User Guide

300Mbps Wireless N Nano Router
TL-WR802N

REV4.1.0 1910012556

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
Underlined	Underlined words or phrases are hyperlinks. You can click to redirect to a website or a specific section.
Teal	Contents to be emphasized and texts on the web page are in teal, including the menus, items, buttons and so on.
>	The menu structures to show the path to load the corresponding page. For example, Advanced > Wireless > MAC Filtering means the MAC Filtering function page is under the Wireless menu that is located in the Advanced tab.
Note:	Ignoring this type of note might result in a malfunction or damage to the device.
Tips:	Indicates important information that helps you make better use of your device.

*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.

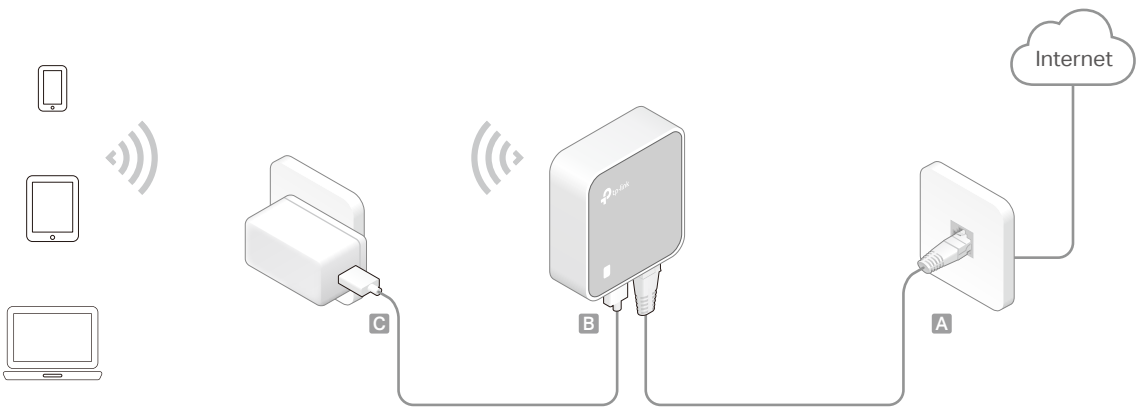
2. 2. 1. Wireless Router Mode

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:

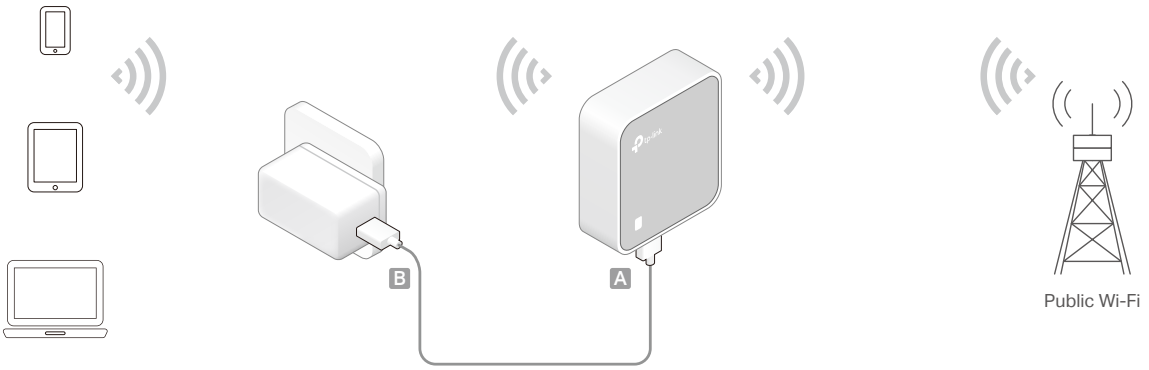
- If the hotel's internet has an authentication process, you will need to authenticate only once and only on one device.
- Check the internet connection on your laptop or smartphone, and please note that:
  - If you can access the internet without any restriction, no configuration is required.
  - If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



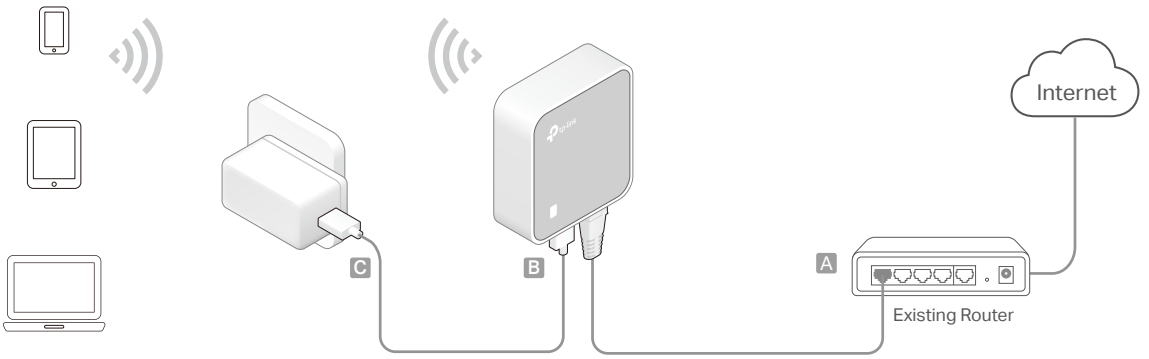
2. 2. 3. Access Point Mode

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.

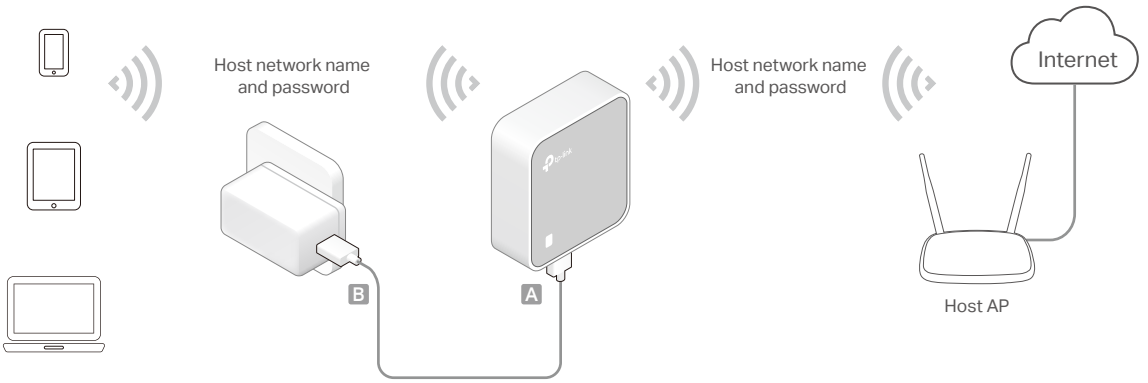


2. 2. 4. Range Extender Mode

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.

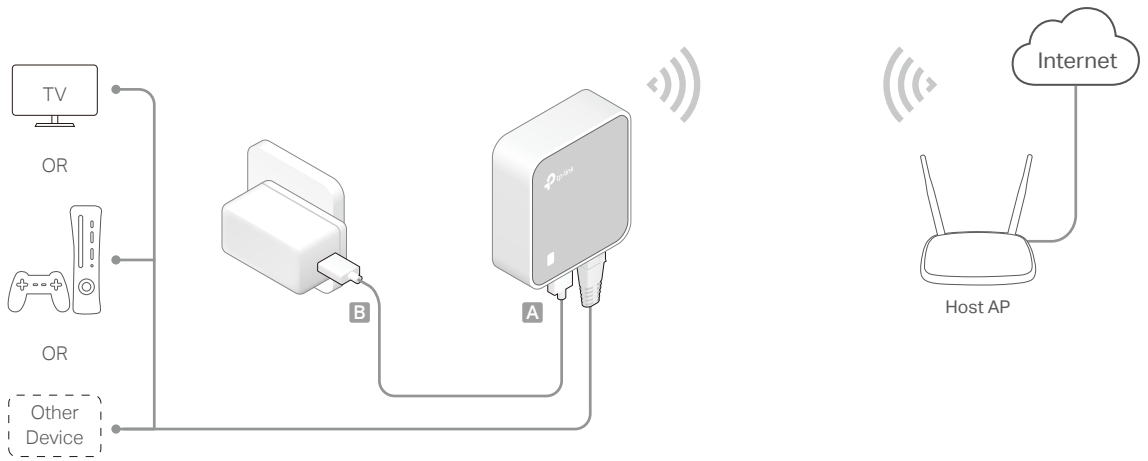
1. Connect the router according to Step A to B.
2. Use the default Wi-Fi Name and Wi-Fi Password printed on the Wi-Fi Info Card or on the product label at the bottom of your router to connect to the Wi-Fi.



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:

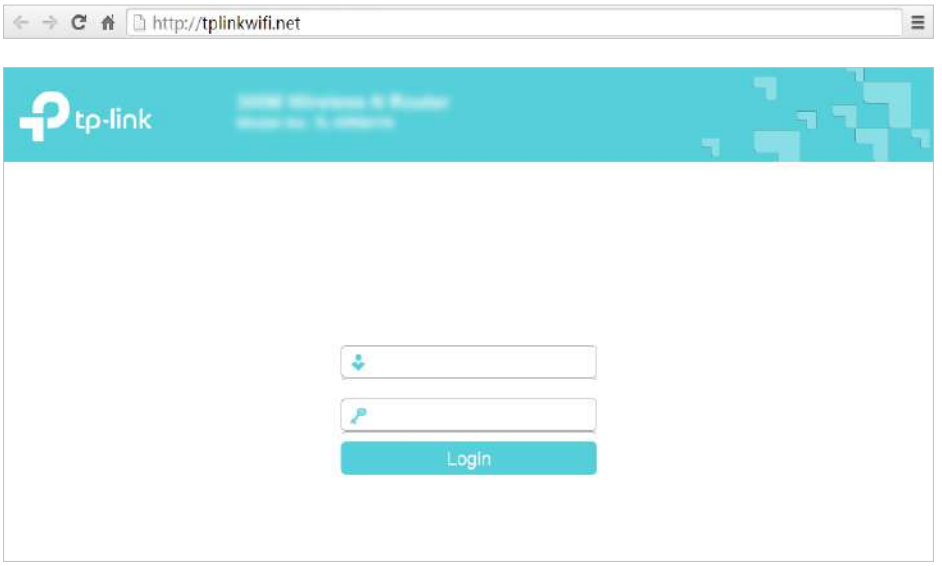
- Log In to the Router
- Set Up Internet Connection

3. 1. Log In to the Router

With a Web-based utility, it is easy to configure and manage the rouer. 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.

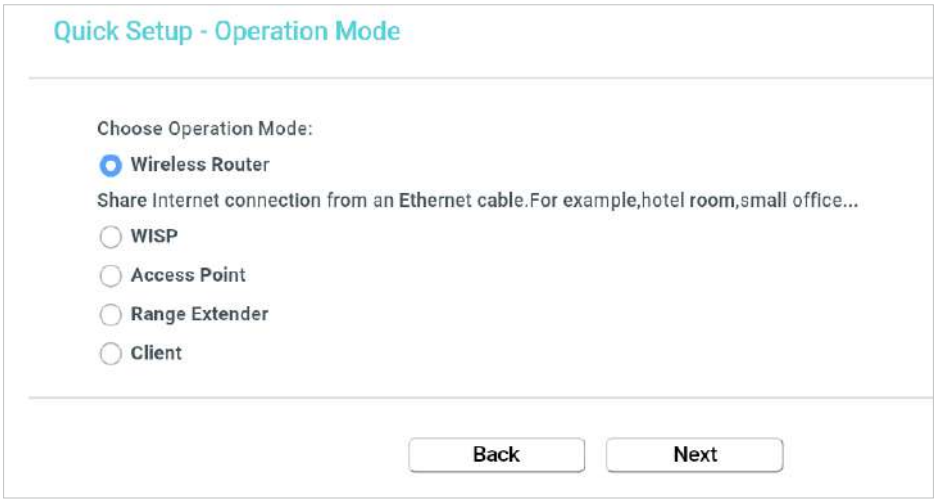


Note:
If the login window does not appear, please refer to FAQ Section.

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.



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

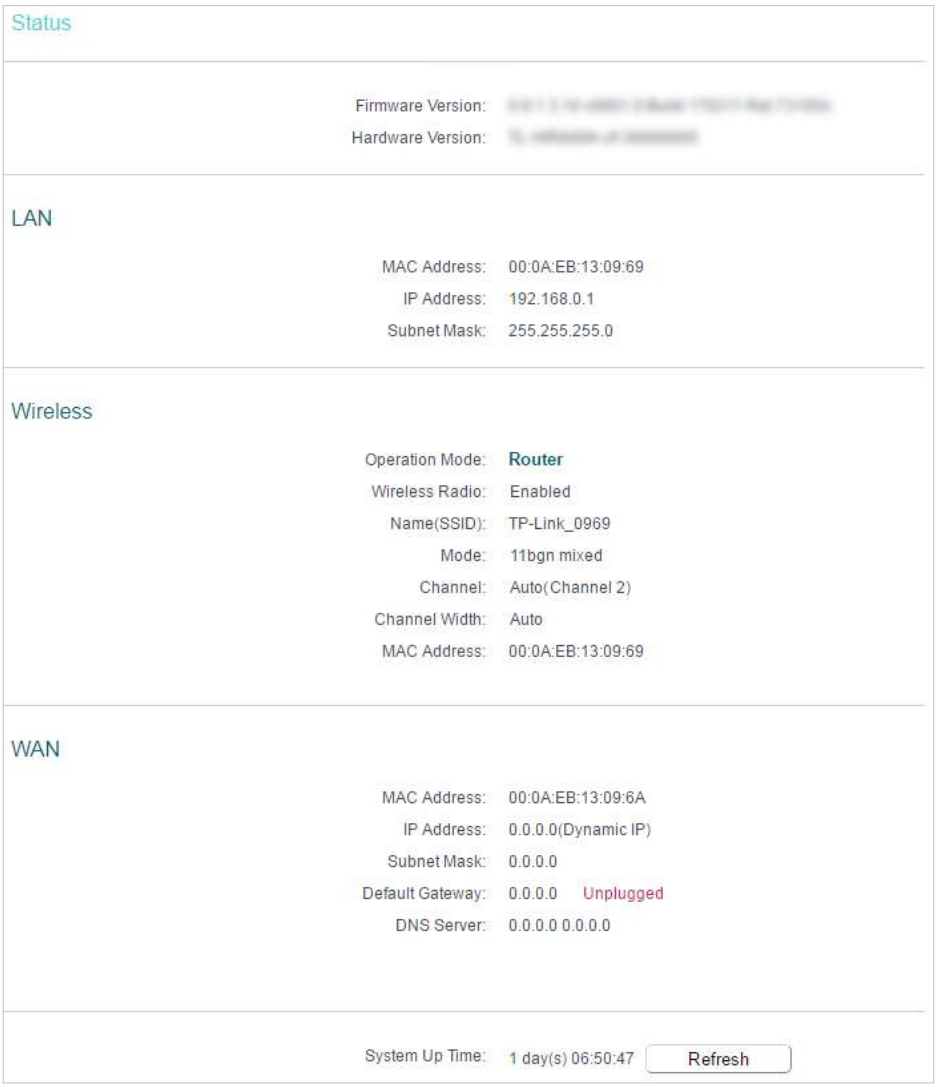
This chapter presents how to configure the various features of the router working as a standard wireless router.

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.



- 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.

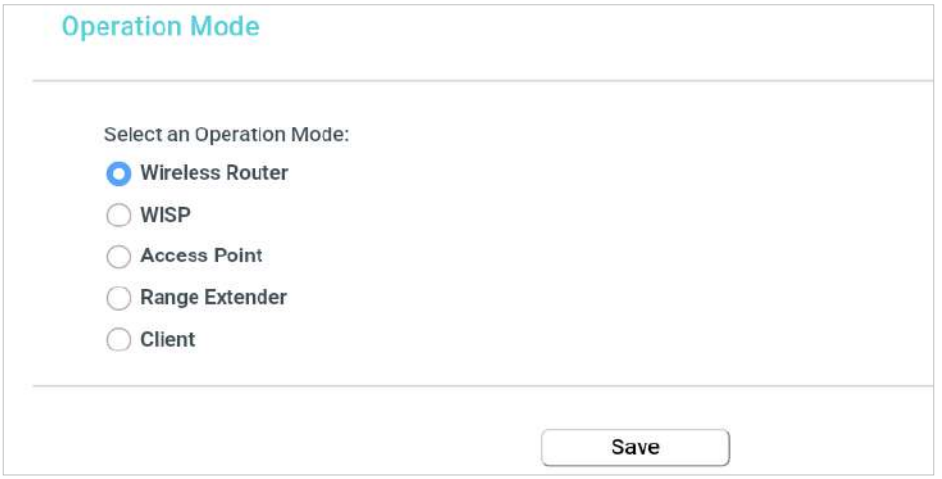
- Operation Mode - The current wireless working mode in use.
- Wireless Radio - Indicates whether the wireless radio feature of the router is enabled or disabled.
- Name(SSID) - The SSID of the router.
- Mode - The current wireless mode which the router works on.
- Channel - The current wireless channel 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.



4. 3. Network

4. 3. 1. WAN

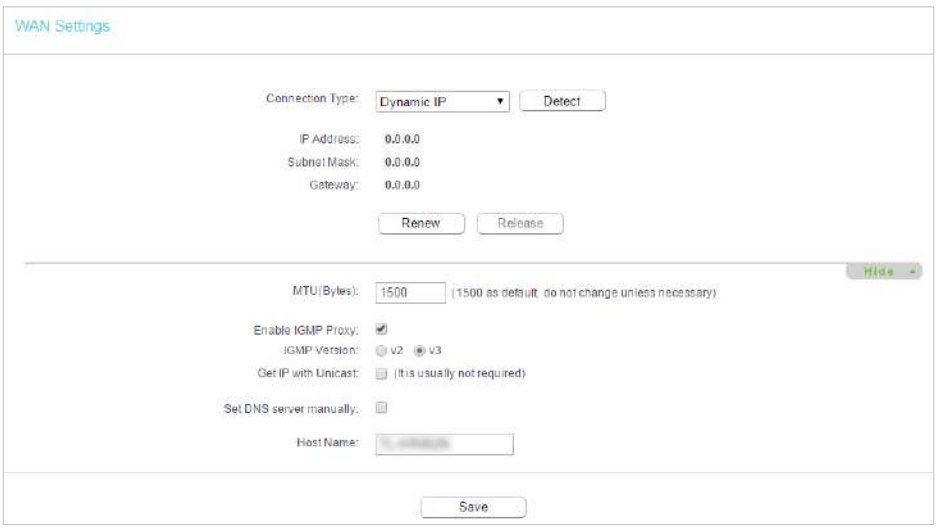
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Network > WAN.
3. Configure the IP parameters of the WAN and click Save.

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.

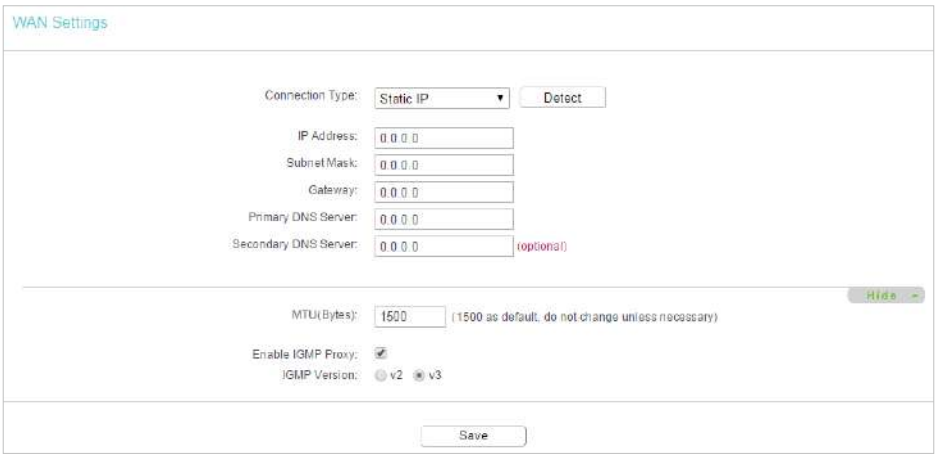
Click Release to release the IP parameters.



- 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.

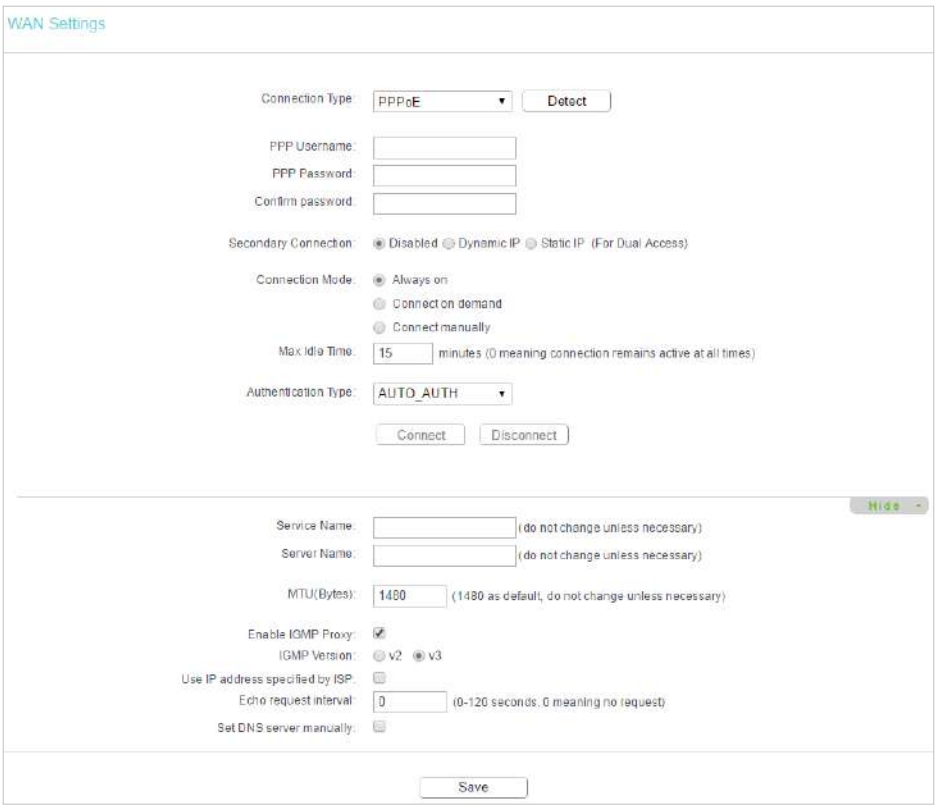


- IP Address - Enter the IP address in dotted-decimal notation provided by your ISP.
- Subnet Mask - Enter the subnet mask in dotted-decimal notation provided by your ISP. Normally 255.255.255.0 is used as the subnet mask.
- Gateway - Enter the gateway IP address in dotted-decimal notation provided by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



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

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

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

- Authentication Type - Choose an authentication type.

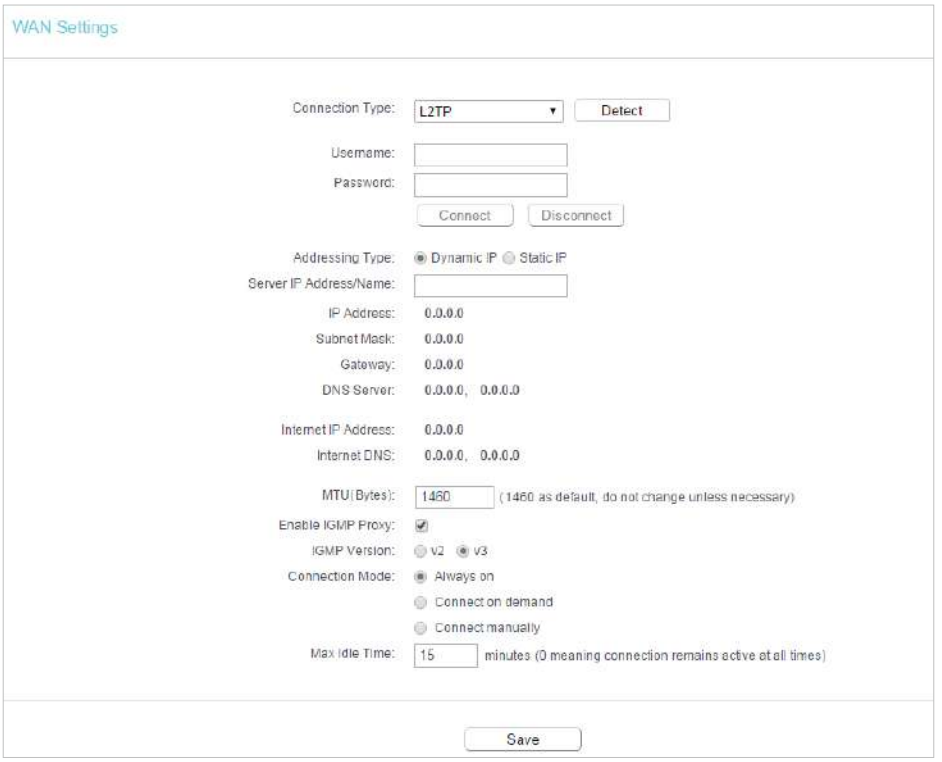
Note:

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

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

L2TP

If your ISP provides L2TP connection, please select L2TP.



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

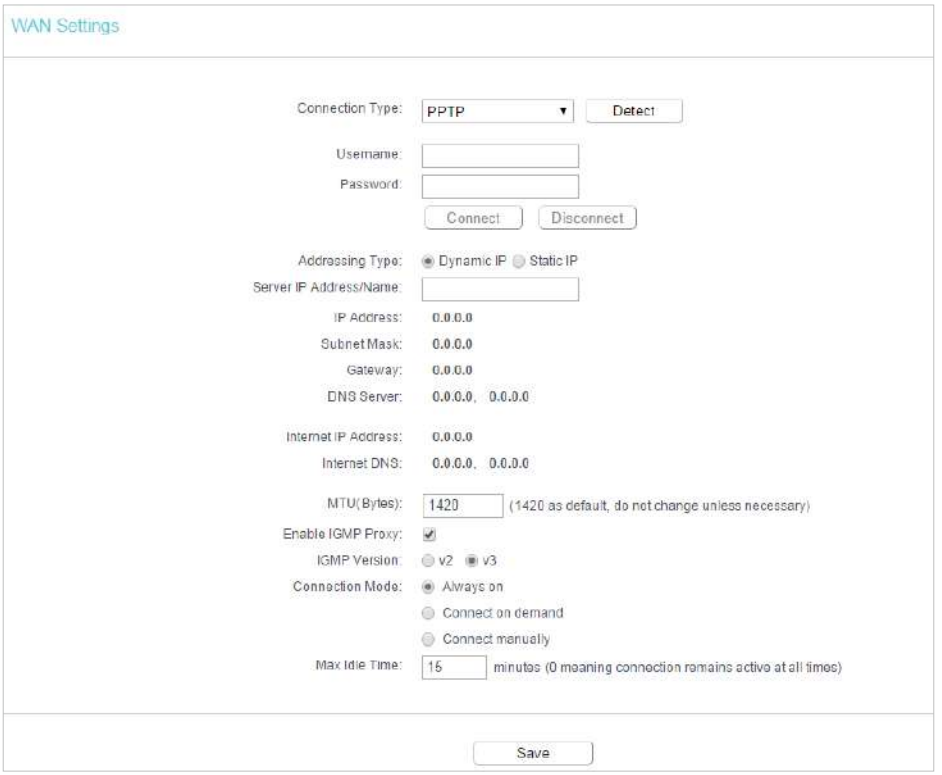
on Demand mode. The internet connection can be disconnected automatically after a specified inactivity period (Max Idle Time) and not be able to re-establish when you attempt to access the internet again.

Note:

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

PPTP

If your ISP provides PPTP connection, please select PPTP.



- 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

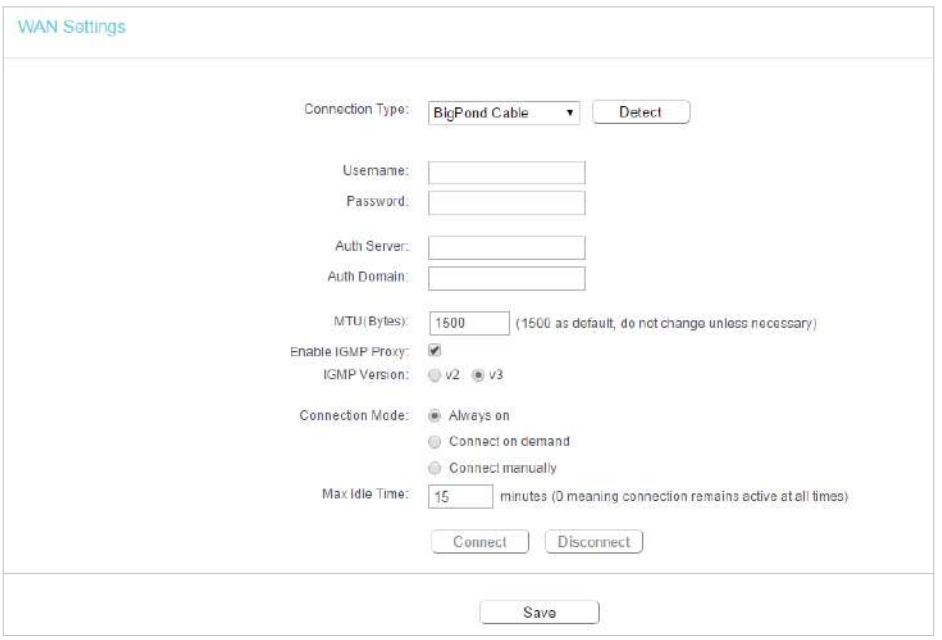
- Always On - In this mode, the internet connection will be active all the time.
- Connect on Demand - In this mode, the internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the internet again. If you 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.



- 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.

- 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.

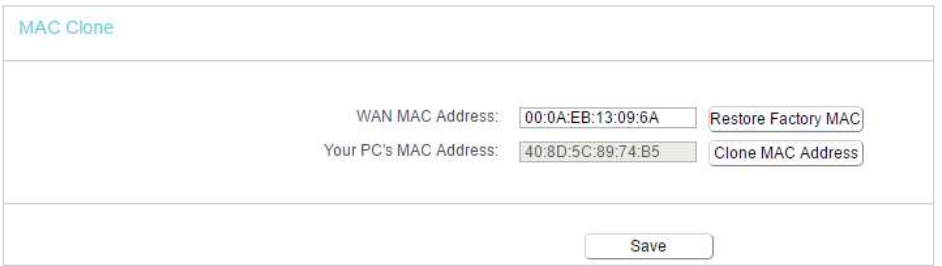
IGMP snooping is especially useful for bandwidth-intensive IP multicast applications such as IPTV.

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.



- 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.

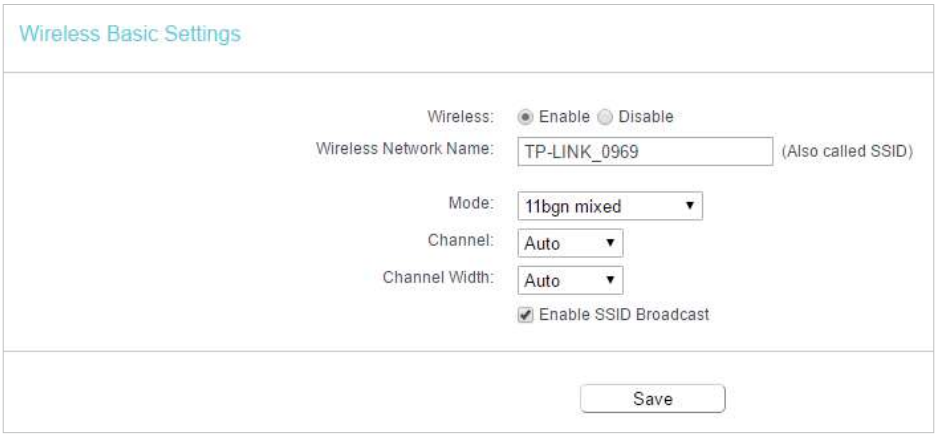
Note:

- 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 - 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.

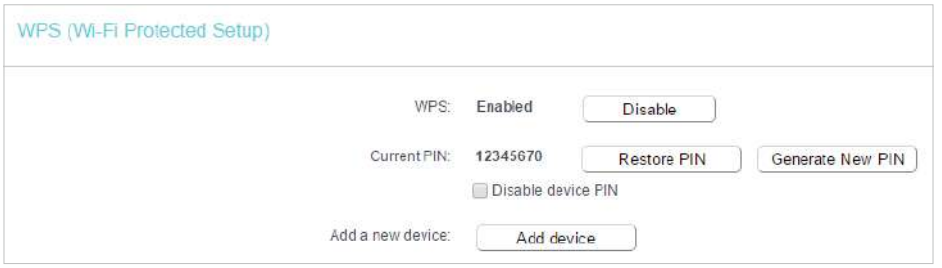
Note:

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.

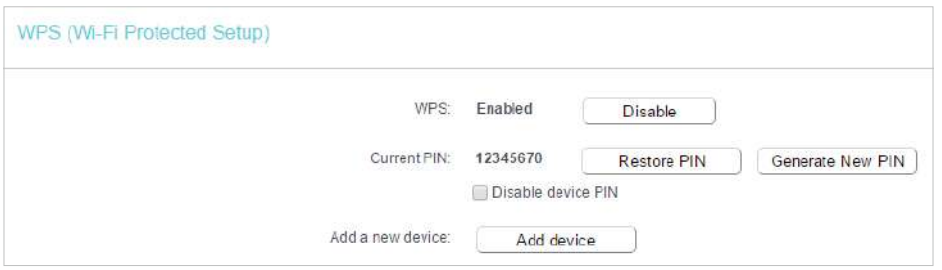


2. Select Press the WPS button of the new device within the next two minutes and click Connect.

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.

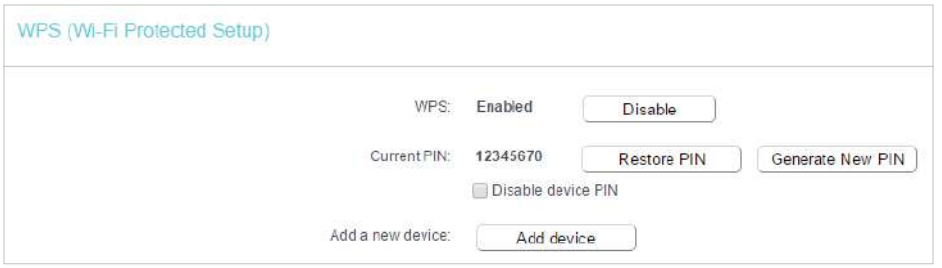


2. Select Enter new device PIN, enter your client device's current PIN in the PIN filed and click Connect.

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

Method Three: Enter the Router's PIN

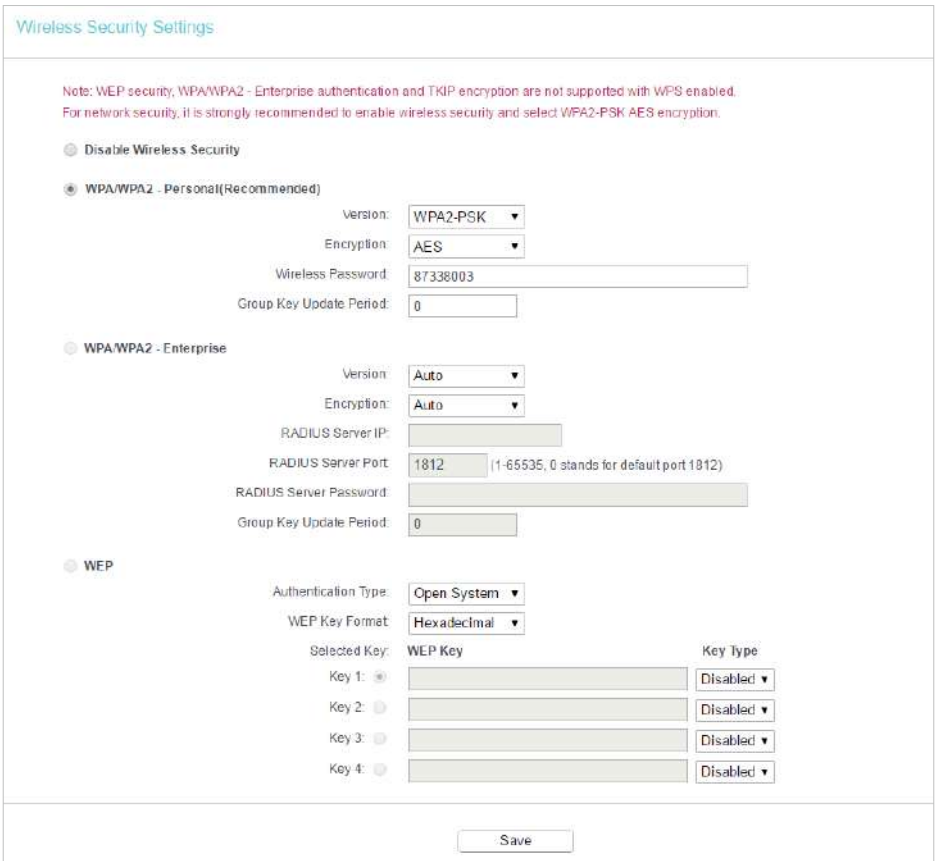
1. Keep the WPS Status as Enabled and get the Current PIN of the router.



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.



- 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.

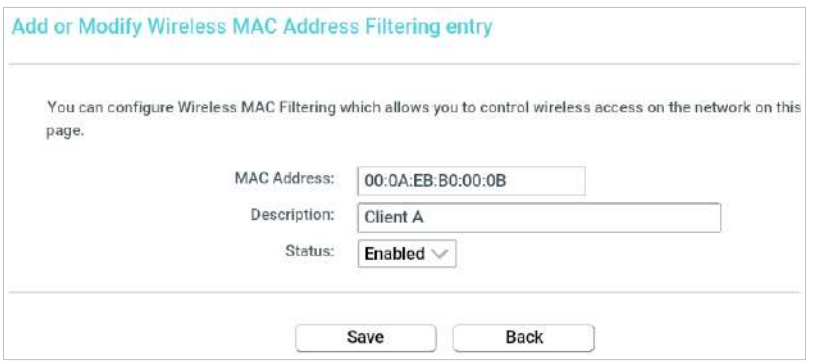
I want to:

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.



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.

Done!

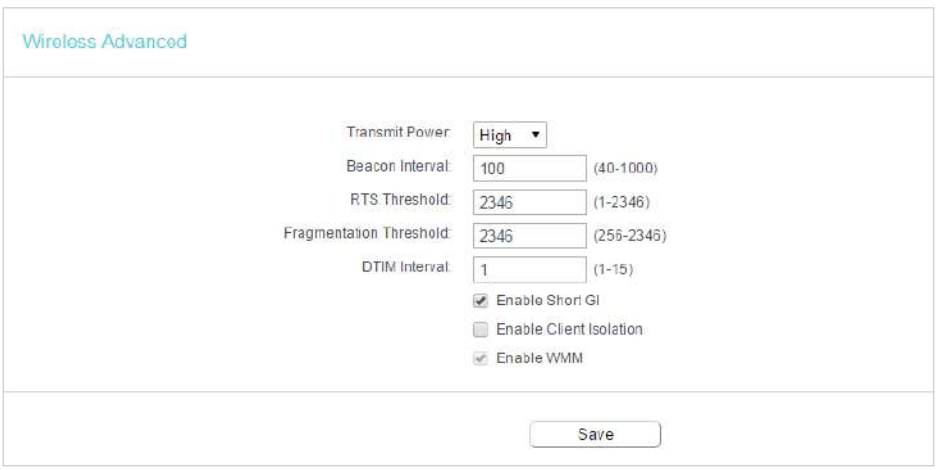
Now only client A and client B can access your network.

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.



- 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

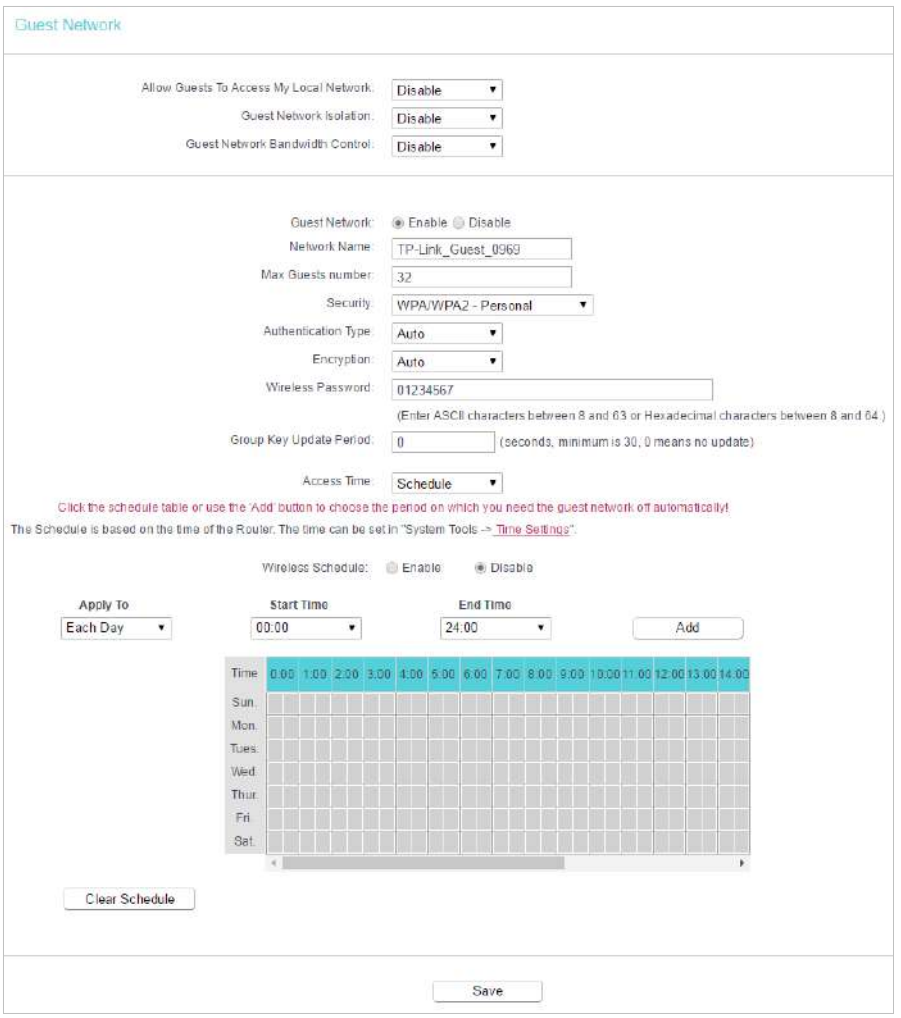
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Wireless > Wireless Statistics to check the data packets sent and received by each client device connected to the router.

- 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.



- 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:

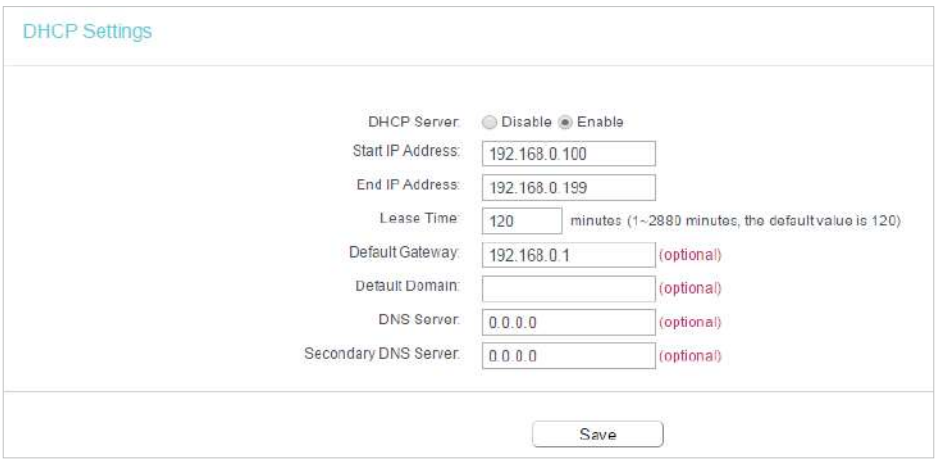
The range of bandwidth for guest network is calculated according to the setting of Bandwidth Control on the Bandwidth Control page.

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 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.

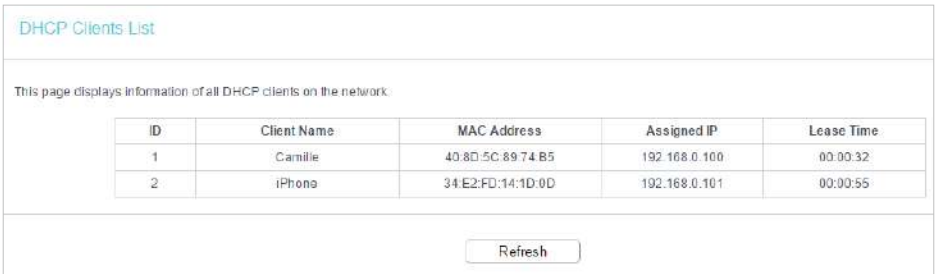
- Address Lease Time - The Address Lease Time is the amount of time a network user will be allowed to connect to the router with the current dynamic IP Address. When time is up, the user will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 2880 minutes. The default value 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.



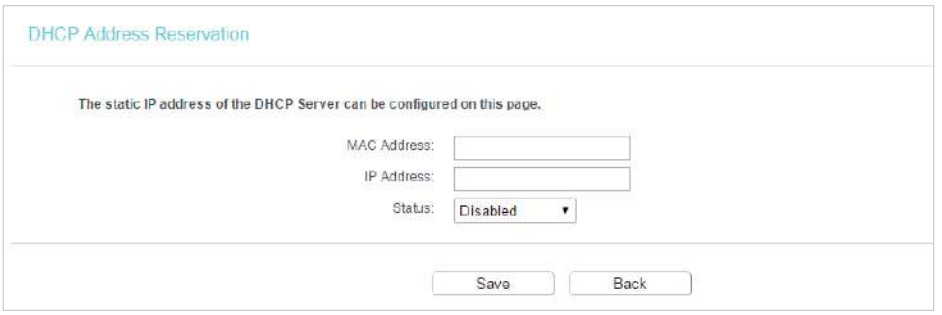
- Client Name - The name of the DHCP client.
- MAC Address - The MAC address of the DHCP client.
- Assigned IP - The IP address that the outer has allocated to the DHCP client.
- Lease Time - The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic IP address will be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



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

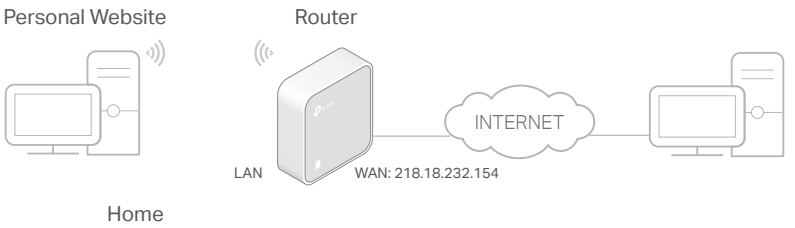
When you build up a server in the local network and want to share it on the internet, Virtual Servers can realize the service and provide it to internet users. At the same time virtual servers can keep the local network safe as other services are still invisible from the internet.

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.

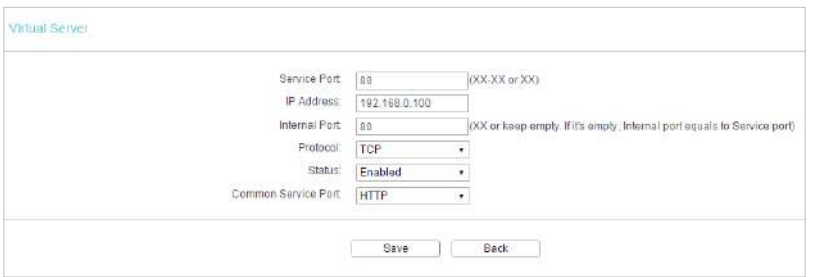
I want to:

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.



5. Leave the status as Enabled and click Save.

Note:

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

Done!

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

Note:

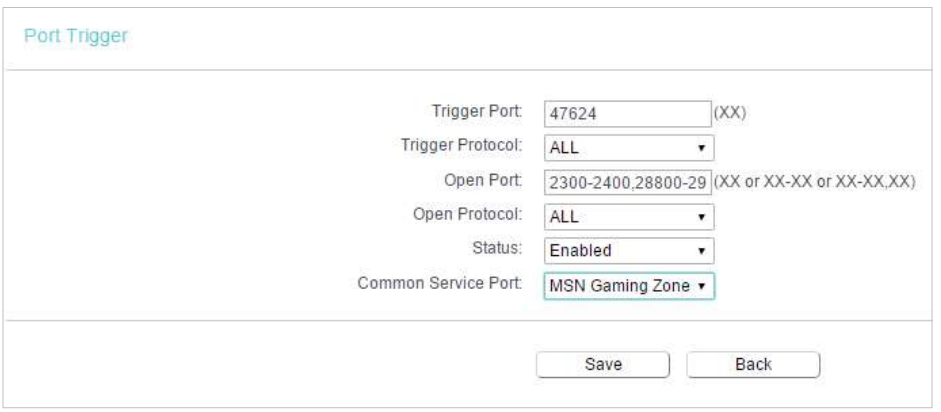
- If you have changed the default Service Port, you should use http:// WAN IP: Service Port to visit the website.
- Some specific service ports are forbidden by the ISP, if you fail to visit the website, please use another service port.

4. 7. 2. Port Triggering

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

Follow the steps below to configure the port triggering rules:

1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Forwarding > Port Triggering.
3. Click Add New. Select the desired application from the Common Service Port list. The Trigger Port amd Open Port will be automatically filled in. The following picture takes application MSN Gaming Zone as an example.



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.

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

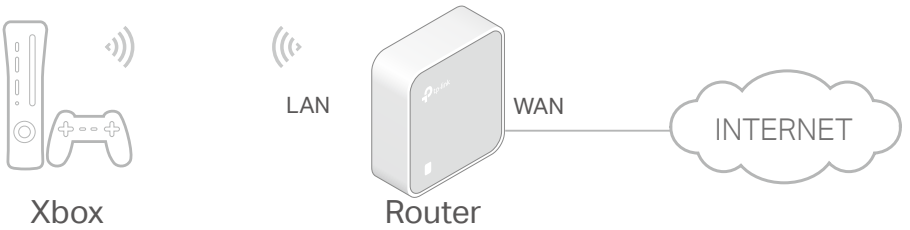
The UPnP (Universal Plug and Play) protocol allows the applications or host devices to automatically find the front-end NAT device and send request to it to open the

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.

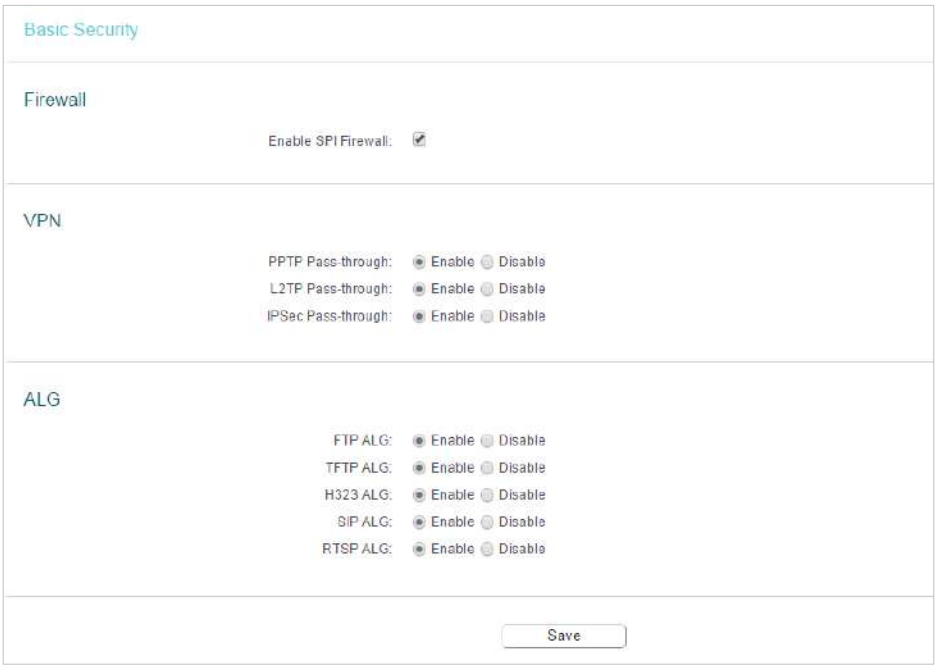
4. 8. Security

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.



- 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

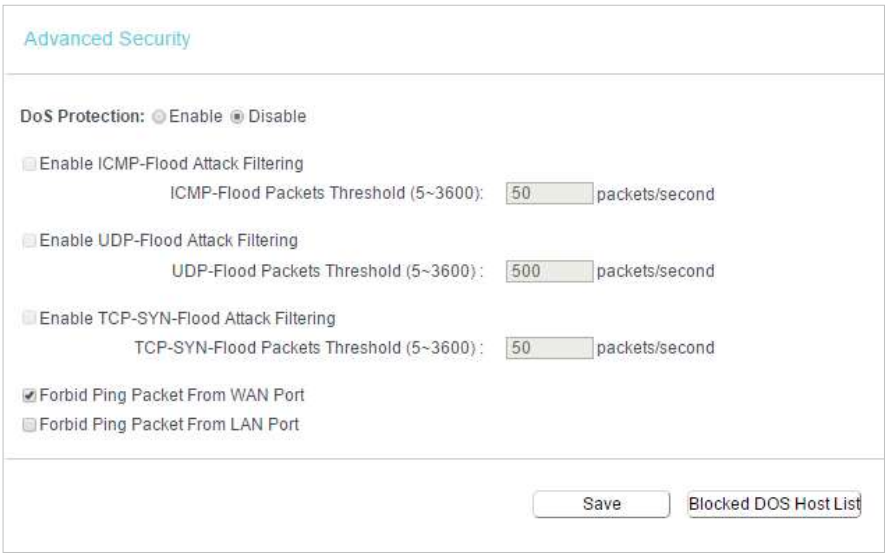
into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc.

- 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.



- 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.

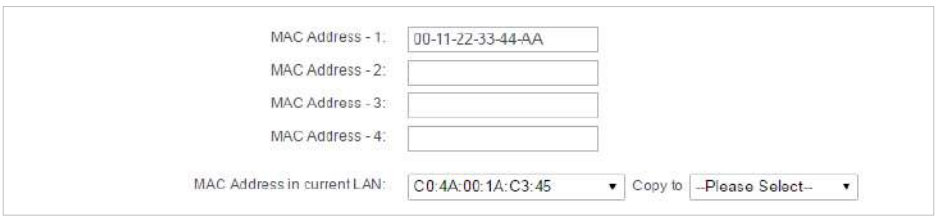
4. 9. Parental Controls

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

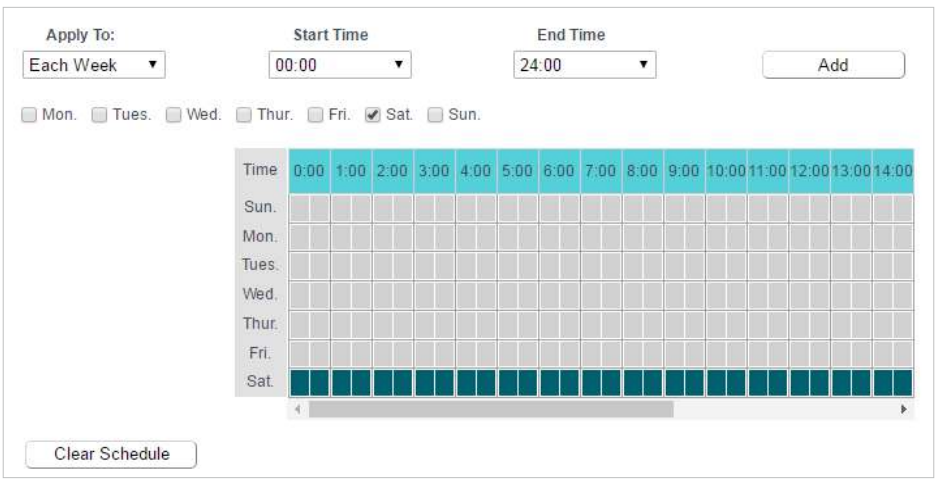
For example, you want the children's PC with the MAC address 00:11:22:33:44:AA can access www.tp-link.com on Saturday only while the parent PC with the MAC address 00:11:22:33:44:BB is without any restriction.

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.

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



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.



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

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:

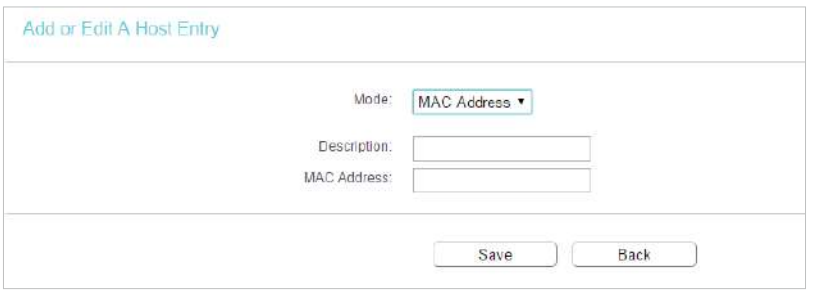
Deny or allow specific client devices to access my network with access tiem and

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:

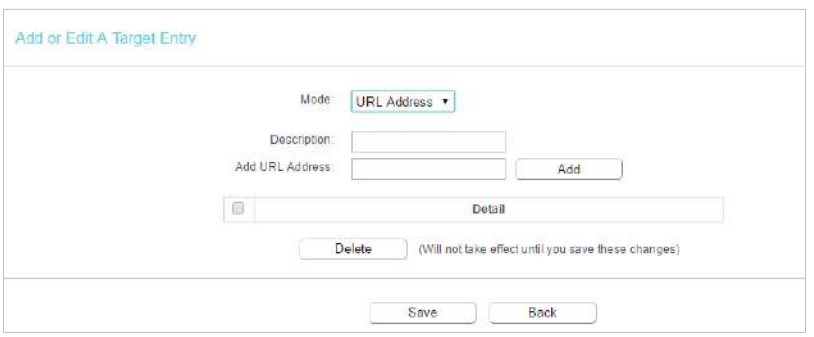
How can I do that?

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 filed.



   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.

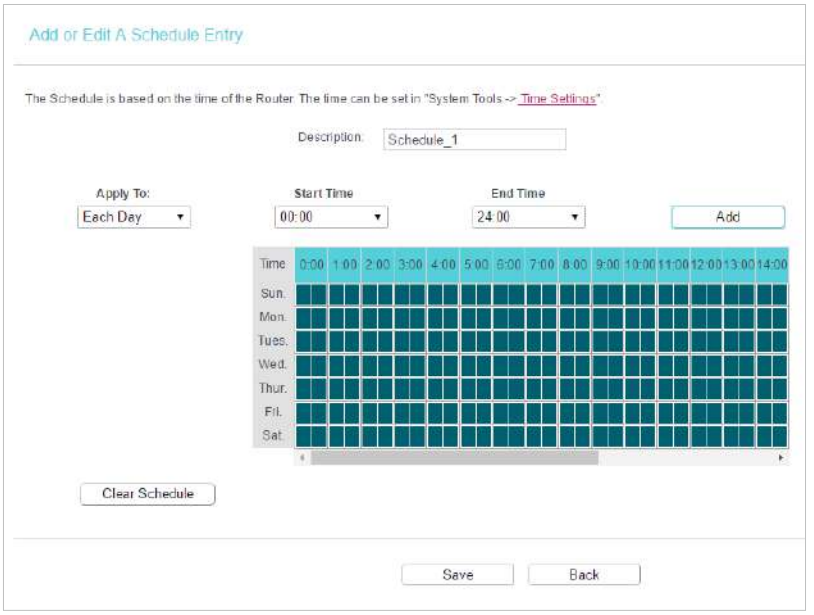
   Note:
   Any URL address with keywords in it (e.g. www.tp-link.com) will be blocked or allowed.



   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.

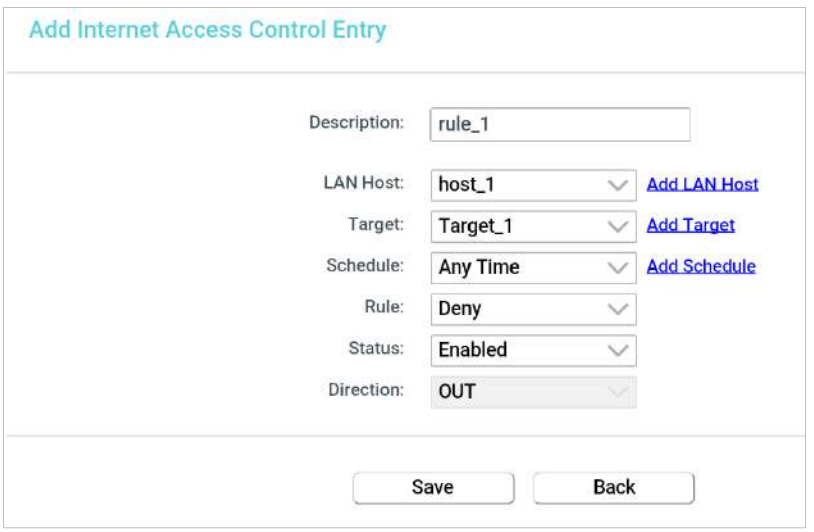


3) Click Save.

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.

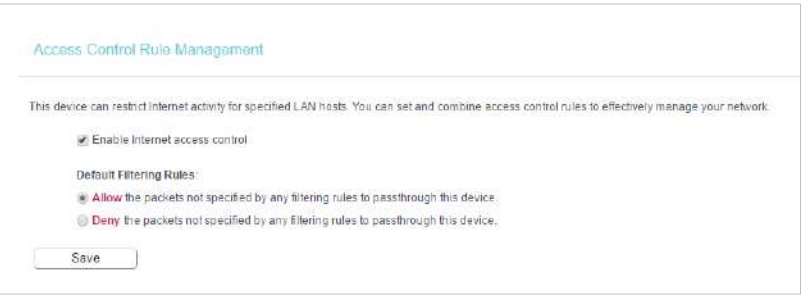


3) Leave the status as Enabled as click Save.

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

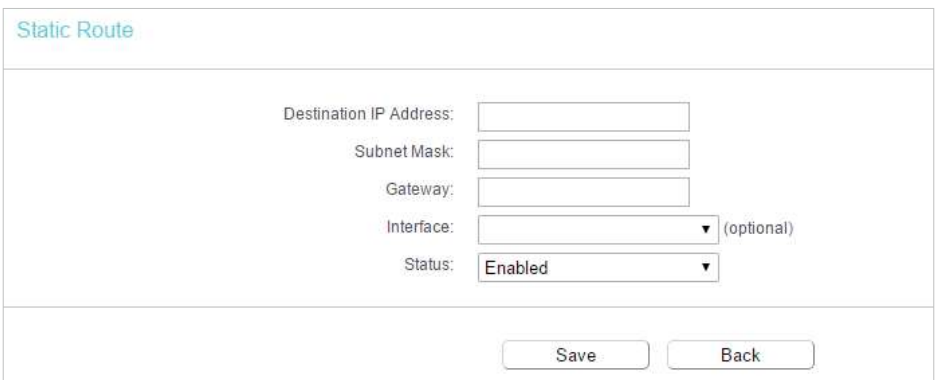
Static Routing is a form of routing that is configured manually by a network administrator or a user by adding entries into a routing table. The manually-configured routing information guides the router in forwarding data packets to the specific destination.

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.

- 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).

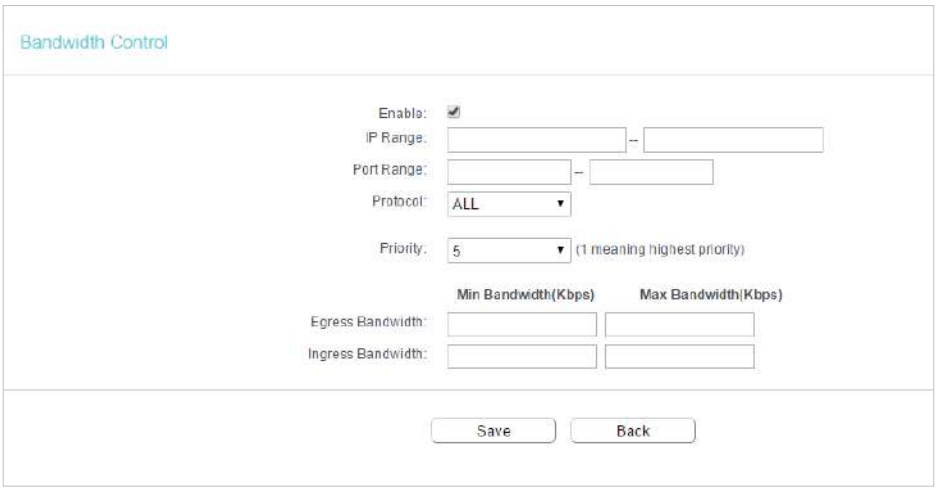
Click Refresh to refresh the data displayed.

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.

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



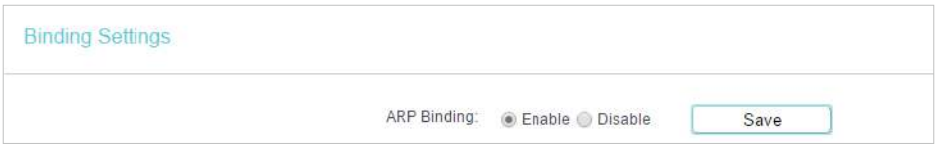
- IP Range - Interior PC address range. If both are blank or 0.0.0.0, the domain is noneffective.
- Port Range - The port range which the Interior PC access the outside PC. If all are blank or 0, the domain is noneffective.
- Protocol - Transport layer protocol, here there are ALL, TCP, UDP.
- Priority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

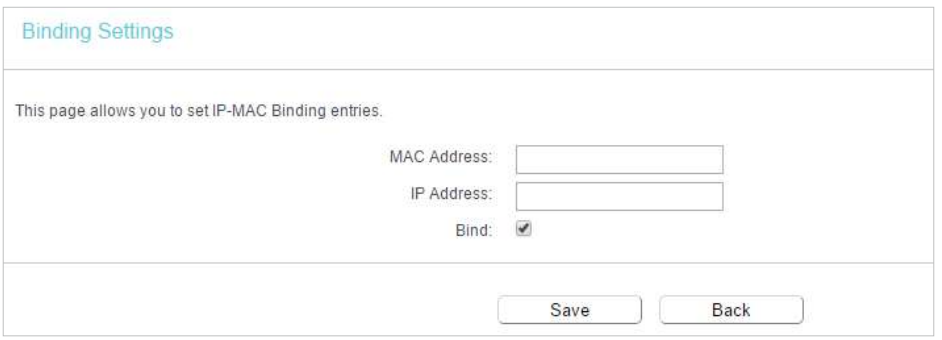
4. 13. 1. Binding Settings

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.



- **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.



- **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.

- 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.

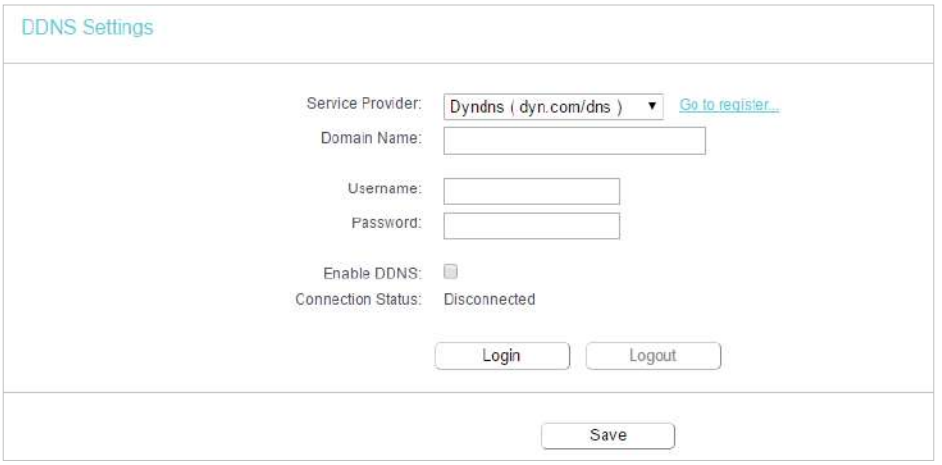
4. 14. Dynamic DNS

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.



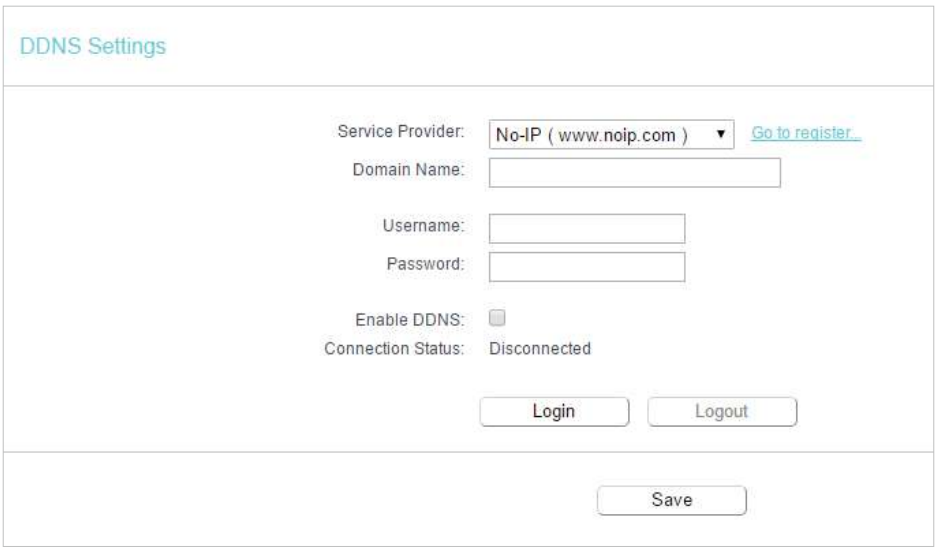
To set up for DDNS, follow these instructions:

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.



To set up for DDNS, follow these instructions:

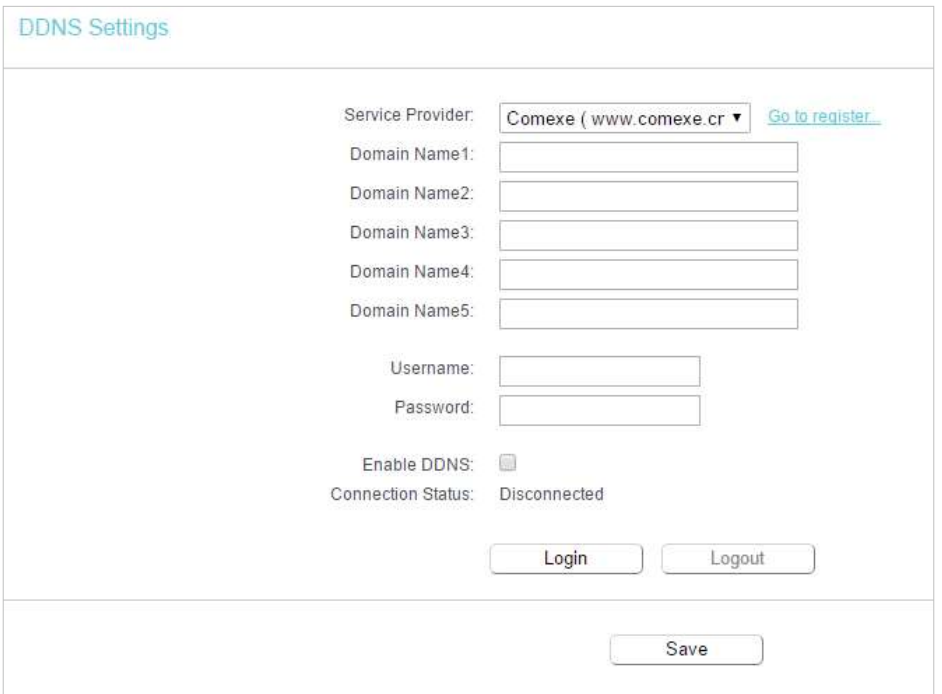
1. Enter the Domain Name you received from dynamic DNS service provider.

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.



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.

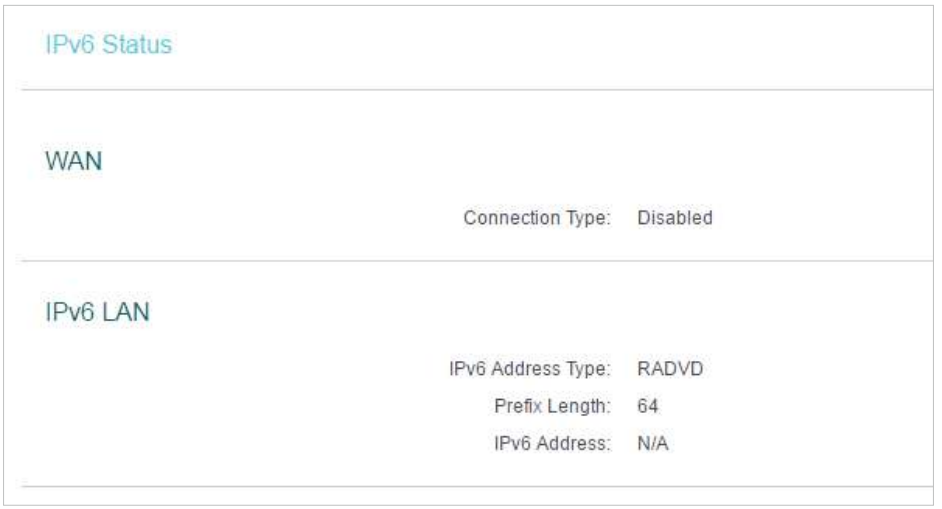
- Connection Status - The status of the DDNS service connection is displayed here.
- Logout - Click Logout to log out of the DDNS service.

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

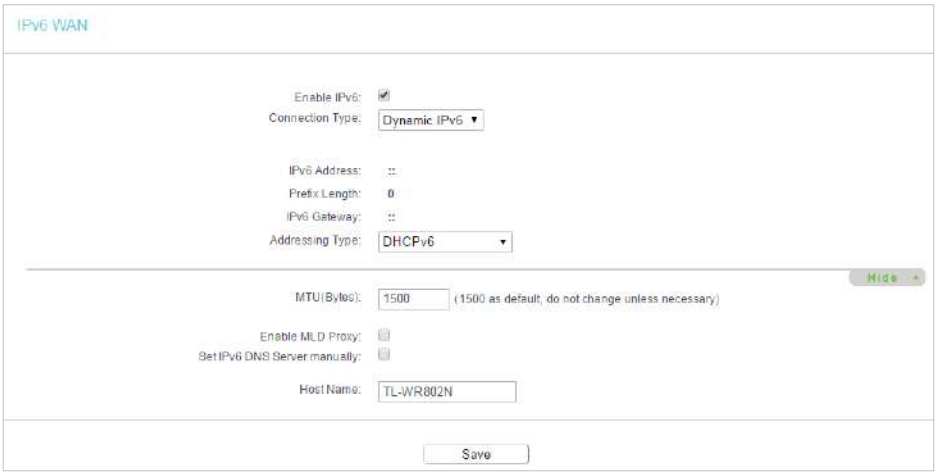
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to IPv6 > IPv6 Status, and you can view the current IPv6 status information of the router.



- WAN - This section shows the current IPv6 Connection Type.
- TPv6 LAN - This section shows the current IPv6 information of the router's LAN port, including IPv6 Address Type, Prefix Length and IPv6 Address.

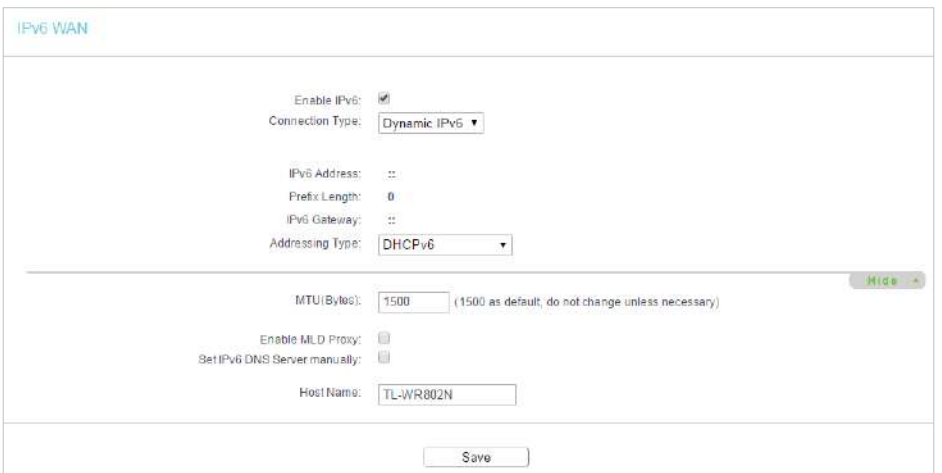
4. 15. 2. IPv6 WAN

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.



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 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 assignation for IPv6 address: SLAAC (Stateless address auto-configuration) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.
- MTU(Bytes) - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs, you may need to modify the

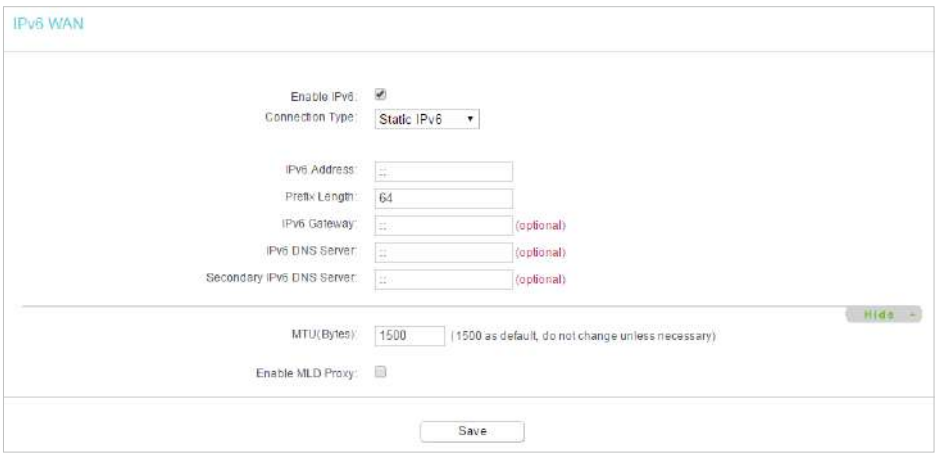
MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

- Enable MLD Proxy - Enable the Multicast Listener Discovery (MLD) Proxy function if you need.
- 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:

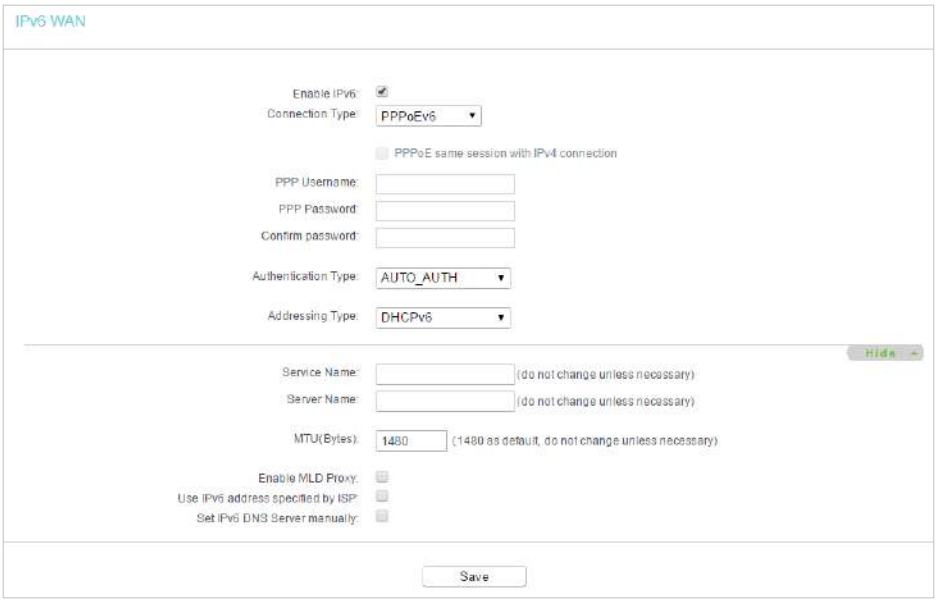
If you get Address not found error when you access a Web site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

Static IPv6



- IPv6 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



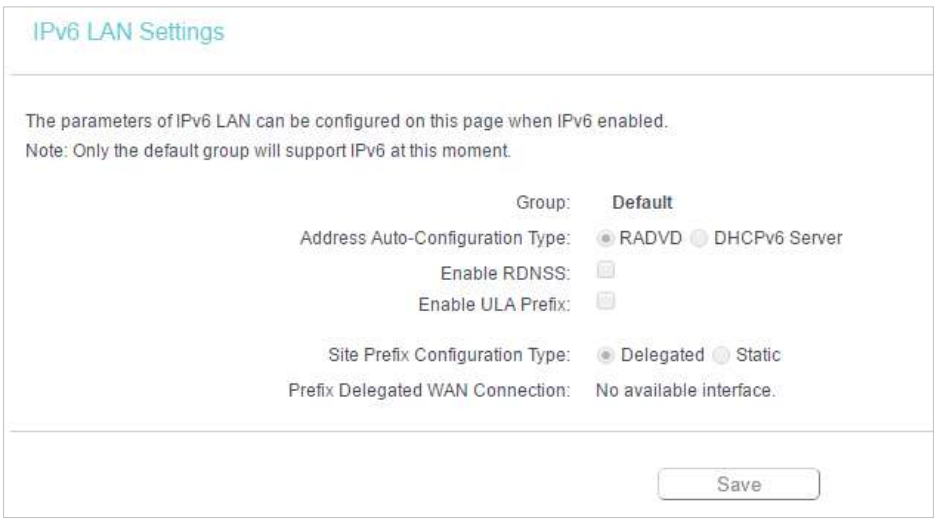
- PPP Username/Password - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- Authentication Type – Choose one authentication type from AUTO-AUTH, PAP, CHAP and MS-CHAP.
- Addressing Type - There are two types of assignation for IPv6 address: SLAAC (Stateless address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

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:

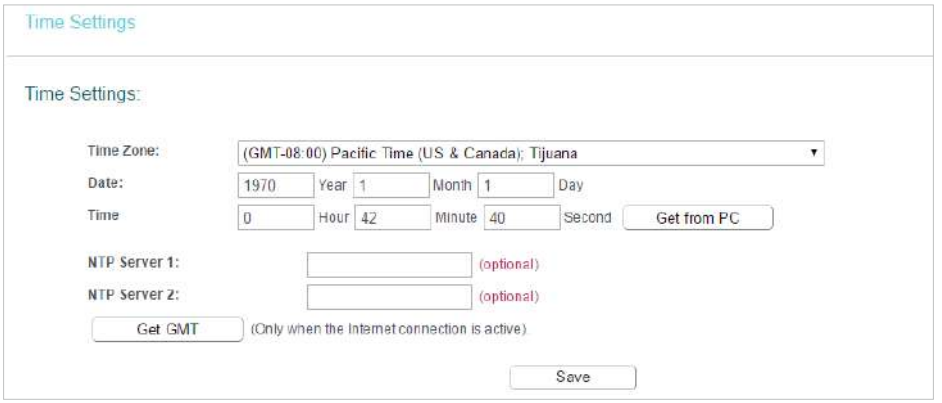
If your IPv6 wan connection type is "Tunnel 6to4", the Site Prefix Configuration Type should be "Static" to make sure "Tunnel 6to4" works properly.

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.



- **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.

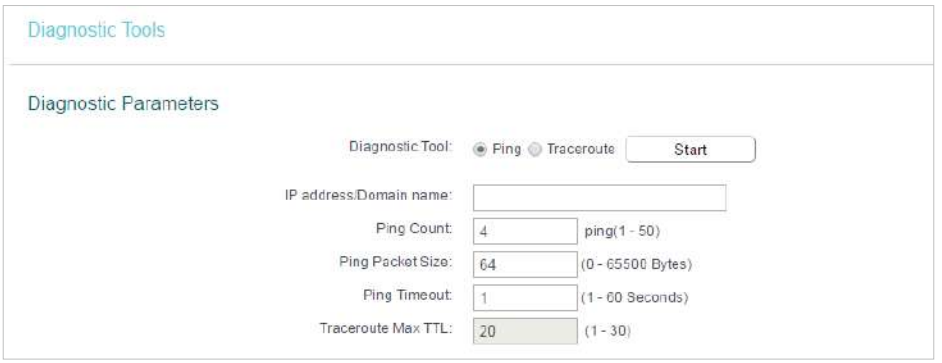
Note:

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.



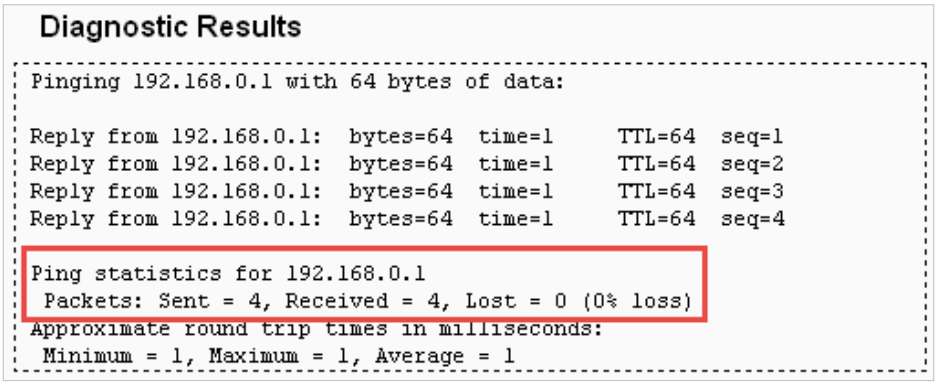
- Diagnostic Tool - Select one diagnostic tool.
  - Ping - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
  - Tracerouter - This diagnostic tool tests the performance of a connection.

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.

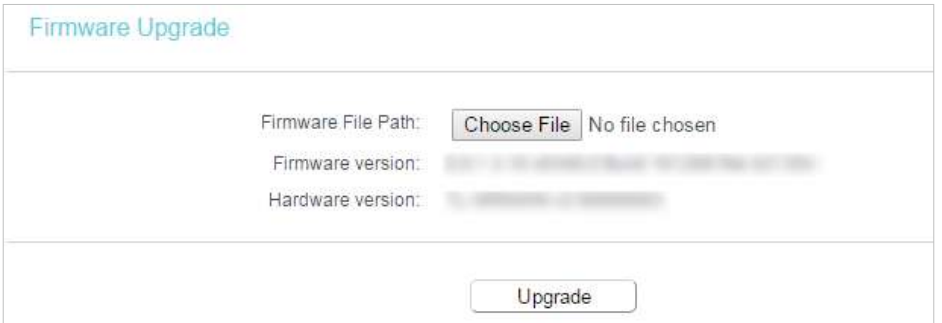
3. Click Start to check the connectivity of the internet.
4. The Diagnostic Results page displays the diagnosis result. If the result is similar to the following figure, the connectivity of the internet is fine.



4. 16. 3. Firmware Upgrade

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

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.



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.

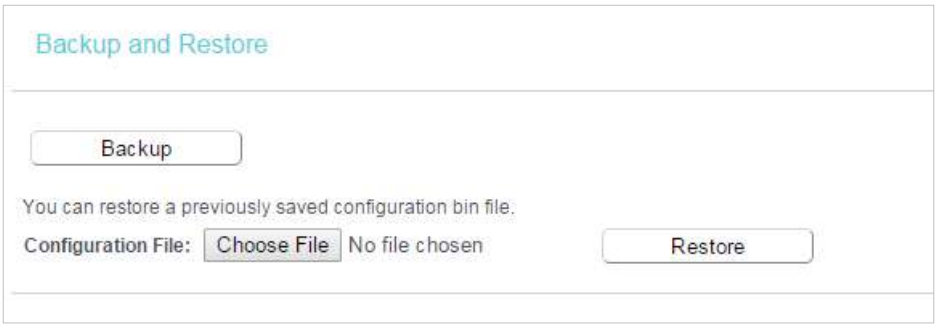
- Default Username: admin
- Default Password: admin

- 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.



- **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:

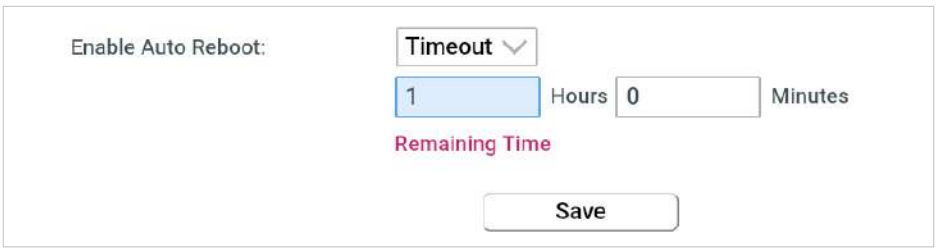
- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Working Modes.
- Change the Web Management Port.
- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router to its factory defaults (system will reboot automatically).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

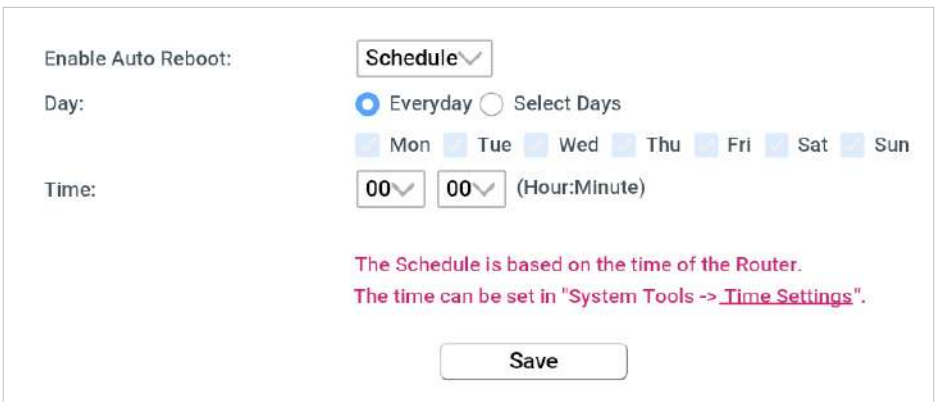
- **To reboot manually**

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.

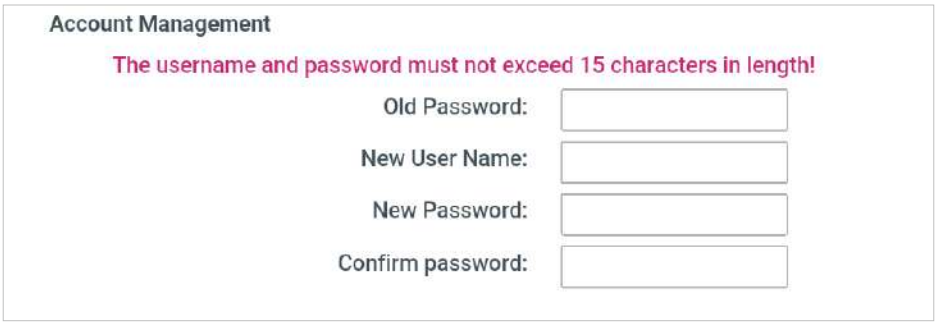


  - Select Schedule in the drop-down list of Enable Auto Reboot and specify the Time when the router reboots and Day which to decide how often it reboots.



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.



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.

- **Allow all LAN conencted 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 disbled.
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.

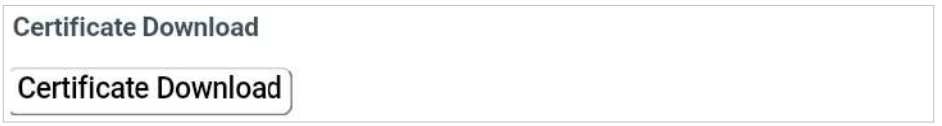
- **Allow a specific device to manage the router locally**

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 disbled.
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.

- **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**

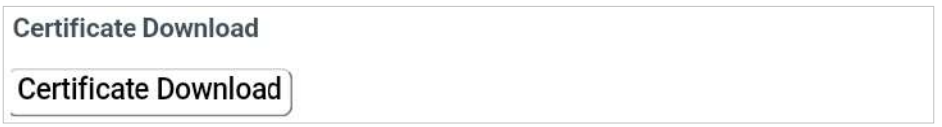
1. Tick the Enable checkbox in HTTP Service.
2. If you want to access the router via both HTTPS and HTTP, please tick the Enable checkbox in HTTPS Service column. Otherwise, keep it disbled.
3. For higher security, you can change the remote management web port by entering a number between 1024 and 65534.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

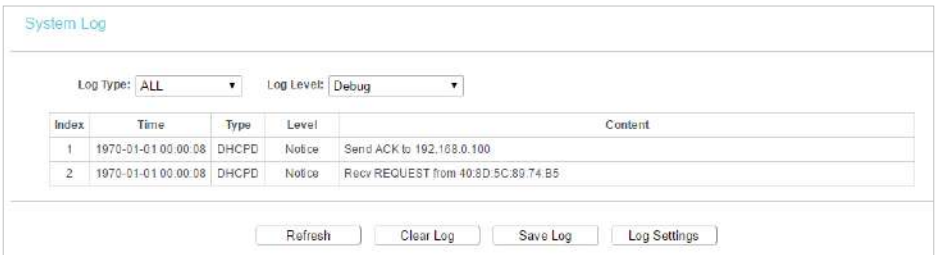


Note:

- 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

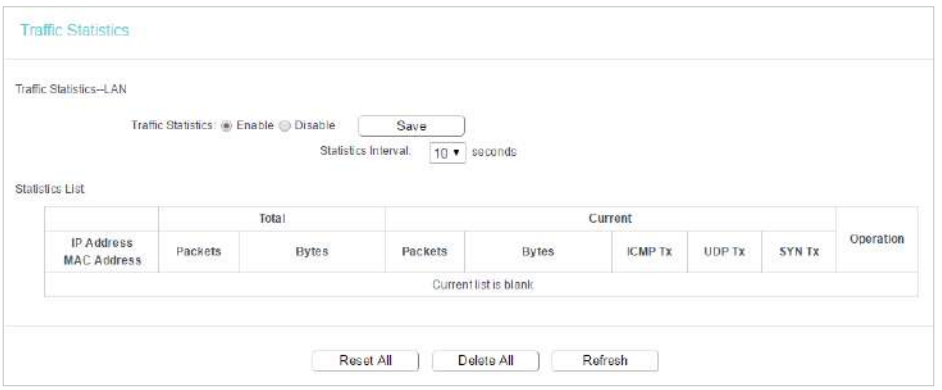
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to System Tools > System Log, and you can view the logs of the router.



- 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.

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.



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)

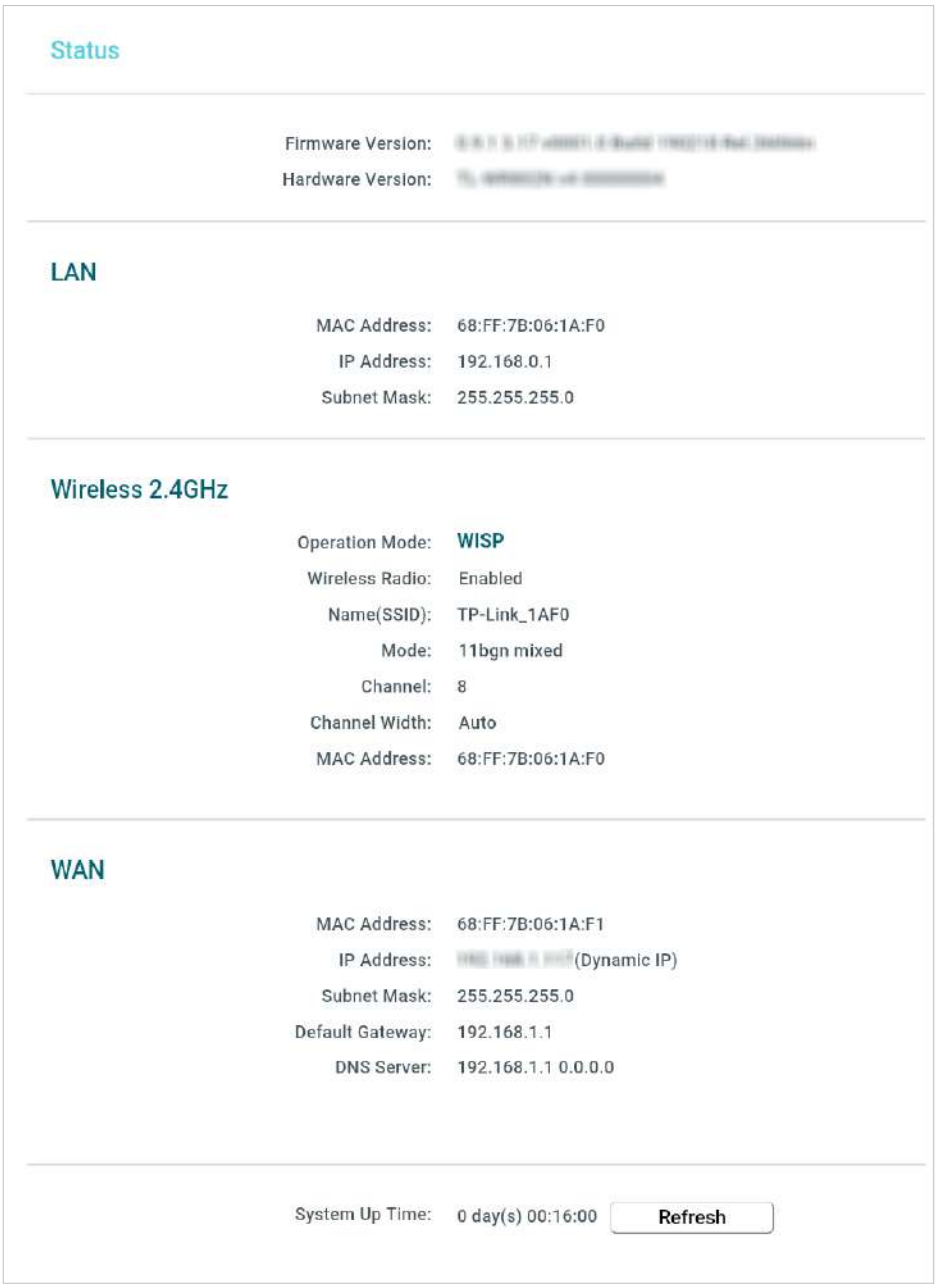
This chapter presents how to configure the various features of the router working as a WISP router (Hotspot router).

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.



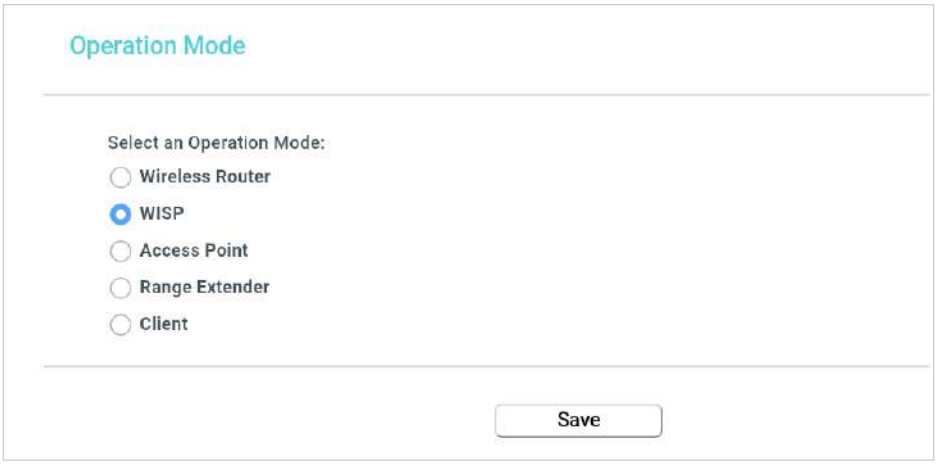
- Firmware Version - The version information of the router's firmware.
- Hardware Version - The version information of the router's hardware.
- LAN - This field displays the current settings of the LAN, and you can configure them on the Network > LAN page.
    - MAC address - The physical address of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



5. 3. Network

5. 3. 1. WAN

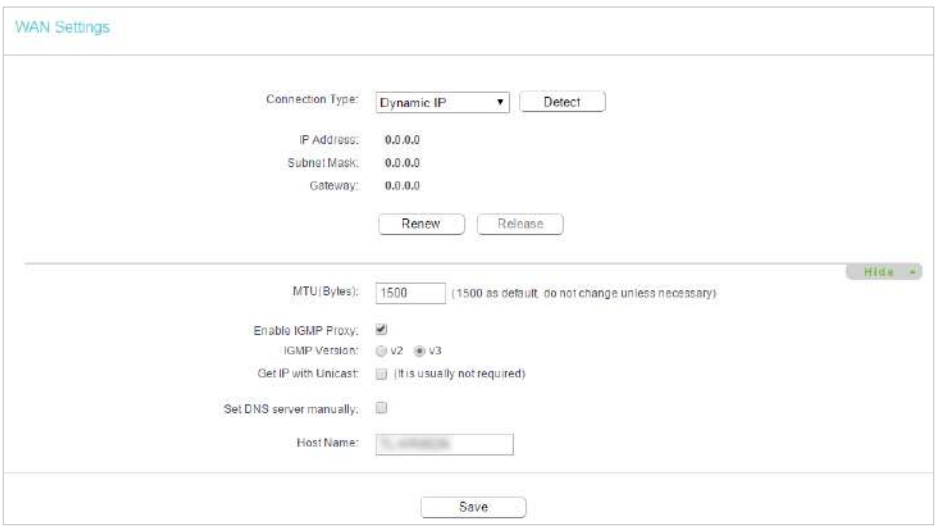
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Network > WAN.
3. Configure the IP parameters of the WAN and click Save.

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.

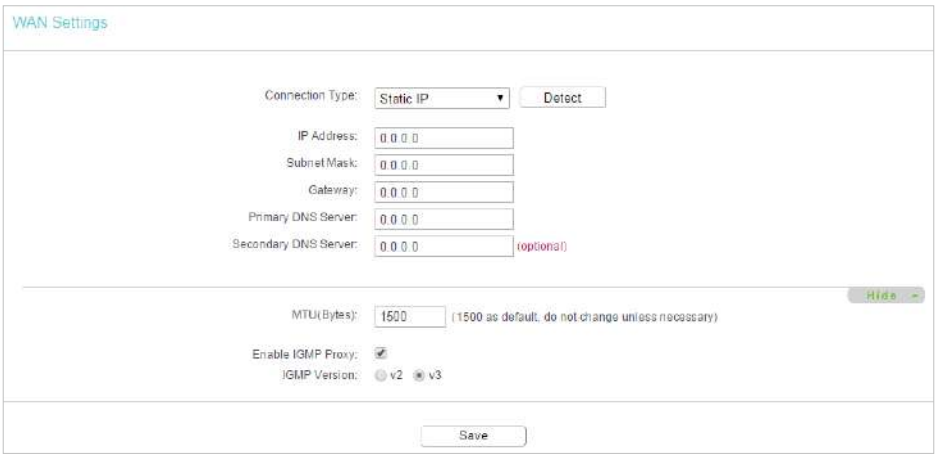
Click Release to release the IP parameters.



- 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.

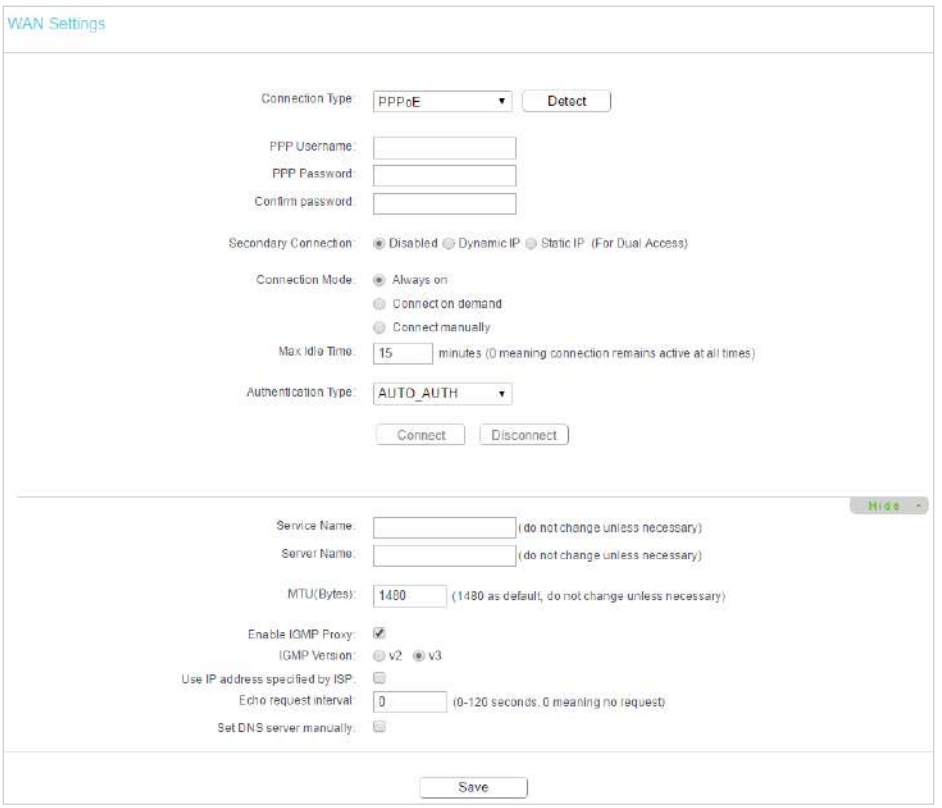


- IP Address - Enter the IP address in dotted-decimal notation provided by your ISP.
- Subnet Mask - Enter the subnet mask in dotted-decimal notation provided by your ISP. Normally 255.255.255.0 is used as the subnet mask.
- Gateway - Enter the gateway IP address in dotted-decimal notation provided by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



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

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

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

- Authentication Type - Choose an authentication type.

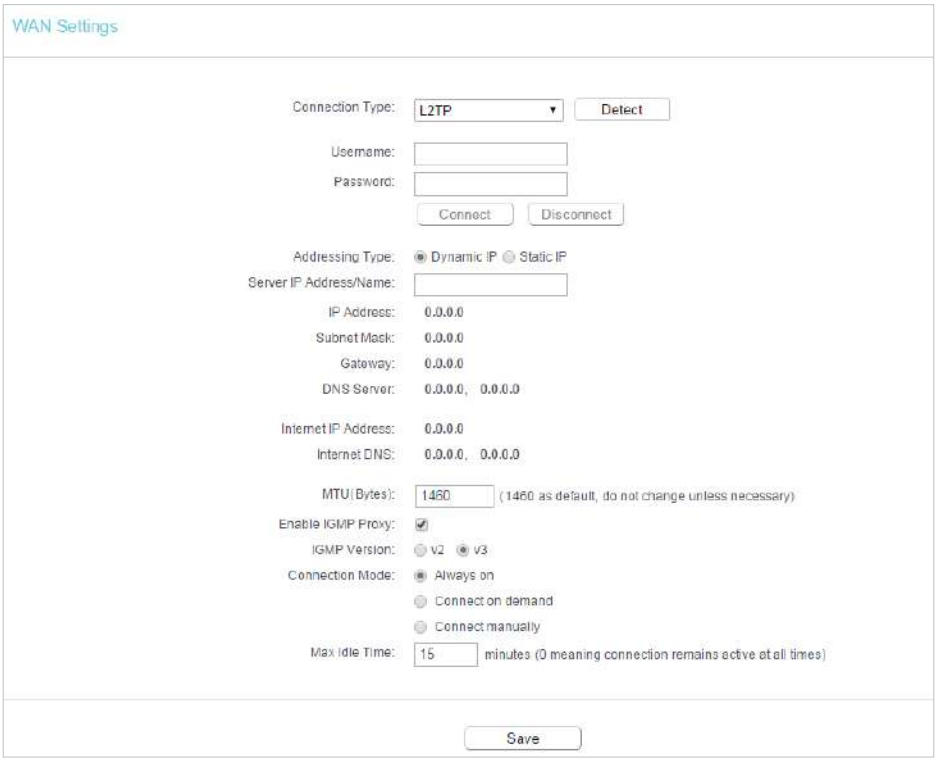
Note:

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

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

L2TP

If your ISP provides L2TP connection, please select L2TP.



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

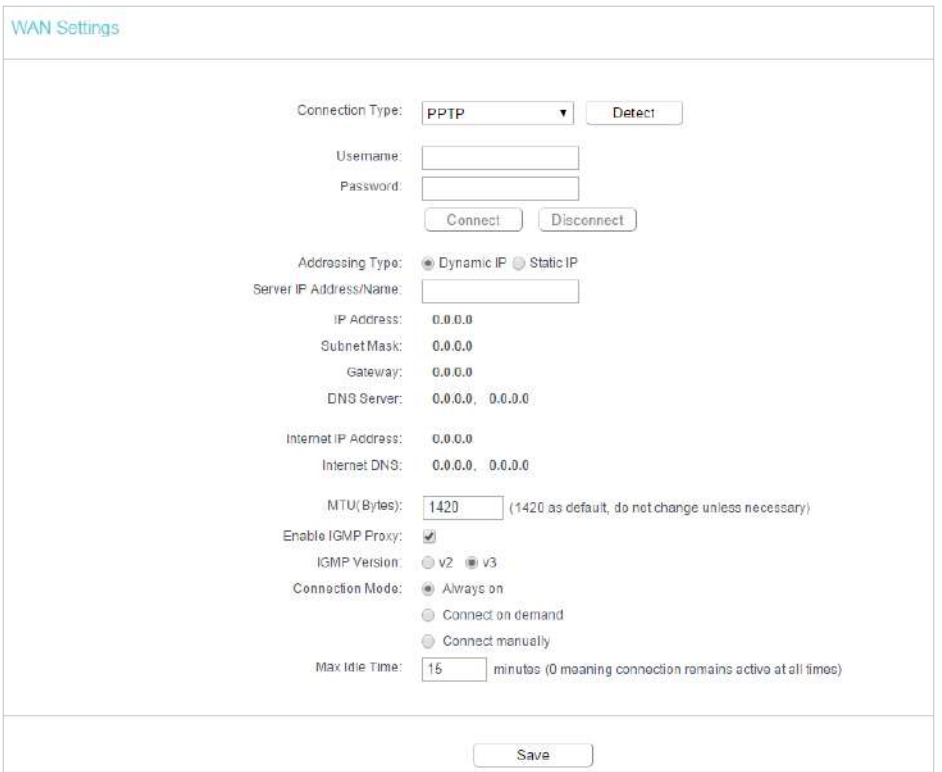
- Connect Manually - You can click Connect/Disconnect to connect/disconnect immediately. This mode also supports the Max Idle Time function as Connect on Demand mode. The internet connection can be disconnected automatically after a specified inactivity period (Max Idle Time) and not be able to re-establish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

Note:

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

PPTP

If your ISP provides PPTP connection, please select PPTP.



- 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.

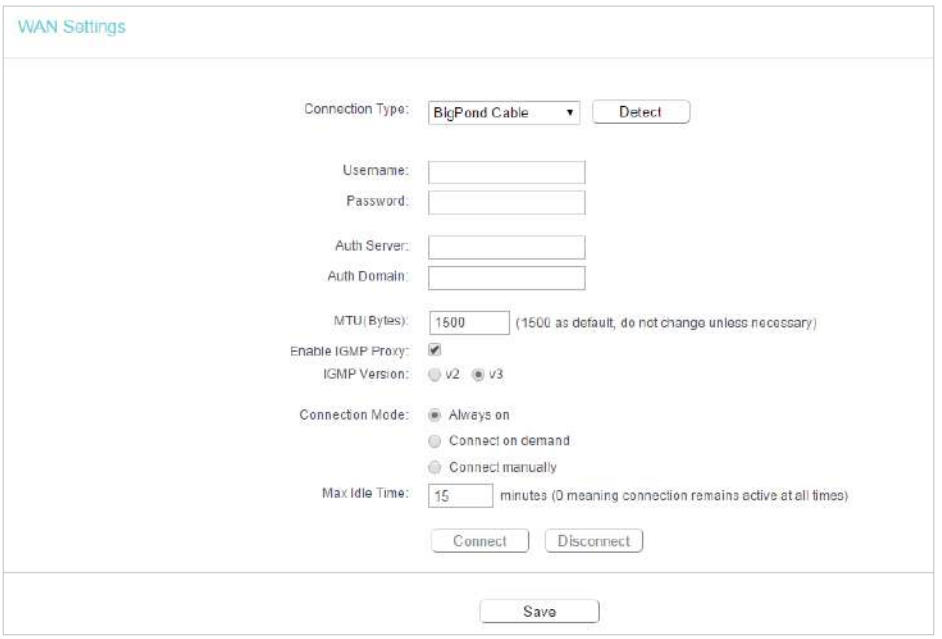
- Connection Mode
  - Always On - In this mode, the internet connection will be active all the time.
  - Connect on Demand - In this mode, the internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the internet 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.

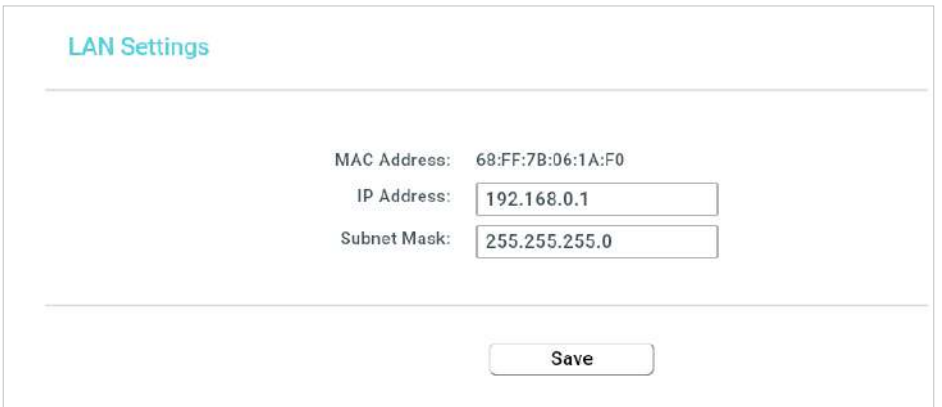


- Username/Password - Enter the username and password provided by your ISP. These fields are case-sensitive.
- Auth Server - Enter the authenticating server IP address or host name.
- Auth Domain - Type in the domain suffix server name based on your location.

- 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.



- 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).

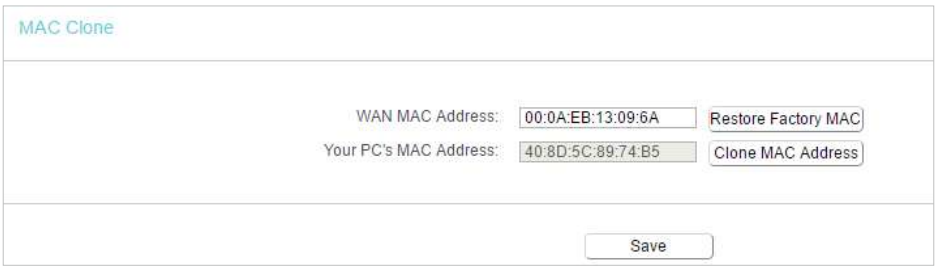
- Subnet Mask - An address code that determines the size of the network. Normally 255.255.255.0 is used as the subnet mask.

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.



- 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.

- 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

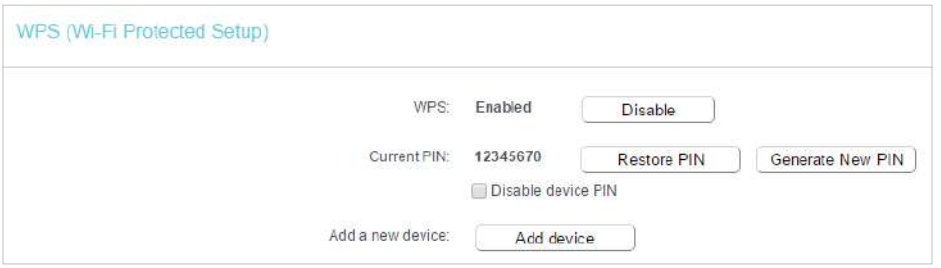
1. Keep the WPS Status as Enabled and click Add Device.

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

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.

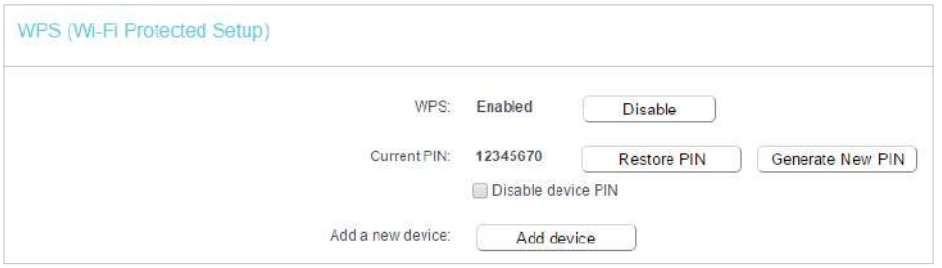


2. Select Enter new device PIN, enter your client device's current PIN in the PIN filed and click Connect.

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

Method Three: Enter the Router's PIN

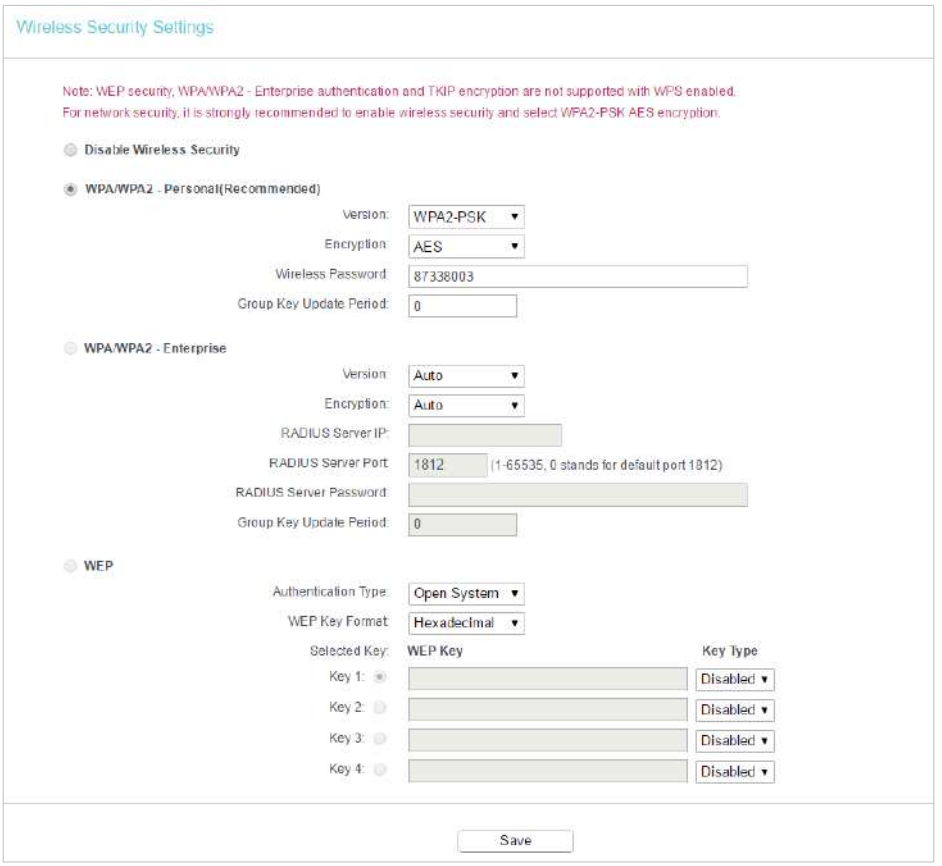
1. Keep the WPS Status as Enabled and get the Current PIN of the router.



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.

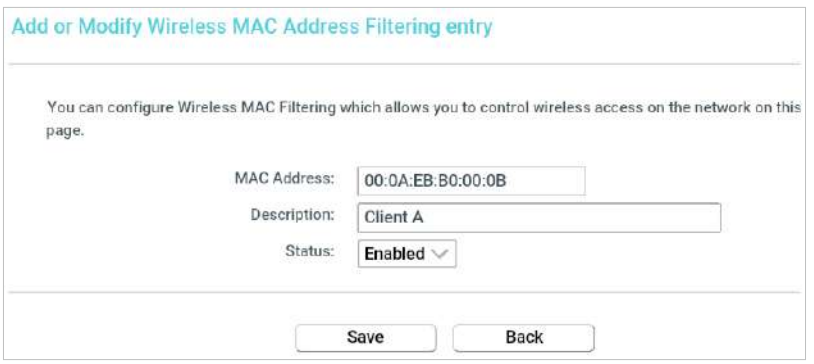
I want to:

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.



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.

Done!

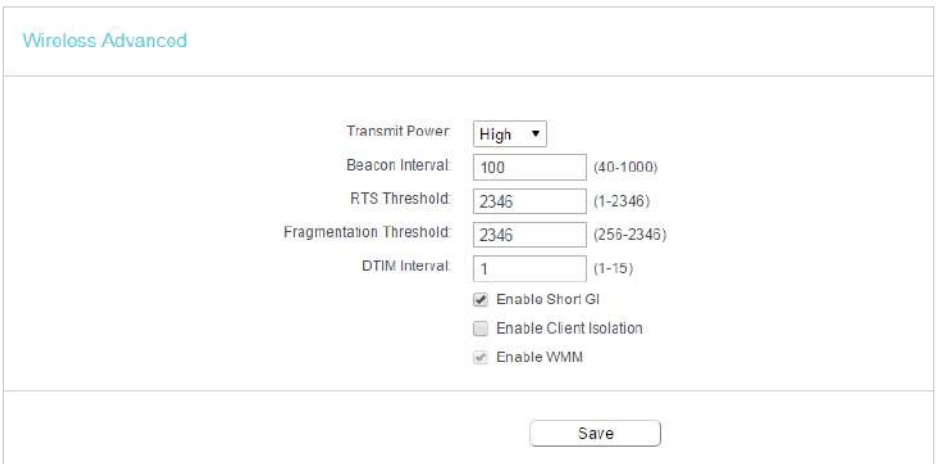
Now only client A and client B can access your network.

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.



- 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

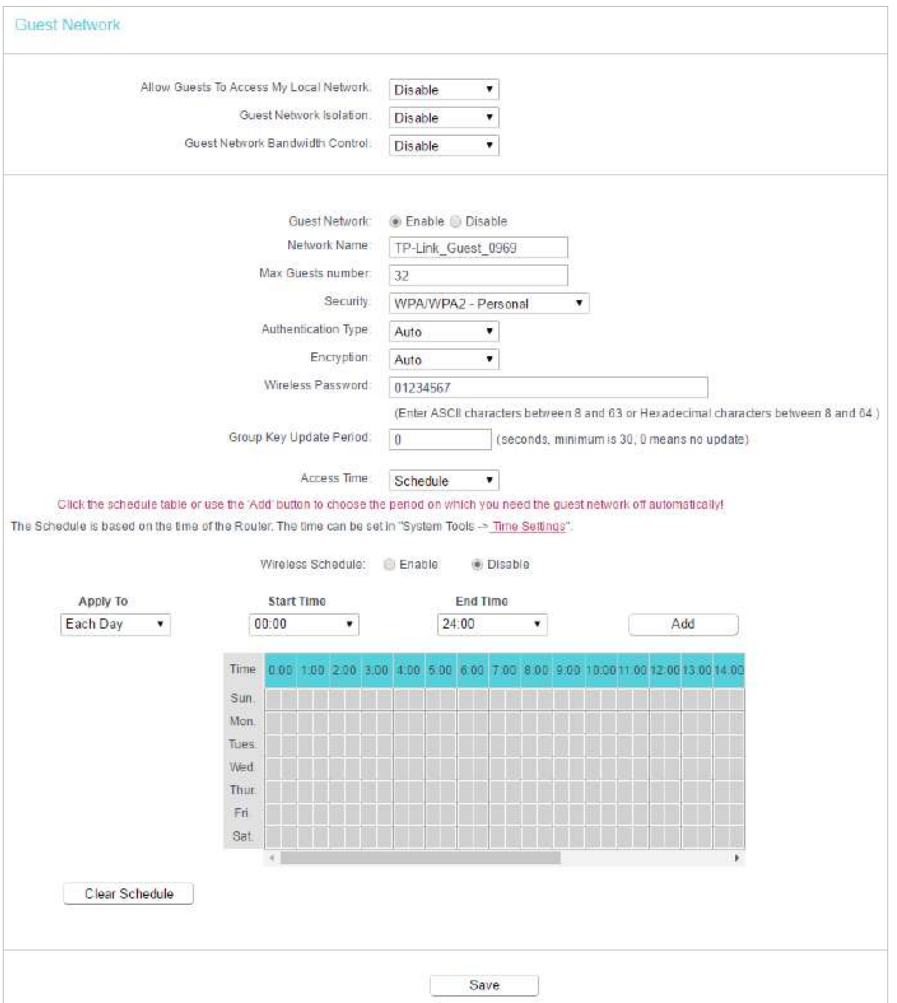
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Wireless > Wireless Statistics to check the data packets sent and received by each client device connected to the router.

- 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 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.



- 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:

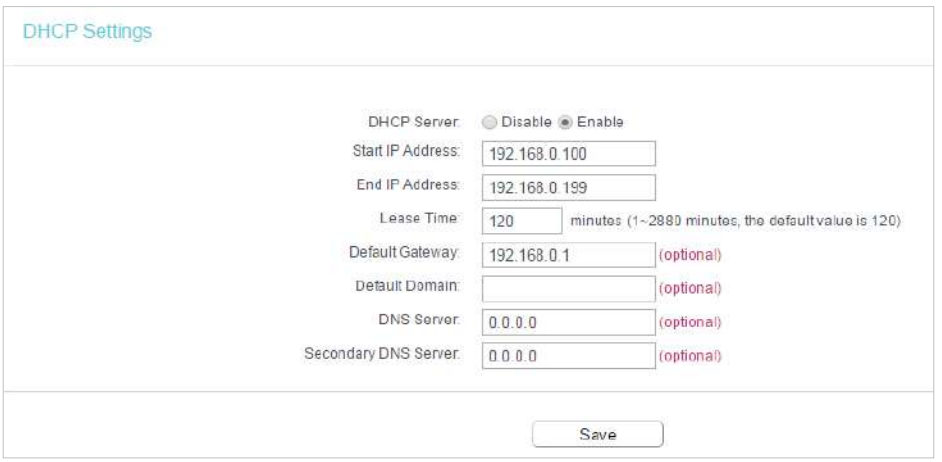
The range of bandwidth for guest network is calculated according to the setting of Bandwidth Control on the Bandwidth Control page.

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 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.

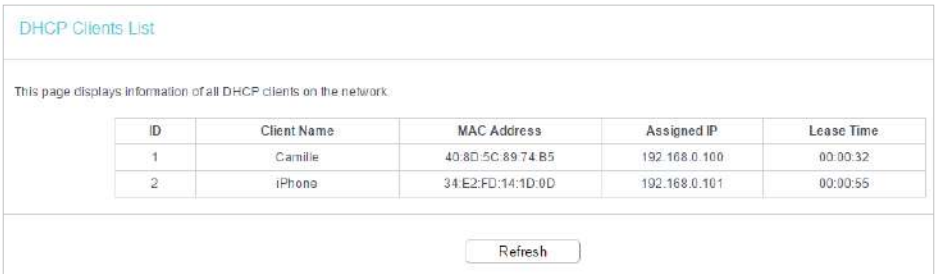
- Address Lease Time - The Address Lease Time is the amount of time a network user will be allowed to connect to the router with the current dynamic IP Address. When time is up, the user will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 2880 minutes. The default value 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.



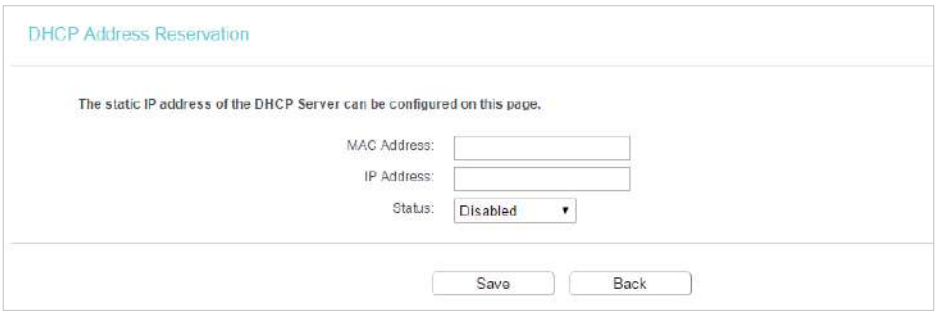
- Client Name - The name of the DHCP client.
- MAC Address - The MAC address of the DHCP client.
- Assigned IP - The IP address that the outer has allocated to the DHCP client.
- Lease Time - The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic IP address will be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

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.



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.

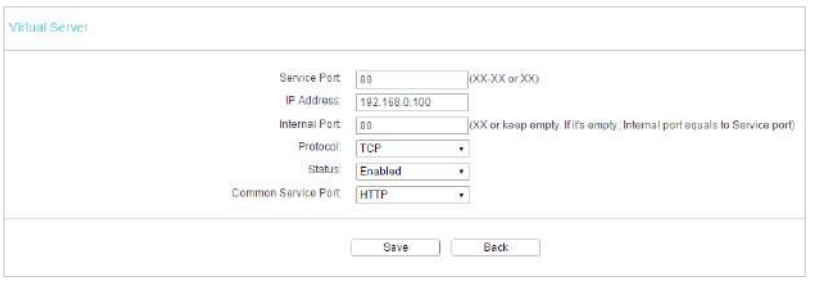
Virtual Servers can be used to set up public services in your local network, such as HTTP, FTP, DNS, POP3/SMTP and Telnet. Different service uses different service port. Port 80 is used in HTTP service, port 21 in FTP service, port 25 in SMTP service and port 110 in POP3 service. Please verify the service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



5. Leave the status as Enabled and click Save.

Note:

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

Done!

Users on the internet can enter http:// WAN IP (in this example: http:// 218.18.232.154)

to visit your personal website.

Note:

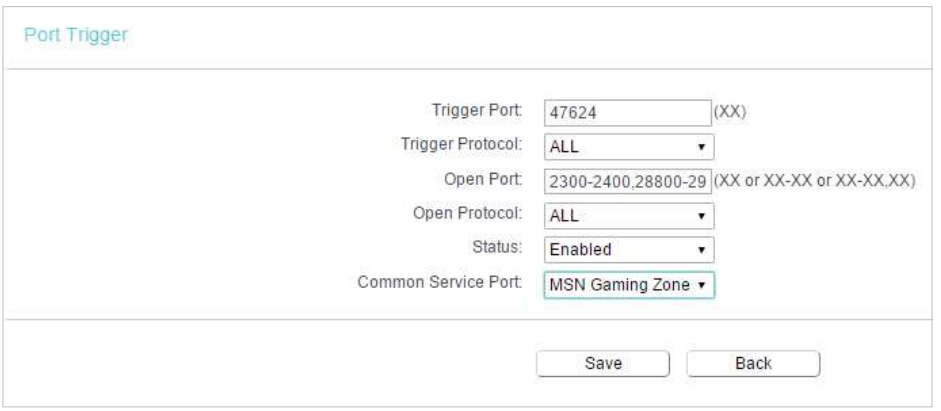
- If you have changed the default Service Port, you should use http:// WAN IP: Service Port to visit the website.
- Some specific service ports are forbidden by the ISP, if you fail to visit the website, please use another service port.

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 amd incoming ports will be automatically filled in. The following picture takes application MSN Gaming Zone as an example.



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.

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.

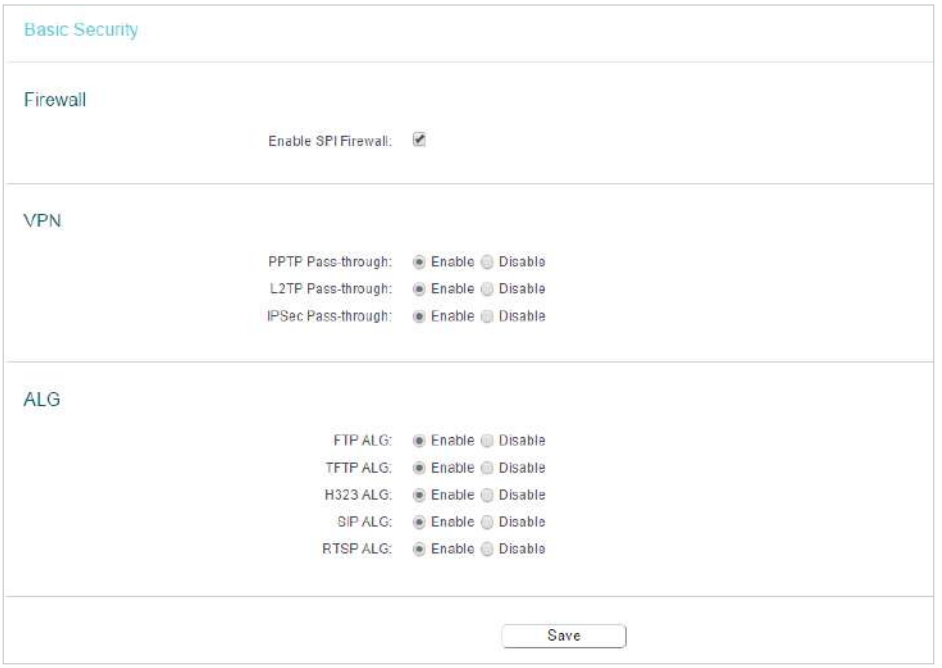
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Forwarding > UPnP.
3. Click Disable or Enable according to your needs.

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.



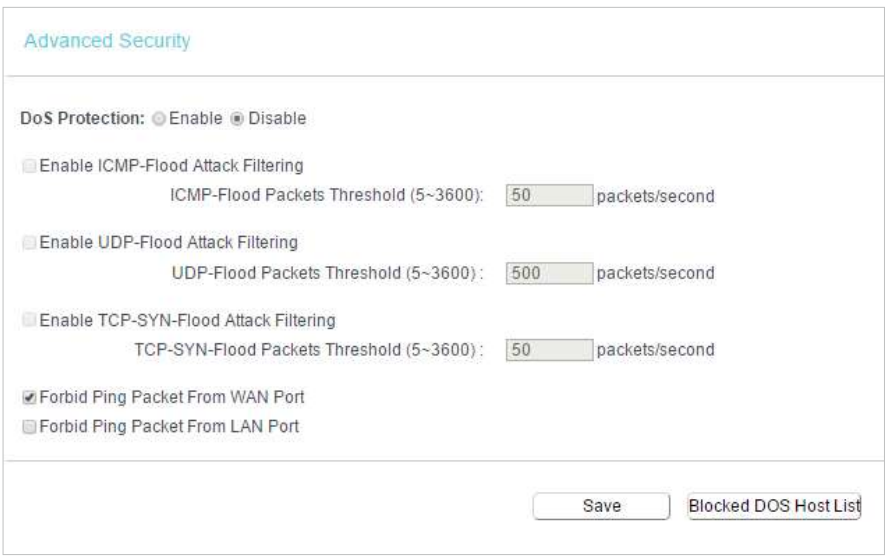
- Firewall - A firewall protects your network from internet attacks.
    - Enable SPI Firewall - SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms 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.



- 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.

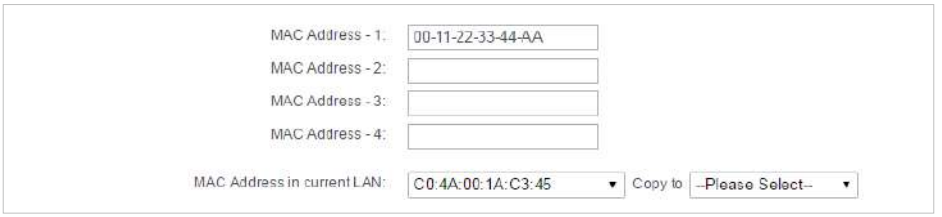
5. 9. Parental Controls

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

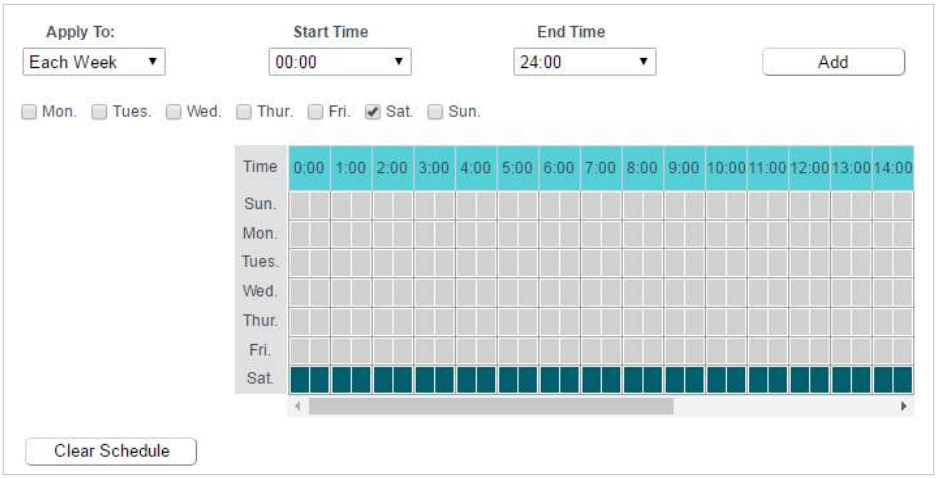
For example, you want the children's PC with the MAC address 00:11:22:33:44:AA can access www.tp-link.com on Saturday only while the parent PC with the MAC address 00:11:22:33:44:BB is without any restriction.

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.

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



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.



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

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.

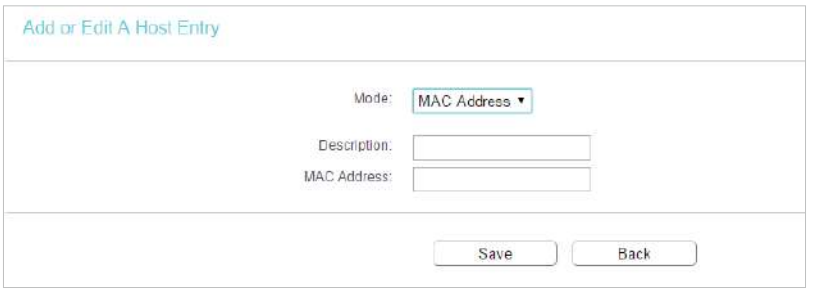
I want to:

Deny or allow specific client devices to access my network with access tiem 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:

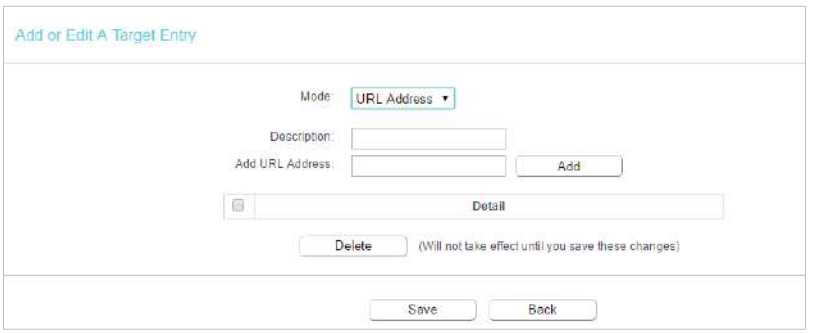
How can I do that?

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 filed.

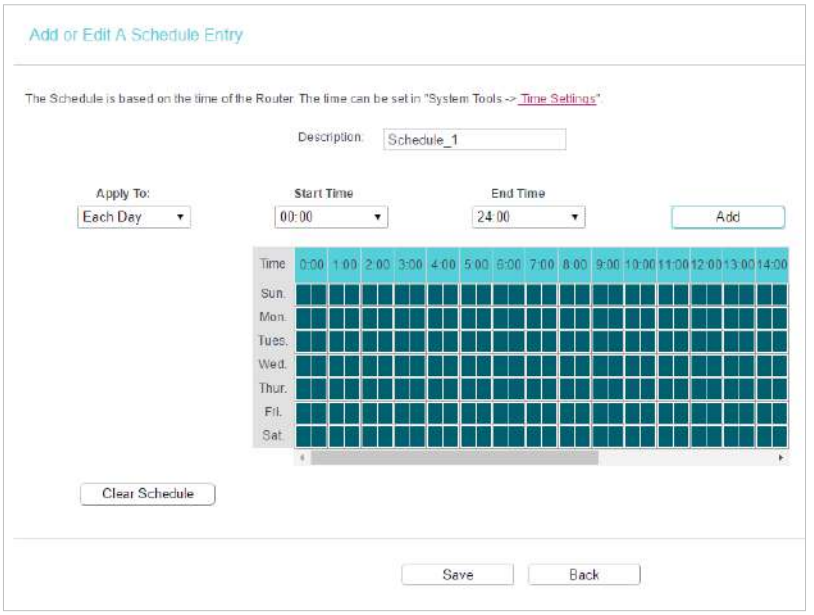


   3) Click Save.
3. Go to Access Control > Target and configure the target settings:
   1) Click Add New.
   2) Select URL Address as the mode type. Create a unique description (e.g. target_1) for the target in the Target Description field and enter the domain name, either the full name or the keywords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

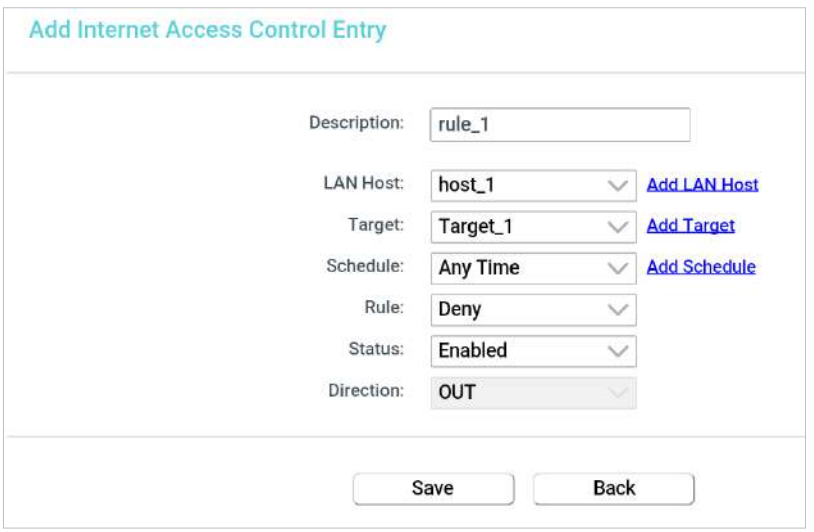


3) Click Save.

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.



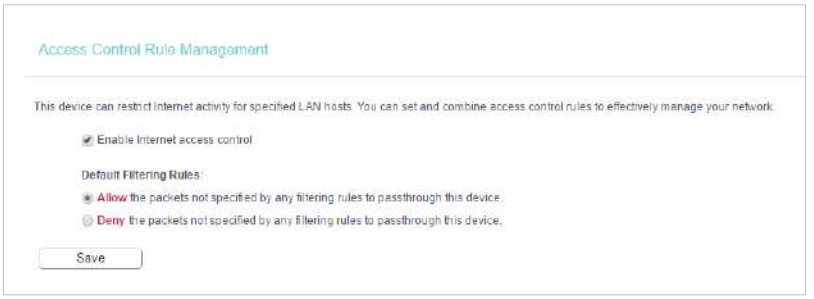
3) Leave the status as Enabled as click Save.

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

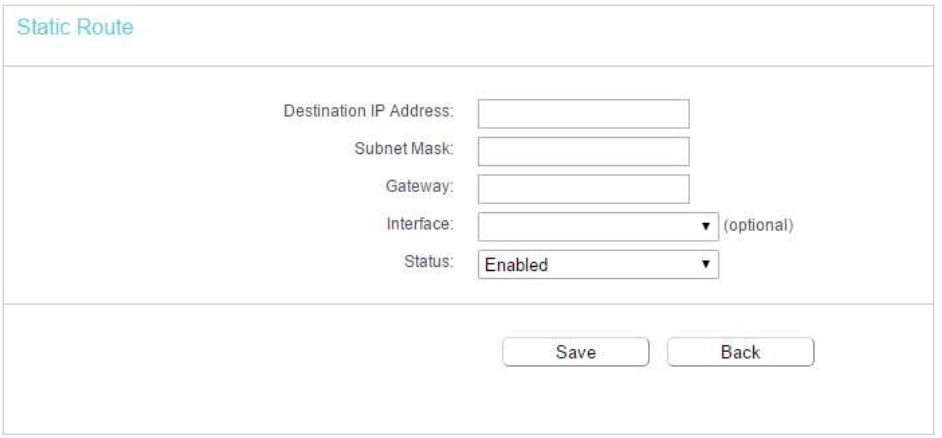
Static Routing is a form of routing that is configured manually by a network administrator or a user by adding entries into a routing table. The manually-configured routing information guides the router in forwarding data packets to the specific destination.

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.

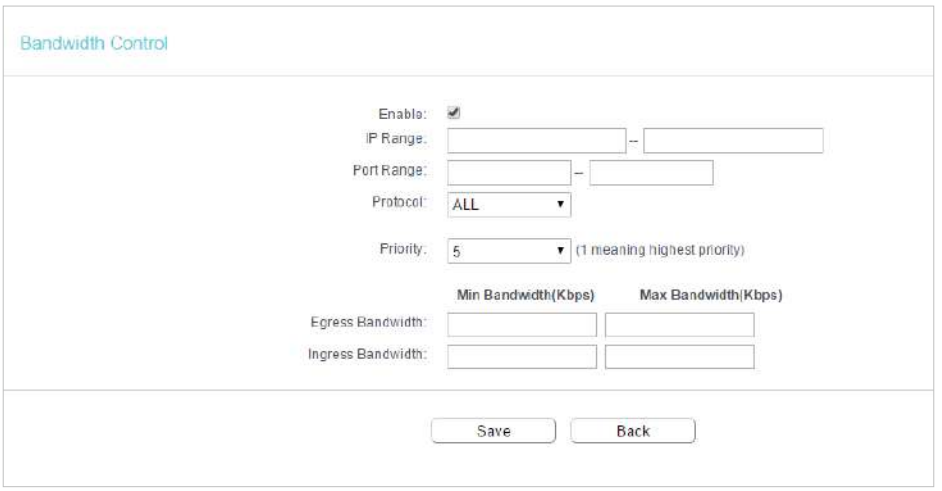
- Destination Network - The Destination Network is the address of the network or host to which the static route is assigned.
- Subnet Mask - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.
- Gateway - This is the IP address of the 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.

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



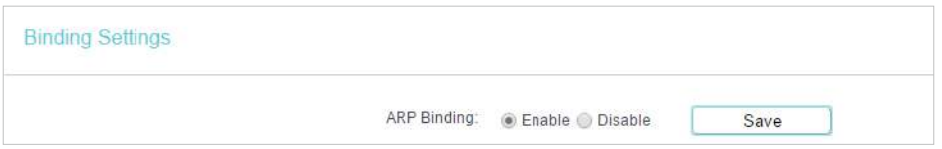
- IP Range - Interior PC address range. If both are blank or 0.0.0.0, the domain is noneffective.
- Port Range - The port range which the Interior PC access the outside PC. If all are blank or 0, the domain is noneffective.
- Protocol - Transport layer protocol, here there are ALL, TCP, UDP.
- Priority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



- **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.

- **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.

- 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.

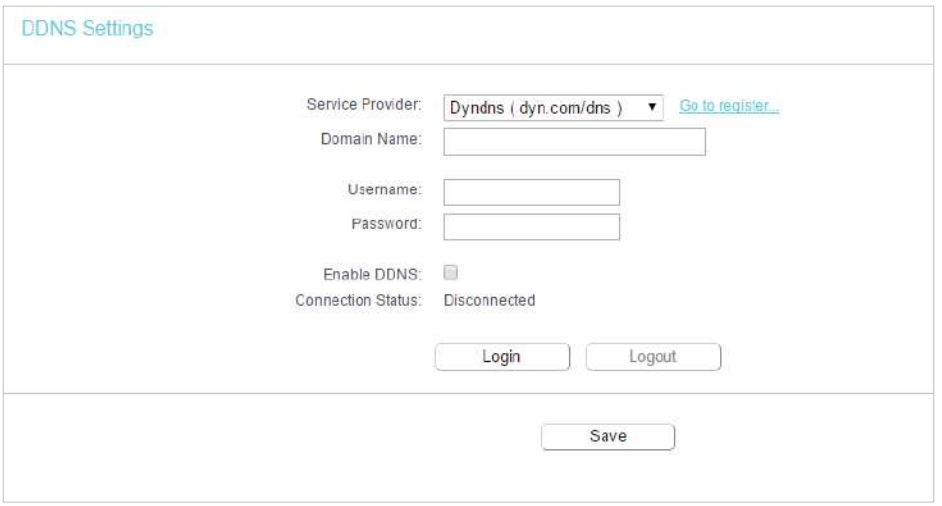
5. 14. Dynamic DNS

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.



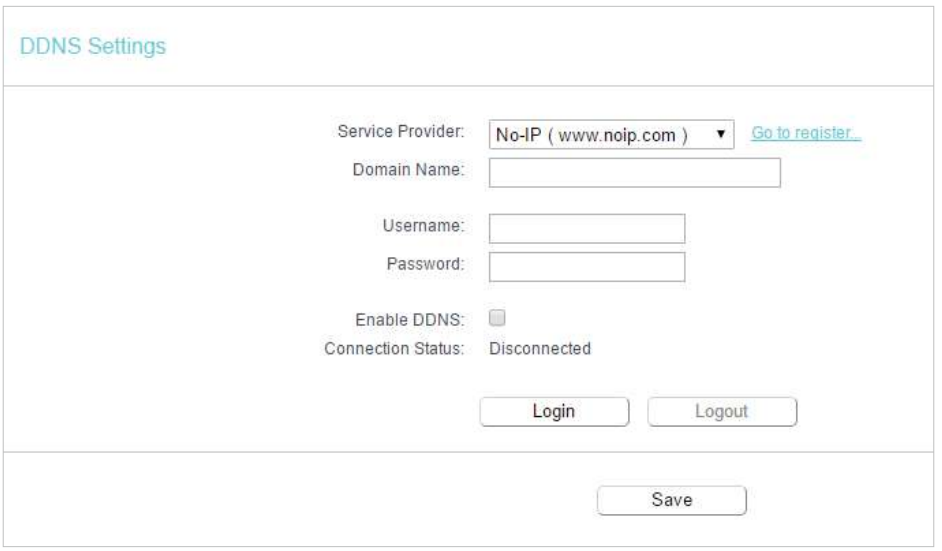
To set up for DDNS, follow these instructions:

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.



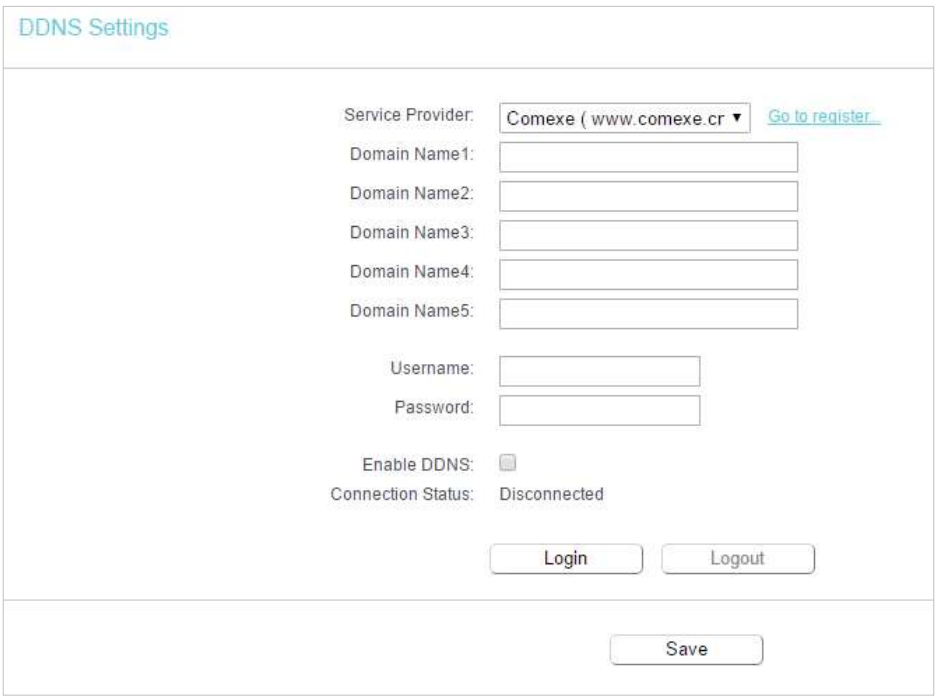
To set up for DDNS, follow these instructions:

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.



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.

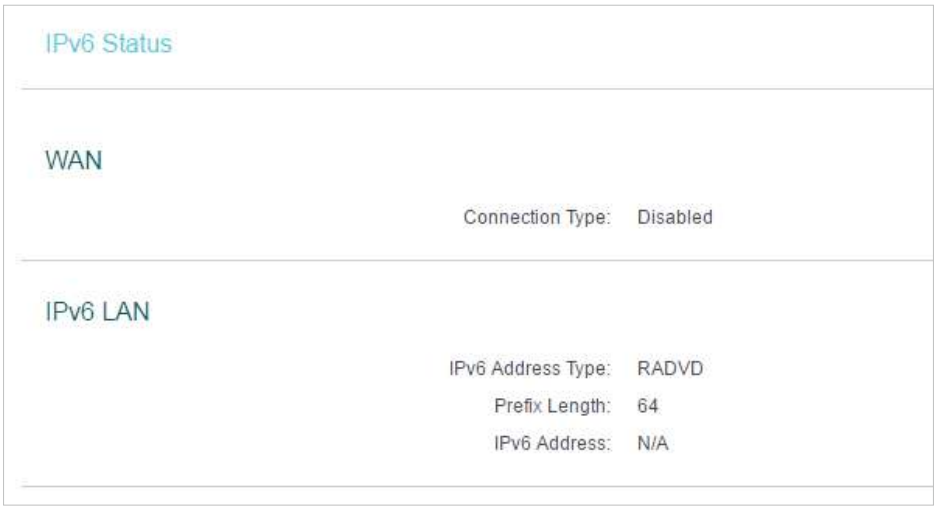
5. 15. IPv6

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.

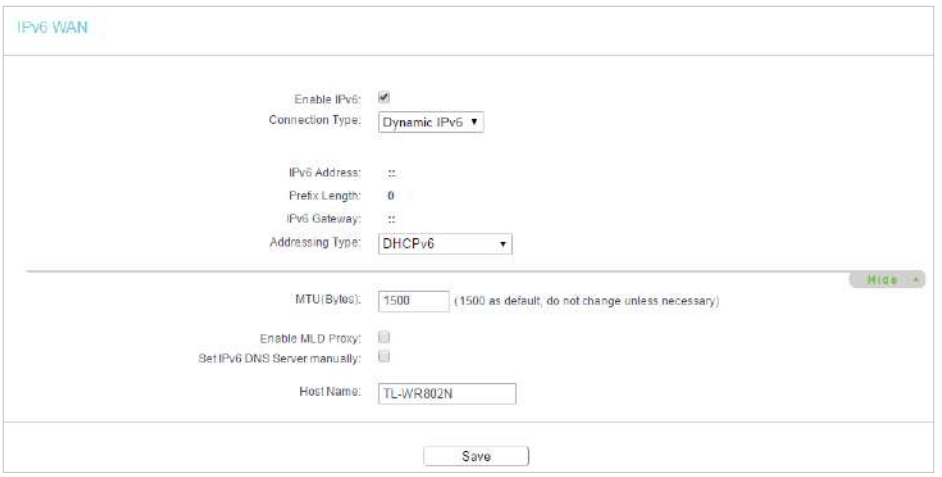
2. Go to IPv6 > IPv6 Status, and you can view the current IPv6 status information of the router.



- WAN - This section shows the current IPv6 Connection Type.
- TPv6 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

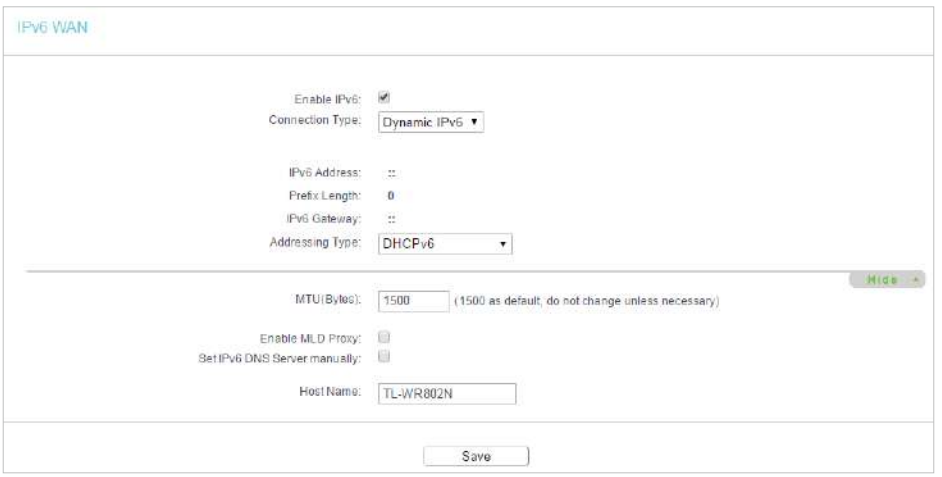
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to IPv6 > IPv6 WAN. Select Enable IPv6.



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

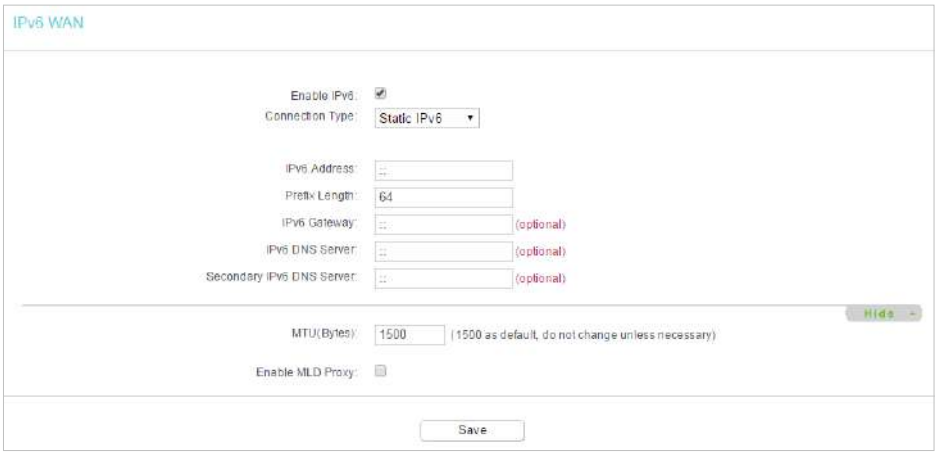


- IPv6 Address - The IPv6 address assigned by your ISP dynamically.
- Prefix Length - The length of IPv6 address prefix.
- IPv6 Gateway - Enter the default gateway provided by your ISP.
- Addressing Type - There are two types of assignation for IPv6 address: SLAAC (Stateless address auto-configuration) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.
- MTU(Bytes) - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs, you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- Enable MLD Proxy - Enable the Multicast Listener Discovery (MLD) Proxy function if you need.
- 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:

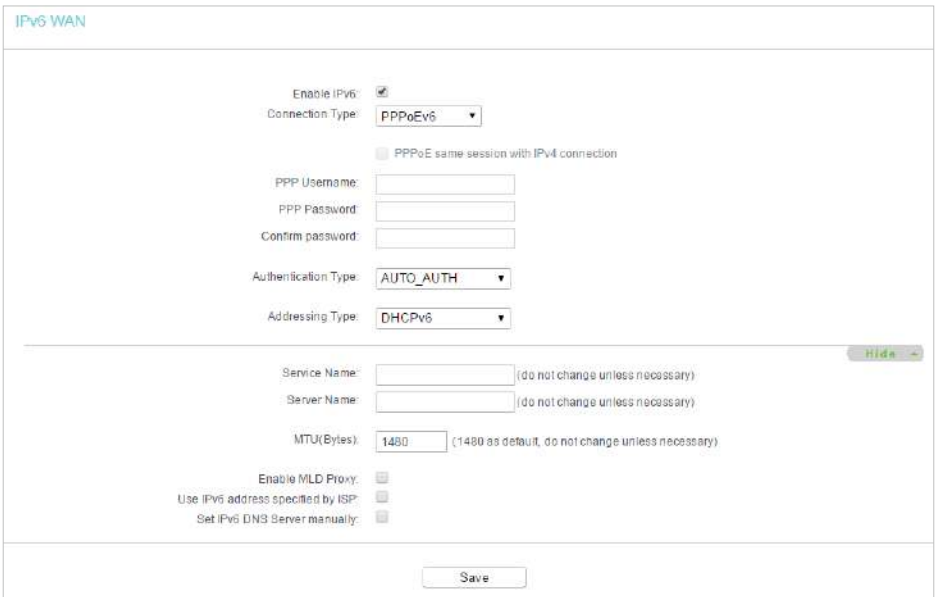
If you get Address not found error when you access a Web site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

Static IPv6



- IPv6 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



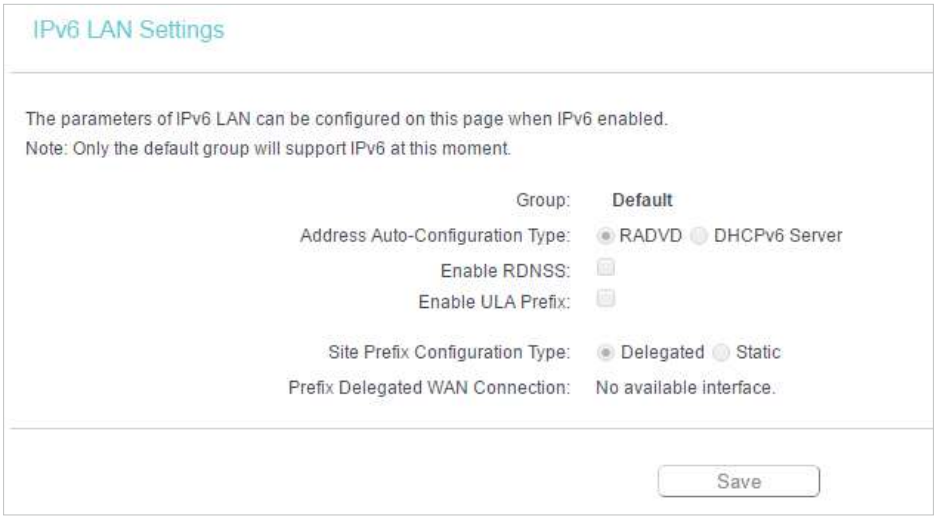
- PPP Username/Password - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- Authentication Type – Choose one authentication type from AUTO-AUTH, PAP, CHAP and MS-CHAP.
- Addressing Type - There are two types of assignation for IPv6 address: SLAAC (Stateless address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

Tunnel 6to4

- 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.



- 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:

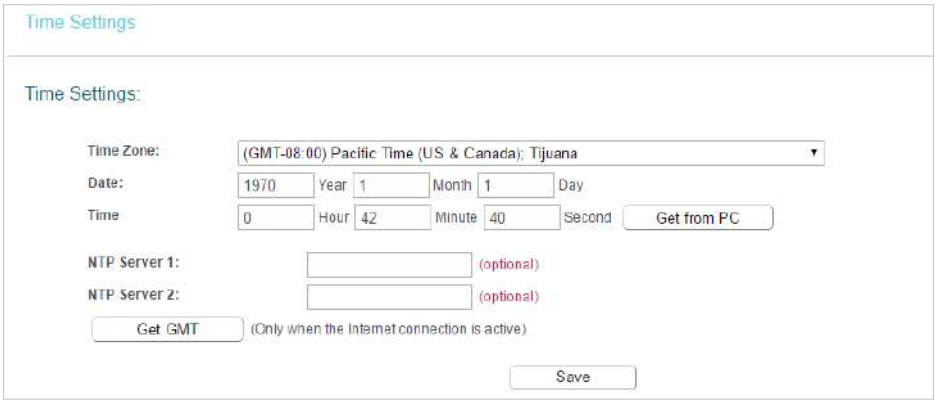
If your IPv6 wan connection type is "Tunnel 6to4", the Site Prefix Configuration Type should be "Static" to make sure "Tunnel 6to4" works properly.

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.

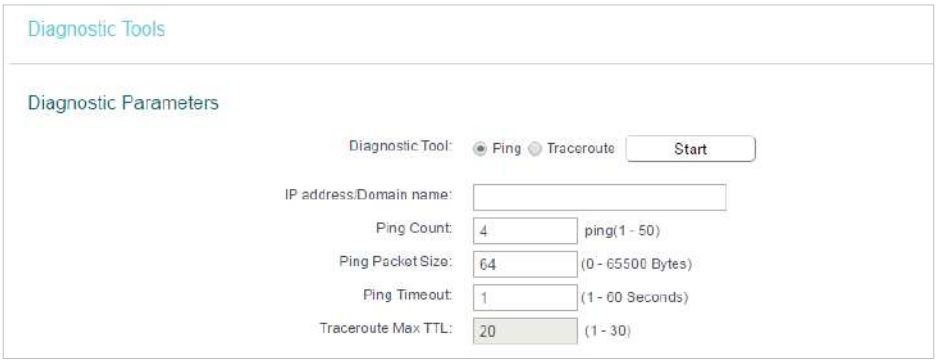
Note:

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.



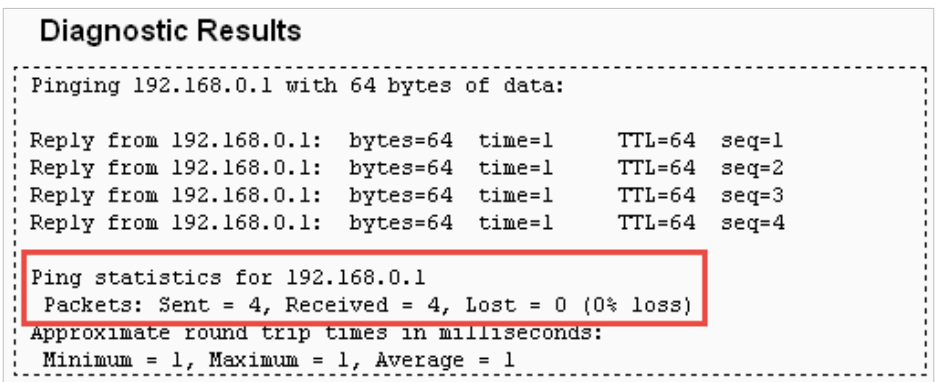
- Diagnostic Tool - Select one diagnostic tool.
  - Ping - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
  - Tracerouter - This diagnostic tool tests the performance of a connection.

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.

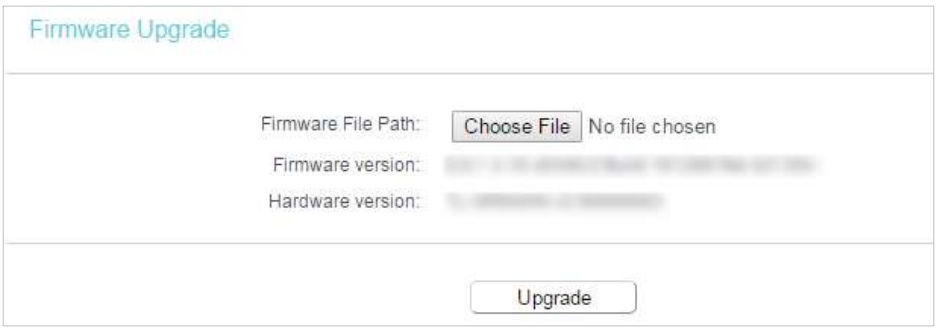


5. 16. 3. Firmware Upgrade

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

www.tp-link.com. You can download the lastest firmware file from the Support page of our website and upgrade the firmware to the latest version.

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



5. 16. 4. Factory Defaults

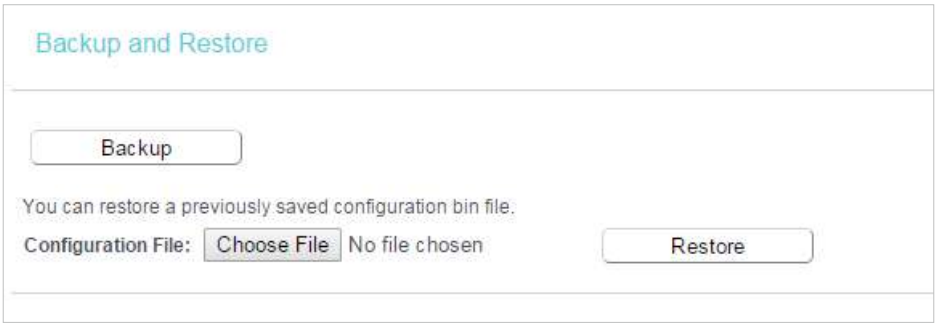
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to System Tools > Factory Defaults. Click Restore to reset all settings to the default values.

- 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

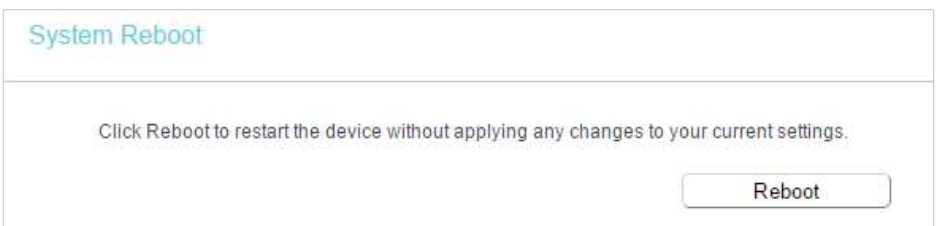
Some settings of the router will take effect only after rebooting, including:

- 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.

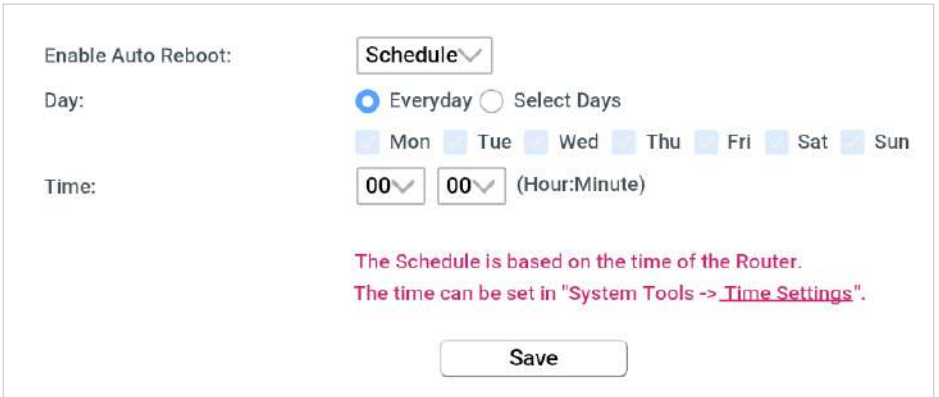
- **To reboot manually**

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



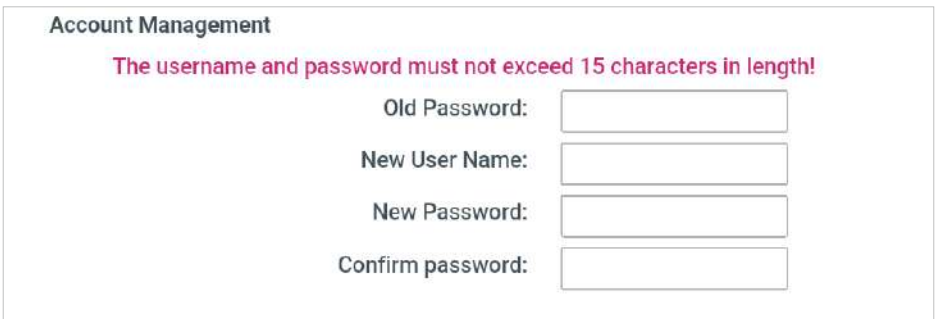
- **To reboot automatically**
  - Select Timeout in the drop-down list of Enable Auto Reboot and specify a time period (1-72hours), then the router will reboot automatically after every this interval.

  - 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.



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.



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.

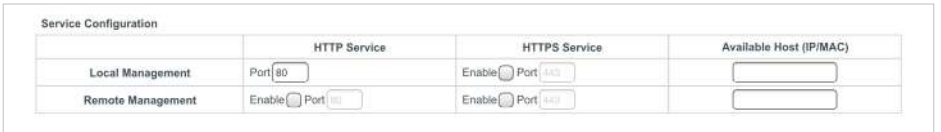
Note:
The new username and password must not exceed 15 characters and not include any spacing.

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.



- **Allow all LAN conencted 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 disbled.
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.

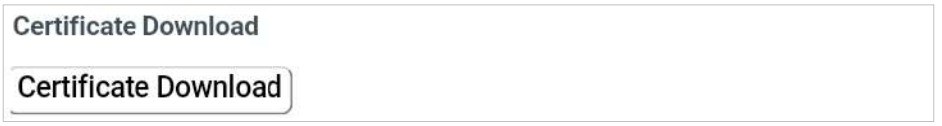
- **Allow a specific device to manage the router locally**

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 disbled.
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**

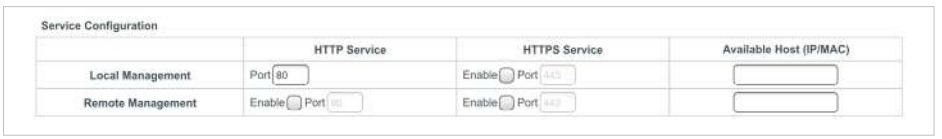
Download and install the certificate for management via HTTPS if you need it. Once the certificate is installed, warnings will not pop up when you access the router via HTTPS.



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.



- **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**

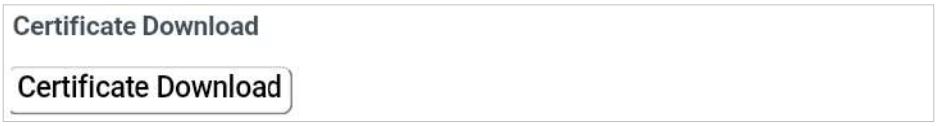
1. Tick the Enable checkbox in HTTP Service.
2. If you want to access the router via both HTTPS and HTTP, please tick the Enable checkbox in HTTPS Service column. Otherwise, keep it disbled.
3. For higher security, you can change the remote management web port by entering a number between 1024 and 65534.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

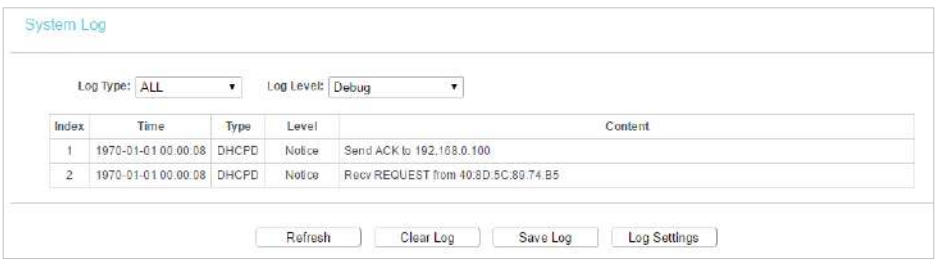


Note:

- 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

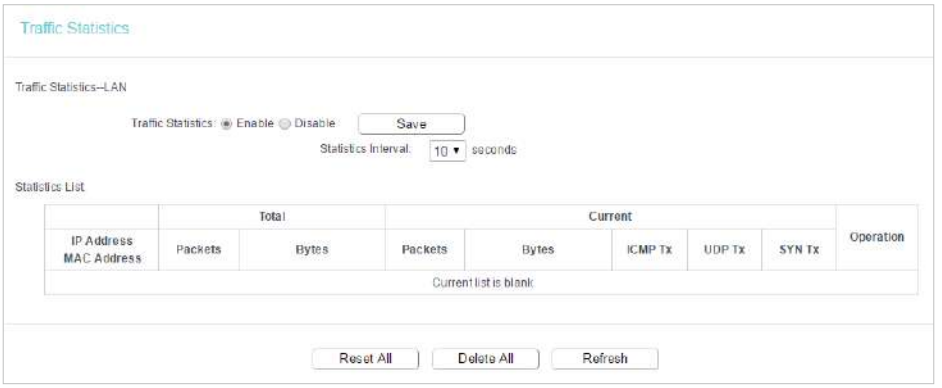
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to System Tools > System Log, and you can view the logs of the router.



- 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.



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

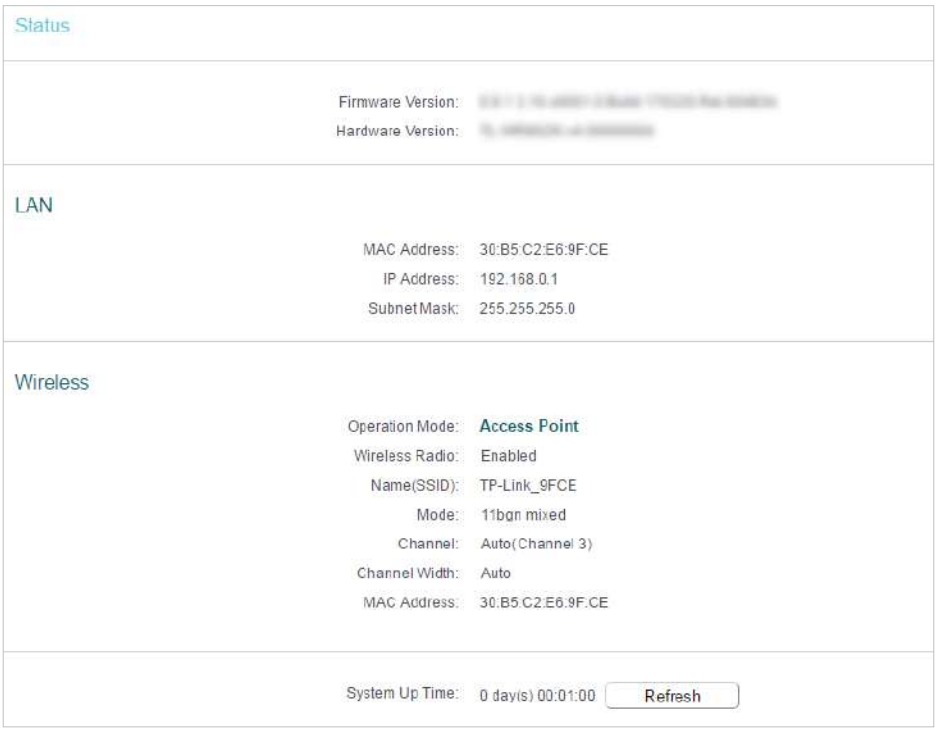
This chapter presents how to configure the various features of the router working as a an access point.

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.



- 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.

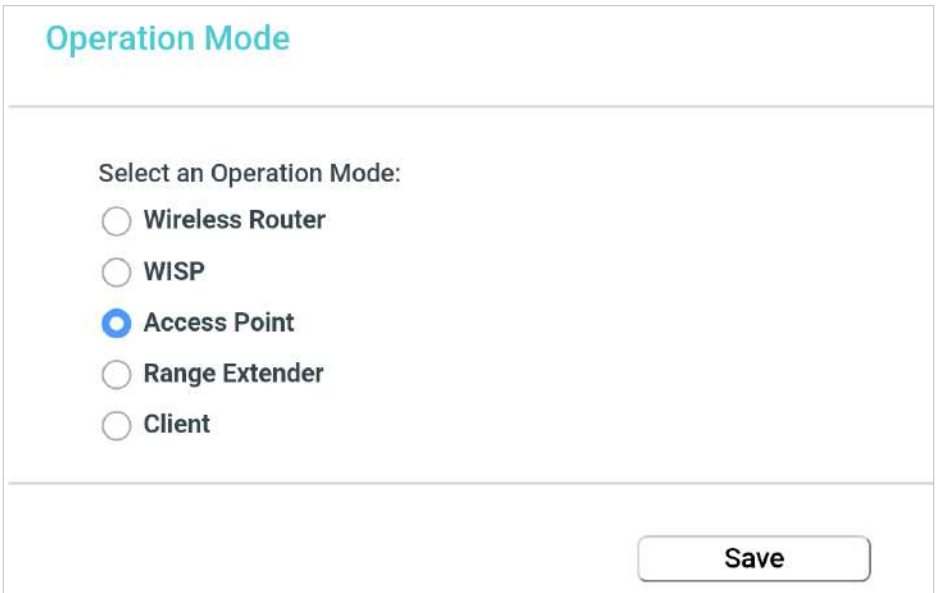
- Channel Width - The current wireless channel width in use.
- MAC Address - The physical address of the router.

- 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

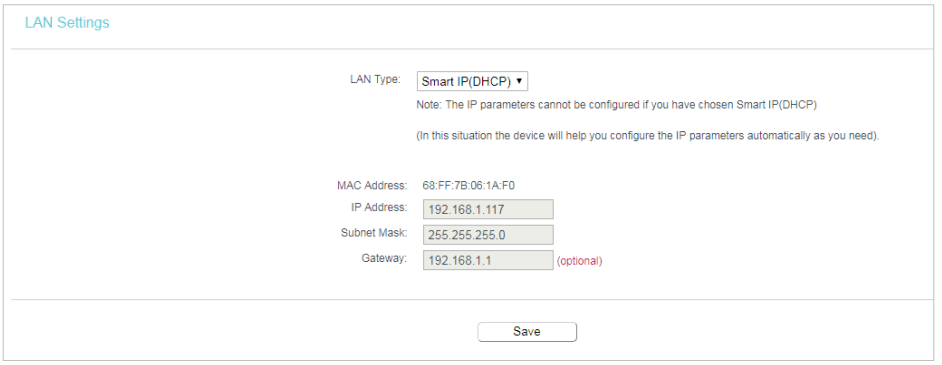
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Operation Mode.
3. Select the working mode as needed and click Save.



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.



- 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.

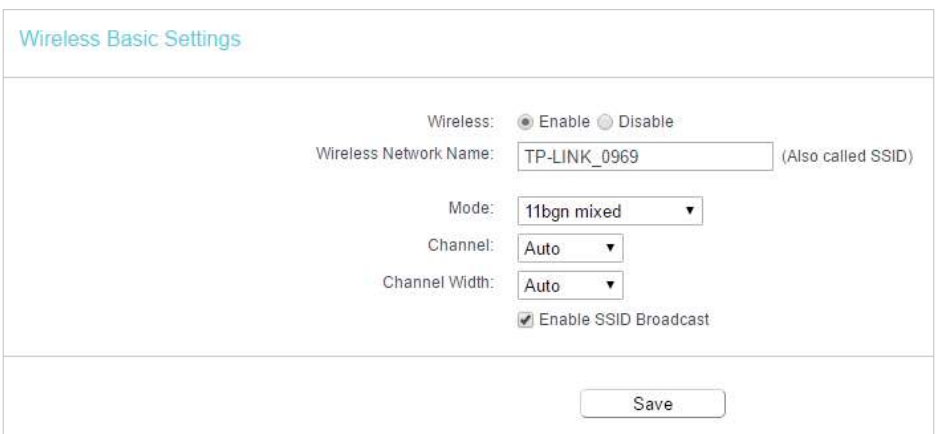
Note:

- 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 - 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

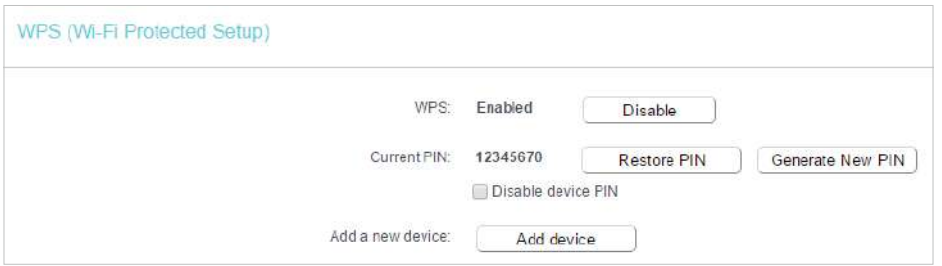
1. Keep the WPS Status as Enabled and click Add Device.

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

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.

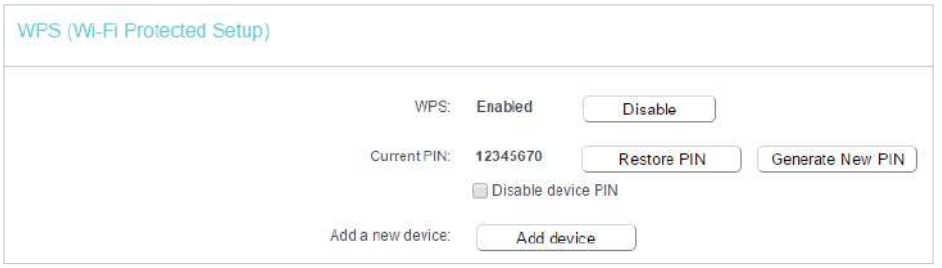


2. Select Enter new device PIN, enter your client device's current PIN in the PIN filed and click Connect.

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

Method Three: Enter the Router's PIN

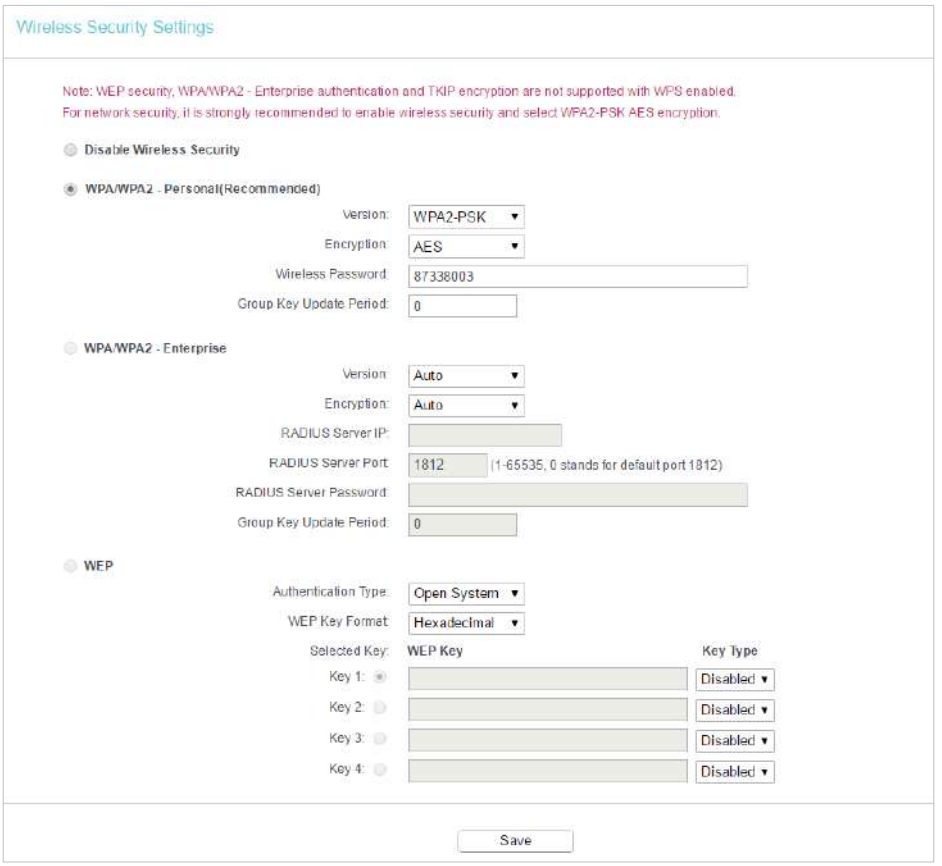
1. Keep the WPS Status as Enabled and get the Current PIN of the router.



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.

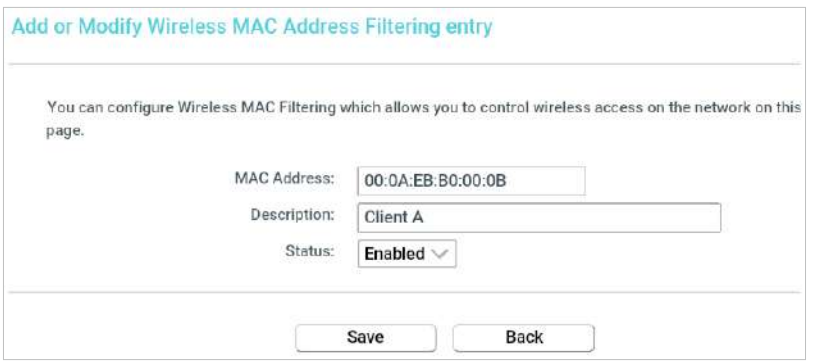
I want to:

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.



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.

Done!

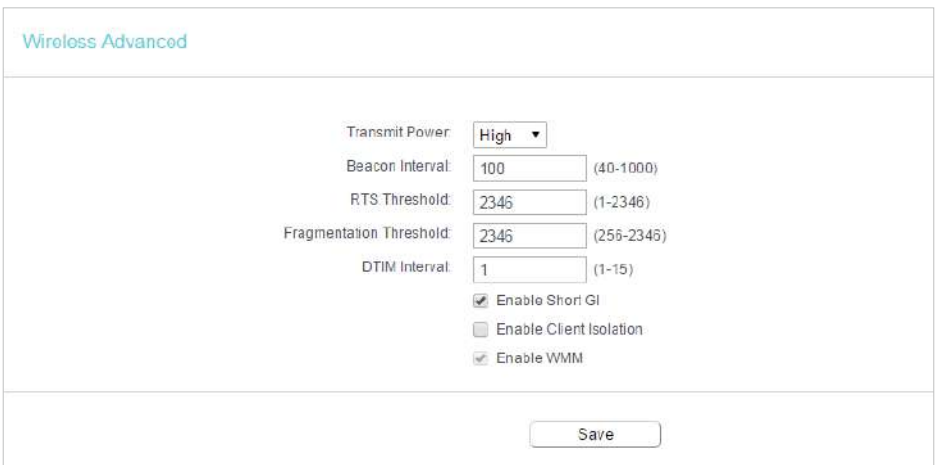
Now only client A and client B can access your network.

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.



- 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

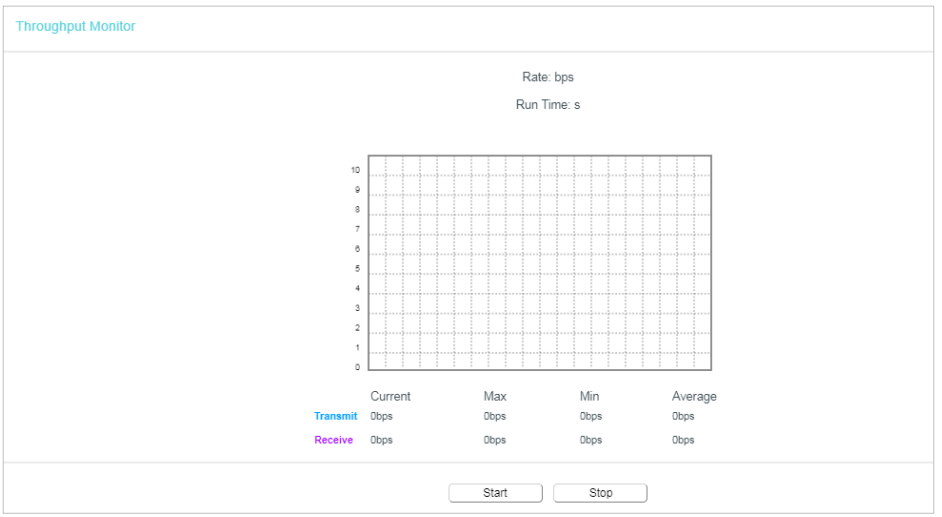
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Wireless > Wireless Statistics to check the data packets sent and received by each client device connected to the router.

- 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.



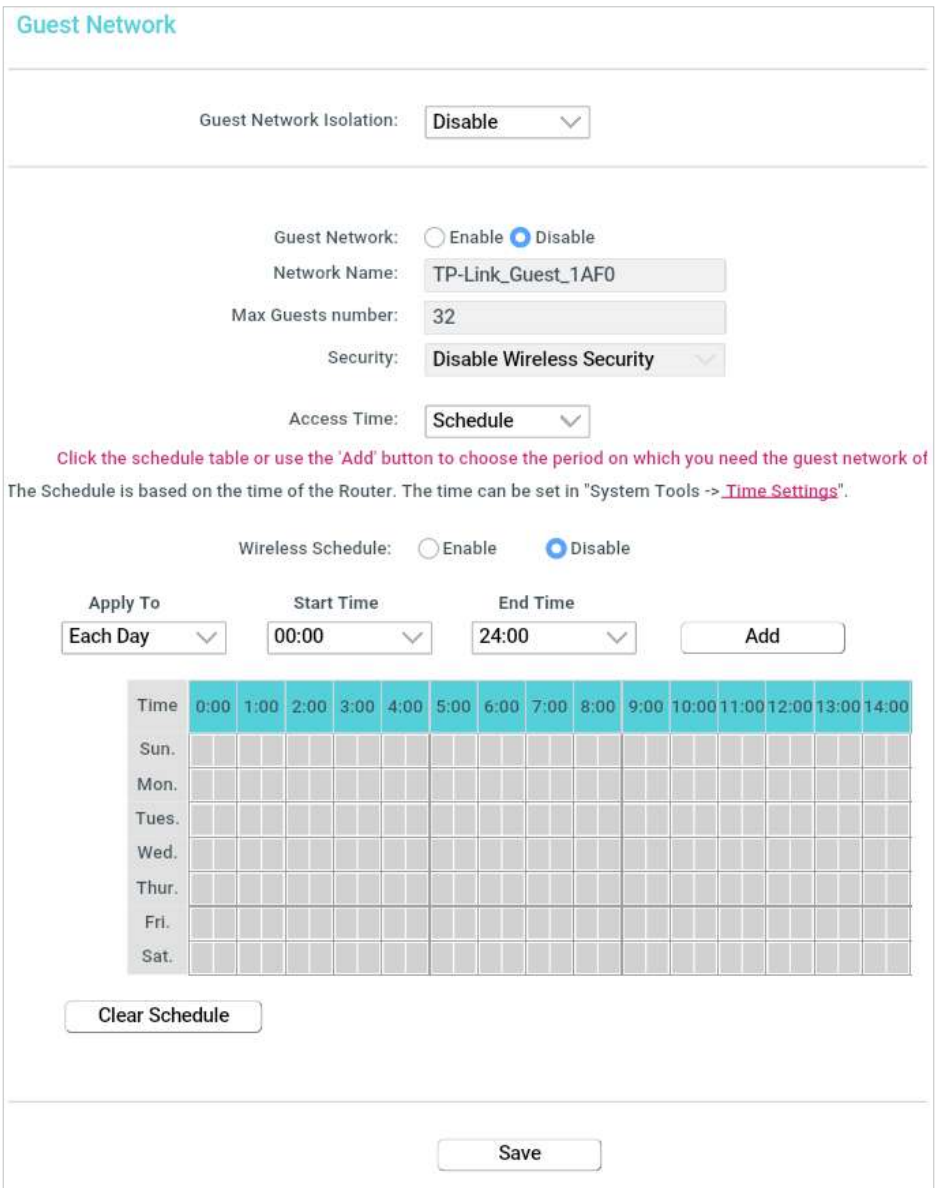
- Rate - The throughput unit.
- Run Time - How long this function is running.
- Transmit - Wireless transmit rate information.
- Transmit - Wireless transmit rate information.
- Receive - Wireless reception rate information.
- Click Start to start wireless throughput monitor.
- Click Stop to stop wireless 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 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 Isolation - If enabled, guests are isolated from each other.

Note:

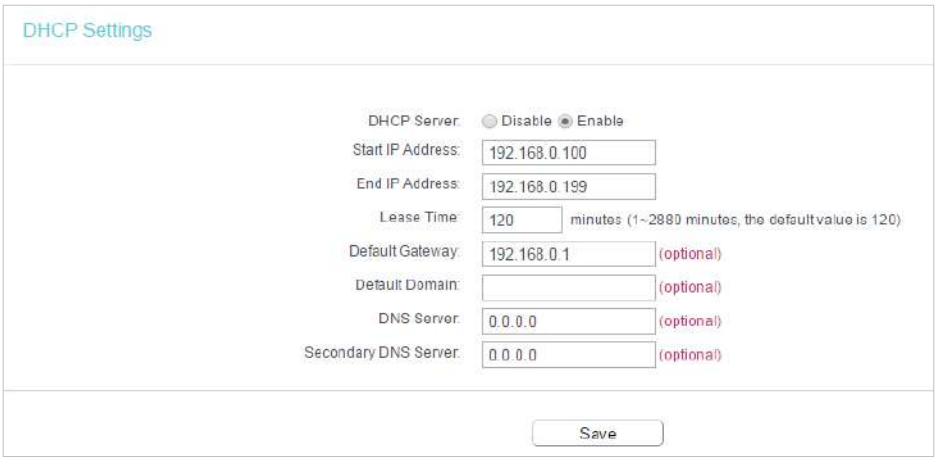
The range of bandwidth for guest network is calculated according to the setting of Bandwidth Control on the Bandwidth Control page.

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.

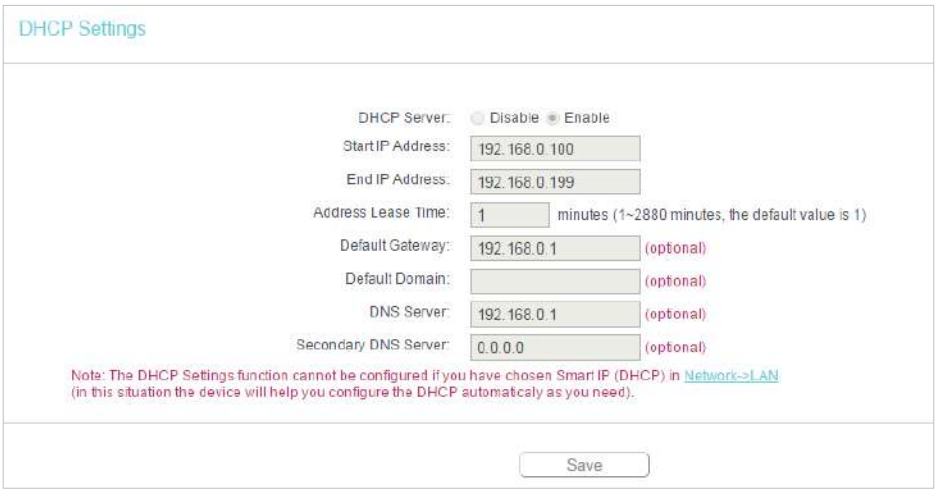


- DHCP Server - Enable or disable the DHCP server. If disabled, you must have another DHCP server within your network or else you must configure the computer manually.
- Start IP Address - Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.0.100 is the default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

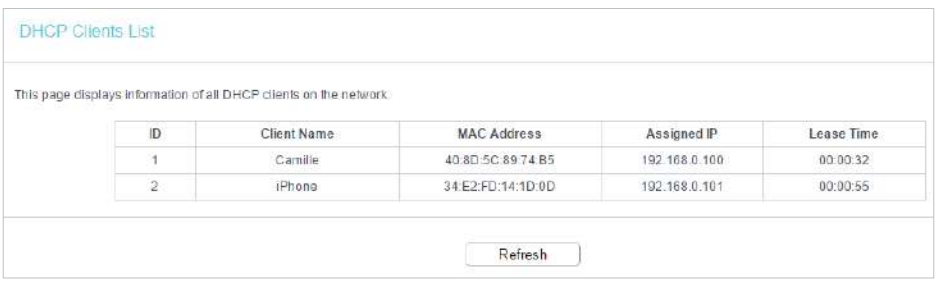
Note:

- 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 willsee the page as below.



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.



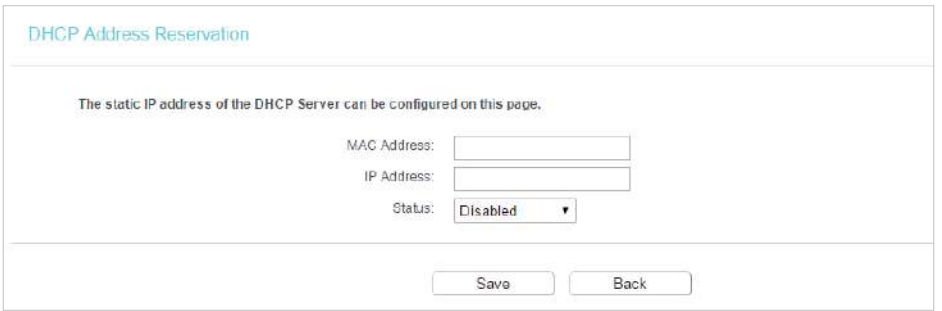
- Client Name - The name of the DHCP client.
- MAC Address - The MAC address of the DHCP client.
- Assigned IP - The IP address that the outer has allocated to the DHCP client.
- Lease Time - The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic IP address will be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

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.



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.

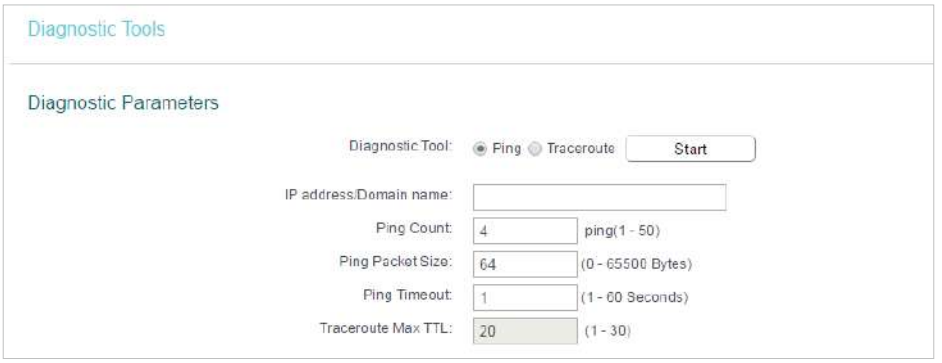
4) Click Save.

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.



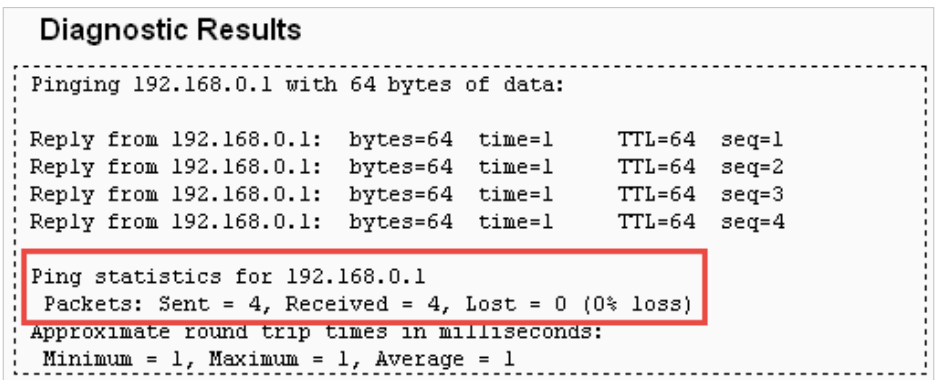
- Diagnostic Tool - Select one diagnostic tool.
  - Ping - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
  - Tracerouter - This diagnostic tool tests the performance of a connection.

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.

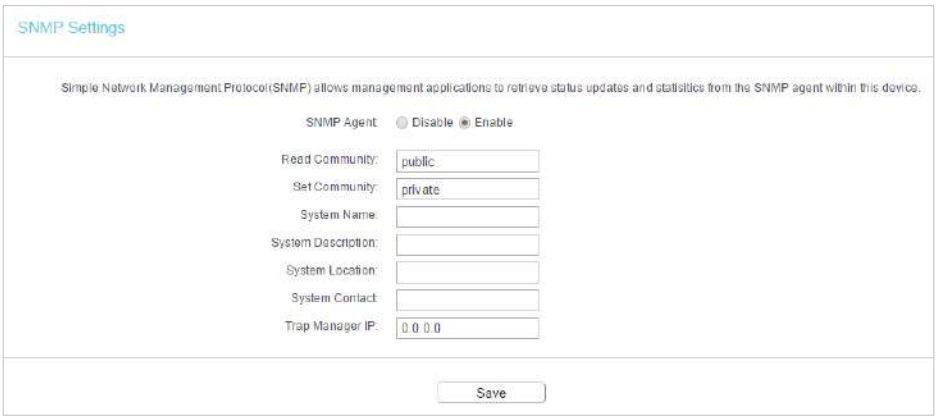
3. Click Start to check the connectivity of the internet.
4. The Diagnostic Results page displays the diagnosis result. If the result is similar to the following figure, the connectivity of the internet is fine.



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.

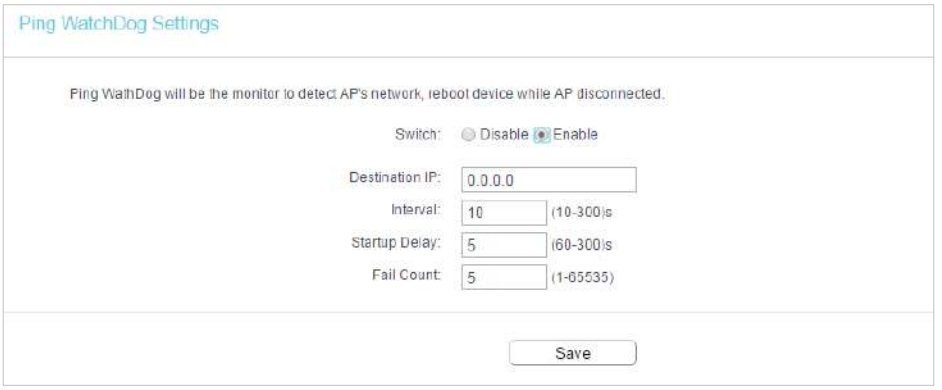


- System Name - An administratively-assigned name for this managed node.
- System Description - The software version information for this managed node.
- System Location - The physical location of this node.
- System Contact - The textual identification of the contact person for this managed node.
- 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.

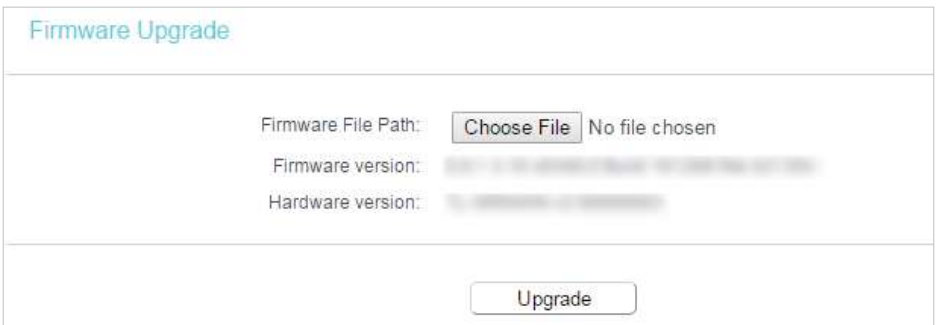


- Enable - Turn on/off Ping Watch Dog.
- Destination IP - The IP address of the target host where the Ping Watch Dog Utility is sending ping packets.
- Interval - Time interval between two ping packets which are sent out continuously.
- Startup Delay - Time delay before first ping packet is sent out 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 richening the product features, giving users a better network experience. We will release the latest firmware at TP-Link official website www.tp-link.com. You can download the lastest firmware file from the Support page of our website and upgrade the firmware to the latest version.

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



6. 7. 5. Factory Defaults

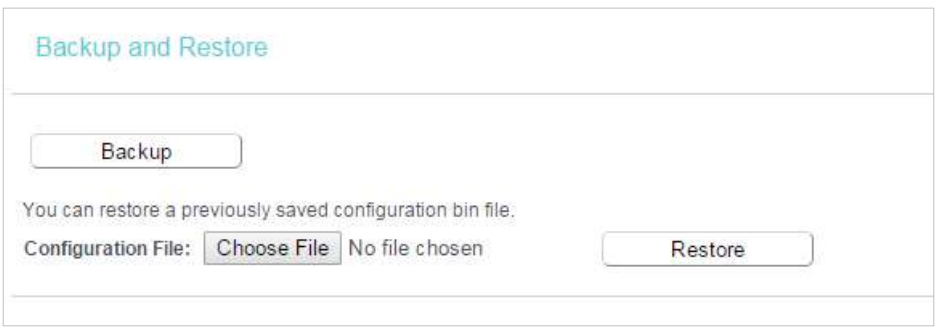
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to System Tools > Factory Defaults. Click Restore to reset all settings to the default values.

- 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:

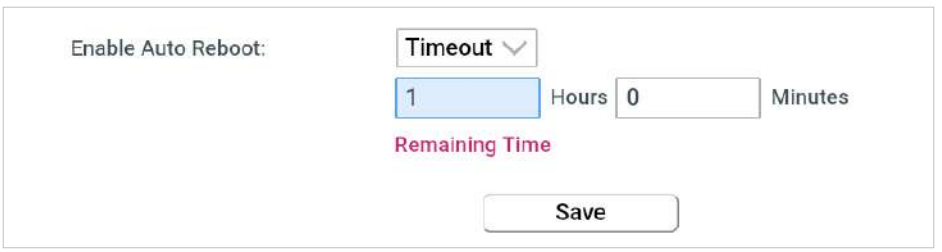
- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Working Modes.
- Change the Web Management Port.
- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router to its factory defaults (system will reboot automatically).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

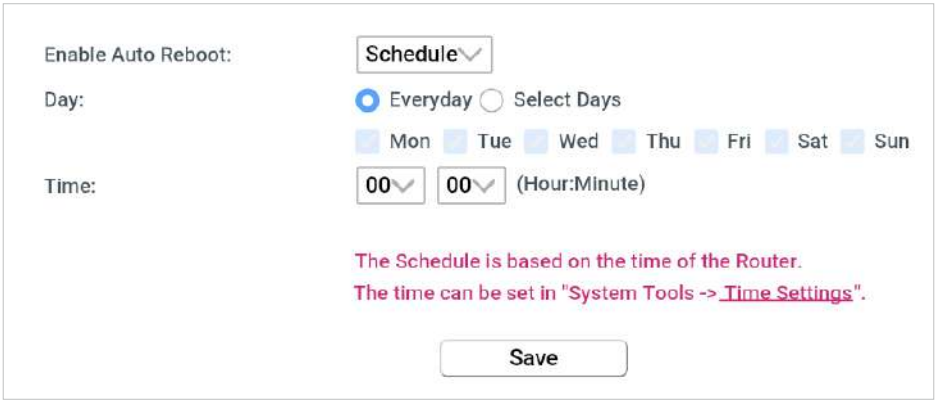
- **To reboot manually**

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.

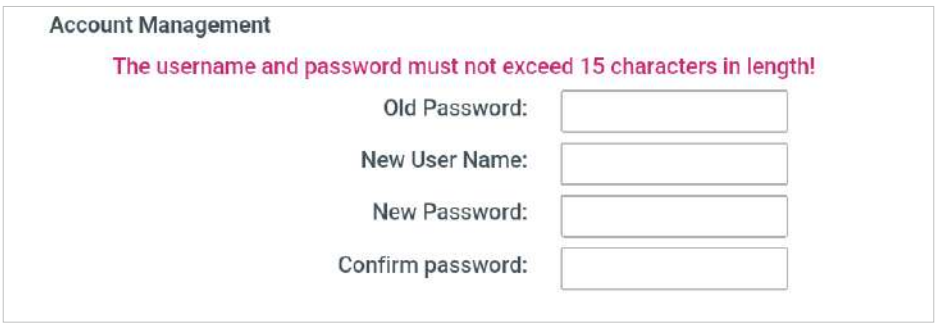


  - Select Schedule in the drop-down list of Enable Auto Reboot and specify the Time when the router reboots and Day which to decide how often it reboots.



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.



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.

- **Allow all LAN conencted 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 disbled.
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 disbled.
3. Keep the Port as default if you don't know which port to use.
4. Click Save.

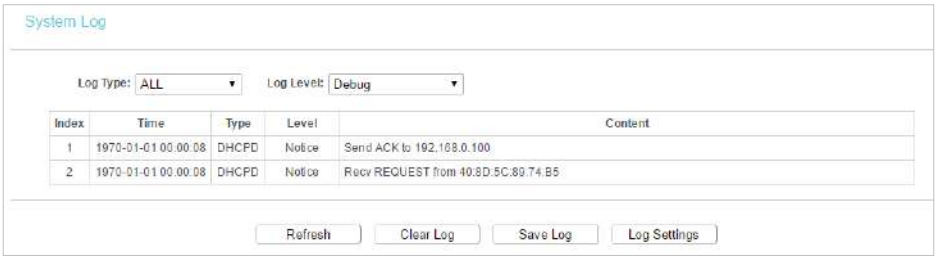
Note:
If your PC is blocked but you want to access the router again, press and hold the Reset button to reset the router to the factory defaults.

- **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.

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.



- 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.

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

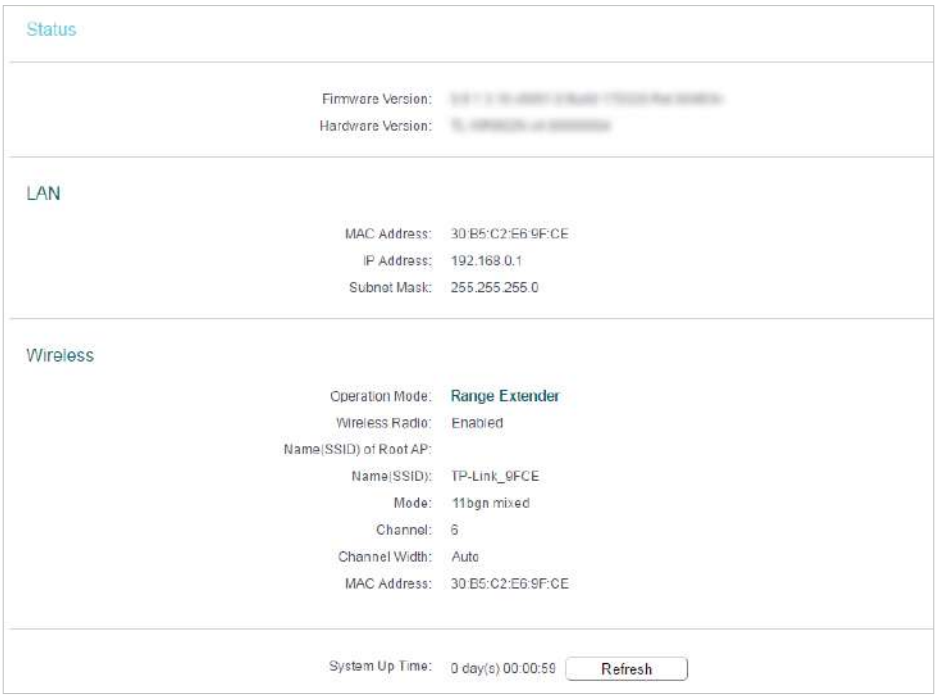
This chapter presents how to configure the various features of the router working as a range extender.

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.



- 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.

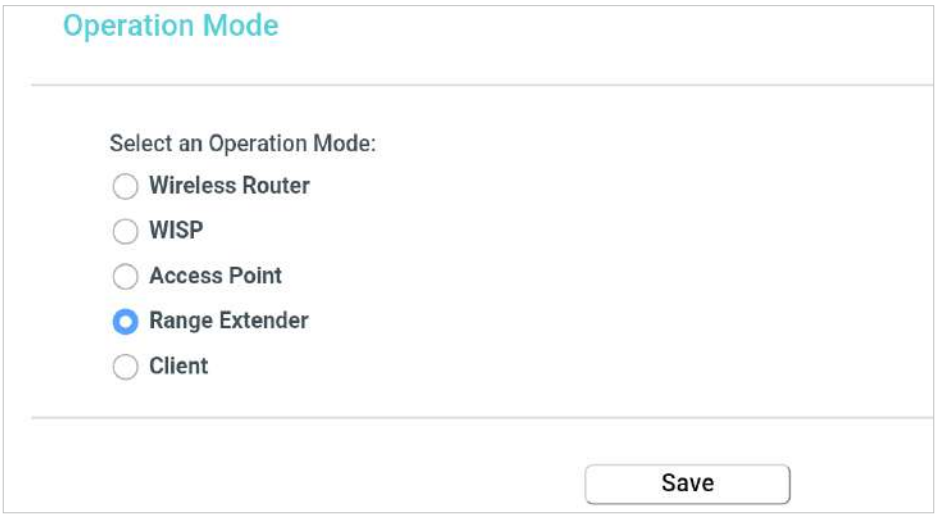
- Channel Width - The current wireless channel width in use.
- MAC Address - The physical address of the router.

- 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

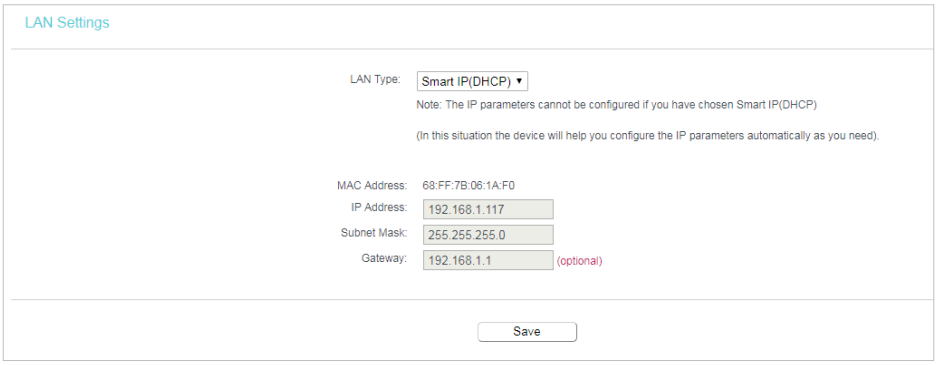
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Operation Mode.
3. Select the working mode as needed and click Save.



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.



- 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.

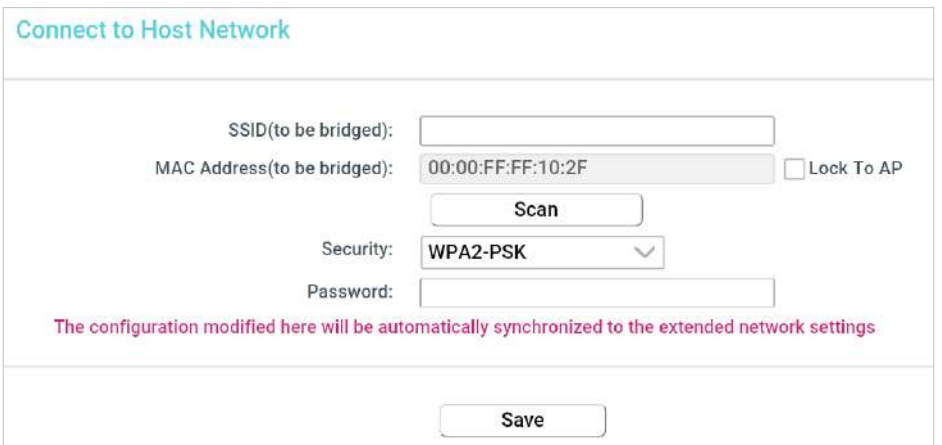
Note:

- 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.

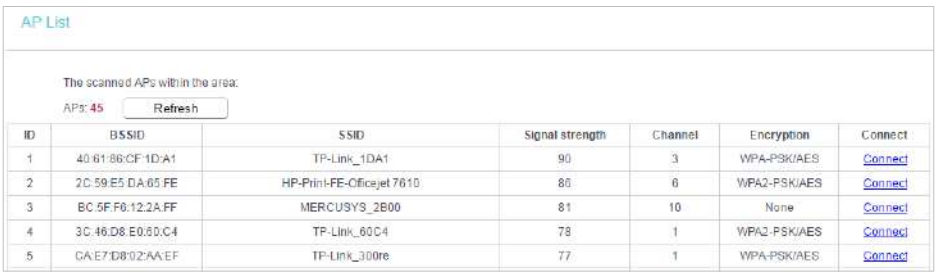
7. 4. Wireless

7. 4. 1. Connect to Network

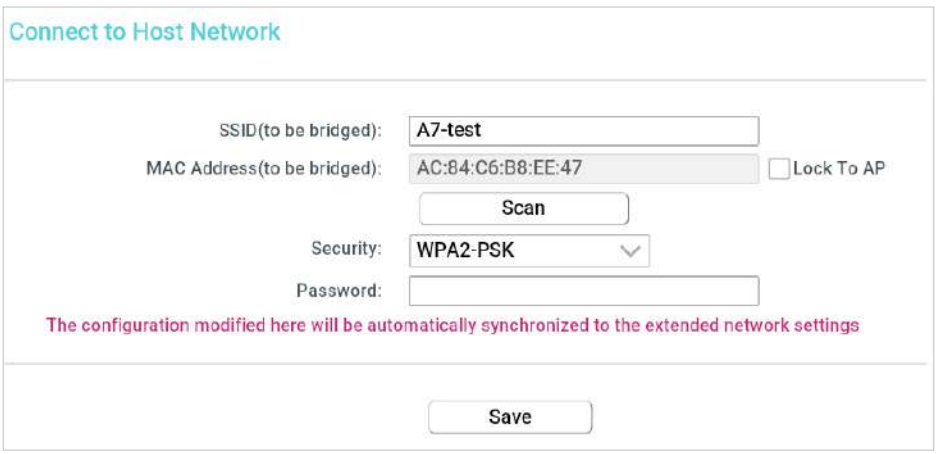
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Wireless > Connect to Network.



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



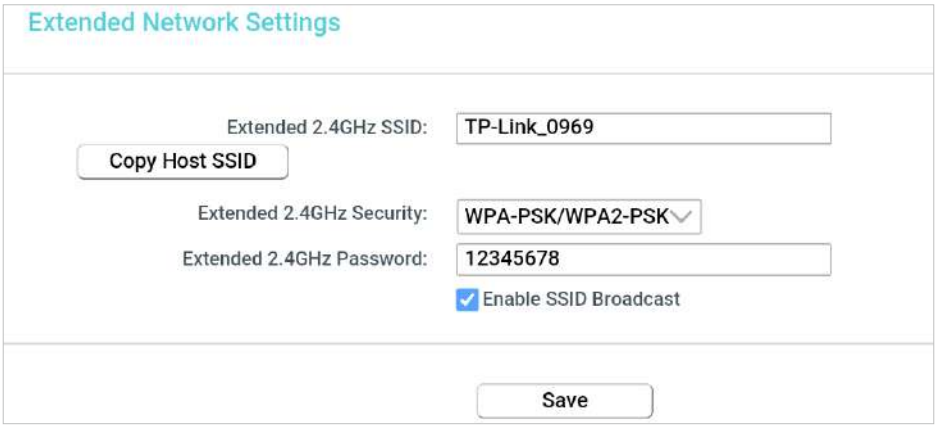
4. Enter your host network's wireless password in the Password field.



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.

7. 4. 2. Extended Network

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



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.

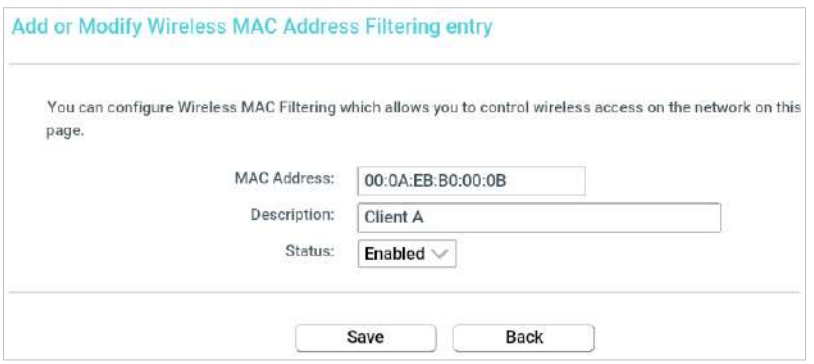
I want to:

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.



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.

Done!

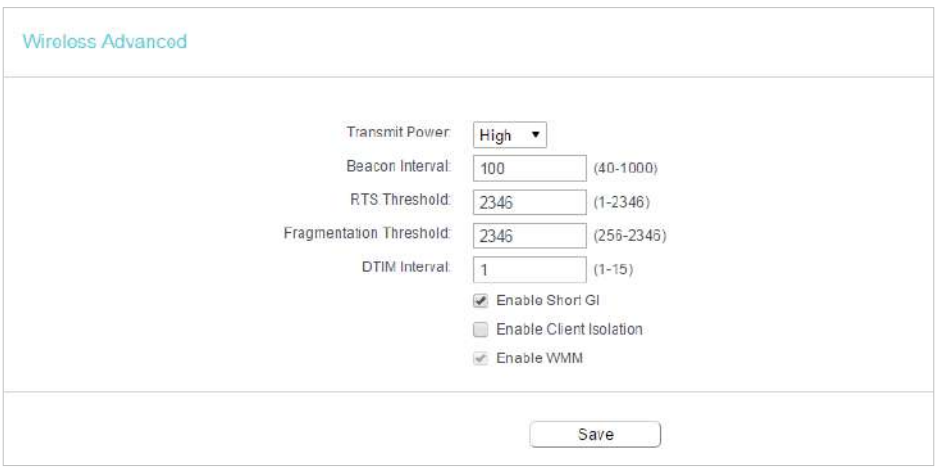
Now only client A and client B can access your network.

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.



- 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.

- MAC Address - The MAC address of the connected wireless client.
- Current Status - The running status of the connected wireless client.

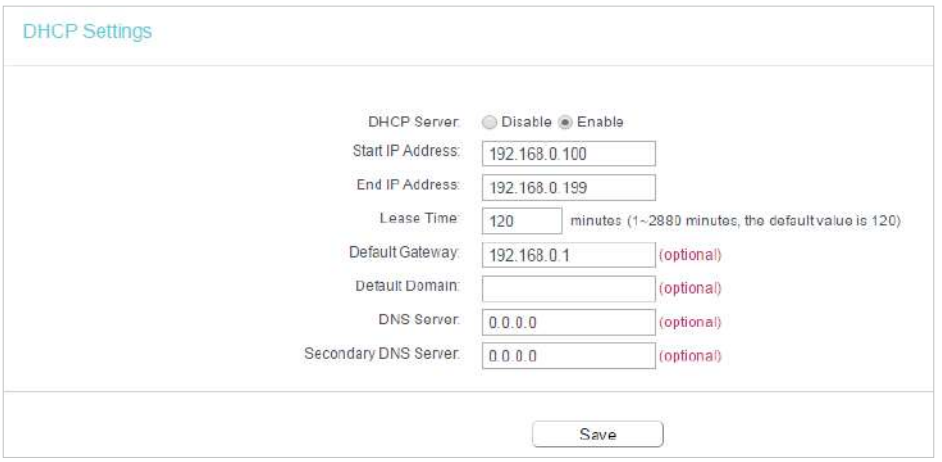
- Received Packets - Packets received by the wireless client.
- Sent Packets - Packets sent by the wireless client.
- SSID - SSID that the station associates with.

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.

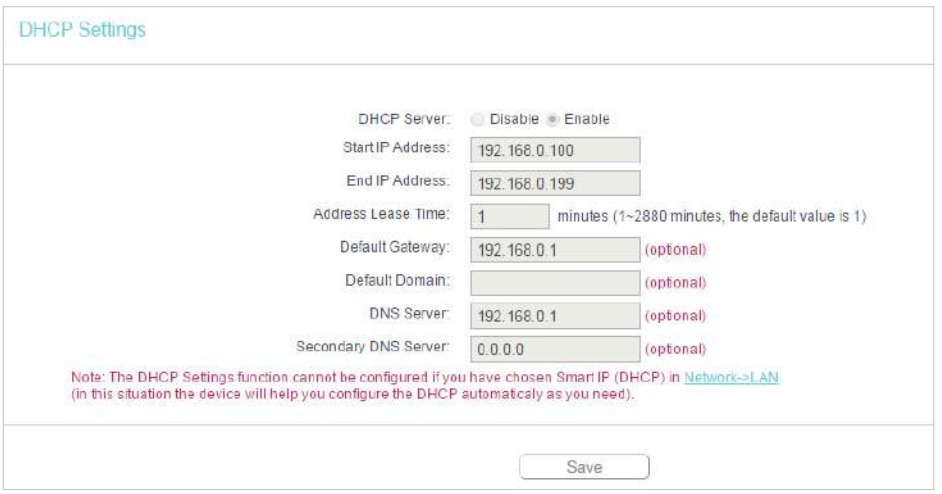


- DHCP Server - Enable or disable the DHCP server. If disabled, you must have another DHCP server within your network or else you must configure the computer manually.
- Start IP Address - Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.0.100 is the default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

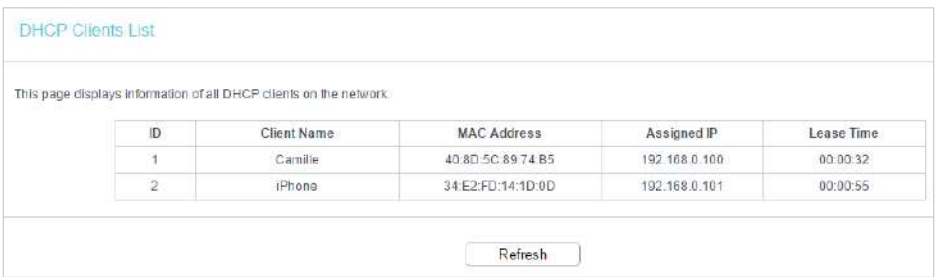
Note:

- 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 willsee the page as below.



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.



- 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.

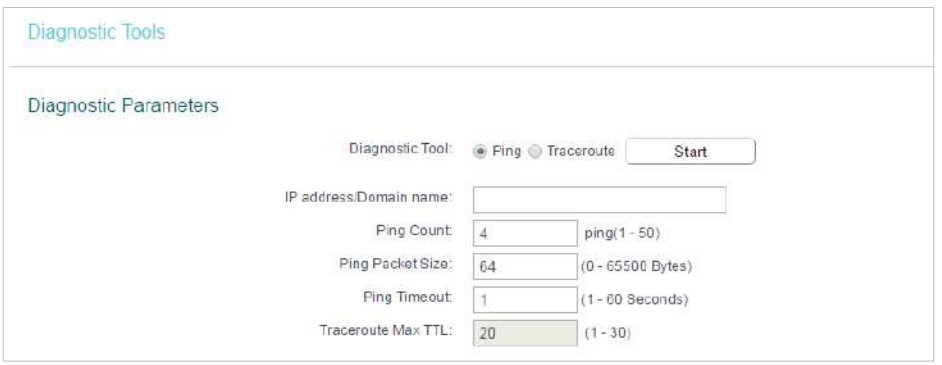
You cannot change any of the values on this page. To update this page and show the current attached devices, click Refresh.

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.



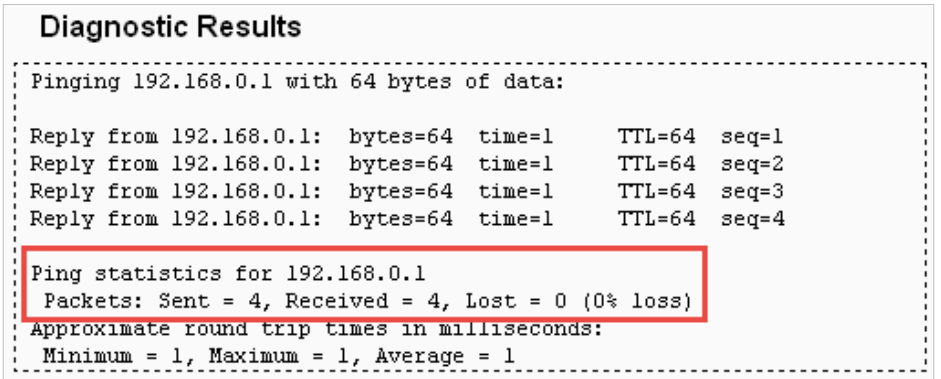
- Diagnostic Tool - Select one diagnostic tool.
  - Ping - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
  - Tracerouter - This diagnostic tool tests the performance of a connection.

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.

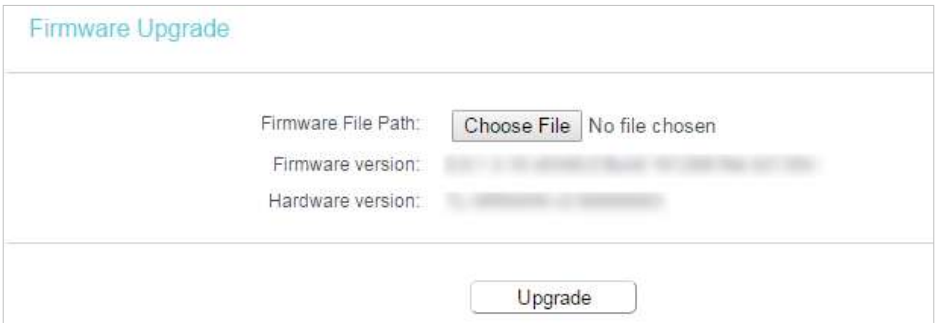
3. Click Start to check the connectivity of the internet.
4. The Diagnostic Results page displays the diagnosis result. If the result is similar to the following figure, the connectivity of the internet is fine.



7. 6. 2. Firmware Upgrade

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

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



7. 6. 3. Factory Defaults

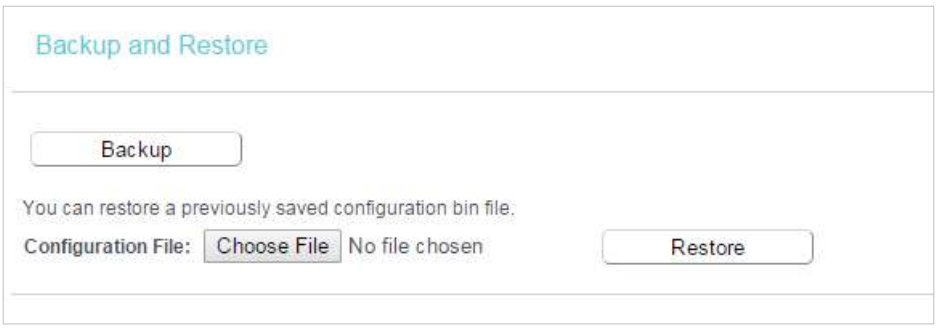
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to System Tools > Factory Defaults. Click Restore to reset all settings to the default values.

- 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.

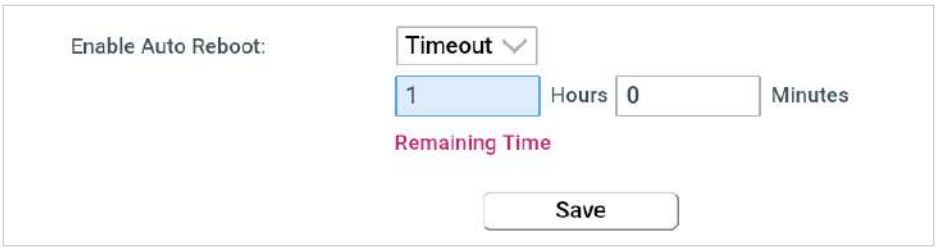
- Change the Web Management Port.
- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router to its factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically).

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

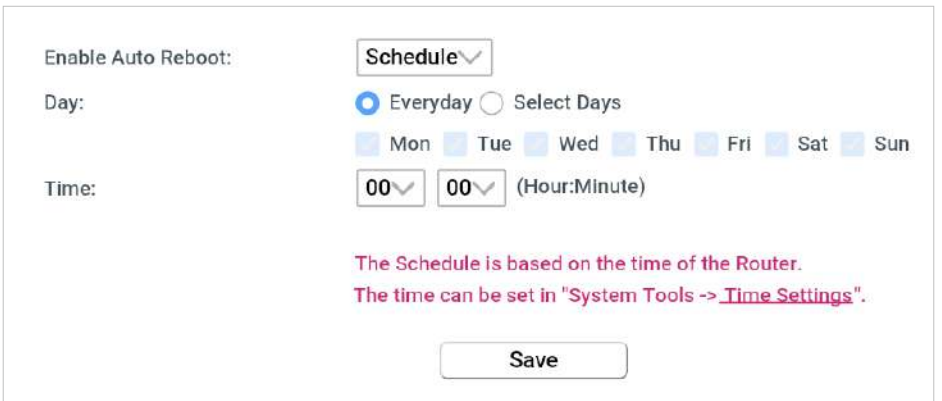
- **To reboot manually**

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

- **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.

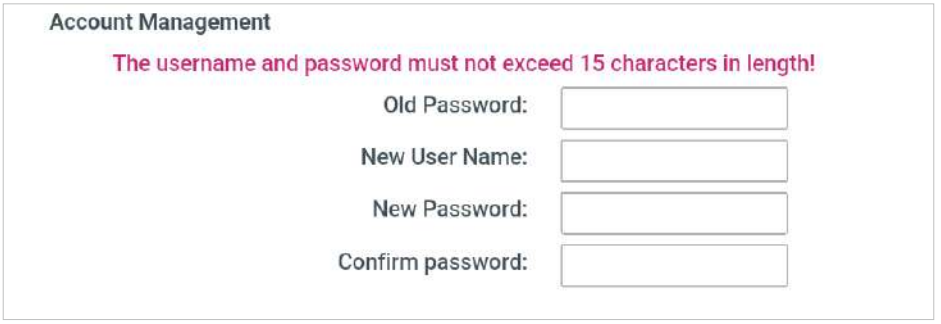


  - Select Schedule in the drop-down list of Enable Auto Reboot and specify the Time when the router reboots and Day which to decide how often it reboots.



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.



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.

- **Allow all LAN conencted 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 disbled.
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 disbled.
3. Keep the Port as default if you don't know which port to use.
4. Click Save.

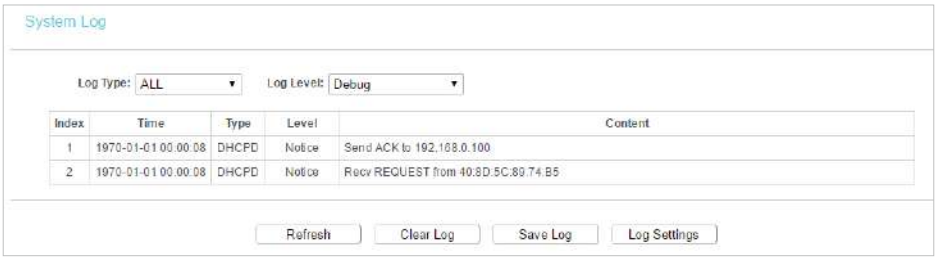
Note:
If your PC is blocked but you want to access the router again, press and hold the Reset button to reset the router to the factory defaults.

- **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

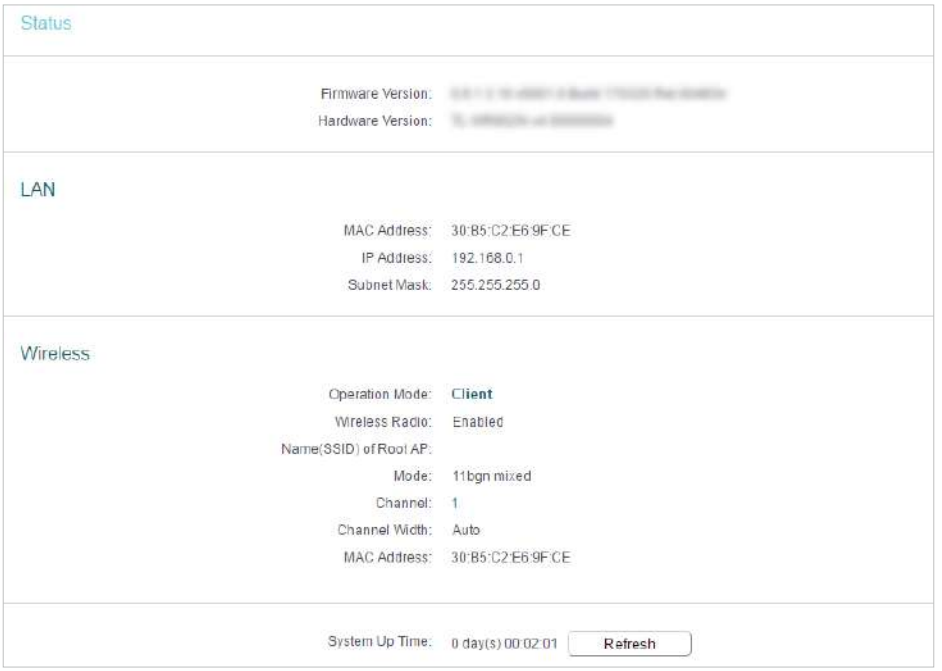
This chapter presents how to configure the various features of the router working as a client.

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.



- 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.

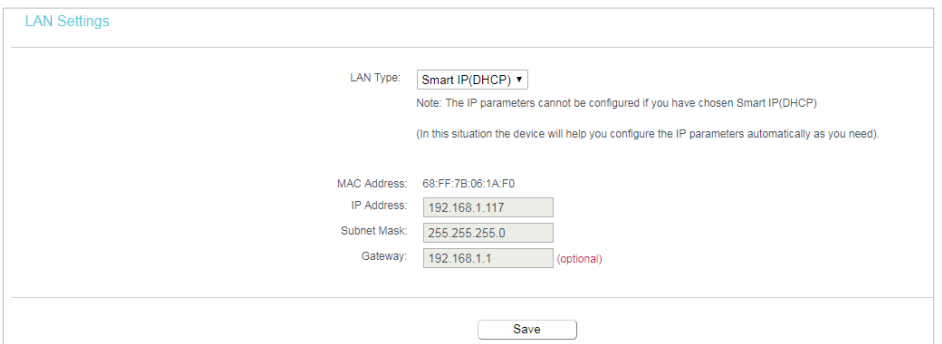
8. 2. Operation Mode

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.

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.



- 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.

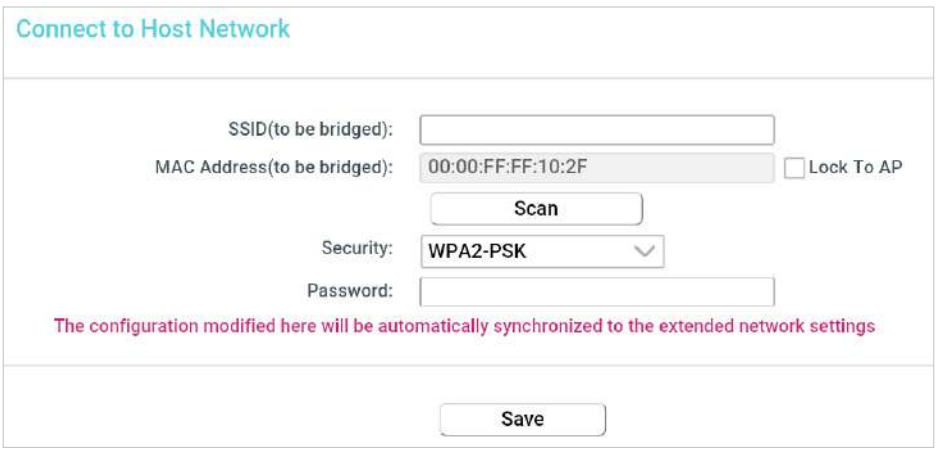
Note:

- 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

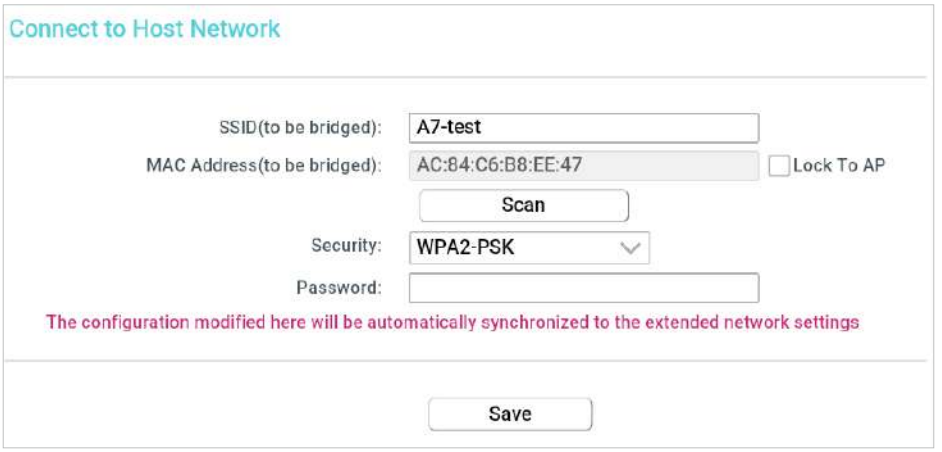
8. 4. 1. Basic Settings

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



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

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



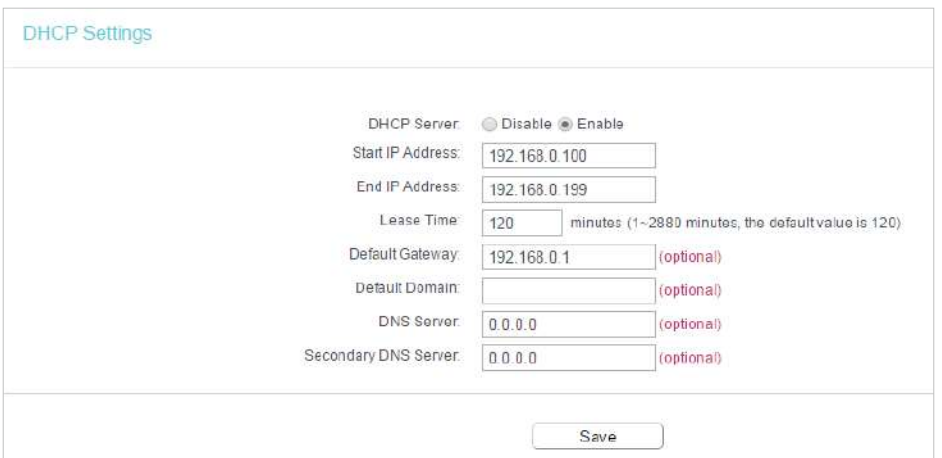
5. Tick Lock to AP checkbox if you want to restrict the device's connection to only the network with this specific MAC address.
6. Click Save.

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

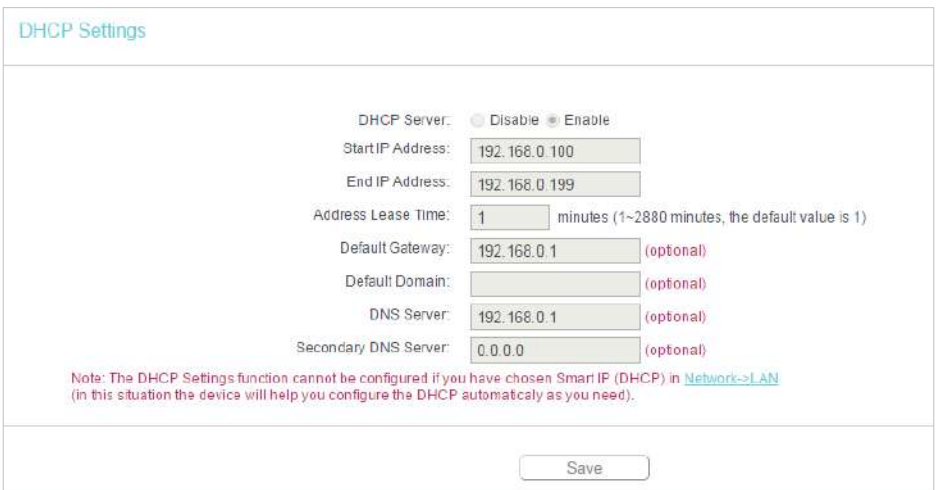
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to DHCP > DHCP Settings.
3. Specify DHCP server settings and click Save.



- DHCP 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.

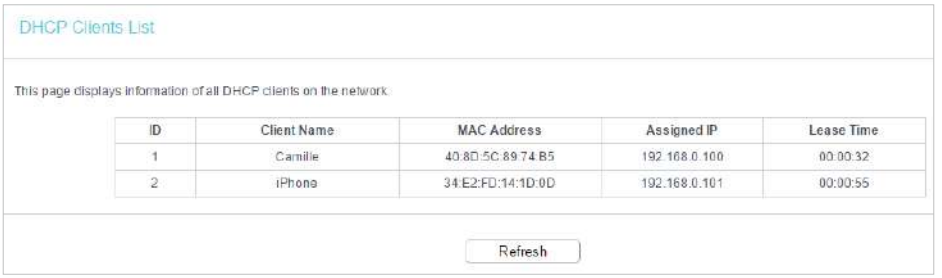
Note:

- 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 willsee the page as below.



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.



- 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.

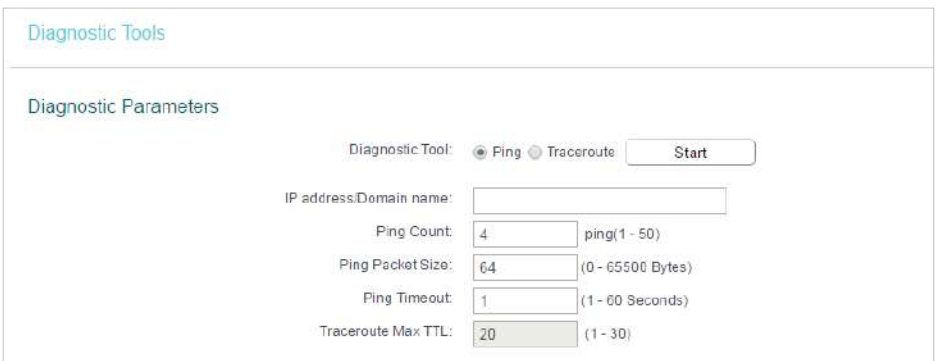
You cannot change any of the values on this page. To update this page and show the current attached devices, click Refresh.

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.



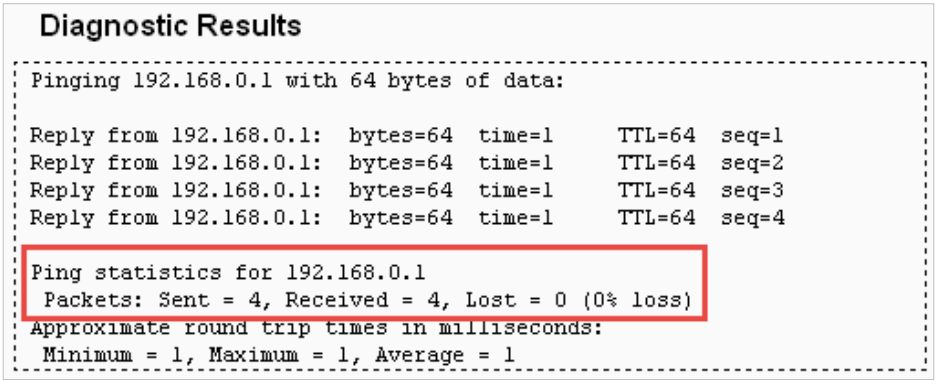
- Diagnostic Tool - Select one diagnostic tool.
  - Ping - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
  - Tracerouter - This diagnostic tool tests the performance of a connection.

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.

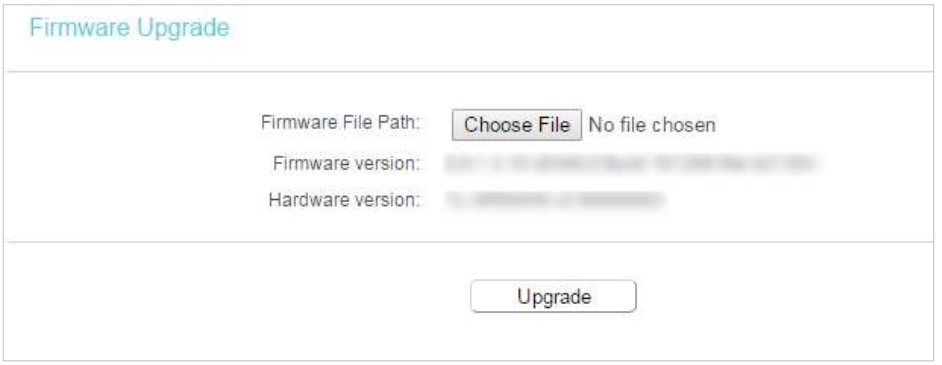
3. Click Start to check the connectivity of the internet.
4. The Diagnostic Results page displays the diagnosis result. If the result is similar to the following figure, the connectivity of the internet is fine.



8. 6. 2. Firmware Upgrade

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

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



8. 6. 3. Factory Defaults

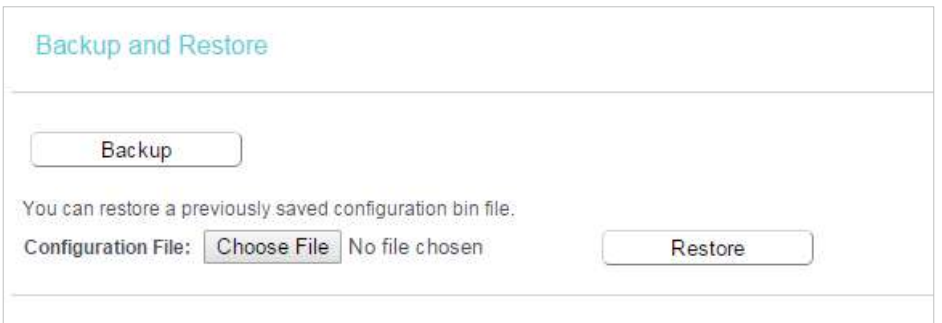
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to System Tools > Factory Defaults. Click Restore to reset all settings to the default values.

- 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.



- **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

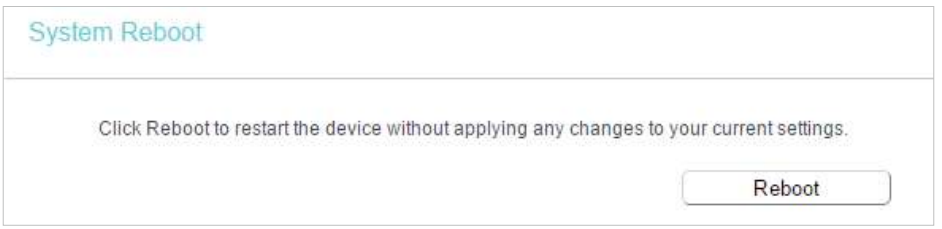
Some settings of the router will take effect only after rebooting, including:

- 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).

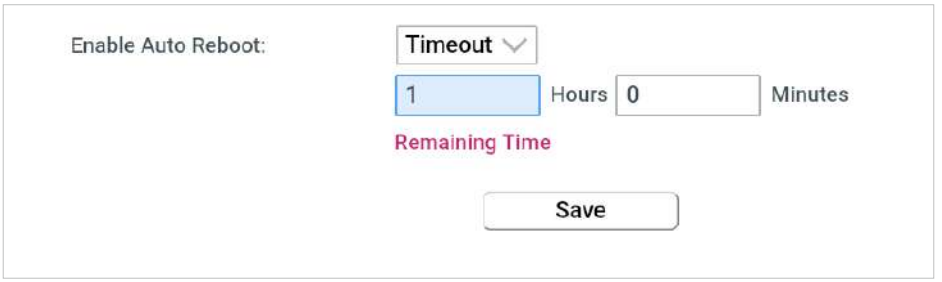
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to System Tools > Reboot.

- **To reboot manually**

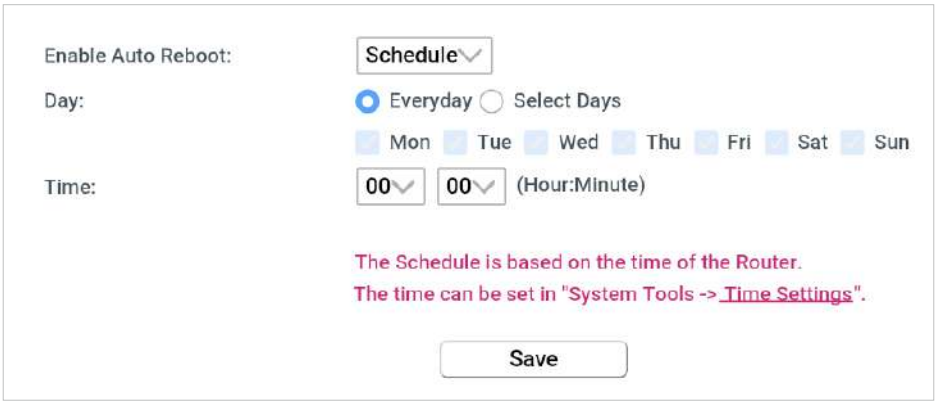
Click Reboot, and wait a few minutes for the router to rebooting.



- **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.

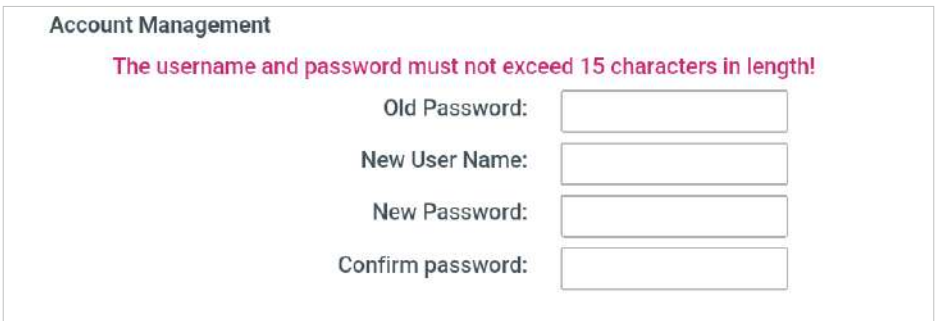


- Select Schedule in the drop-down list of Enable Auto Reboot and specify the Time when the router reboots and Day which to decide how often it reboots.



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.



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.

- **Allow all LAN conencted 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 disbled.
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**

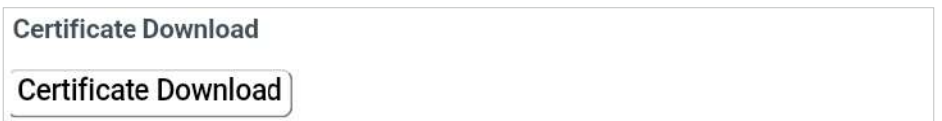
1. Enter the IP or MAC address of the host that you want to manage the router in the Available Host (IP/MAC) entry. The format of the MAC address is XX:XX:XX:XX:XX:XX (X is any hexadecimal digit).
2. If you want to access the router via both HTTPS and HTTP, please tick the Enable box in HTTPS Service column. Otherwise, keep it disbled.
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**

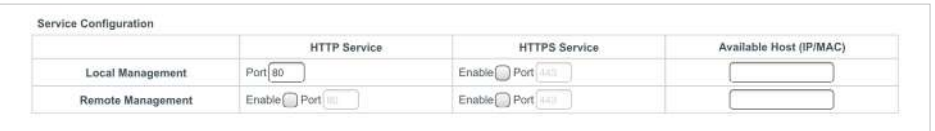
Download and install the certificate for management via HTTPS if you need it. Once the certificate is installed, warnings will not pop up when you access the router via HTTPS.



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.



- **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 disbled.
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 disbled.
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**

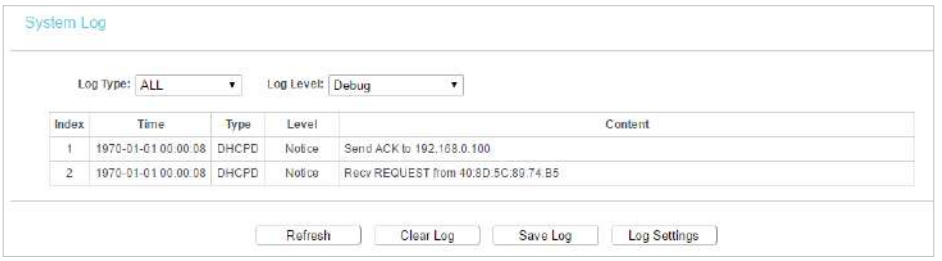
Download and install the certificate for management via HTTPS if you need it. Once the certificate is installed, warnings will not pop up when you access the router via HTTPS.

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.

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.



- 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. tp-link is a registered trademark of TP-Link Technologies Co., Ltd. Other brands and product names are trademarks or registered trademarks of their respective holders.

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

CE

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

OPERATING FREQUENCY

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