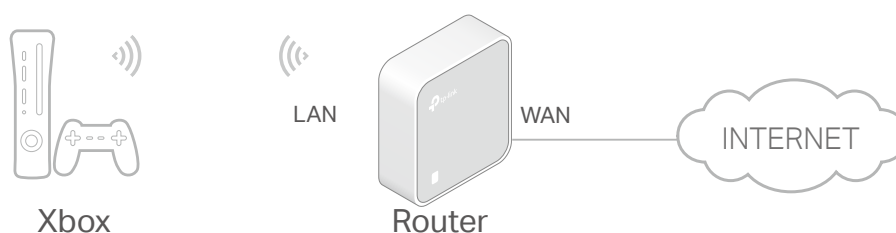
The UPnP (Universal Plug and Play) protocol allows the applications or host devices to automatically find the front-end NAT device and send request to it to open the

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: <input checked="" type="radio"/> Enabled <input type="radio"/> Disable						
Current UPnP Settings List						
ID	App Description	External Port	Protocol	Internal Port	IP Address	Status
<input type="button" value="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.

The screenshot shows the 'Basic Security' configuration page. It has a title bar 'Basic Security' and three main sections: 'Firewall', 'VPN', and 'ALG'.
- In the 'Firewall' section, there is a checkbox for 'Enable SPI Firewall' which is checked.
- In the 'VPN' section, there are three rows of radio buttons: 'PPTP Pass-through', 'L2TP Pass-through', and 'IPSec Pass-through'. Each row has 'Enable' selected and 'Disable' unselected.
- In the 'ALG' section, there are five rows of radio buttons: 'FTP ALG', 'TFTP ALG', 'H323 ALG', 'SIP ALG', and 'RTSP ALG'. Each row has 'Enable' selected and 'Disable' unselected.
- At the bottom right of the page is a 'Save' button.

- **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](#)

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:**

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.															

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

Add URL:

[Details](#)

(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.

The screenshot shows a web form titled "Add or Edit A Host Entry". It contains a "Mode" dropdown menu currently set to "MAC Address". Below it are two text input fields: "Description" and "MAC Address", both of which are empty. At the bottom of the form are two buttons: "Save" and "Back".

- 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.

The screenshot shows a web form titled "Add or Edit A Target Entry". It contains a "Mode" dropdown menu currently set to "URL Address". Below it are two text input fields: "Description" and "Add URL Address", both of which are empty. An "Add" button is positioned to the right of the "Add URL Address" field. Below these fields is a "Detail" field with a small square icon to its left. A "Delete" button is located below the "Detail" field, with the text "(Will not take effect until you save these changes)" next to it. At the bottom of the form are two buttons: "Save" and "Back".

- 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: Each Day ▼

Start Time: 00:00 ▼

End Time: 24:00 ▼

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.															

- 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: host_1 ▼ [Add LAN Host](#)

Target: Target_1 ▼ [Add Target](#)

Schedule: Any Time ▼ [Add Schedule](#)

Rule: Deny ▼

Status: Enabled ▼

Direction: OUT ▼

- 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**.

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.

- **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

- **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.

Bandwidth Control

Enable Bandwidth Control

Egress Bandwidth: Kbps

Ingress Bandwidth: Kbps

4. Click **Add New**, fill in the blanks and click **Save**.

Bandwidth Control

Enable:

IP Range: --

Port Range: --

Protocol:

Priority: (1 meaning highest priority)

	Min Bandwidth(Kbps)	Max Bandwidth(Kbps)
Egress Bandwidth:	<input type="text"/>	<input type="text"/>
Ingress Bandwidth:	<input type="text"/>	<input type="text"/>

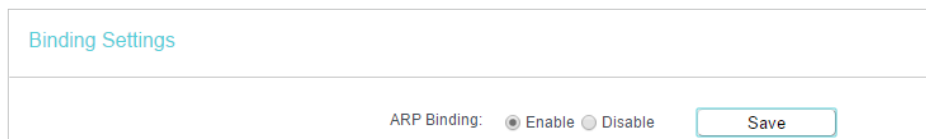
- **IP Range** - Interior PC address range. If both are blank or 0.0.0.0, the domain is noneffective.
- **Port Range** - The port range which the Interior PC access the outside PC. If all are blank or 0, the domain is noneffective.
- **Protocol** - Transport layer protocol, here there are ALL, TCP, UDP.
- **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

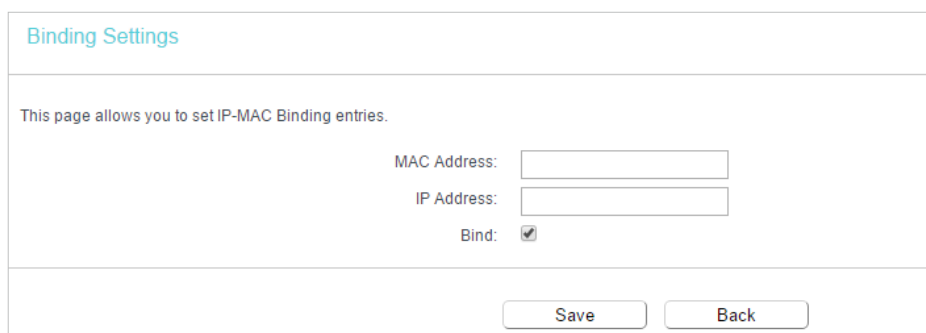
1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [IP & MAC Binding](#) > [Binding Settings](#).
3. Select [Enable](#) for ARP Binding and click [Save](#).



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 a form to add a new entry. The form has a header 'Binding Settings' and a sub-header 'This page allows you to set IP-MAC Binding entries.' Below this, there are three input fields: 'MAC Address:', 'IP Address:', and 'Bind:'. The 'Bind:' field has a checked checkbox. At the bottom of the form, 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

<input type="checkbox"/>	MAC Address	IP Address	Status
<input type="checkbox"/>	00:E0:4C:00:07:BE	192.168.0.4	Bound
<input type="checkbox"/>	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.

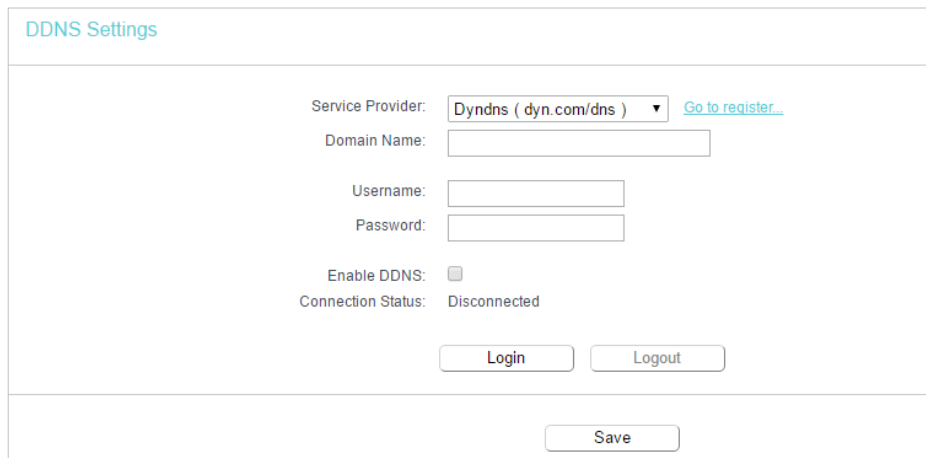
4. 14. Dynamic DNS

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 displayed in blue. Below the title, there are several input fields and controls:

- Service Provider:** A dropdown menu is set to 'DynDNS (dyn.com/dns)'. To its right is a blue link that says 'Go to register..'
- Domain Name:** An empty text input field.
- Username:** An empty text input field.
- Password:** An empty text input field.
- Enable DDNS:** A checkbox that is currently unchecked.
- Connection Status:** The text 'Disconnected' is displayed.
- At the bottom of the form area, there are two buttons: 'Login' and 'Logout'.
- Below the form area, centered, is a 'Save' button.

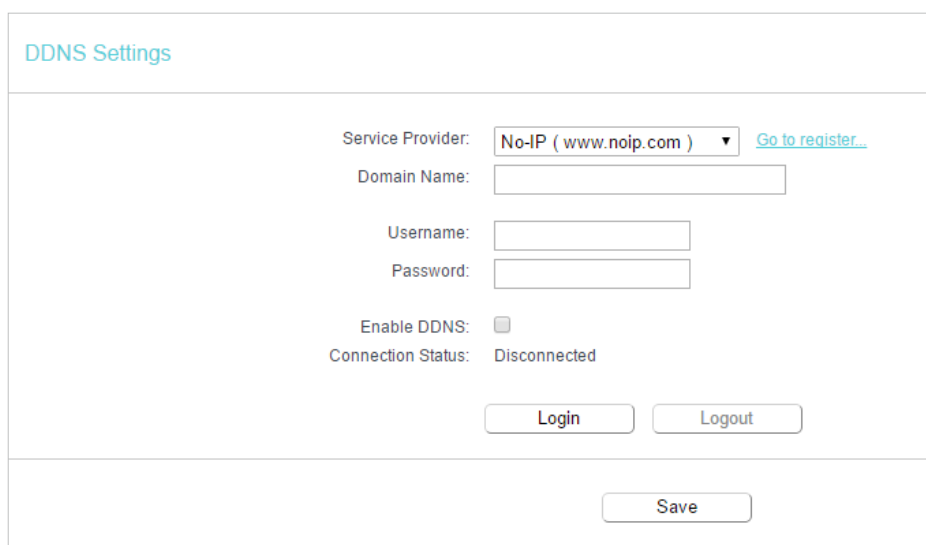
To set up for DDNS, follow these instructions:

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.
- **Login** - Click **Login** 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. At the top, the title 'DDNS Settings' is displayed in blue. Below the title, there are several input fields and controls:

- Service Provider:** A dropdown menu is set to 'No-IP (www.noip.com)'. To its right is a blue link that says 'Go to register..'
- Domain Name:** An empty text input field.
- Username:** An empty text input field.
- Password:** An empty text input field.
- Enable DDNS:** A checkbox that is currently unchecked.
- Connection Status:** The text 'Disconnected' is displayed.
- At the bottom of the form area, there are two buttons: 'Login' and 'Logout'.
- Below the form area, centered, is a 'Save' button.

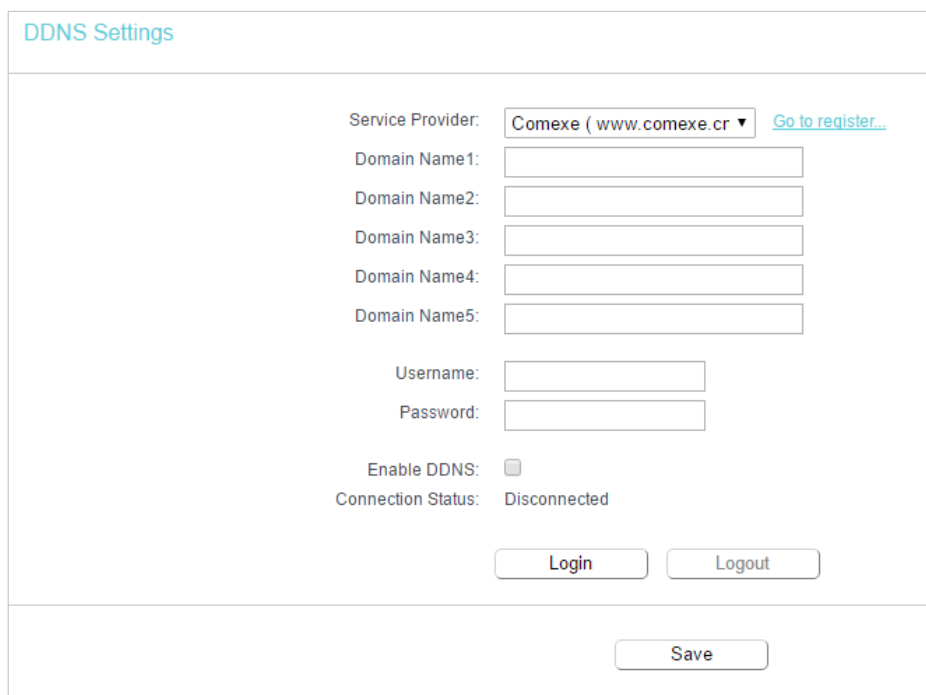
To set up for DDNS, follow these instructions:

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.



The screenshot shows the 'DDNS Settings' page. At the top left, the title 'DDNS Settings' is displayed in blue. Below the title, the 'Service Provider' is set to 'Comexe (www.comexe.cn)' with a dropdown arrow and a link 'Go to register..'. There are five input fields for 'Domain Name1' through 'Domain Name5'. Below these are input fields for 'Username' and 'Password'. An 'Enable DDNS' checkbox is currently unchecked. The 'Connection Status' is shown as 'Disconnected'. At the bottom, there are three buttons: 'Login', 'Logout', and 'Save'.

To set up for DDNS, follow these instructions:

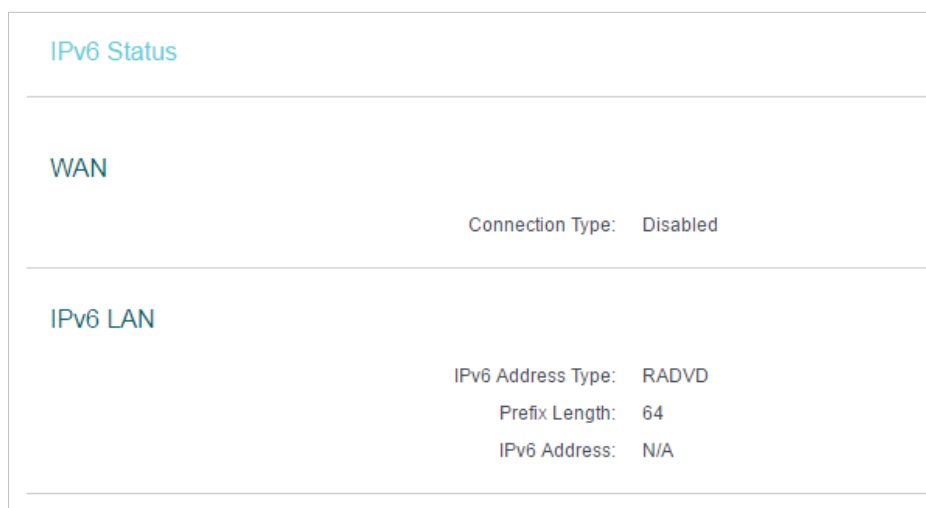
1. Enter the [Domain Name](#) received from your dynamic DNS service provider.
 2. Enter the [Username](#) for your DDNS account.
 3. Enter the [Password](#) for your DDNS account.
 4. Click [Login](#).
 5. Click [Save](#).
- [Connection Status](#) - The status of the DDNS service connection is displayed 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 as default, do not change unless necessary)

Enable MLD Proxy:

Set IPv6 DNS Server manually:

Host Name:

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 as default, do not change unless necessary)

Enable MLD Proxy:

Set IPv6 DNS Server manually:

Host Name:

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

The screenshot shows the IPv6 WAN configuration interface. It includes the following fields and options:

- Enable IPv6:**
- Connection Type:** Static IPv6 (dropdown menu)
- 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:**

A "Save" button is located at the bottom center of the form.

- **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

IPv6 WAN

Enable IPv6:

Connection Type:

PPPoE same session with IPv4 connection

PPP Username:

PPP Password:

Confirm password:

Authentication Type:

Addressing Type:

Service Name: (do not change unless necessary)

Server Name: (do not change unless necessary)

MTU(Bytes): (1480 as default, do not change unless necessary)

Enable MLD Proxy:

Use IPv6 address specified by ISP:

Set IPv6 DNS Server manually:

- **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 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.
- **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.

Tunnel 6to4

- **WAN Connection** - Display the available wan connection.

4. 15. 3. IPv6 LAN

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **IPv6 > IPv6 LAN** and configure the IPv6 LAN settings as needed.

- **Address Auto-Configuration Type** - Select a type to assign IPv6 addresses to the computers in your LAN. RADVD and DHCPv6 Server are provided. I
- **Site Prefix Configuration Type** - The type of IPv6 address prefix.
 - **Delegated** - Get the IPv6 address prefix from the ISP automatically, and the device will delegate it to the LAN.
 - **Static** - Configure the **Site Prefix** and **Site Prefix Length** manually. Please contact your ISP to get more information before you configure them.

Note:

If your IPv6 wan connection type is "Tunnel 6to4", the Site Prefix Configuration Type should be "Static" to make sure "Tunnel 6to4" works properly.

4. 16. System Tools

4. 16. 1. Time Settings

This page allows you to set the time manually or to configure automatic time synchronization. The router can automatically update the time from an NTP server via the internet.

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

Time Settings

Time Settings:

Time Zone: (GMT-08:00) Pacific Time (US & Canada); Tijuana

Date: 1970 Year 1 Month 1 Day

Time: 0 Hour 42 Minute 40 Second

NTP Server 1: (optional)

NTP Server 2: (optional)

(Only when the Internet connection is active.)

- **To set time manually:**

1. Select your local [Time Zone](#).
2. Enter the [Date](#) in Month/Day/Year format.
3. Enter the [Time](#) in Hour/Minute/Second format.
4. Click [Save](#).

- **To set time automatically:**

5. Select your local [Time Zone](#).
6. Enter the address or domain of the [NTP Server 1](#) or [NTP Server 2](#).
7. Click [Get GMT](#) to get time from the internet if you have connected to the internet.

- **To set Daylight Saving Time:**

1. Select [Enable Daylight Saving](#).
2. Select the start time from the drop-down list in the [Start](#) fields.
3. Select the end time from the drop-down list in the [End](#) fields.
4. Click [Save](#).

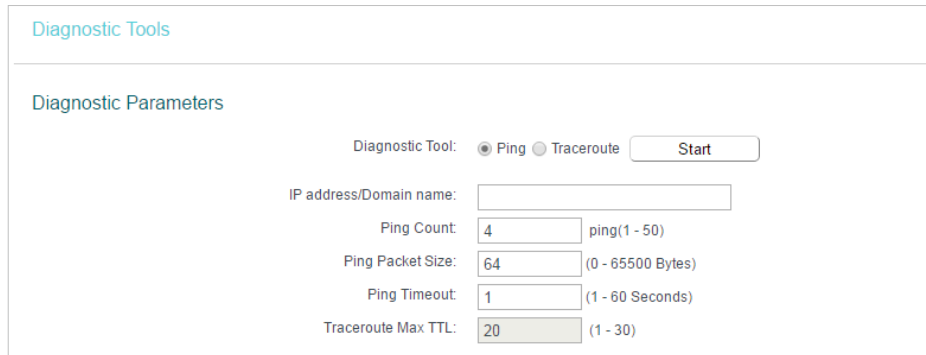
Note:

This setting will be used for some time-based functions such as firewall. You must specify your time zone once you log in to the router successfully; otherwise, time-based functions will not take effect.

4. 16. 2. Diagnostic

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

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



Diagnostic Tools

Diagnostic Parameters

Diagnostic Tool: Ping Traceroute

IP address/Domain name:

Ping Count: ping(1 - 50)

Ping Packet Size: (0 - 65500 Bytes)

Ping Timeout: (1 - 60 Seconds)

Traceroute Max TTL: (1 - 30)

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

Note:

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

- **IP Address/Domain Name** - Enter the destination IP address (such as 192.168.0.1) or Domain name (such as www.tp-link.com).
 - **Pings Count** - The number of Ping packets for a Ping connection.
 - **Ping Packet Size** - The size of Ping packet.
 - **Ping Timeout** - Set the waiting time for the reply of each Ping packet. If there is no reply in the specified time, the connection is overtime.
 - **Traceroute Max TTL** - The max number of hops for a Traceroute connection.
3. Click **Start** to check the connectivity of the internet.
 4. The **Diagnostic Results** page displays the diagnosis result. If the result is similar to the following figure, the connectivity of the internet is fine.

```

Diagnostic Results
-----
Pinging 192.168.0.1 with 64 bytes of data:

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

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

```

4. 16. 3. Firmware Upgrade

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

1. Download the latest firmware file for the router from our website www.tp-link.com.
2. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
3. Go to [System Tools > Firmware Upgrade](#).
4. Click [Choose File](#) to locate the downloaded firmware file, and click [Upgrade](#).

Firmware Upgrade

Firmware File Path: No file chosen

Firmware version: XXXXXXXXXX

Hardware version: XXXXXXXXXX

4. 16. 4. Factory Defaults

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [System Tools > Factory Defaults](#). Click [Restore](#) to reset all settings to the default values.

Factory Defaults

Click to restore all settings within this device back to factory defaults. It is strongly recommended that you back up your current configurations before you restore factory defaults.

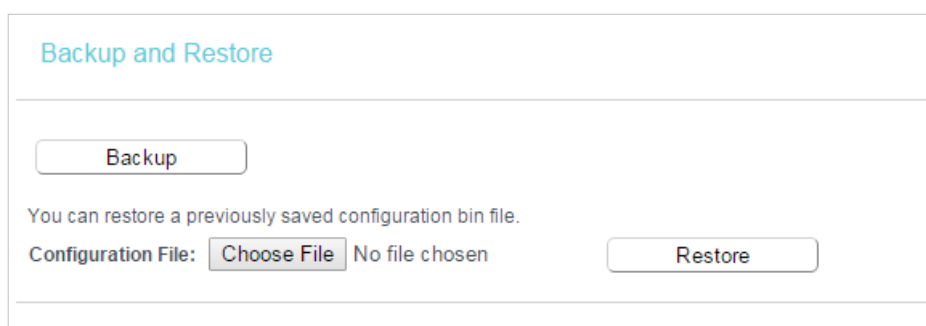
- Default **Username**: admin
- Default **Password**: admin

- Default **IP Address**: 192.168.0.1
- Default **Subnet Mask**: 255.255.255.0

4. 16. 5. Backup & Restore

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

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



The screenshot shows the 'Backup and Restore' page. At the top, there is a 'Backup' button. Below it, a message states: 'You can restore a previously saved configuration bin file.' Underneath this message, there is a 'Configuration File:' label, a 'Choose File' button, the text 'No file chosen', and a 'Restore' button.

- **To backup configuration settings:**

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

- **To restore configuration settings:**

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

Note:

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

4. 16. 6. Reboot

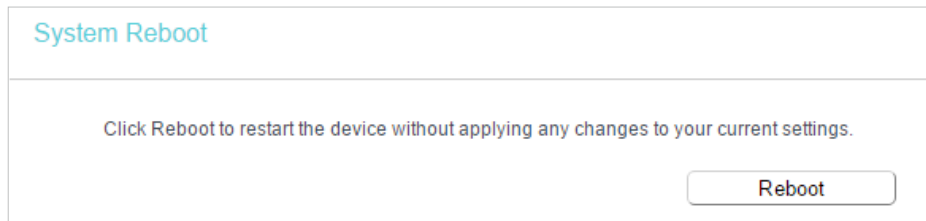
Some settings of the router will take effect only after rebooting, including:

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Working Modes.
- Change the Web Management Port.
- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router to its factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically).

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [System Tools > Reboot](#).

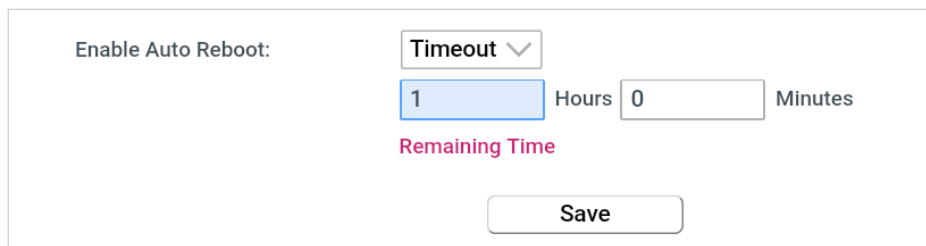
- **To reboot manually**

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

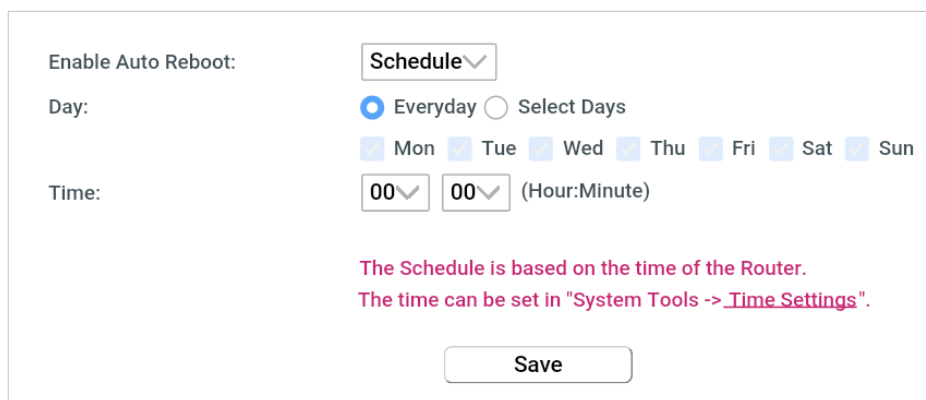


- **To reboot automatically**

- Select [Timeout](#) in the drop-down list of [Enable Auto Reboot](#) and specify a time period (1-72hours), then the router will reboot automatically after every this interval.



- Select [Schedule](#) in the drop-down list of [Enable Auto Reboot](#) and specify the [Time](#) when the router reboots and [Day](#) which to decide how often it reboots.



4. 16. 7. Account Management

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [System Tools > Administrator](#), and focus on the [Account Management](#) section. You can change the factory default username and password of the router.

Account Management

The username and password must not exceed 15 characters in length!

Old Password:

New User Name:

New Password:

Confirm password:

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

Note:

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

3. Click [Save](#).

4. 16. 8. Local Management

This feature allows you to block computers on the LAN from accessing the router by using the MAC/IP-based authentication.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [System Tools > Administrator](#), and focus on the [Service Configuration](#) section.

Service Configuration			
	HTTP Service	HTTPS Service	Available Host (IP/MAC)
Local Management	Port <input type="text" value="80"/>	Enable <input type="checkbox"/> Port <input type="text" value="443"/>	<input type="text"/>
Remote Management	Enable <input type="checkbox"/> Port <input type="text" value="80"/>	Enable <input type="checkbox"/> Port <input type="text" value="443"/>	<input type="text"/>

- **Allow all LAN connected devices to manage the router locally**

1. Keep the [Available Host \(IP/MAC\)](#) empty, which means you don't specify any host to manage the router.
2. If you want to access the router via both HTTPS and HTTP, please tick the [Enable](#) checkbox in [HTTPS Service](#) column. Otherwise, keep it disabled.
3. Keep the local management port as default if you don't know which port to use.
4. Click [Save](#).

Note:

If the web management port conflicts with the one used for [Virtual Server](#) entry, the entry will be automatically disabled after the setting is saved.

- **Allow a specific device to manage the router locally**

1. Enter the IP or MAC address of the host that you want to manage the router in the [Available Host \(IP/MAC\)](#) entry. The format of the MAC address is XX:XX:XX:XX:XX:XX (X is any hexadecimal digit).
2. If you want to access the router via both HTTPS and HTTP, please tick the [Enable](#) box in [HTTPS Service](#) column. Otherwise, keep it disabled.
3. Keep the Port as default if you don't know which port to use.
4. Click [Save](#).

Note:

If your PC is blocked but you want to access the router again, press and hold the [Reset](#) button to reset the router to the factory defaults.

- **Certificate**

Download and install the certificate for management via HTTPS if you need it. Once the certificate is installed, warnings will not pop up when you access the router via HTTPS.



4. 16. 9. Remote Management

This feature allows you to manage your router from a remote location via the internet.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [System Tools > Administrator](#), and focus on the [Service Configuration](#) section.

Service Configuration			
	HTTP Service	HTTPS Service	Available Host (IP/MAC)
Local Management	Port <input type="text" value="80"/>	Enable <input type="checkbox"/> Port <input type="text" value="443"/>	<input type="text"/>
Remote Management	Enable <input type="checkbox"/> Port <input type="text" value="80"/>	Enable <input type="checkbox"/> Port <input type="text" value="443"/>	<input type="text"/>

- **Forbid all devices to manage the router remotely**

Do not tick the [Enable](#) checkbox in both [HTTP Service](#) and [HTTPS Service](#).

- **Allow all devices to manage the router remotely**

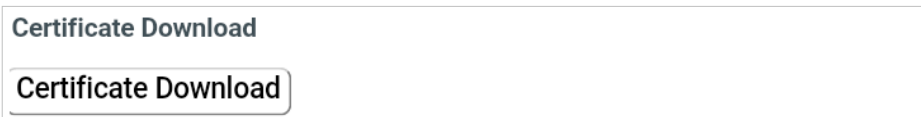
1. Tick the [Enable](#) checkbox in [HTTP Service](#).
2. If you want to access the router via both HTTPS and HTTP, please tick the [Enable](#) checkbox in [HTTPS Service](#) column. Otherwise, keep it disabled.
3. For higher security, you can change the remote management web port by entering a number between 1024 and 65534.
4. Click [Save](#).

- **Allow a specific device to manage the router remotely**

1. Tick the **Enable** checkbox in **HTTP Service**.
2. If you want to access the router via both HTTPS and HTTP, please tick the **Enable** checkbox in **HTTPS Service** column. Otherwise, keep it disabled.
3. For higher security, you can change the remote management web port by entering a number between 1024 and 65534.
4. Enter the IP or MAC address of the host that you want to manage the router in the **Available Host (IP/MAC)** entry. The format of the MAC address is XX:XX:XX:XX:XX:XX (X is any hexadecimal digit).
5. Click **Save**.

- **Certificate**

Download and install the certificate for management via HTTPS if you need it. Once the certificate is installed, warnings will not pop up when you access the router via HTTPS.

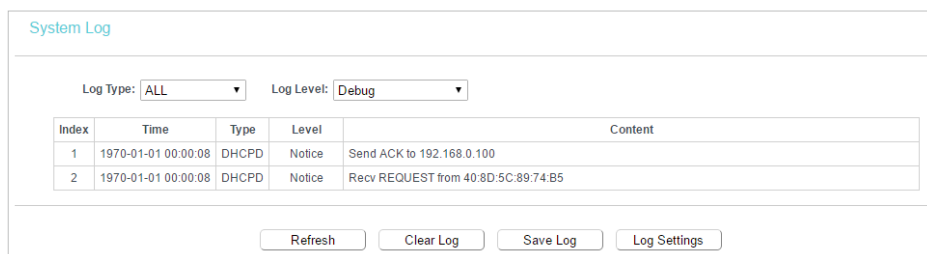


Note:

- To access the router, enter your router's WAN IP address in your browser's address bar, followed by a colon and the custom port number. For example, if your router's WAN address is 202.96.12.8, and the port number used is 8080, please enter `http://202.96.12.8:8080` in your browser. Later, you may be asked for the router's password. After successfully entering the username and password, you will be able to access the router's web management page.
- Be sure to change the router's default password for security purposes.

4. 16. 10. System Log

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



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

4. 16. 11. Statistics

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [System Tools > Traffic Statistics](#).
3. Select [Enable](#) and click [Save](#). You can view the network traffic of each PC on the LAN, including total traffic and the value of the last Packets Statistic interval in seconds.

Traffic Statistics

Traffic Statistics--LAN

Traffic Statistics: Enable Disable

Statistics Interval: seconds

Statistics List

IP Address MAC Address	Total		Current				Operation
	Packets	Bytes	Packets	Bytes	ICMP Tx	UDP Tx	
Current list is blank							

4. 17. Log out

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

Chapter 5

Configure the Router in WISP Mode (Hotspot Mode)

This chapter presents how to configure the various features of the router working as a WISP router (Hotspot 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](#)

5.1. Status

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

Status

Firmware Version: 4.0.0.10 (17/08/2015) (Build 11902118) (Rev. 20150805)
Hardware Version: V1.0 (20150805) (Rev. 20150805)

LAN

MAC Address: 68:FF:7B:06:1A:F0
IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0

Wireless 2.4GHz

Operation Mode: **WISP**
Wireless Radio: Enabled
Name(SSID): TP-Link_1AF0
Mode: 11bgn mixed
Channel: 8
Channel Width: Auto
MAC Address: 68:FF:7B:06:1A:F0

WAN

MAC Address: 68:FF:7B:06:1A:F1
IP Address: 192.168.1.1 (Dynamic IP)
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1
DNS Server: 192.168.1.1 0.0.0.0

System Up Time: 0 day(s) 00:16:00 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.

5.2. Operation Mode

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

Operation Mode

Select an Operation Mode:

Wireless Router

WISP

Access Point

Range Extender

Client

5.3. Network

5.3.1. 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.

WAN Settings

Connection Type:

IP Address:

Subnet Mask:

Gateway:

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

Enable IGMP Proxy:

IGMP Version: v2 v3

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

Set DNS server manually:

Host Name:

- **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' configuration page. At the top, 'Connection Type' is set to 'Static IP' with a 'Detect' button. 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)'. A horizontal separator line is present. Below the line, 'MTU(Bytes)' is set to '1500' with a note '(1500 as default, do not change unless necessary)' and a 'Hide' button. 'Enable IGMP Proxy' is checked, and 'IGMP Version' is set to 'v3'. A 'Save' button is at the bottom.

- **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 for a PPPoE connection. The 'Connection Type' is set to 'PPPoE'. Below this are fields for 'PPP Username', 'PPP Password', and 'Confirm password'. The 'Secondary Connection' options are 'Disabled', 'Dynamic IP', and 'Static IP'. The 'Connection Mode' options are 'Always on', 'Connect on demand', and 'Connect manually'. The 'Max Idle Time' is set to 15 minutes. The 'Authentication Type' is set to 'AUTO_AUTH'. There are 'Connect' and 'Disconnect' buttons. A 'Hide' button is visible on the right side of the form. Below the main form, there are additional fields for 'Service Name', 'Server Name', and 'MTU(Bytes)'. The 'Enable IGMP Proxy' checkbox is checked, and the 'IGMP Version' is set to 'v3'. There are also checkboxes for 'Use IP address specified by ISP', 'Echo request interval', and 'Set DNS server manually'. A 'Save' button is 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.

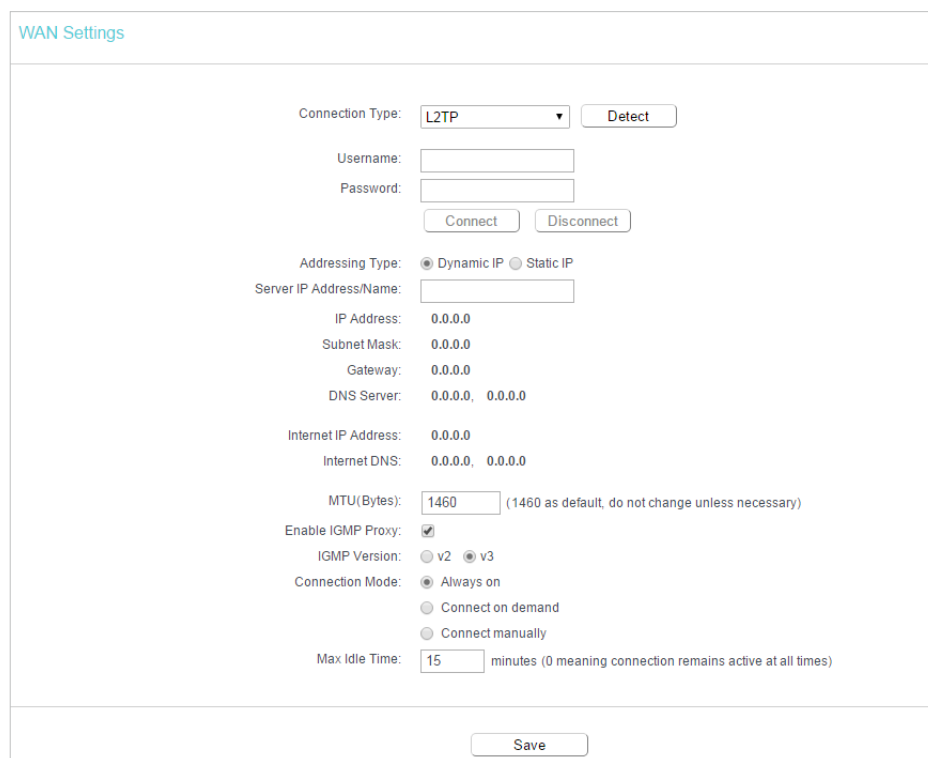
Note:

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](#).



The screenshot shows the WAN Settings page for L2TP configuration. The page is titled "WAN Settings" and contains the following fields and options:

- Connection Type:** A dropdown menu set to "L2TP" with a "Detect" button next to it.
- Username:** An empty text input field.
- Password:** An empty text input field.
- Connect/Disconnect:** Two buttons, "Connect" and "Disconnect", located below the password field.
- Addressing Type:** Radio buttons for "Dynamic IP" (selected) and "Static IP".
- Server IP Address/Name:** An empty text input field.
- IP Address:** 0.0.0.0
- Subnet Mask:** 0.0.0.0
- Gateway:** 0.0.0.0
- DNS Server:** 0.0.0.0, 0.0.0.0
- Internet IP Address:** 0.0.0.0
- Internet DNS:** 0.0.0.0, 0.0.0.0
- MTU(Bytes):** 1460 (1460 as default, do not change unless necessary)
- Enable IGMP Proxy:** A checked checkbox.
- IGMP Version:** Radio buttons for "v2" and "v3" (selected).
- Connection Mode:** Radio buttons for "Always on" (selected), "Connect on demand", and "Connect manually".
- Max Idle Time:** 15 minutes (0 meaning connection remains active at all times)
- Save:** A button at the bottom of the page.

- **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. The 'Connection Type' is set to 'PPTP'. There are input fields for 'Username' and 'Password', and buttons for 'Connect' and 'Disconnect'. The 'Addressing Type' is set to 'Dynamic IP'. Below that are fields for 'Server IP Address/Name', 'IP Address', 'Subnet Mask', 'Gateway', and 'DNS Server', all with default values of 0.0.0.0. There are also fields for 'Internet IP Address' and 'Internet DNS'. The 'MTU(Bytes)' is set to 1420. The 'Enable IGMP Proxy' checkbox is checked. The 'IGMP Version' is set to v3. The 'Connection Mode' is set to 'Always on'. The 'Max Idle Time' is set to 15 minutes.

- **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**.

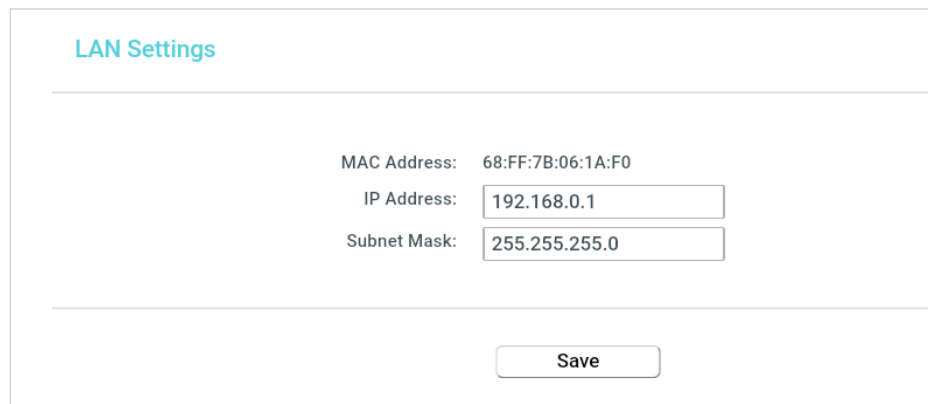
The screenshot shows the WAN Settings configuration page. The 'Connection Type' is set to 'BigPond Cable' with a 'Detect' button. Below this are input fields for 'Username', 'Password', 'Auth Server', and 'Auth Domain'. The 'MTU(Bytes)' is set to 1500, with a note '(1500 as default, do not change unless necessary)'. The 'Enable IGMP Proxy' checkbox is checked, and the 'IGMP Version' is set to 'v3'. The 'Connection Mode' is set to 'Always on'. 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.

5.3.2. 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: 68:FF:7B:06:1A:F0

IP Address:

Subnet Mask:

- **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.

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.

5.3.3. 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:	<input type="text" value="00:0A:EB:13:09:6A"/> <input type="button" value="Restore Factory MAC"/>
Your PC's MAC Address:	<input type="text" value="40:8D:5C:89:74:B5"/> <input type="button" value="Clone MAC Address"/>
<input type="button" value="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.

5.4. Wireless

5.4.1. Basic Settings

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

The screenshot shows the 'Wireless Settings' configuration page. It is divided into two main sections: 'Client Setting' and 'AP Setting'.
Client Setting:
 - SSID(to be bridged): [Empty text box]
 - MAC Address(to be bridged): [00:00:FF:FF:10:2F] e.g. 00:1D:0F:11:22:33 Lock to AP
 - Scan: [Scan button]
 - Key Type: [WPA2-PSK dropdown]
 - WEP Index: [1 dropdown]
 - Authentication Type: [Open System dropdown]
 - Encryption: [AES dropdown]
 - Wireless Password: [Empty text box]
AP Setting:
 - Wireless Network Name: [Empty text box] (Also called SSID)
 - Mode: [11bgn mixed dropdown]
 - Channel: [8 dropdown]
 - Channel Width: [Auto dropdown]
 - Enable SSID Broadcast
 - Save: [Save button]

- **Client Settings** - The settings of the public Wi-Fi your router is going to connect to.
 - **SSID(to be bridged)** - The SSID of the public Wi-Fi your router is going to connect to as a client.
 - **MAC Address(to be bridged)** - The MAC address of the public Wi-Fi your router is going to connect to as a client.
 - **Lock to AP** - If selected, the device's connection will be restricted to only the network with this specific MAC address.
 - **Scan** - Click this button to search the public Wi-Fi.
 - **Key type** - Select the key type according to the public Wi-Fi's security configuration. It is recommended that the key type is the same as the public Wi-Fi's security type.
 - **WEP Index** - Select which of the four keys will be used if the key type is WEP (ASCII) or WEP (HEX).
 - **Authentication Type** - Select the authorization type if the key type is WEP (ASCII) or WEP(HEX).
 - **Encryption** - Select the encryption type is the key type is WPA-PSK or WPA2-PSK.
 - **Password** - Enter the public Wi-Fi's password if required.
- **AP Settings** - The wireless settings of your router.
 - **Local Wireless Network Name** - Enter a string of up to 32 characters. It is strongly recommended that you change your network name (SSID). This value is case-sensitive. For example, TEST is NOT the same as test.
 - **Mode** - You can choose the appropriate "Mixed" mode.

- **Channel** - This field determines which operating frequency will be used. The default channel is set to **Auto**. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Channel Width** - This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point. If you select auto, then AP will choose the best channel automatically.
- **Enable SSID Broadcast** - If enabled, the router will broadcast the wireless network name (SSID).

5.4.2. WPS

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

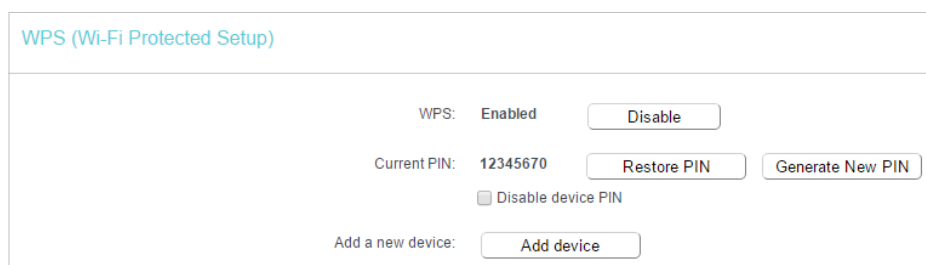
Note:

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

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

Method ONE: Press the WPS Button on Your Client Device

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



WPS (Wi-Fi Protected Setup)

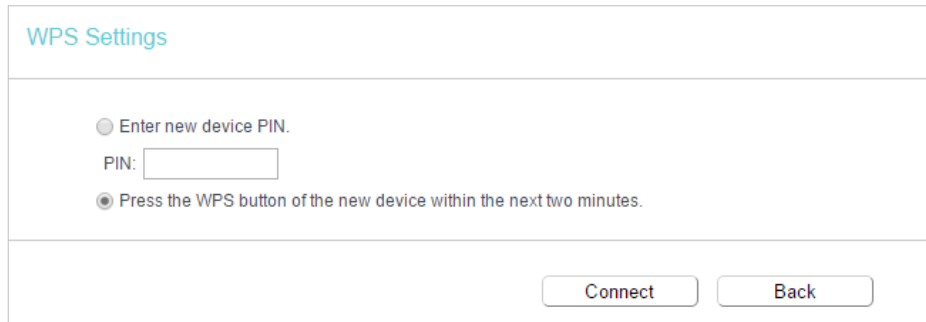
WPS: Enabled

Current PIN: 12345670

Disable device PIN

Add a new device:

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

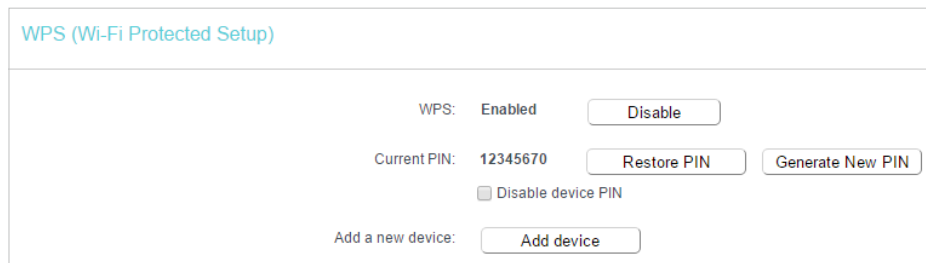


The screenshot shows the 'WPS Settings' page. At the top, the title 'WPS Settings' is displayed in blue. Below the title, there are two radio button options. The first option, 'Enter new device PIN.', is selected. Below this option is a text input field labeled 'PIN:'. The second option, 'Press the WPS button of the new device within the next two minutes.', is unselected. At the bottom of the page, there are two buttons: 'Connect' and '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.

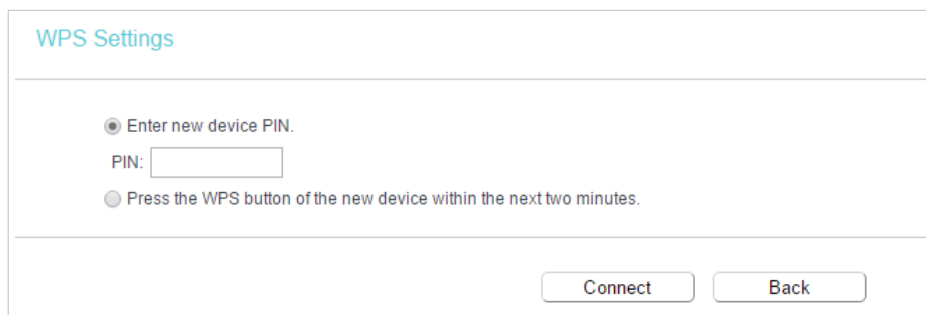
Method TWO: Enter the Client's PIN

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



The screenshot shows the 'WPS (Wi-Fi Protected Setup)' page. At the top, the title 'WPS (Wi-Fi Protected Setup)' is displayed in blue. Below the title, the WPS status is shown as 'Enabled' with a 'Disable' button next to it. The current PIN is displayed as '12345670' with 'Restore PIN' and 'Generate New PIN' buttons next to it. There is also a checkbox labeled 'Disable device PIN' which is currently unchecked. At the bottom, there is an 'Add a new device:' section with an 'Add device' button.

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



The screenshot shows the 'WPS Settings' page. At the top, the title 'WPS Settings' is displayed in blue. Below the title, there are two radio button options. The first option, 'Enter new device PIN.', is selected. Below this option is a text input field labeled 'PIN:'. The second option, 'Press the WPS button of the new device within the next two minutes.', is unselected. At the bottom of the page, there are two buttons: 'Connect' and '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.

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

5.4.3. Wireless Security

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

- **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.

5.4.4. Wireless MAC Filtering

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

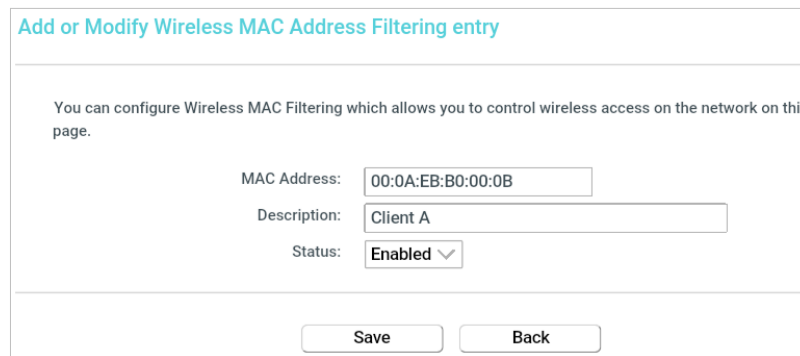
I want to:

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

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

How can I do that?

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [Wireless > Wireless MAC Filtering](#).
3. Click [Enable](#) to enable the Wireless MAC Filtering function.
4. Select [Allow the stations specified by any enabled entries in the list to access](#) as the filtering rule.
5. Delete all or disable all entries if there are any entries already.
6. Click [Add New](#) and fill in the blank.



Add or Modify Wireless MAC Address Filtering entry

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

MAC Address:

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.

<input type="checkbox"/>	MAC Address	Status	Host	Description	Edit
<input checked="" type="checkbox"/>	00:0A:EB:00:00:0B	Enabled	TP-LINK_7AFF	client A	Edit
<input checked="" type="checkbox"/>	00:0A:EB:00:07:5F	Enabled	TP-LINK_7AFF	Client B	Edit

Done!

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

5.4.5. Wireless Advanced

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [Wireless > Wireless Advanced](#).
3. Configure the advanced settings of your wireless network and click [Save](#).

Note:

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

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.

5.4.6. Wireless Statistics

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

The screenshot shows the 'Wireless Stations Status' page. At the top, it indicates 'Wireless Stations Currently Connected: 1' with a 'Refresh' button. Below this is a table with the following data:

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.

5.5. 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:

Guest Network Isolation:

Guest Network Bandwidth Control:

Guest Network: Enable Disable

Network Name:

Max Guests number:

Security:

Authentication Type:

Encryption:

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:

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:

Start Time: End Time:

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.															

- [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.

5.6. 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.

5.6.1. 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](#).

5. 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
<input type="button" value="Refresh"/>				

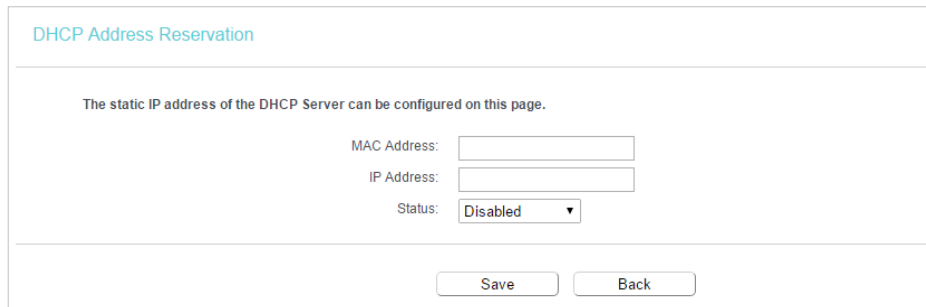
- **Client Name** - The name of the DHCP client.
- **MAC Address** - The MAC address of the DHCP client.
- **Assigned IP** - The IP address that the router has allocated to the DHCP client.
- **Lease Time** - The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic 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](#).

5. 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:

- 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**.

5.7. 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.

5.7.1. Virtual Server

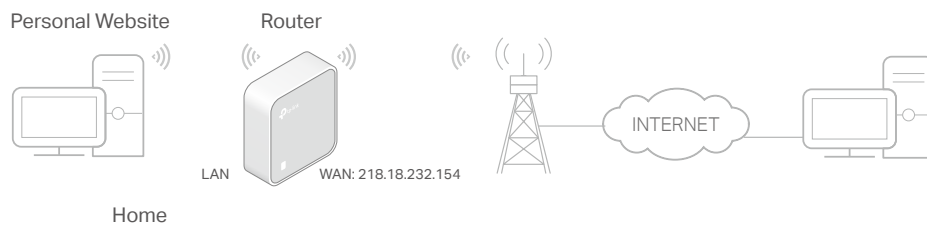
When you build up a server in the local network and want to share it on the internet, Virtual Servers can realize the service and provide it to internet users. At the same time virtual servers can keep the local network safe as other services are still invisible from the internet.

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
<input type="button" value="Save"/> <input type="button" value="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](http://WAN IP) (in this example: [http:// 218.18.232.154](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.

5.7.2. 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 Applications** list. The trigger port and incoming ports 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.

5.7.3. 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.

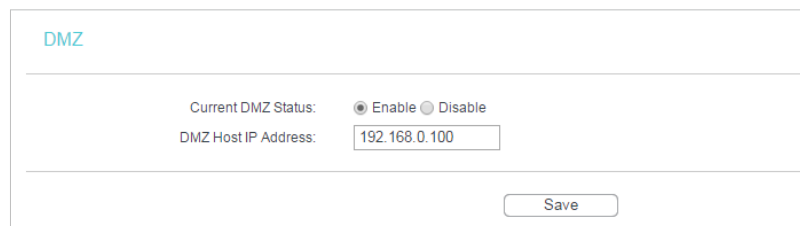
I want to:

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** filed.



DMZ

Current DMZ Status: Enable Disable

DMZ Host IP Address:

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.

5.7.4. 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:**

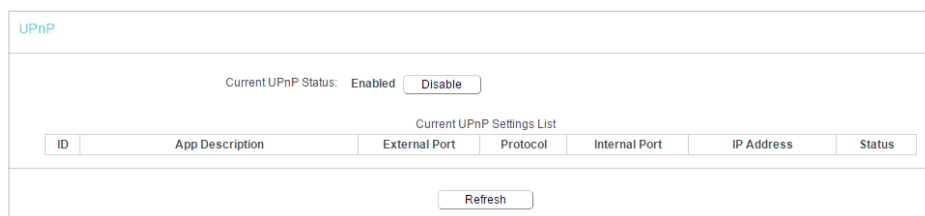
- UPnP is enabled by default in this router.
- Only the application supporting UPnP protocol can use this feature.
- UPnP feature needs the support of operating system (e.g. Windows Vista/ Windows 7/ Windows 8, etc. Some of operating system need to install the UPnP components).

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.



5.8. Security

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

5.8.1. 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**.

5.8.2. 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.

5.9. Parental Controls

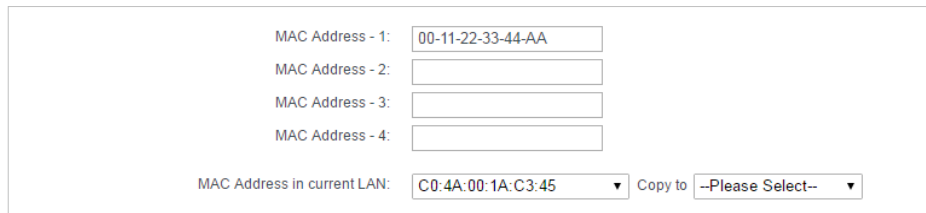
Parental Controls allows you to block inappropriate and malicious websites, and control access to specific websites at specific time for your children's devices.

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**.

The screenshot shows the 'Parental Controls' configuration page. At the top, there is a title 'Parental Controls' and a descriptive paragraph: '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".' Below this, there is a checkbox labeled 'Enable Parental Controls' which is checked. Underneath, there are two input fields: 'MAC Address Of Parental PC:' with the value '00:11:22:33:44:BB' and 'MAC Address of Current PC:' with the value 'C0:4A:00:1A:C3:45'. To the right of the second field is a 'Copy to Above' button. At the bottom left, there is a 'Save' button.

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



MAC Address - 1:

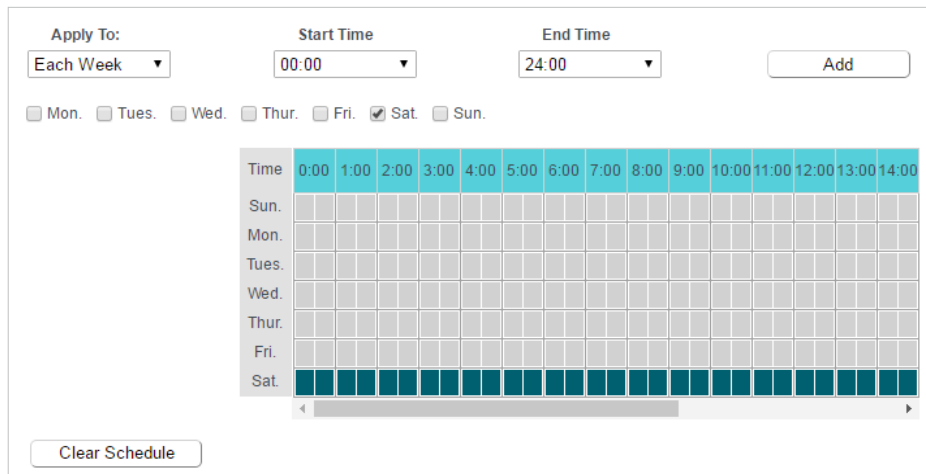
MAC Address - 2:

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:

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.															

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



Add URL:

(Will not take effect until you save these changes)

7. Click **Save**.

5. 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:

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.															

- 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:

- 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](#).

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.

5. 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.

5. 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.

- **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**.

5. 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

- **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.

5. 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.

Bandwidth Control

Enable Bandwidth Control

Egress Bandwidth: Kbps

Ingress Bandwidth: Kbps

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

Bandwidth Control

Enable:

IP Range: --

Port Range: --

Protocol:

Priority: (1 meaning highest priority)

	Min Bandwidth(Kbps)	Max Bandwidth(Kbps)
Egress Bandwidth:	<input type="text"/>	<input type="text"/>
Ingress Bandwidth:	<input type="text"/>	<input type="text"/>

- **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 through the WAN port.
- **Ingress Bandwidth** - The max and the min download speed through the WAN port.

5. 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.

5.13.1. 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 bottom, there is a section for 'ARP Binding' with two radio buttons: 'Enable' (which is 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 a form for adding a new entry. The form includes the following fields and controls:

- A heading: 'This page allows you to set IP-MAC Binding entries.'
- 'MAC Address:' followed by a text input field.
- 'IP Address:' followed by a text input field.
- 'Bind:' followed by a checked checkbox.
- 'Save' and 'Back' buttons at the bottom.

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

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

5.13.2. 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.

The screenshot shows the 'ARP List' page. It features a table with the following data:

	MAC Address	IP Address	Status
<input type="checkbox"/>	00:E0:4C:00:07:BE	192.168.0.4	Bound
<input type="checkbox"/>	40:8D:5C:89:74:B5	192.168.0.100	Unloaded

Below the table are two buttons: 'Load Selected' and 'Delete Selected'. At the bottom of the page is a 'Refresh' button.

- **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.

5. 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.

DDNS Settings

Service Provider: Dyndns (dyn.com/dns) [Go to register...](#)

Domain Name:

Username:

Password:

Enable DDNS:

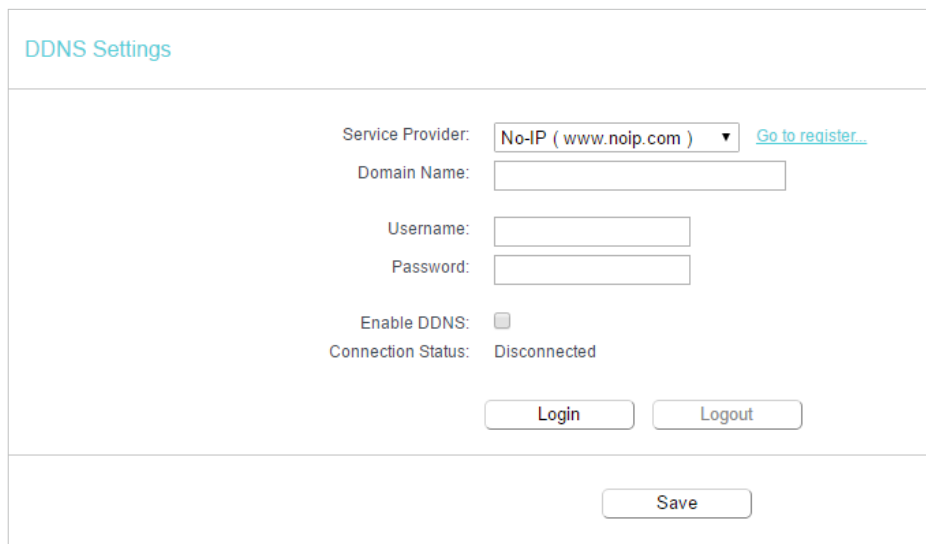
Connection Status: Disconnected

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. At the top left, the title 'DDNS Settings' is displayed in blue. Below the title, there are several input fields and controls:

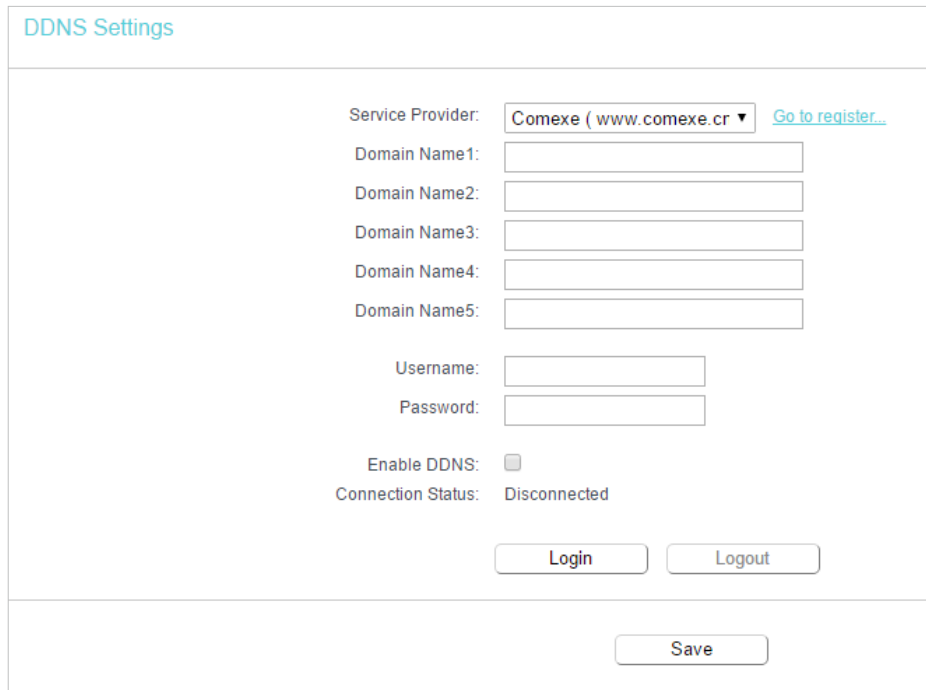
- Service Provider:** A dropdown menu is set to 'No-IP (www.noip.com)'. To its right is a blue link that says 'Go to register..'
- Domain Name:** An empty text input field.
- Username:** An empty text input field.
- Password:** An empty text input field.
- Enable DDNS:** A checkbox that is currently unchecked.
- Connection Status:** The text 'Disconnected' is displayed.
- At the bottom of the form area, there are two buttons: 'Login' and 'Logout'.
- Below the form area, centered, is a 'Save' button.

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.



The screenshot shows the 'DDNS Settings' page. At the top left, the title 'DDNS Settings' is displayed in blue. Below the title, the 'Service Provider' is set to 'Comexe (www.comexe.cn)' with a dropdown arrow and a blue link 'Go to register...'. There are five input fields for 'Domain Name1' through 'Domain Name5'. Below these are input fields for 'Username' and 'Password'. An 'Enable DDNS' checkbox is currently unchecked. The 'Connection Status' is shown as 'Disconnected'. At the bottom of the form area, there are 'Login' and 'Logout' buttons. Below the form area, there is a 'Save' button.

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.

5. 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).

5. 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.

The screenshot shows the 'IPv6 Status' page. It has a title bar 'IPv6 Status' and two main sections. The first section is 'WAN', which displays 'Connection Type: Disabled'. The second section is 'IPv6 LAN', which displays 'IPv6 Address Type: RADVD', 'Prefix Length: 64', and '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**.

5. 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**.

The screenshot shows the 'IPv6 WAN' configuration page. It has a title bar 'IPv6 WAN' and several configuration fields. 'Enable IPv6' is checked. 'Connection Type' is set to 'Dynamic IPv6'. 'IPv6 Address' is set to '::', 'Prefix Length' is set to '0', and 'IPv6 Gateway' is set to '::'. 'Addressing Type' is set to 'DHCPv6'. There is a 'Hide' button next to the 'Addressing Type' dropdown. Below this, 'MTU (Bytes)' is set to '1500' with a note '(1500 as default, do not change unless necessary)'. 'Enable MLD Proxy' and 'Set IPv6 DNS Server manually' are unchecked. 'Host Name' is set to 'TL-WR802N'. A 'Save' button is at the bottom.

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 as default, do not change unless necessary) [Hide](#)

Enable MLD Proxy:

Set IPv6 DNS Server manually:

Host Name:

[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) Hide

Enable MLD Proxy:

- **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

IPv6 WAN

Enable IPv6:

Connection Type: PPPoEv6

PPPoE same session with IPv4 connection

PPP Username:

PPP Password:

Confirm password:

Authentication Type: AUTO_AUTH

Addressing Type: DHCPv6

Service Name: (do not change unless necessary)

Server Name: (do not change unless necessary)

MTU(Bytes): (1480 as default, do not change unless necessary) Hide

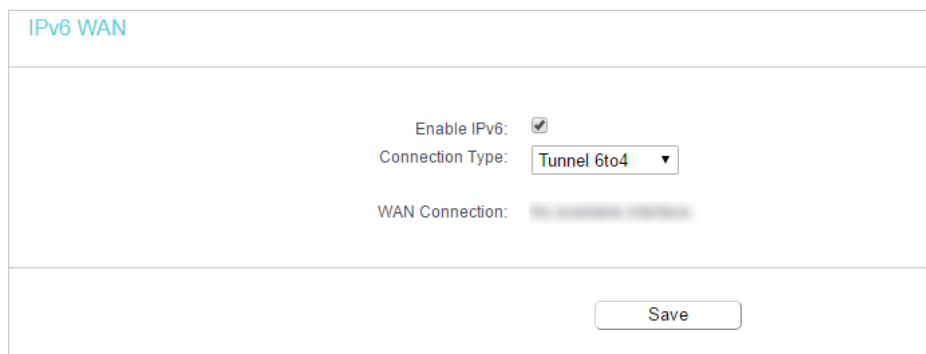
Enable MLD Proxy:

Use IPv6 address specified by ISP:

Set IPv6 DNS Server manually:

- **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 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.
- **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.

Tunnel 6to4



The screenshot shows the 'IPv6 WAN' configuration interface. It includes a section for 'Enable IPv6' with a checked checkbox. Below it, the 'Connection Type' is set to 'Tunnel 6to4' via a dropdown menu. The 'WAN Connection' field is currently blank. A 'Save' button is located at the bottom right of the configuration area.

- **WAN Connection** - Display the available wan connection.

5. 15. 3. IPv6 LAN

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **IPv6 > IPv6 LAN** and configure the IPv6 LAN settings as needed.

IPv6 LAN Settings

The parameters of IPv6 LAN can be configured on this page when IPv6 enabled.
 Note: Only the default group will support IPv6 at this moment.

Group: **Default**

Address Auto-Configuration Type: RADVD DHCPv6 Server

Enable RDNSS:

Enable ULA Prefix:

Site Prefix Configuration Type: Delegated Static

Prefix Delegated WAN Connection: No available interface.

- **Address Auto-Configuration Type** - Select a type to assign IPv6 addresses to the computers in your LAN. RADVD and DHCPv6 Server are provided. I
- **Site Prefix Configuration Type** - The type of IPv6 address prefix.
 - **Delegated** - Get the IPv6 address prefix from the ISP automatically, and the device will delegate it to the LAN.
 - **Static** - Configure the **Site Prefix** and **Site Prefix Length** manually. Please contact your ISP to get more information before you configure them.

Note:

If your IPv6 wan connection type is "Tunnel 6to4", the Site Prefix Configuration Type should be "Static" to make sure "Tunnel 6to4" works properly.

5. 16. System Tools

5. 16. 1. Time Settings

This page allows you to set the time manually or to configure automatic time synchronization. The router can automatically update the time from an NTP server via the internet.

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

- **To set time manually:**

1. Select your local [Time Zone](#).
2. Enter the [Date](#) in Month/Day/Year format.
3. Enter the [Time](#) in Hour/Minute/Second format.
4. Click [Save](#).

- **To set time automatically:**

5. Select your local [Time Zone](#).
6. Enter the address or domain of the [NTP Server 1](#) or [NTP Server 2](#).
7. Click [Get GMT](#) to get time from the internet if you have connected to the internet.

- **To set Daylight Saving Time:**

1. Select [Enable Daylight Saving](#).
2. Select the start time from the drop-down list in the [Start](#) fields.
3. Select the end time from the drop-down list in the [End](#) fields.
4. Click [Save](#).

Note:

This setting will be used for some time-based functions such as firewall. You must specify your time zone once you log in to the router successfully; otherwise, time-based functions will not take effect.

5.16.2. Diagnostic

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

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [System Tools > Diagnostic](#).

Diagnostic Tools

Diagnostic Parameters

Diagnostic Tool: Ping Traceroute

IP address/Domain name:

Ping Count: ping(1 - 50)

Ping Packet Size: (0 - 65500 Bytes)

Ping Timeout: (1 - 60 Seconds)

Traceroute Max TTL: (1 - 30)

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

Note:

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

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

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

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

Diagnostic Results

Pinging 192.168.0.1 with 64 bytes of data:

```

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

```

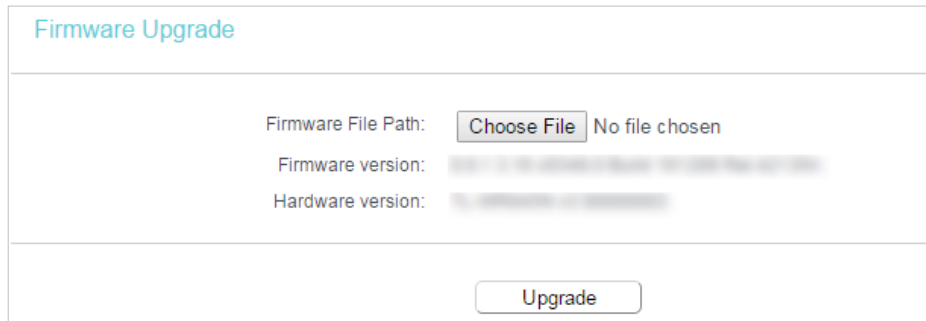
Ping statistics for 192.168.0.1
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milliseconds:
Minimum = 1, Maximum = 1, Average = 1

5. 16. 3. Firmware Upgrade

TP-Link is dedicated to improving and enriching the product features, giving users a better network experience. We will release the latest firmware at TP-Link official website

www.tp-link.com. You can download the latest firmware file from the [Support](#) page of our website and upgrade the firmware to the latest version.

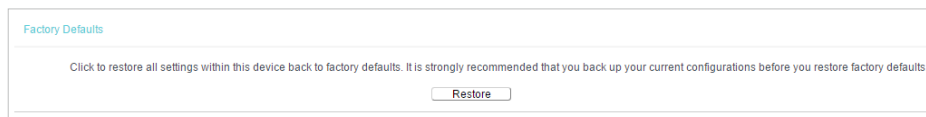
1. Download the latest firmware file for the router from our website www.tp-link.com.
2. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
3. Go to [System Tools > Firmware Upgrade](#).
4. Click [Choose File](#) to locate the downloaded firmware file, and click [Upgrade](#).



The screenshot shows the 'Firmware Upgrade' page. At the top, the title 'Firmware Upgrade' is displayed. Below the title, there are three rows of information: 'Firmware File Path:' with a 'Choose File' button and the text 'No file chosen'; 'Firmware version:' with a blurred value; and 'Hardware version:' with a blurred value. At the bottom of the page, there is a large 'Upgrade' button.

5. 16. 4. Factory Defaults

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [System Tools > Factory Defaults](#). Click [Restore](#) to reset all settings to the default values.



The screenshot shows the 'Factory Defaults' page. At the top, the title 'Factory Defaults' is displayed. Below the title, there is a warning message: 'Click to restore all settings within this device back to factory defaults. It is strongly recommended that you back up your current configurations before you restore factory defaults.' At the bottom of the page, there is a 'Restore' button.

- Default [Username](#): admin
- Default [Password](#): admin
- Default [IP Address](#): 192.168.0.1
- Default [Subnet Mask](#): 255.255.255.0

5. 16. 5. Backup & Restore

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

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

- **To backup configuration settings:**

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

- **To restore configuration settings:**

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

📌 **Note:**

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

5.16.6. Reboot

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

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Working Modes.
- Change the Web Management Port.
- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router to its factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically).

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [System Tools > Reboot](#).

- **To reboot manually**

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

- **To reboot automatically**

- Select **Timeout** in the drop-down list of **Enable Auto Reboot** and specify a time period (1-72hours), then the router will reboot automatically after every this interval.

Enable Auto Reboot: **Timeout** ▼

1 Hours **0** Minutes

Remaining Time

Save

- Select **Schedule** in the drop-down list of **Enable Auto Reboot** and specify the **Time** when the router reboots and **Day** which to decide how often it reboots.

Enable Auto Reboot: **Schedule** ▼

Day: Everyday Select Days

Mon Tue Wed Thu Fri Sat Sun

Time: **00** ▼ **00** ▼ (Hour:Minute)

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

Save

5. 16. 7. Account Management

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **System Tools > Administrator**, and focus on the **Account Management** section. You can change the factory default username and password of the router.

Account Management

The username and password must not exceed 15 characters in length!

Old Password:

New User Name:

New Password:

Confirm password:

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

Note:

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

3. Click **Save**.

5.16.8. Local Management

This feature allows you to block computers on the LAN from accessing the router by using the MAC/IP-based authentication.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **System Tools > Administrator**, and focus on the **Service Configuration** section.

Service Configuration			
	HTTP Service	HTTPS Service	Available Host (IP/MAC)
Local Management	Port <input type="text" value="80"/>	Enable <input type="checkbox"/> Port <input type="text" value="443"/>	<input type="text"/>
Remote Management	Enable <input type="checkbox"/> Port <input type="text" value="80"/>	Enable <input type="checkbox"/> Port <input type="text" value="443"/>	<input type="text"/>

- **Allow all LAN connected devices to manage the router locally**

1. Keep the **Available Host (IP/MAC)** empty, which means you don't specify any host to manage the router.
2. If you want to access the router via both HTTPS and HTTP, please tick the **Enable** checkbox in **HTTPS Service** column. Otherwise, keep it disabled.
3. Keep the local management port as default if you don't know which port to use.
4. Click **Save**.

Note:

If the web management port conflicts with the one used for **Virtual Server** entry, the entry will be automatically disabled after the setting is saved.

- **Allow a specific device to manage the router locally**

1. Enter the IP or MAC address of the host that you want to manage the router in the **Available Host (IP/MAC)** entry. The format of the MAC address is XX:XX:XX:XX:XX:XX (X is any hexadecimal digit).
2. If you want to access the router via both HTTPS and HTTP, please tick the **Enable** box in **HTTPS Service** column. Otherwise, keep it disabled.
3. Keep the Port as default if you don't know which port to use.
4. Click **Save**.

Note:

If your PC is blocked but you want to access the router again, press and hold the **Reset** button to reset the router to the factory defaults.

- **Certificate**

Download and install the certificate for management via HTTPS if you need it. Once the certificate is installed, warnings will not pop up when you access the router via HTTPS.



5.16.9. Remote Management

This feature allows you to manage your router from a remote location via the internet.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **System Tools > Administrator**, and focus on the **Service Configuration** section.

Service Configuration			
	HTTP Service	HTTPS Service	Available Host (IP/MAC)
Local Management	Port <input type="text" value="80"/>	Enable <input type="checkbox"/> Port <input type="text" value="443"/>	<input type="text"/>
Remote Management	Enable <input type="checkbox"/> Port <input type="text" value="80"/>	Enable <input type="checkbox"/> Port <input type="text" value="443"/>	<input type="text"/>

- **Forbid all devices to manage the router remotely**

Do not tick the **Enable** checkbox in both **HTTP Service** and **HTTPS Service**.

- **Allow all devices to manage the router remotely**

1. Tick the **Enable** checkbox in **HTTP Service**.
2. If you want to access the router via both HTTPS and HTTP, please tick the **Enable** checkbox in **HTTPS Service** column. Otherwise, keep it disabled.
3. For higher security, you can change the remote management web port by entering a number between 1024 and 65534.
4. Click **Save**.

- **Allow a specific device to manage the router remotely**

1. Tick the **Enable** checkbox in **HTTP Service**.
2. If you want to access the router via both HTTPS and HTTP, please tick the **Enable** checkbox in **HTTPS Service** column. Otherwise, keep it disabled.
3. For higher security, you can change the remote management web port by entering a number between 1024 and 65534.
4. Enter the IP or MAC address of the host that you want to manage the router in the **Available Host (IP/MAC)** entry. The format of the MAC address is XX:XX:XX:XX:XX:XX (X is any hexadecimal digit).
5. Click **Save**.

- **Certificate**

Download and install the certificate for management via HTTPS if you need it. Once the certificate is installed, warnings will not pop up when you access the router via HTTPS.

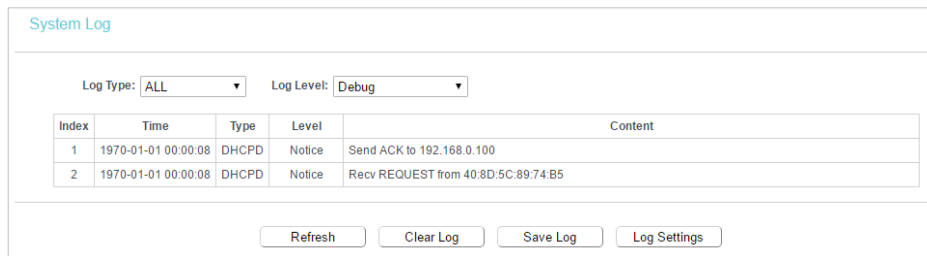


Note:

- To access the router, enter your router's WAN IP address in your browser's address bar, followed by a colon and the custom port number. For example, if your router's WAN address is 202.96.12.8, and the port number used is 8080, please enter `http://202.96.12.8:8080` in your browser. Later, you may be asked for the router's password. After successfully entering the username and password, you will be able to access the router's web management page.
- Be sure to change the router's default password for security purposes.

5.16.10. System Log

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



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

5.16.11. Statistics

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **System Tools > Traffic Statistics**.
3. Select **Enable** and click **Save**. You can view the network traffic of each PC on the LAN, including total traffic and the value of the last Packets Statistic interval in seconds.

Traffic Statistics

Traffic Statistics--LAN

Traffic Statistics: Enable Disable

Statistics Interval: seconds

Statistics List

IP Address MAC Address	Total		Current				Operation
	Packets	Bytes	Packets	Bytes	ICMP Tx	UDP Tx	
Current list is blank							

5. 17. Log out

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

Chapter 6

Configure the Router in Access Point Mode

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

It contains the following sections:

- [Status](#)
- [Operation Mode](#)
- [Network](#)
- [Wireless](#)
- [DHCP](#)
- [System Tools](#)
- [Log out](#)

6.1. 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:	3.0.1.0 (2018.08.01)
Hardware Version:	V1.0 (2018.08.01)
LAN	
MAC Address:	30:B5:C2:E6:9F:CE
IP Address:	192.168.0.1
Subnet Mask:	255.255.255.0
Wireless	
Operation Mode:	Access Point
Wireless Radio:	Enabled
Name(SSID):	TP-Link_9FCE
Mode:	11bgn mixed
Channel:	Auto(Channel 3)
Channel Width:	Auto
MAC Address:	30:B5:C2:E6:9F:CE
System Up Time:	0 day(s) 00:01:00 <input type="button" value="Refresh"/>

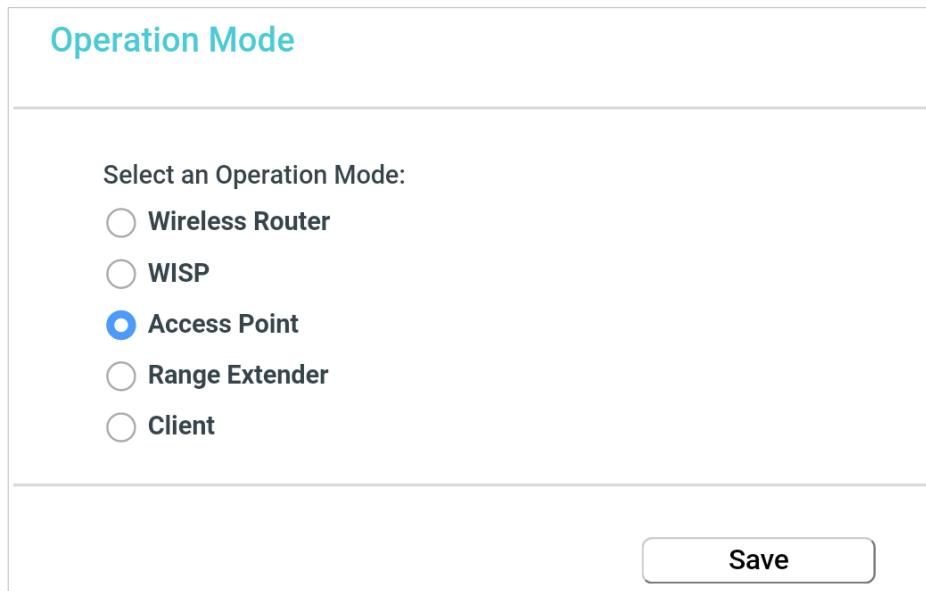
- **Firmware Version** - The version information of the router's firmware.
- **Hardware Version** - The version information of the router's hardware.
- **LAN** - This field displays the current settings of the LAN, and you can configure them on the **Network > LAN** page.
 - **MAC address** - The physical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

6.2. Operation Mode

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



Operation Mode

Select an Operation Mode:

- Wireless Router
- WISP
- Access Point
- Range Extender
- Client

[Save](#)

6.3. Network

6.3.1. LAN

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

LAN Settings

LAN Type: ▼

Note: The IP parameters cannot be configured if you have chosen Smart IP(DHCP)
(In this situation the device will help you configure the IP parameters automatically as you need).

MAC Address: 68:FF:7B:06:1A:F0

IP Address:

Subnet Mask:

Gateway: (optional)

- **Type** - Either select **Smart IP(DHCP)** to get IP address from DHCP server, or **Static IP** to configure IP address manually.
- **MAC Address** - The physical address of the LAN ports. The value can not be changed.
- **IP Address** - Enter the IP address in dotted-decimal notation of your router if you select **Static IP** (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.

Note:

- If you have changed the IP address, you must use the new IP address to log in.
- If you select **Smart IP(DHCP)**, the DHCP server of the router will not start up.
- If the new IP address you set is not in the same subnet as the old one, the IP address pool in the DHCP Server will be configured automatically, but the Virtual Server and DMZ Host will not take effect until they are re-configured.

6. 4. Wireless

6. 4. 1. Basic Settings

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

Wireless Basic Settings

Wireless: Enable Disable

Wireless Network Name: (Also called SSID)

Mode: ▼

Channel: ▼

Channel Width: ▼

Enable SSID Broadcast

- **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).

6.4.2. WPS

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

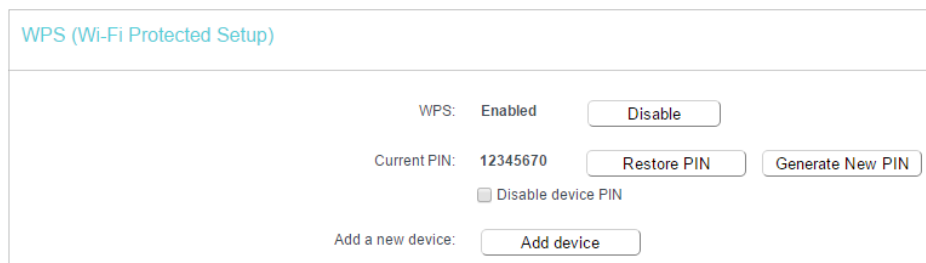
Note:

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

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

Method ONE: Press the WPS Button on Your Client Device

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



WPS (Wi-Fi Protected Setup)

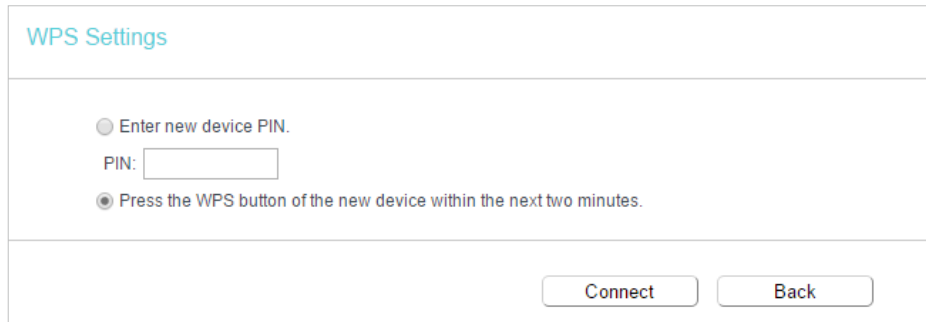
WPS: Enabled

Current PIN: 12345670

Disable device PIN

Add a new device:

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

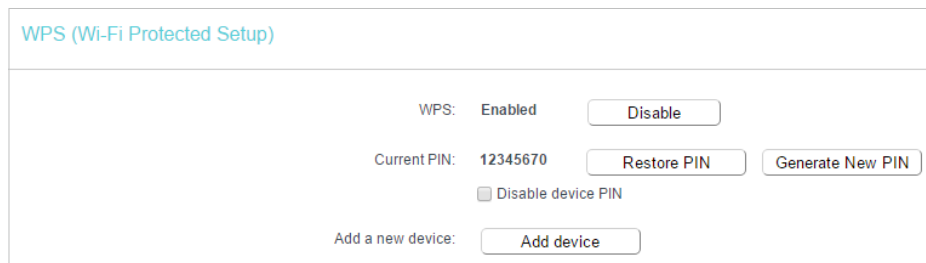


The screenshot shows the 'WPS Settings' page. At the top, the title 'WPS Settings' is displayed in blue. Below the title, there are two radio button options. The first option, 'Enter new device PIN.', is selected. Below this option is a text input field labeled 'PIN:'. The second option, 'Press the WPS button of the new device within the next two minutes.', is not selected. At the bottom of the page, there are two buttons: 'Connect' and '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.

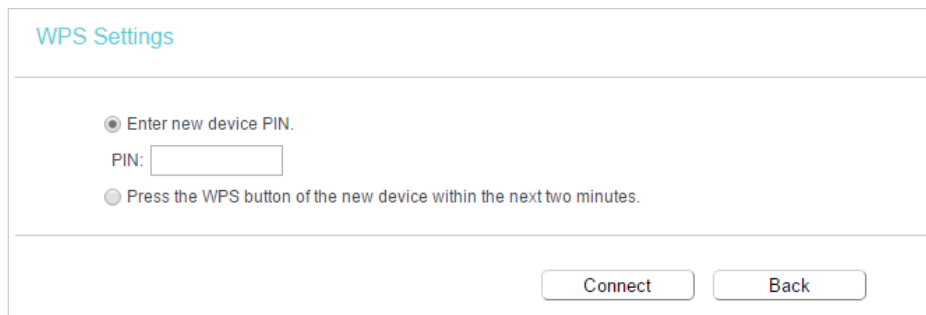
Method TWO: Enter the Client's PIN

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



The screenshot shows the 'WPS (Wi-Fi Protected Setup)' page. At the top, the title 'WPS (Wi-Fi Protected Setup)' is displayed in blue. Below the title, there are several controls. The 'WPS:' status is 'Enabled', with a 'Disable' button next to it. The 'Current PIN:' is '12345670', with 'Restore PIN' and 'Generate New PIN' buttons next to it. There is a checkbox labeled 'Disable device PIN' which is currently unchecked. At the bottom, there is an 'Add a new device:' section with an 'Add device' button.

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



The screenshot shows the 'WPS Settings' page. At the top, the title 'WPS Settings' is displayed in blue. Below the title, there are two radio button options. The first option, 'Enter new device PIN.', is selected. Below this option is a text input field labeled 'PIN:'. The second option, 'Press the WPS button of the new device within the next two minutes.', is not selected. At the bottom of the page, there are two buttons: 'Connect' and '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.

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

6.4.3. 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**.

- **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.

6.4.4. Wireless MAC Filtering

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

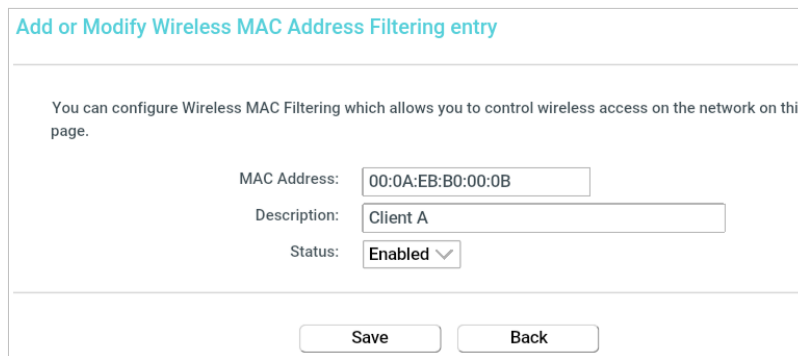
I want to:

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.

<input type="checkbox"/>	MAC Address	Status	Host	Description	Edit
<input checked="" type="checkbox"/>	00:0A:EB:00:00:0B	Enabled	TP-LINK_7AFF	client A	Edit
<input checked="" type="checkbox"/>	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.

6.4.5. 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.

6.4.6. 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.

The screenshot shows the 'Wireless Stations Status' page. At the top, it says 'Wireless Stations Currently Connected: 1' with a 'Refresh' button. Below this is a table with the following data:

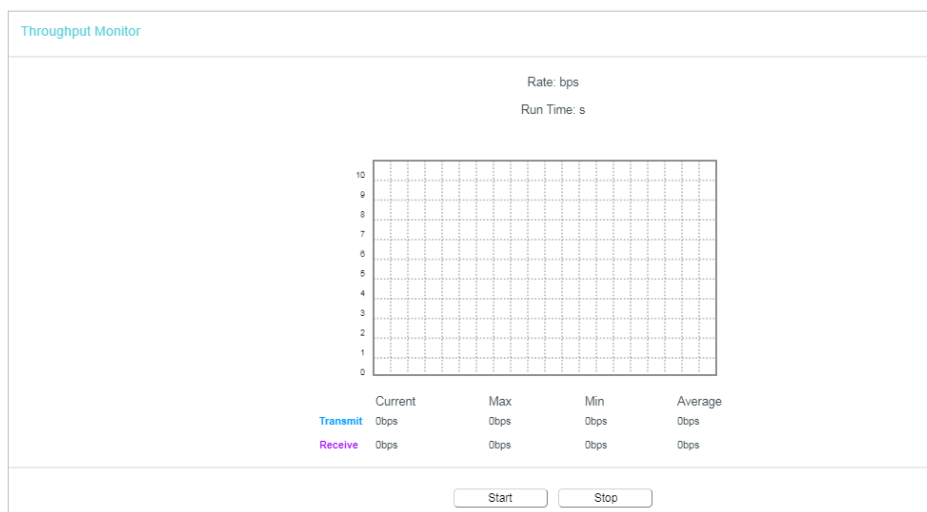
ID	MAC Address	Current Status	Received Packets	Sent Packets	SSID
1	44:00:10:BF:3B:A7	Associated	29	19	

- **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.

6.4.7. Throughput Monitor

Throughput monitor records the wireless throughput information.

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



- **Rate** - The throughput unit.
- **Run Time** - How long this function is running.
- **Transmit** - Wireless transmit rate information.
- **Transmit** - Wireless transmit rate information.
- **Receive** - Wireless reception rate information.
- Click **Start** to start wireless throughput monitor.
- Click **Stop** to stop wireless throughput monitor.

6.5. 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

Guest Network Isolation: Disable ▼

Guest Network: Enable Disable

Network Name: TP-Link_Guest_1AF0

Max Guests number: 32

Security: Disable Wireless Security ▼

Access Time: Schedule ▼

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

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

- [Guest Network Isolation](#) - If enabled, guests are isolated from each other.

Note:

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

6. 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.

6. 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](#).
- When you choose [Smart IP\(DHCP\)](#) in [Network > LAN](#), the DHCP Server function will be disabled. You will see the page as below.

DHCP Settings

DHCP Server: Disable Enable

Start IP Address:

End IP Address:

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

Default Gateway: (optional)

Default Domain: (optional)

DNS Server: (optional)

Secondary DNS Server: (optional)

Note: The DHCP Settings function cannot be configured if you have chosen Smart IP (DHCP) in [Network->LAN](#) (in this situation the device will help you configure the DHCP automatically as you need).

6.6.2. 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

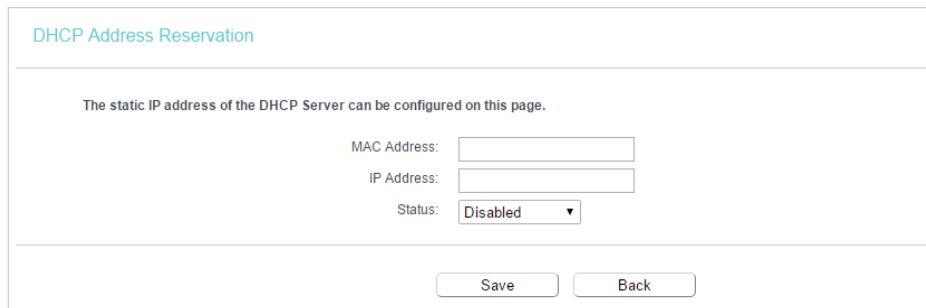
- **Client Name** - The name of the DHCP client.
- **MAC Address** - The MAC address of the DHCP client.
- **Assigned IP** - The IP address that the router has allocated to the DHCP client.
- **Lease Time** - The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic 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](#).

6.6.3. 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:

- 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**.

6.7. System Tools

6.7.1. Diagnostic

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

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

Diagnostic Tools

Diagnostic Parameters

Diagnostic Tool: Ping Traceroute Start

IP address/Domain name:

Ping Count: ping(1 - 50)

Ping Packet Size: (0 - 65500 Bytes)

Ping Timeout: (1 - 60 Seconds)

Traceroute Max TTL: (1 - 30)

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

Note:

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

- **IP Address/Domain Name** - Enter the destination IP address (such as 192.168.0.1) or Domain name (such as www.tp-link.com).
 - **Ping Count** - The number of Ping packets for a Ping connection.
 - **Ping Packet Size** - The size of Ping packet.
 - **Ping Timeout** - Set the waiting time for the reply of each Ping packet. If there is no reply in the specified time, the connection is overtime.
 - **Traceroute Max TTL** - The max number of hops for a Traceroute connection.
3. Click **Start** to check the connectivity of the internet.
 4. The **Diagnostic Results** page displays the diagnosis result. If the result is similar to the following figure, the connectivity of the internet is fine.

Diagnostic Results

Pinging 192.168.0.1 with 64 bytes of data:

```

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

```

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

6.7.2. SNMP Settings

Enable this function if you want to have remote control through SNMPv1/v2 agent with MIB-II.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **System Tools > SNMP Settings**.
3. Select **Enable**, configure the parameters and click **Save**.

SNMP Settings

Simple Network Management Protocol(SNMP) allows management applications to retrieve status updates and statistics from the SNMP agent within this device.

SNMP Agent: Disable Enable

Read Community:

Set Community:

System Name:

System Description:

System Location:

System Contact:

Trap Manager IP:

Save

- **System Name** - An administratively-assigned name for this managed node.
- **System Description** - The software version information for this managed node.
- **System Location** - The physical location of this node.
- **System Contact** - The textual identification of the contact person for this managed node.
- **Trap Manage IP** - Displays the IP address of the host to receive the traps.

6.7.3. Ping WatchDog

The Ping Watch Dog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. It makes the router continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, the router will automatically reboot.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **System Tools > Ping WatchDog**.
3. Configure the settings and click **Save**.

Ping WatchDog Settings

Ping WatchDog will be the monitor to detect AP's network, reboot device while AP disconnected.

Switch: Disable Enable

Destination IP:

Interval: (10-300)s

Startup Delay: (60-300)s

Fail Count: (1-65535)

Save

- **Enable** - Turn on/off Ping Watch Dog.
- **Destination IP** - The IP address of the target host where the Ping Watch Dog Utility is sending ping packets.
- **Interval** - Time interval between two ping packets which are sent out continuously.
- **Startup Delay** - Time delay before first ping packet is sent out when the router is restarted.
- **Fail Count** - Upper limit of the ping packets the router can drop continuously. If this value is overrun, the router will restart automatically.

6.7.4. Firmware Upgrade

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

1. Download the latest firmware file for the router from our website www.tp-link.com.
2. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
3. Go to [System Tools > Firmware Upgrade](#).
4. Click [Choose File](#) to locate the downloaded firmware file, and click [Upgrade](#).

Firmware Upgrade

Firmware File Path: No file chosen

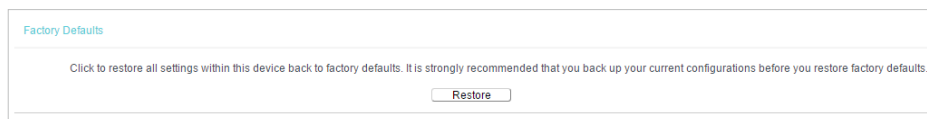
Firmware version:

Hardware version:

Upgrade

6.7.5. Factory Defaults

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **System Tools > Factory Defaults**. Click **Restore** to reset all settings to the default values.

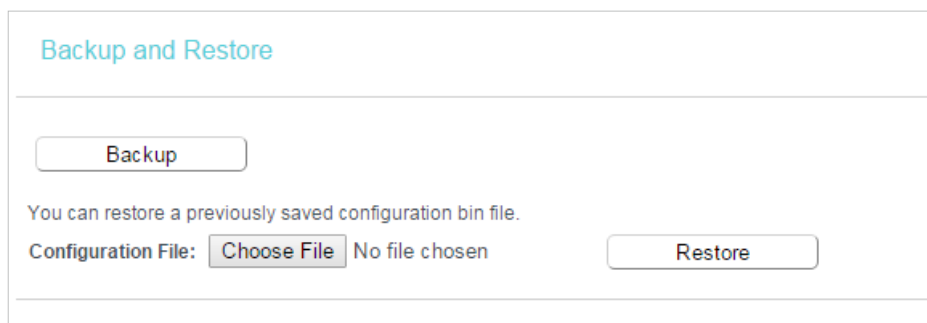


- Default **Username**: admin
- Default **Password**: admin
- Default **IP Address**: 192.168.0.1
- Default **Subnet Mask**: 255.255.255.0

6.7.6. Backup & Restore

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

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



- **To backup configuration settings:**

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

- **To restore configuration settings:**

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

Note:

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

6.7.7. Reboot

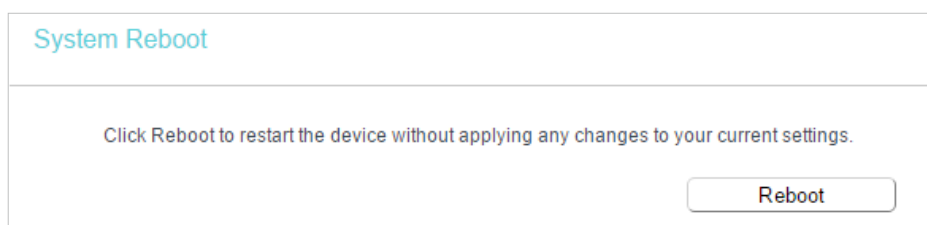
Some settings of the router will take effect only after rebooting, including:

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Working Modes.
- Change the Web Management Port.
- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router to its factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically).

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [System Tools > Reboot](#).

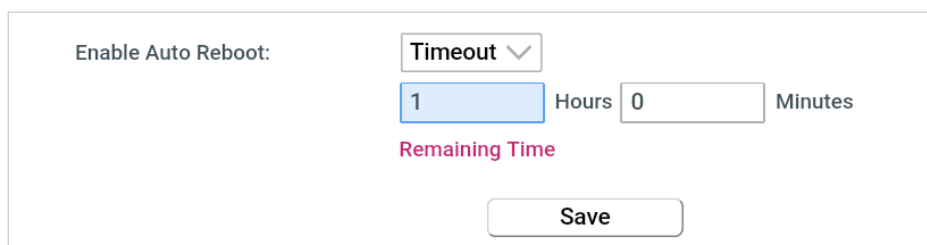
- **To reboot manually**

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



- **To reboot automatically**

- Select [Timeout](#) in the drop-down list of [Enable Auto Reboot](#) and specify a time period (1-72hours), then the router will reboot automatically after every this interval.



- Select [Schedule](#) in the drop-down list of [Enable Auto Reboot](#) and specify the [Time](#) when the router reboots and [Day](#) which to decide how often it reboots.

Enable Auto Reboot:

Day: Everyday Select Days

Mon Tue Wed Thu Fri Sat Sun

Time: (Hour:Minute)

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

6.7.8. Account Management

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [System Tools](#) > [Administrator](#), and focus on the [Account Management](#) section. You can change the factory default username and password of the router.

Account Management

The username and password must not exceed 15 characters in length!

Old Password:

New User Name:

New Password:

Confirm password:

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

Note:

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

3. Click [Save](#).

6.7.9. Local Management

This feature allows you to block computers on the LAN from accessing the router by using the MAC/IP-based authentication.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [System Tools](#) > [Administrator](#), and focus on the [Service Configuration](#) section.

Service Configuration			
Local Management	HTTP Service	HTTPS Service	Available Host (IP/MAC)
Port: 80	Enable <input type="checkbox"/> Port: 80	Enable <input type="checkbox"/> Port: 443	<input type="text"/>

- **Allow all LAN connected devices to manage the router locally**

1. Keep the [Available Host \(IP/MAC\)](#) empty, which means you don't specify any host to manage the router.
2. If you want to access the router via both HTTPS and HTTP, please tick the [Enable](#) checkbox in [HTTPS Service](#) column. Otherwise, keep it disabled.
3. Keep the local management port as default if you don't know which port to use.
4. Click [Save](#).

Note:

If the web management port conflicts with the one used for [Virtual Server](#) entry, the entry will be automatically disabled after the setting is saved.

- **Allow a specific device to manage the router locally**

1. Enter the IP or MAC address of the host that you want to manage the router in the [Available Host \(IP/MAC\)](#) entry. The format of the MAC address is XX:XX:XX:XX:XX:XX (X is any hexadecimal digit).
2. If you want to access the router via both HTTPS and HTTP, please tick the [Enable](#) box in [HTTPS Service](#) column. Otherwise, keep it disabled.
3. Keep the Port as default if you don't know which port to use.
4. Click [Save](#).

Note:

If your PC is blocked but you want to access the router again, press and hold the [Reset](#) button to reset the router to the factory defaults.

- **Certificate**

Download and install the certificate for management via HTTPS if you need it. Once the certificate is installed, warnings will not pop up when you access the router via HTTPS.

Certificate Download
Certificate Download

6.7.10. System Log

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

System Log

Log Type: Log Level:

Index	Time	Type	Level	Content
1	1970-01-01 00:00:08	DHCPD	Notice	Send ACK to 192.168.0.100
2	1970-01-01 00:00:08	DHCPD	Notice	Recv REQUEST from 40:8D:5C:89:74:B5

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

6.8. Log out

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

Chapter 7

Configure the Router in Range Extender Mode

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

It contains the following sections:

- [Status](#)
- [Operation Mode](#)
- [Network](#)
- [Wireless](#)
- [DHCP](#)
- [System Tools](#)
- [Log out](#)

7.1. 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:	3.0.1.1 (3.0.1.1) (3.0.1.1) (3.0.1.1) (3.0.1.1)
Hardware Version:	V1.0 (V1.0) (V1.0) (V1.0) (V1.0)
LAN	
MAC Address:	30:B5:C2:E6:9F:CE
IP Address:	192.168.0.1
Subnet Mask:	255.255.255.0
Wireless	
Operation Mode:	Range Extender
Wireless Radio:	Enabled
Name(SSID) of Root AP:	
Name(SSID):	TP-Link_9FCE
Mode:	11bgn mixed
Channel:	6
Channel Width:	Auto
MAC Address:	30:B5:C2:E6:9F:CE
System Up Time:	0 day(s) 00:00:59 <input type="button" value="Refresh"/>

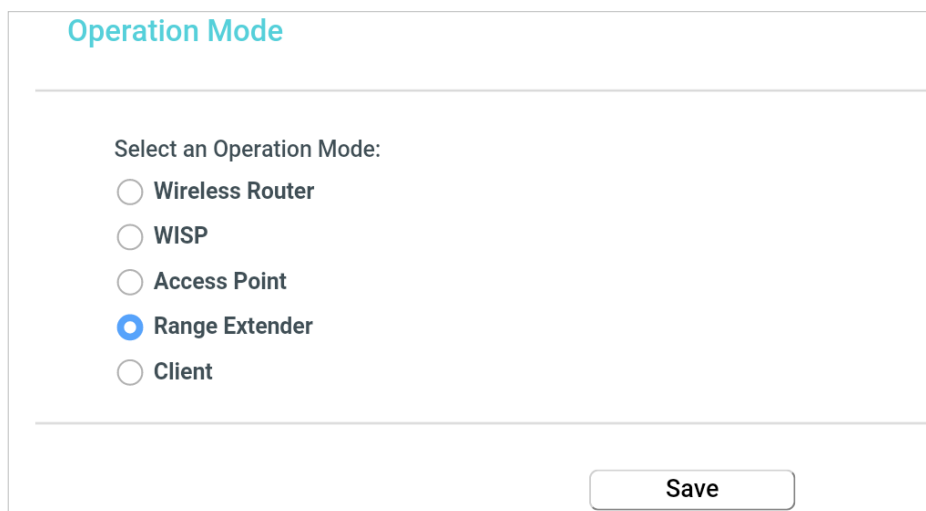
- **Firmware Version** - The version information of the router's firmware.
- **Hardware Version** - The version information of the router's hardware.
- **LAN** - This field displays the current settings of the LAN, and you can configure them on the **Network > LAN** page.
 - **MAC address** - The physical 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) of Root AP** - The wireless name of the root router.
 - **Name(SSID)** - The wireless name of the router.
 - **Mode** - The current wireless mode which the router works on.
 - **Channel** - The current wireless channel in use.

- **Channel Width** - The current wireless channel width in use.
- **MAC Address** - The physical address of the router.
- **System Up Time** - The length of the time since the router was last powered on or reset.

Click [Refresh](#) to get the latest status and settings of the router.

7.2. Operation Mode

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



Operation Mode

Select an Operation Mode:

Wireless Router

WISP

Access Point

Range Extender

Client

[Save](#)

7.3. Network

7.3.1. LAN

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

LAN Settings

LAN Type: ▼

Note: The IP parameters cannot be configured if you have chosen Smart IP(DHCP)
(In this situation the device will help you configure the IP parameters automatically as you need).

MAC Address: 68:FF:7B:06:1A:F0

IP Address:

Subnet Mask:

Gateway: (optional)

- **Type** - Either select **Smart IP(DHCP)** to get IP address from DHCP server, or **Static IP** to configure IP address manually.
- **MAC Address** - The physical address of the LAN ports. The value can not be changed.
- **IP Address** - Enter the IP address in dotted-decimal notation of your router if you select **Static IP** (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.

Note:

- If you have changed the IP address, you must use the new IP address to log in.
- If you select **Smart IP(DHCP)**, the DHCP server of the router will not start up.
- If the new IP address you set is not in the same subnet as the old one, the IP address pool in the DHCP Server will be configured automatically, but the Virtual Server and DMZ Host will not take effect until they are re-configured.

7.4. Wireless

7.4.1. Connect to Network

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

Connect to Host Network

SSID(to be bridged):

MAC Address(to be bridged): Lock To AP

Security: ▼

Password:

The configuration modified here will be automatically synchronized to the extended network settings

- Click [Scan](#), select your host network from the [AP List](#) and click [Connect](#).

AP List

The scanned APs within the area:

APs: 45

ID	BSSID	SSID	Signal strength	Channel	Encryption	Connect
1	40:61:86:CF:1D:A1	TP-Link_1DA1	90	3	WPA-PSK/AES	Connect
2	2C:59:E5:DA:65:FE	HP-Print-FE-Officejet 7610	86	6	WPA2-PSK/AES	Connect
3	BC:5F:F6:12:2A:FF	MERCUSYS_2B00	81	10	None	Connect
4	3C:46:D8:E0:60:C4	TP-Link_60C4	78	1	WPA2-PSK/AES	Connect
5	CA:E7:D8:02:AA:EF	TP-Link_300re	77	1	WPA-PSK/AES	Connect

- Enter your host network's wireless password in the [Password](#) field.

Connect to Host Network

SSID(to be bridged):

MAC Address(to be bridged): Lock To AP

Security: ▼

Password:

The configuration modified here will be automatically synchronized to the extended network settings

- Tick [Lock to AP](#) checkbox if you want to restrict the device's connection to only the network with this specific MAC address.
- Click [Save](#).

7.4.2. Extended Network

- Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
- Go to [Wireless](#) > [Extended Network](#), you can view the SSID and password of the router (Range Extender)'s wireless network.
- If you want to share the same SSID of the host router, click [Copy Host SSID](#) and click [Save](#).

Extended Network Settings

Extended 2.4GHz SSID:

Extended 2.4GHz Security:

Extended 2.4GHz Password:

Enable SSID Broadcast

7.4.3. 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**

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.

<input type="checkbox"/>	MAC Address	Status	Host	Description	Edit
<input type="checkbox"/>	00:0A:EB:B0:00:0B	Enabled	TP-LINK_7AFF	client A	Edit
<input type="checkbox"/>	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.

7.4.4. 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: **High** ▼

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.

7.4.5. 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 <input type="button" value="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.

7.5. 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.

7.5.1. 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](#).
- When you choose **Smart IP(DHCP)** in **Network > LAN**, the DHCP Server function will be disabled. You will see the page as below.

DHCP Settings

DHCP Server: Disable Enable

Start IP Address:

End IP Address:

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

Default Gateway: (optional)

Default Domain: (optional)

DNS Server: (optional)

Secondary DNS Server: (optional)

Note: The DHCP Settings function cannot be configured if you have chosen Smart IP (DHCP) in [Network->LAN](#) (in this situation the device will help you configure the DHCP automatically as you need).

7.5.2. 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

- **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](#).

7.6. System Tools

7.6.1. Diagnostic

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

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [System Tools > Diagnostic](#).

The screenshot shows the 'Diagnostic Tools' section of a router's web interface. It features a 'Diagnostic Parameters' area with the following controls:

- Diagnostic Tool:** Radio buttons for 'Ping' (selected) and 'Traceroute', followed by a 'Start' button.
- IP address/Domain name:** A text input field.
- Ping Count:** A numeric input field set to '4', with a range of 'ping(1 - 50)'.
- Ping Packet Size:** A numeric input field set to '64', with a range of '(0 - 65500 Bytes)'.
- Ping Timeout:** A numeric input field set to '1', with a range of '(1 - 60 Seconds)'.
- Traceroute Max TTL:** A numeric input field set to '20', with a range of '(1 - 30)'.

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

Note:

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

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

3. Click [Start](#) to check the connectivity of the internet.
4. The [Diagnostic Results](#) page displays the diagnosis result. If the result is similar to the following figure, the connectivity of the internet is fine.

```
Diagnostic Results
-----
Pinging 192.168.0.1 with 64 bytes of data:

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

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

7.6.2. Firmware Upgrade

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

1. Download the latest firmware file for the router from our website www.tp-link.com.
2. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
3. Go to [System Tools > Firmware Upgrade](#).
4. Click [Choose File](#) to locate the downloaded firmware file, and click [Upgrade](#).

Firmware Upgrade

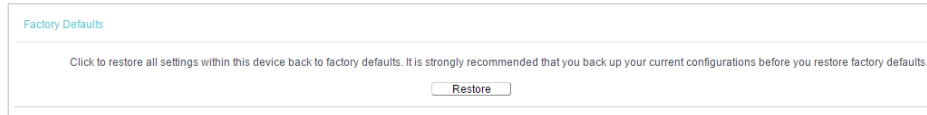
Firmware File Path: No file chosen

Firmware version:

Hardware version:

7.6.3. Factory Defaults

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [System Tools > Factory Defaults](#). Click [Restore](#) to reset all settings to the default values.

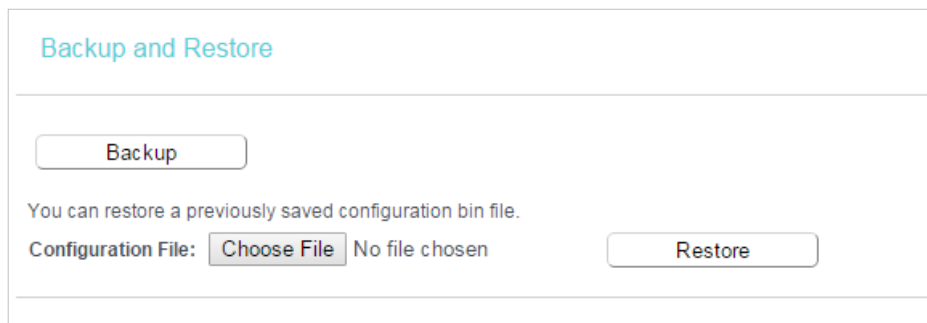


- Default **Username**: admin
- Default **Password**: admin
- Default **IP Address**: 192.168.0.1
- Default **Subnet Mask**: 255.255.255.0

7.6.4. Backup & Restore

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

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



- **To backup configuration settings:**

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

- **To restore configuration settings:**

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

Note:

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

7.6.5. Reboot

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

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

- Change the Web Management Port.
 - Upgrade the firmware of the router (system will reboot automatically).
 - Restore the router to its factory defaults (system will reboot automatically).
 - Update the configuration with the file (system will reboot automatically).
1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
 2. Go to [System Tools > Reboot](#).

- **To reboot manually**

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

System Reboot

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

- **To reboot automatically**

- Select [Timeout](#) in the drop-down list of [Enable Auto Reboot](#) and specify a time period (1-72hours), then the router will reboot automatically after every this interval.

Enable Auto Reboot: Timeout ▾

Hours
 Minutes

Remaining Time

- Select [Schedule](#) in the drop-down list of [Enable Auto Reboot](#) and specify the [Time](#) when the router reboots and [Day](#) which to decide how often it reboots.

Enable Auto Reboot: Schedule ▾

Day: Everyday Select Days

Mon
 Tue
 Wed
 Thu
 Fri
 Sat
 Sun

Time: (Hour:Minute)

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

7.6.6. Account Management

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **System Tools > Administrator**, and focus on the **Account Management** section. You can change the factory default username and password of the router.

Account Management

The username and password must not exceed 15 characters in length!

Old Password:

New User Name:

New Password:

Confirm password:

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

Note:

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

3. Click **Save**.

7.6.7. Local Management

This feature allows you to block computers on the LAN from accessing the router by using the MAC/IP-based authentication.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to **System Tools > Administrator**, and focus on the **Service Configuration** section.

Service Configuration			
	HTTP Service	HTTPS Service	Available Host (IP/MAC)
Local Management	Port <input style="width: 30px;" type="text" value="80"/>	Enable <input type="checkbox"/> Port <input style="width: 30px;" type="text" value="443"/>	<input style="width: 100px;" type="text"/>

- **Allow all LAN connected devices to manage the router locally**

1. Keep the **Available Host (IP/MAC)** empty, which means you don't specify any host to manage the router.
2. If you want to access the router via both HTTPS and HTTP, please tick the **Enable** checkbox in **HTTPS Service** column. Otherwise, keep it disabled.
3. Keep the local management port as default if you don't know which port to use.
4. Click **Save**.

Note:

If the web management port conflicts with the one used for [Virtual Server](#) entry, the entry will be automatically disabled after the setting is saved.

- **Allow a specific device to manage the router locally**

1. Enter the IP or MAC address of the host that you want to manage the router in the [Available Host \(IP/MAC\)](#) entry. The format of the MAC address is XX:XX:XX:XX:XX:XX (X is any hexadecimal digit).
2. If you want to access the router via both HTTPS and HTTP, please tick the [Enable](#) box in [HTTPS Service](#) column. Otherwise, keep it disabled.
3. Keep the Port as default if you don't know which port to use.
4. Click [Save](#).

Note:

If your PC is blocked but you want to access the router again, press and hold the [Reset](#) button to reset the router to the factory defaults.

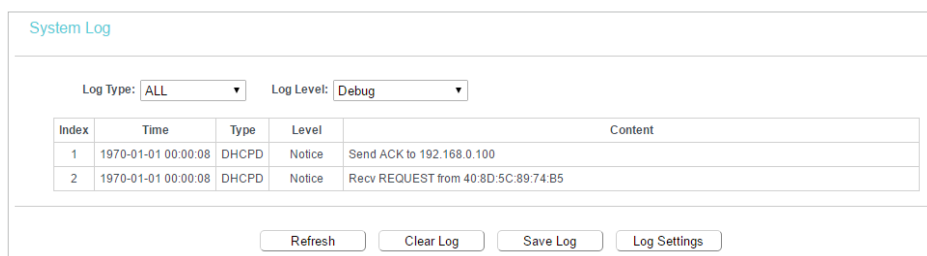
- **Certificate**

Download and install the certificate for management via HTTPS if you need it. Once the certificate is installed, warnings will not pop up when you access the router via HTTPS.



7.6.8. System Log

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



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

7.7. Log out

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

Chapter 8

Configure the Router in Client Mode

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

It contains the following sections:

- [Status](#)
- [Operation Mode](#)
- [Network](#)
- [Wireless](#)
- [DHCP](#)
- [System Tools](#)
- [Log out](#)

8.1. 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:	3.0.1.1 (3.0.1.1) (3.0.1.1) (3.0.1.1) (3.0.1.1)
Hardware Version:	V1.0 (V1.0) (V1.0) (V1.0) (V1.0)
LAN	
MAC Address:	30:B5:C2:E6:9F:CE
IP Address:	192.168.0.1
Subnet Mask:	255.255.255.0
Wireless	
Operation Mode:	Client
Wireless Radio:	Enabled
Name(SSID) of Root AP:	
Mode:	11bgn mixed
Channel:	1
Channel Width:	Auto
MAC Address:	30:B5:C2:E6:9F:CE
System Up Time:	0 day(s) 00:02:01 <input type="button" value="Refresh"/>

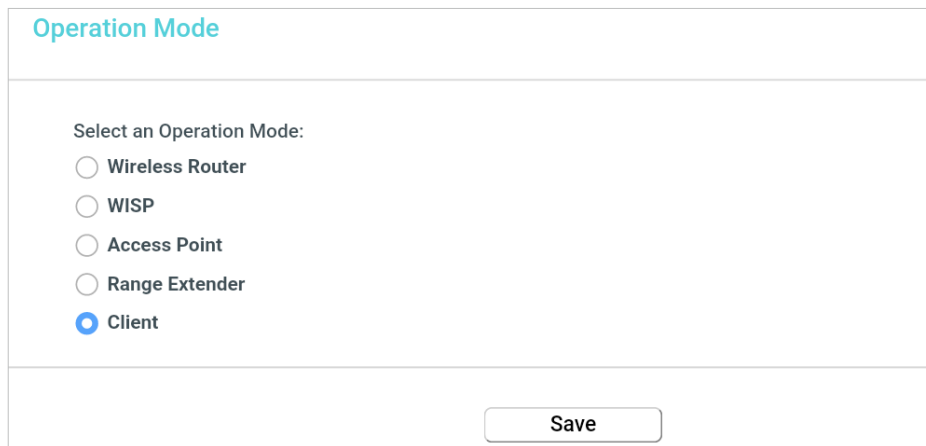
- **Firmware Version** - The version information of the router's firmware.
- **Hardware Version** - The version information of the router's hardware.
- **LAN** - This field displays the current settings of the LAN, and you can configure them on the [Network > LAN](#) page.
 - **MAC address** - The physical 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) of Root AP** - The wireless name of the root router.
 - **Mode** - The current wireless mode which the router works on.
 - **Channel** - The current wireless channel in use.
 - **Channel Width** - The current wireless channel width in use.

- **MAC Address** - The physical address of the router.
- **System Up Time** - The length of the time since the router was last powered on or reset.

Click [Refresh](#) to get the latest status and settings of the router.

8.2. Operation Mode

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



Operation Mode

Select an Operation Mode:

Wireless Router

WISP

Access Point

Range Extender

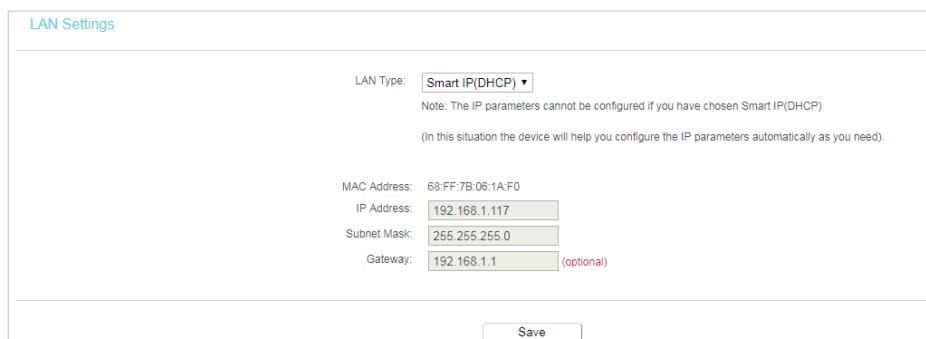
Client

Save

8.3. Network

8.3.1. LAN

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



LAN Settings

LAN Type: Smart IP(DHCP) ▼

Note: The IP parameters cannot be configured if you have chosen Smart IP(DHCP)
(In this situation the device will help you configure the IP parameters automatically as you need).

MAC Address: 68:FF:7B:06:1A:F0

IP Address: 192.168.1.117

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1 (optional)

Save

- **Type** - Either select **Smart IP(DHCP)** to get IP address from DHCP server, or **Static IP** to configure IP address manually.
- **MAC Address** - The physical address of the LAN ports. The value can not be changed.
- **IP Address** - Enter the IP address in dotted-decimal notation of your router if you select **Static IP** (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.

Note:

- If you have changed the IP address, you must use the new IP address to log in.
- If you select **Smart IP(DHCP)**, the DHCP server of the router will not start up.
- If the new IP address you set is not in the same subnet as the old one, the IP address pool in the DHCP Server will be configured automatically, but the Virtual Server and DMZ Host will not take effect until they are re-configured.

8. 4. Wireless

8. 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**.

Connect to Host Network

SSID(to be bridged):

MAC Address(to be bridged): Lock To AP

Security: ▼

Password:

The configuration modified here will be automatically synchronized to the extended network settings

3. Click **Scan**, select your host network from the **AP List** and click **Conenct**.

AP List

The scanned APs within the area:

APs: 45

ID	BSSID	SSID	Signal strength	Channel	Encryption	Connect
1	40:61:86:CF:1D:A1	TP-Link_1DA1	90	3	WPA-PSK/AES	Connect
2	2C:59:E5:DA:65:FE	HP-Print-FE-Officejet 7610	86	6	WPA2-PSK/AES	Connect
3	BC:5F:F6:12:2A:FF	MERCUSYS_2B00	81	10	None	Connect
4	3C:46:D8:E0:60:C4	TP-Link_60C4	78	1	WPA2-PSK/AES	Connect
5	CA:E7:D8:02:AA:EF	TP-Link_300re	77	1	WPA-PSK/AES	Connect

4. Enter your host network's wireless password in the **Password** field.

Connect to Host Network

SSID(to be bridged):

MAC Address(to be bridged): Lock To AP

Security: ▼

Password:

The configuration modified here will be automatically synchronized to the extended network settings

5. Tick **Lock to AP** checkbox if you want to restrict the device's connection to only the network with this specific MAC address.
6. Click **Save**.

8.5. 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.

8.5.1. 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](#).
- When you choose [Smart IP\(DHCP\)](#) in [Network > LAN](#), the DHCP Server function will be disabled. You will see the page as below.

DHCP Settings

DHCP Server: Disable Enable

Start IP Address:

End IP Address:

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

Default Gateway: (optional)

Default Domain: (optional)

DNS Server: (optional)

Secondary DNS Server: (optional)

Note: The DHCP Settings function cannot be configured if you have chosen Smart IP (DHCP) in [Network->LAN](#) (in this situation the device will help you configure the DHCP automatically as you need).

8.5.2. 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

- **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](#).

8. 6. System Tools

8. 6. 1. Diagnostic

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

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [System Tools > Diagnostic](#).

Diagnostic Tools	
Diagnostic Parameters	
Diagnostic Tool:	<input checked="" type="radio"/> Ping <input type="radio"/> Traceroute <input type="button" value="Start"/>
IP address/Domain name:	<input type="text"/>
Ping Count:	<input type="text" value="4"/> ping(1 - 50)
Ping Packet Size:	<input type="text" value="64"/> (0 - 65500 Bytes)
Ping Timeout:	<input type="text" value="1"/> (1 - 60 Seconds)
Traceroute Max TTL:	<input type="text" value="20"/> (1 - 30)

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

Note:

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

- **IP Address/Domain Name** - Enter the destination IP address (such as 192.168.0.1) or Domain name (such as www.tp-link.com).
 - **Pings Count** - The number of Ping packets for a Ping connection.
 - **Ping Packet Size** - The size of Ping packet.
 - **Ping Timeout** - Set the waiting time for the reply of each Ping packet. If there is no reply in the specified time, the connection is overtime.
 - **Traceroute Max TTL** - The max number of hops for a Traceroute connection.
3. Click **Start** to check the connectivity of the internet.
 4. The **Diagnostic Results** page displays the diagnosis result. If the result is similar to the following figure, the connectivity of the internet is fine.

```
Diagnostic Results
-----
Pinging 192.168.0.1 with 64 bytes of data:

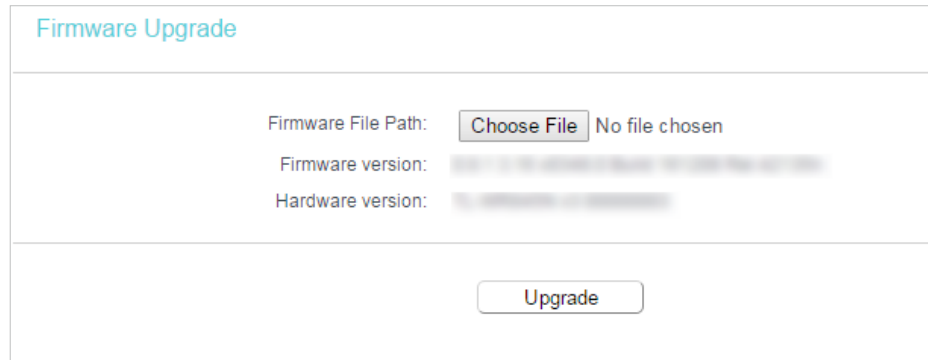
Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=1
Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=2
Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=3
Reply from 192.168.0.1: bytes=64 time=1 TTL=64 seq=4

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

8.6.2. Firmware Upgrade

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

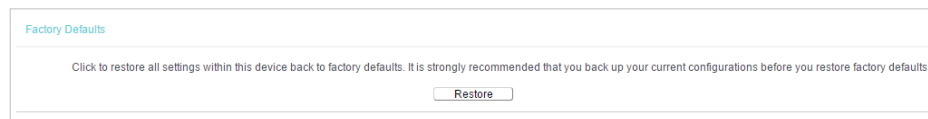
1. Download the latest firmware file for the router from our website www.tp-link.com.
2. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
3. Go to **System Tools > Firmware Upgrade**.
4. Click **Choose File** to locate the downloaded firmware file, and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



The screenshot shows the 'Firmware Upgrade' page. At the top, the title 'Firmware Upgrade' is displayed in blue. Below the title, there are three lines of information: 'Firmware File Path:' followed by a 'Choose File' button and the text 'No file chosen'; 'Firmware version:' followed by a blurred text field; and 'Hardware version:' followed by another blurred text field. At the bottom center of the page, there is a single 'Upgrade' button.

8. 6. 3. Factory Defaults

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [System Tools > Factory Defaults](#). Click [Restore](#) to reset all settings to the default values.



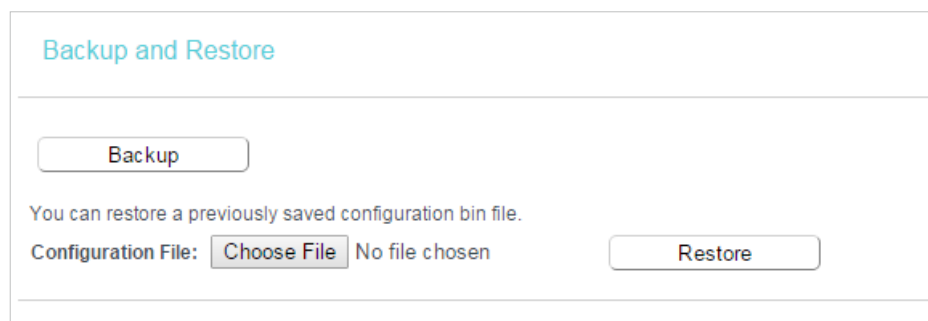
The screenshot shows the 'Factory Defaults' page. At the top, the title 'Factory Defaults' is displayed in blue. Below the title, there is a line of text: 'Click to restore all settings within this device back to factory defaults. It is strongly recommended that you back up your current configurations before you restore factory defaults.' At the bottom center of the page, there is a single 'Restore' button.

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

8. 6. 4. Backup & Restore

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

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



The screenshot shows the 'Backup and Restore' page. At the top, the title 'Backup and Restore' is displayed in blue. Below the title, there is a 'Backup' button. Underneath, there is a line of text: 'You can restore a previously saved configuration bin file.' Below this text, there are two elements: 'Configuration File:' followed by a 'Choose File' button and the text 'No file chosen', and a 'Restore' button.

- **To backup configuration settings:**

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

- **To restore configuration settings:**

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

Note:

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

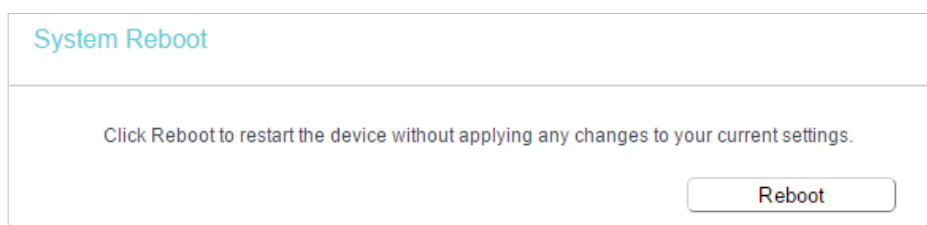
8.6.5. Reboot

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

- Change the LAN IP Address (system will reboot automatically).
 - Change the DHCP Settings.
 - Change the Working Modes.
 - Change the Web Management Port.
 - Upgrade the firmware of the router (system will reboot automatically).
 - Restore the router to its factory defaults (system will reboot automatically).
 - Update the configuration with the file (system will reboot automatically).
1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
 2. Go to [System Tools > Reboot](#).

- **To reboot manually**

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



- **To reboot automatically**

- Select [Timeout](#) in the drop-down list of [Enable Auto Reboot](#) and specify a time period (1-72hours), then the router will reboot automatically after every this interval.

Enable Auto Reboot: ▾

Hours Minutes

Remaining Time

- Select [Schedule](#) in the drop-down list of [Enable Auto Reboot](#) and specify the [Time](#) when the router reboots and [Day](#) which to decide how often it reboots.

Enable Auto Reboot: ▾

Day: Everyday Select Days

Mon Tue Wed Thu Fri Sat Sun

Time: (Hour:Minute)

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

8. 6. 6. Account Management

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [System Tools](#) > [Administrator](#), and focus on the [Account Management](#) section. You can change the factory default username and password of the router.

Account Management

The username and password must not exceed 15 characters in length!

Old Password:

New User Name:

New Password:

Confirm password:

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

Note:

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

3. Click [Save](#).

8.6.7. Local Management

This feature allows you to block computers on the LAN from accessing the router by using the MAC/IP-based authentication.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [System Tools > Administrator](#), and focus on the [Service Configuration](#) section.

Service Configuration			
	HTTP Service	HTTPS Service	Available Host (IP/MAC)
Local Management	Port <input type="text" value="80"/>	Enable <input type="checkbox"/> Port <input type="text" value="443"/>	<input type="text"/>
Remote Management	Enable <input type="checkbox"/> Port <input type="text" value="80"/>	Enable <input type="checkbox"/> Port <input type="text" value="443"/>	<input type="text"/>

- **Allow all LAN connected devices to manage the router locally**

1. Keep the [Available Host \(IP/MAC\)](#) empty, which means you don't specify any host to manage the router.
2. If you want to access the router via both HTTPS and HTTP, please tick the [Enable](#) checkbox in [HTTPS Service](#) column. Otherwise, keep it disabled.
3. Keep the local management port as default if you don't know which port to use.
4. Click [Save](#).

■ **Note:**

If the web management port conflicts with the one used for [Virtual Server](#) entry, the entry will be automatically disabled after the setting is saved.

- **Allow a specific device to manage the router locally**

1. Enter the IP or MAC address of the host that you want to manage the router in the [Available Host \(IP/MAC\)](#) entry. The format of the MAC address is XX:XX:XX:XX:XX:XX (X is any hexadecimal digit).
2. If you want to access the router via both HTTPS and HTTP, please tick the [Enable](#) box in [HTTPS Service](#) column. Otherwise, keep it disabled.
3. Keep the Port as default if you don't know which port to use.
4. Click [Save](#).

■ **Note:**

If your PC is blocked but you want to access the router again, press and hold the [Reset](#) button to reset the router to the factory defaults.

- **Certificate**

Download and install the certificate for management via HTTPS if you need it. Once the certificate is installed, warnings will not pop up when you access the router via HTTPS.

Certificate Download
Certificate Download

8.6.8. Remote Management

This feature allows you to manage your router from a remote location via the internet.

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Go to [System Tools > Remote Management](#), and focus on the [Service Configuration](#) section.

Service Configuration			
	HTTP Service	HTTPS Service	Available Host (IP/MAC)
Local Management	Port <input type="text" value="80"/>	Enable <input type="checkbox"/> Port <input type="text" value="443"/>	<input type="text"/>
Remote Management	Enable <input type="checkbox"/> Port <input type="text" value="80"/>	Enable <input type="checkbox"/> Port <input type="text" value="443"/>	<input type="text"/>

- **Forbid all devices to manage the router remotely**

Do not tick the [Enable](#) checkbox in both [HTTP Service](#) and [HTTPS Service](#).

- **Allow all devices to manage the router remotely**

1. Tick the [Enable](#) checkbox in [HTTP Service](#).
2. If you want to access the router via both HTTPS and HTTP, please tick the [Enable](#) checkbox in [HTTPS Service](#) column. Otherwise, keep it disabled.
3. For higher security, you can change the remote management web port by entering a number between 1024 and 65534.
4. Click [Save](#).

- **Allow a specific device to manage the router remotely**

1. Tick the [Enable](#) checkbox in [HTTP Service](#).
2. If you want to access the router via both HTTPS and HTTP, please tick the [Enable](#) checkbox in [HTTPS Service](#) column. Otherwise, keep it disabled.
3. For higher security, you can change the remote management web port by entering a number between 1024 and 65534.
4. Enter the IP or MAC address of the host that you want to manage the router in the [Available Host \(IP/MAC\)](#) entry. The format of the MAC address is XX:XX:XX:XX:XX:XX (X is any hexadecimal digit).
5. Click [Save](#).

- **Certificate**

Download and install the certificate for management via HTTPS if you need it. Once the certificate is installed, warnings will not pop up when you access the router via HTTPS.

Certificate Download
Certificate Download

Note:

- To access the router, enter your router's WAN IP address in your browser's address bar, followed by a colon and the custom port number. For example, if your router's WAN address is 202.96.12.8, and the port number used is 8080, please enter <http://202.96.12.8:8080> in your browser. Later, you may be asked for the router's password. After successfully entering the username and password, you will be able to access the router's web management page.
- Be sure to change the router's default password for security purposes.

8.6.9. System Log

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

The screenshot shows the 'System Log' interface. At the top, there are two dropdown menus: 'Log Type' set to 'ALL' and 'Log Level' set to 'Debug'. Below these is a table with the following data:

Index	Time	Type	Level	Content
1	1970-01-01 00:00:08	DHCPD	Notice	Send ACK to 192.168.0.100
2	1970-01-01 00:00:08	DHCPD	Notice	Recv REQUEST from 40:8D:5C:89:74:B5

At the bottom of the interface, there are four buttons: 'Refresh', 'Clear Log', 'Save Log', and 'Log Settings'.

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

8.7. Log out

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

FAQ

Q1. What should I do if I cannot access the internet?

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

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

With the router powered on, press and hold the [Reset](#) button until the LED blinks and then release the button.

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

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

- If you have not changed the default wireless password, it can be found on the Wi-Fi Info Card or on the label of the router.
- Otherwise, connect a computer to the router via an Ethernet cable. Log in to the Web Management page, and go to [Wireless](#) > [Wireless Security](#) to retrieve or reset your wireless password.

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

The default username and password of the web management page are [admin](#) (in lowercase). If you have altered the password:

1. Reset the router to factory default settings: With the router powered on, press and hold the [Reset](#) button until the LED blinks and then release the button.
2. Visit <http://tplinkwifi.net>, enter [admin](#) (in lowercase) as both username and password to login.

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

Q5. What do I need to do if I want to use NetMeeting?

If you start NetMeeting as a sponsor, you don't need to do anything with the router. If you start as a response, please follow the steps below to configure the router:

1. Visit <http://tplinkwifi.net>, and log in with the username and password you set for the router.
2. Enable DMZ: Go to [Forwarding](#) > [DMZ](#). Select [Enable](#) and enter your IP address in the [DMZ Host IP Address](#) field, and then Click [Save](#).


3. Enable H323 ALG: Go to [Security > Basic Security](#), enable [H323 ALG](#) and click [Save](#).
Now you can enjoy your net meeting normally.

Q6. What should I do if my wireless signal is unstable or weak?

It may be caused by too much interference.

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

COPYRIGHT & TRADEMARKS

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

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-Link Technologies Co., Ltd. Copyright © 2019 TP-Link Technologies Co., Ltd. All rights reserved.

FCC Compliance Information Statement



Product Name: 300Mbps Wireless N Nano Router

Model Number: TL-WR802N

Responsible party:

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

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

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

Tel: +1 626 333 0234

Fax: +1 909 527 6803

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

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

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

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

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

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

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

FCC RF Radiation Exposure Statement

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

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

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

Issue Date: 2019.3.26

CE Mark Warning



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

OPERATING FREQUENCY

2400 MHz -2483.5 MHz(20dBm)

EU declaration of conformity

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

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

RF Exposure Information

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

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

Canadian Compliance Statement

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

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

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

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

Radiation Exposure Statement:

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

Déclaration d'exposition aux radiations:

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

Industry Canada Statement

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

Korea Warning Statements:

당해 무선설비는 운용중 전파혼신 가능성이 있음.

NCC Notice & BSMI Notice:

注意!

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性或功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機需忍受合法通信或工業、科學以及醫療用電波輻射性電機設備之干擾。

安全諮詢及注意事項

- 請使用原裝電源供應器或只能按照本產品注明的電源類型使用本產品。
- 清潔本產品之前請先拔掉電源線。請勿使用液體、噴霧清潔劑或濕布進行清潔。
- 注意防潮，請勿將水或其他液體潑灑到本產品上。
- 插槽與開口供通風使用，以確保本產品的操作可靠並防止過熱，請勿堵塞或覆蓋開口。
- 請勿將本產品置放於靠近熱源的地方。除非有正常的通風，否則不可放在密閉位置中。
- 請不要私自打開機殼，不要嘗試自行維修本產品，請由授權的專業人士進行此項工作。

限用物質含有情況標示聲明書

產品元件名稱	限用物質及其化學符號					
	鉛 Pb	鎘 Cd	汞 Hg	六價鉻 CrVI	多溴聯苯 PBB	多溴二苯醚 PBDE
PCB	○	○	○	○	○	○
外殼	○	○	○	○	○	○
備考1. 超出0.1 wt %” 及 “超出0.01 wt %” 系指限用物質之百分比含量超出百分比含量基準值。						
備考2. “○” 系指該項限用物質之百分比含量未超出百分比含量基準值。						
備考3. “— “ 系指該項限用物質為排除項目。						



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



Safety Information

- Keep the device away from water, fire, humidity or hot environments.
- Do not attempt to disassemble, repair, or modify the device.
- Do not use damaged charger or USB cable to charge the device.
- Do not use the device where wireless devices are not allowed.

Explanations of the symbols on the product label

Symbol	Explanation
	DC voltage
	Indoor use only
	<p>RECYCLING</p> <p>This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/ EU in order to be recycled or dismantled to minimize its impact on the environment.</p> <p>User has the choice to give his product to a competent recycling organization or to the retailer when he buys a new electrical or electronic equipment.</p>