Guía de Usuario

Tabla de contenido

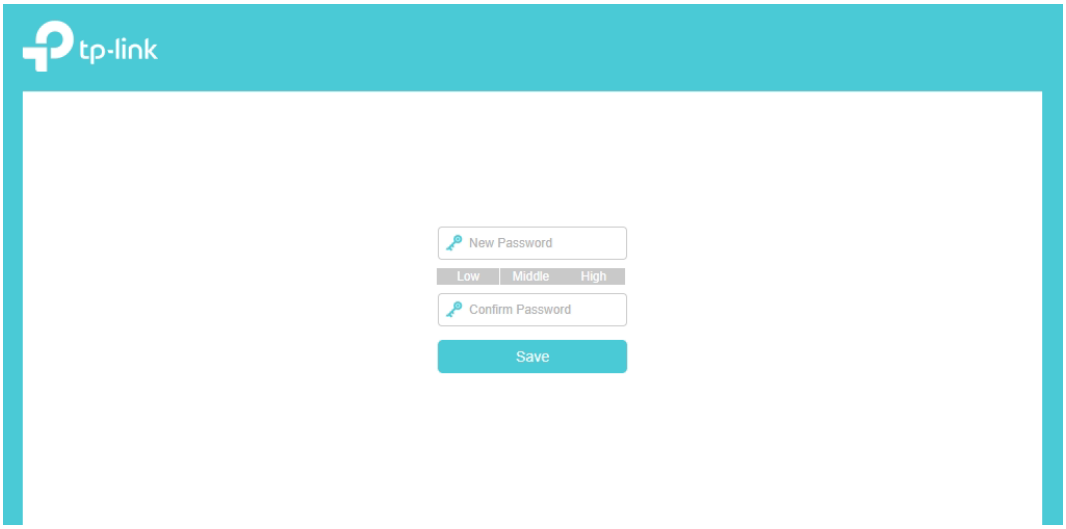
Configuraciones generales

Acceso al dispositivo

Con una utilidad basada en web, es fácil configurar y gestionar el dispositivo. La utilidad basada en web puede utilizarse en cualquier sistema operativo Windows, Mac OS o UNIX con un navegador web, como Microsoft Internet Explorer, Mozilla Firefox o Apple Safari.

Sigue los pasos que se indican a continuación para iniciar sesión en el dispositivo:

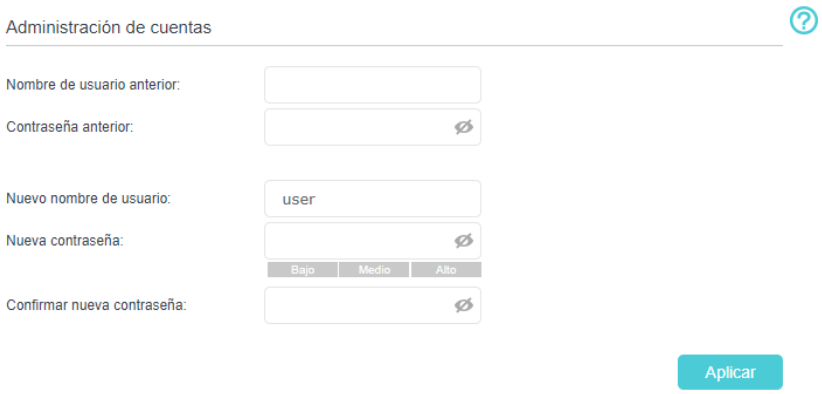
1. Configura el protocolo TCP/IP en modo “Obtener una dirección IP” automáticamente en tu ordenador.
2. Visita http://192.168.1.1 o http://192.168.0.1, en adelante siempre nos referiremos a http://192.168.1.1
3. Establece la contraseña para acceder al dispositivo.



Cambiar la contraseña

Sigue los pasos que se indican a continuación para cambiar tu contraseña de usuario:

1. Visita http://192.168.1.1 e inicia sesión con el usuario “user” y la contraseña que se configuro en el primer inicio.
2. Accede a la página ***Avanzado > Herramientas del Sistema > Administración***
3. En “Administración de cuentas”, escribe tu nueva contraseña en “Nueva contraseña”, repite la nueva contraseña en “Confirmar nueva contraseña”.
4. Haz clic en “Aplicar”.

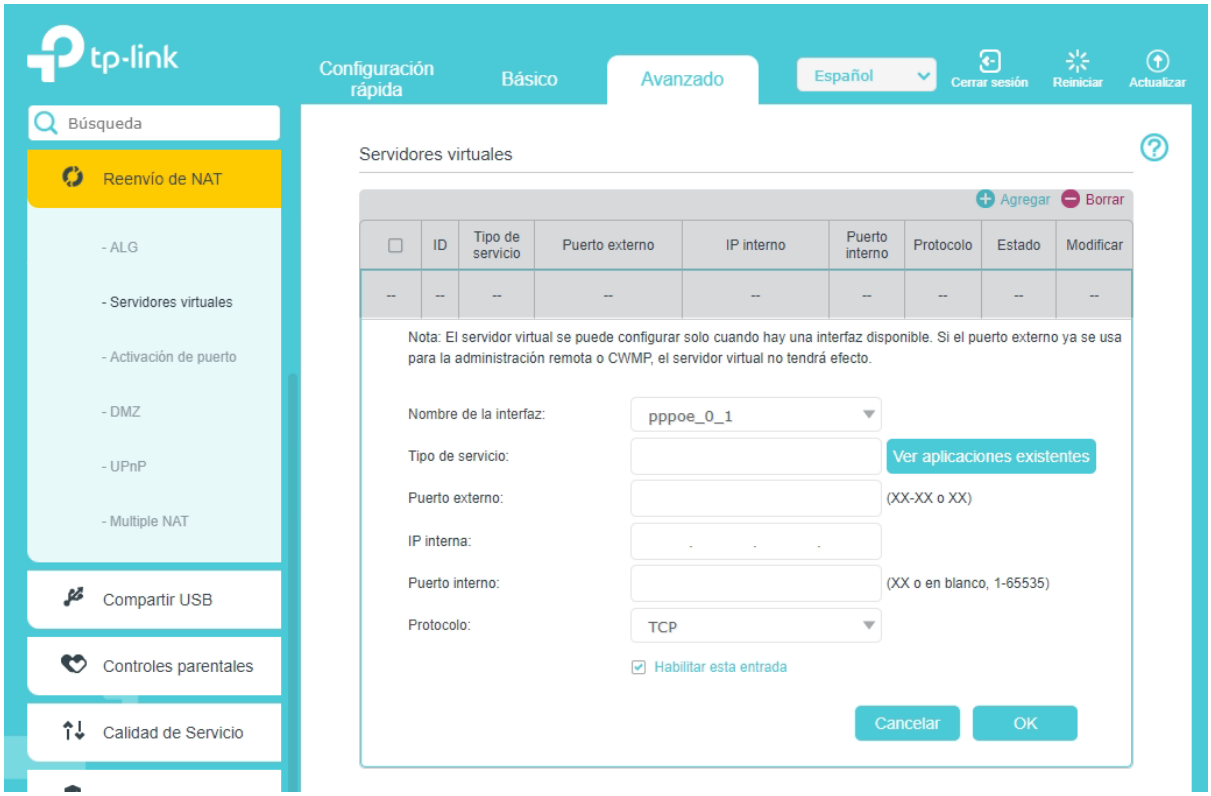


Abrir o cerrar puertos

Los servidores virtuales se utilizan para configurar servicios públicos en la red local. Un servidor virtual se define como un puerto externo, y todas las peticiones de Internet a este puerto externo se redirigirán a un dispositivo designado, que debe configurarse con una dirección IP estática o reservada.

Sigue los pasos que se indican a continuación para abrir o cerrar puertos en el dispositivo:

1. Visita http://192.168.1.1 e inicia sesión con el usuario “user” y la contraseña que se configuro en el primer inicio.
2. Accede a la página ***Avanzado > Reenvío NAT > Servidores Virtuales*** y haz clic en “Agregar”



1. Selecciona un **nombre** de interfaz en la lista desplegable.
2. Haz clic en “Ver aplicaciones existentes” para seleccionar un servicio de la lista y rellenar automáticamente el número de puerto adecuado en los campos “Puerto externo” y “Puerto interno”. Si el servicio no aparece en la lista, introduce el número de “Puerto externo” (por ejemplo, 21) o un intervalo de puertos (por ejemplo, 21-25). Deja el “Puerto interno” en blanco si es el mismo que el “Puerto externo” o introduce un número de puerto específico (por ejemplo, 21) si el “Puerto externo” es un puerto único.
3. Introduce la dirección IP del ordenador que ejecuta la aplicación de servicio en el campo “IP interna”.
4. Selecciona un protocolo para la aplicación de servicio (TCP, UDP o Todos) en la lista desplegable “Protocolo”.
5. Selecciona “Habilitar esta entrada”.
6. Haz clic en “OK”.

Consejos

Si deseas desactivar esta entrada, haz clic en el icono de la **bombilla** (1). Se recomienda mantener la configuración predeterminada de “Puerto interno” y “Protocolo” si no tienes claro qué puerto o protocolo utilizar.

Si el dispositivo host local aloja más de un tipo de servicios disponibles, deberás crear una regla para cada servicio. Ten en cuenta que el puerto externo **NO** debe solaparse.

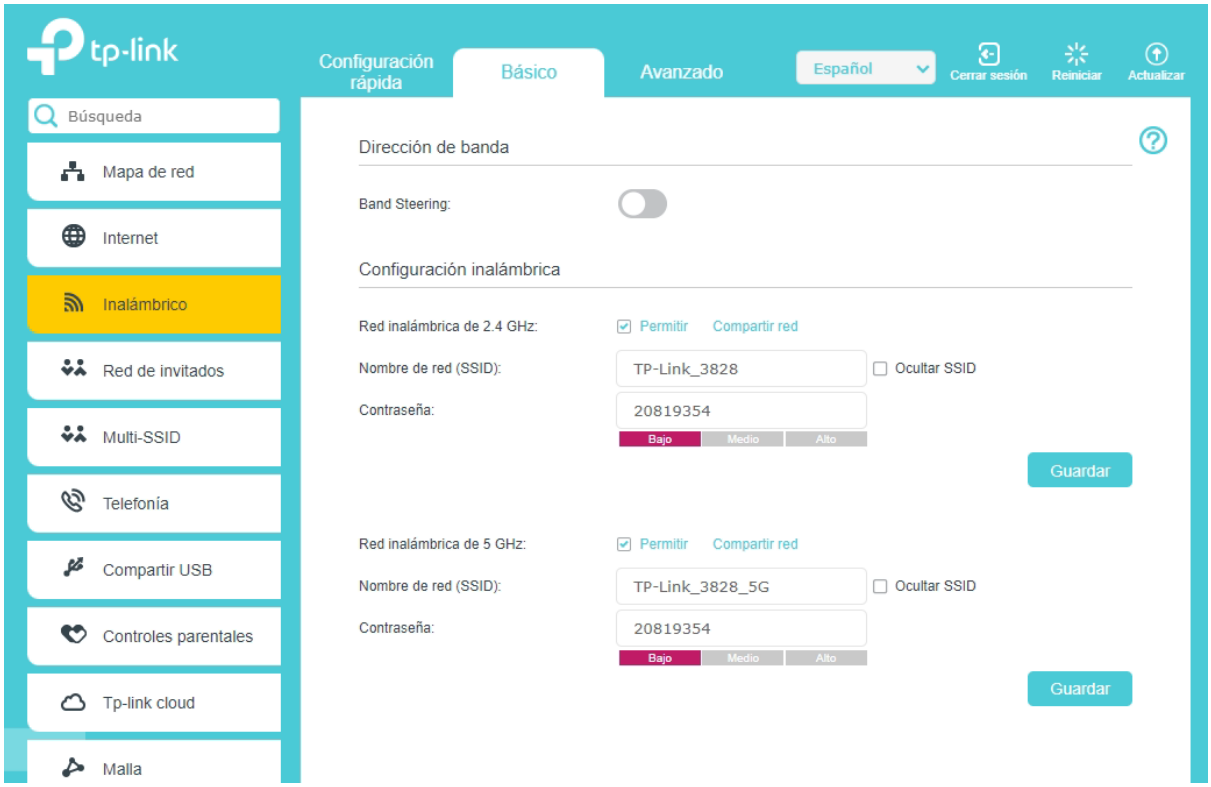
(1)Cuando un usuario crea una regla para abrir puertos, aparece una regla webUI y se visualiza un icono de bombilla.

Configuración red 2,4GHz y 5GHz

El nombre y la contraseña de la red inalámbrica (SSID) y la opción de seguridad del dispositivo vienen pre - configurados de fábrica. El SSID y la contraseña preestablecidos se encuentran en la etiqueta del producto. Puedes personalizar la configuración inalámbrica según tus necesidades.

Sigue los pasos que se indican a continuación para cambiar tu configuración inalámbrica:

1. Visita http://192.168.0.1 e inicia sesión con el usuario “user” y la contraseña que se configuro en el primer inicio.
2. Accede a la página **Básico > Inalámbrico**



Habilitar/Desactivar funciones inalámbricas:

La red inalámbrica está activada por defecto. Si deseas desactivar la función inalámbrica del dispositivo, simplemente desactiva las casillas de verificación “Permitir”. En este caso, todos los ajustes inalámbricos no serán válidos.

Modificar SSID y contraseña:

Introduce un nuevo SSID (32 caracteres como máximo) en el campo Nombre de red (SSID) y una nueva contraseña en el campo “Contraseña” y haz clic en “Guardar”. El SSID y la contraseña distinguen entre mayúsculas y minúsculas.

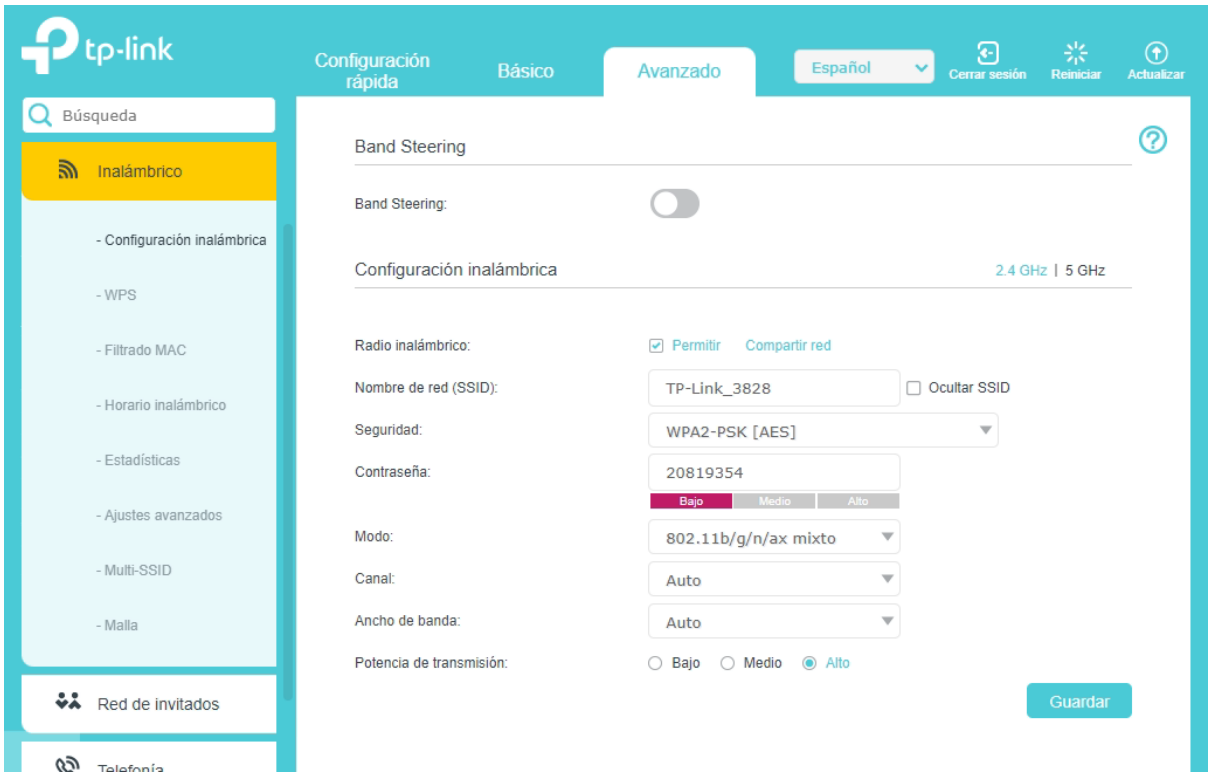
Ocultar SSID:

Selecciona “Ocultar SSID” y tu SSID no se difundirá. Tu SSID no se mostrará en tus dispositivos inalámbricos cuando busques redes inalámbricas locales y tendrás que unirte manualmente a la red.

Configuración red 2,4GHz y 5GHz (Avanzada)

Sigue los pasos que se indican a continuación para cambiar tu configuración inalámbrica (Avanzada):

1. Visita http://192.168.1.1 e inicia sesión con el usuario “user” y la contraseña que se configuro en el primer inicio.
2. Accede a la página ***Avanzado > Inalámbrico > Configuración inalámbrica***



Modificar Modo o Canal:

Selecciona el modo o el canal de la red inalámbrica y haz clic en “Guardar” para que la configuración sea efectiva.

Modo:

Selecciona el modo de transmisión deseado:

- **802.11b/g/n mixto:** Selecciona esta opción si estás utilizando una combinación de clientes inalámbricos 802.11b, 11g y 11n.
- **802.11b/g/n/ax mixto:** Selecciona esta opción si estás utilizando una combinación de clientes inalámbricos 802.11b, 11g, 11n y 11ax.
- **802.11a/n/ac mixto:** Selecciona esta opción si utilizas una combinación de clientes inalámbricos 802.11a, 11n y 11ac.
- **802.11a/n/ac/ax mixto:** Selecciona esta opción si estás utilizando una combinación de clientes inalámbricos 802.11a, 11n, 11ac y 11ax.

Nota: Cuando se selecciona el modo solo 802.11n, solo las estaciones inalámbricas 802.11n pueden conectarse al dispositivo.

Se recomienda encarecidamente seleccionar 802.11b/g/n mixto (para 2,4 GHz) y 802.1 a/n/ac/ax mixto (para 5 GHz), y todas las estaciones inalámbricas 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac y 802.11ax podrán conectarse al dispositivo.

Canal:

Selecciona el canal que deseas utilizar en la lista desplegable. Este campo determina la frecuencia de funcionamiento que se utilizará. No es necesario cambiar el canal inalámbrico a menos que observes problemas de interferencias con otro punto de acceso cercano.

Modificar Ancho de Canal:

Selecciona el ancho de canal en la lista desplegable. La configuración por defecto es “Auto”, que puede ajustar el ancho de canal para tus clientes de forma automática.

Modificar Potencia:

Selecciona “Baja/Media/Alta” para especificar la potencia de transmisión de datos. La configuración predeterminada y recomendada es “Alta”.

Modificar Seguridad:

Selecciona una opción de la lista desplegable “Seguridad” y configura los parámetros deseados.

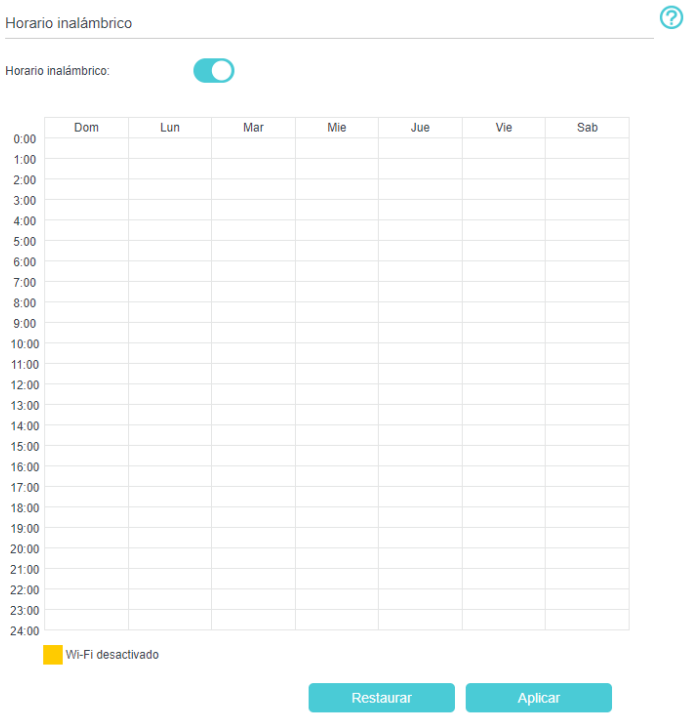
El dispositivo dispone de 4 opciones:

1. Sin seguridad
2. WPA-PSK[TKIP]+WPA2- PSK[AES]
3. WPA2-PSK[AES]
4. WPA2-PSK[AES]+WPA3-Personal

WPA3 utiliza el estándar más reciente y el nivel de seguridad es el más alto. Te recomendamos que no cambies la configuración predeterminada a menos que sea necesario.

Programación de horario inalámbrico

1. Accede a la página ***Avanzado > Inalámbrico > Horario Inalámbrico***
2. Activa la función de programación inalámbrica



Haz clic en “Añadir” para establecer la hora de desconexión inalámbrica y haz clic en “Aplicar” para que la configuración sea efectiva.

Habilitar red de invitados

Sigue los pasos que se indican a continuación para habilitar una red de invitados inalámbrica:

1. Accede a http://192.168.1.1 e inicia sesión con el usuario “user” y la contraseña que se configuro en el primer inicio.
2. Ve a la página ***Básico > Red de Invitados***
3. Crea una red de invitados según sea necesario:

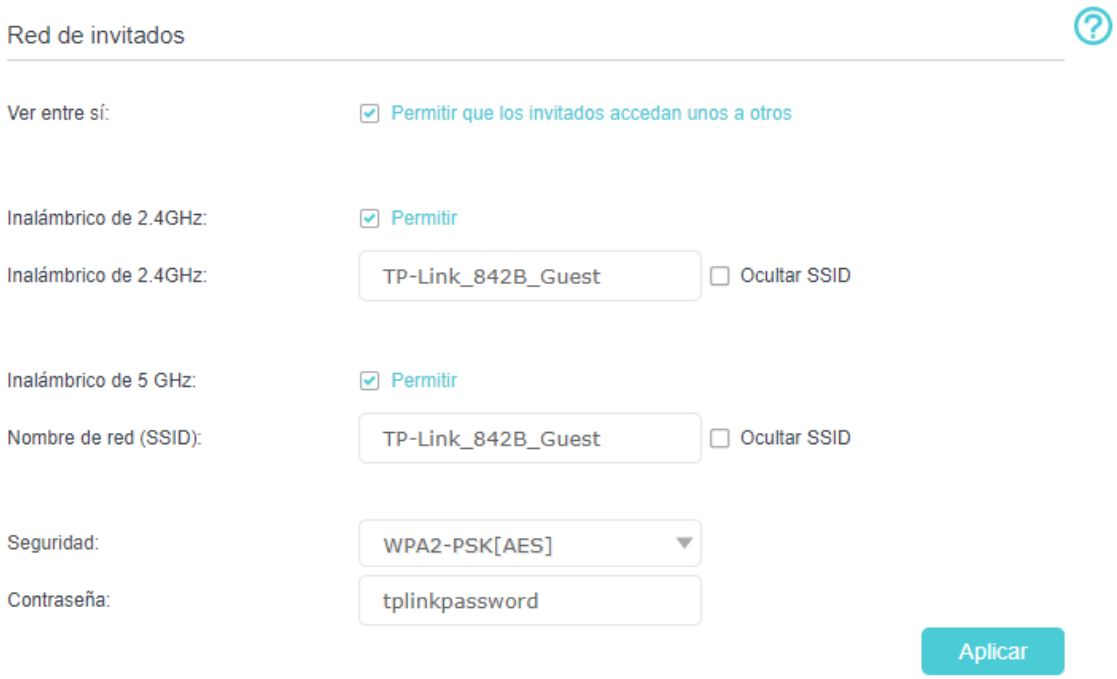
- Permitir que los invitados se vean entre sí:

Marca esta casilla si deseas permitir que los dispositivos inalámbricos de tu red de invitados se comuniquen entre sí a través de métodos como vecinos de red y Ping.

- Marca la casilla “Habilitar” para la red inalámbrica de 2,4 GHz o 5 GHz.

- Personaliza el SSID: No selecciones “Ocultar SSID” a menos que desees que tus invitados introduzcan manualmente el SSID para acceder a la red de invitados.

- Selecciona el tipo de “Seguridad” y personaliza tu propia contraseña. Si se selecciona “Sin seguridad”, no se necesita contraseña para acceder a la red de invitados (No recomendado).

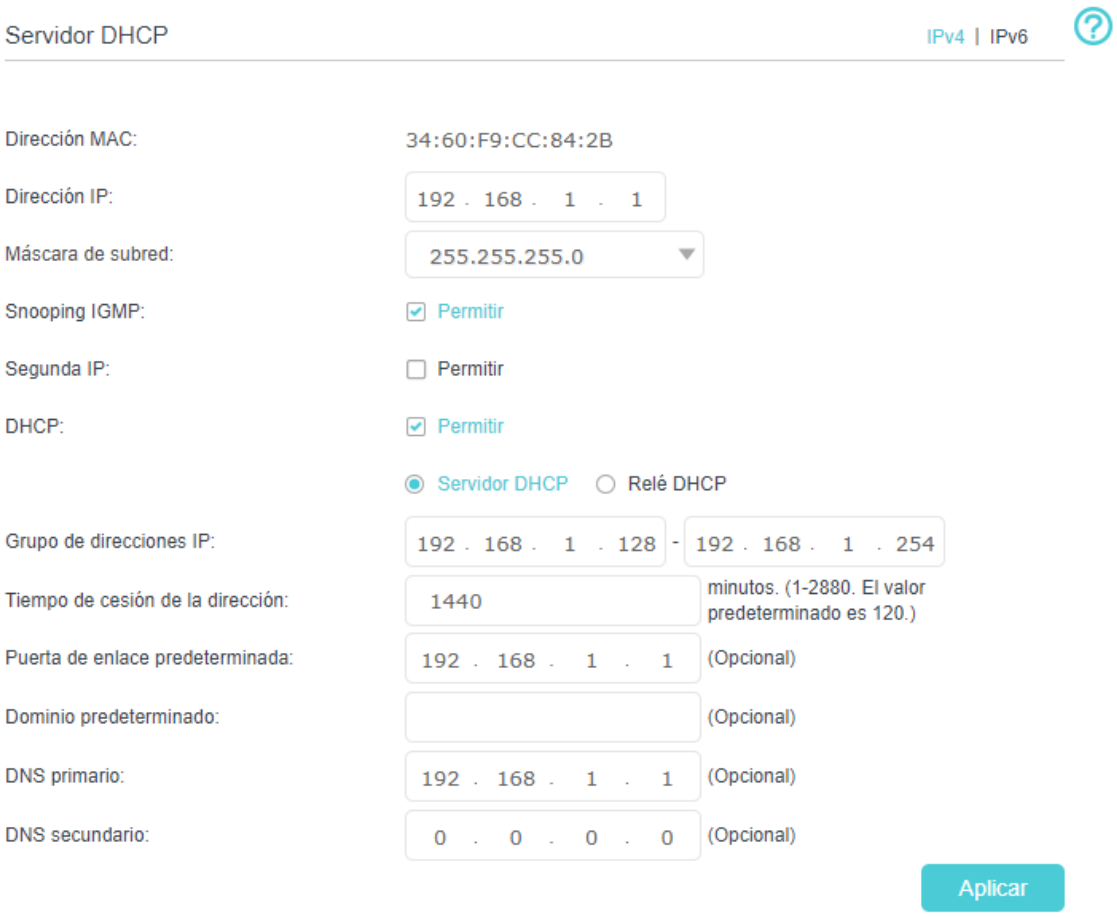


Configuración LAN

El dispositivo está preconfigurado con una IP LAN por defecto 192.168.1.1, que puedes utilizar para iniciar sesión en tu página de gestión web. La dirección IP LAN, junto con la máscara de subred, también define la subred en la que se encuentran los dispositivos conectados. Si la dirección IP entra en conflicto con otro dispositivo de tu red local o tu red requiere una subred IP específica, puedes cambiarla.

Sigue los pasos que se indican a continuación para cambiar tu dirección IP:

1. Visita http://192.168.1.1 e inicia sesión con el usuario “user” y la contraseña que se configuro en el primer inicio.
2. Accede a la página ***Avanzado > Red > Configuración de LAN***



1. Introduce una nueva dirección IP adecuada a tus necesidades.
2. Selecciona la máscara de subred en la lista desplegable. La máscara de subred junto con la dirección IP identifica la subred IP local.
3. Mantén activado “IGMP Snooping” por defecto. “IGMP snooping” es el proceso de escuchar el tráfico de red IGMP (Internet Group Management Protocol). Esta función impide que los hosts de una red local reciban tráfico de un grupo de multidifusión al que no se hayan unido explícitamente.
4. Puedes configurar la segunda IP y la máscara de subred del dispositivo para la interfaz LAN a través de la cual también puedes acceder a la página de gestión web.
5. DNS primario y secundario: Puedes configurar servidores DNS diferentes a los predeterminados para tu red LAN.
6. Haz clic en “Aplicar” para hacer efectiva la configuración.

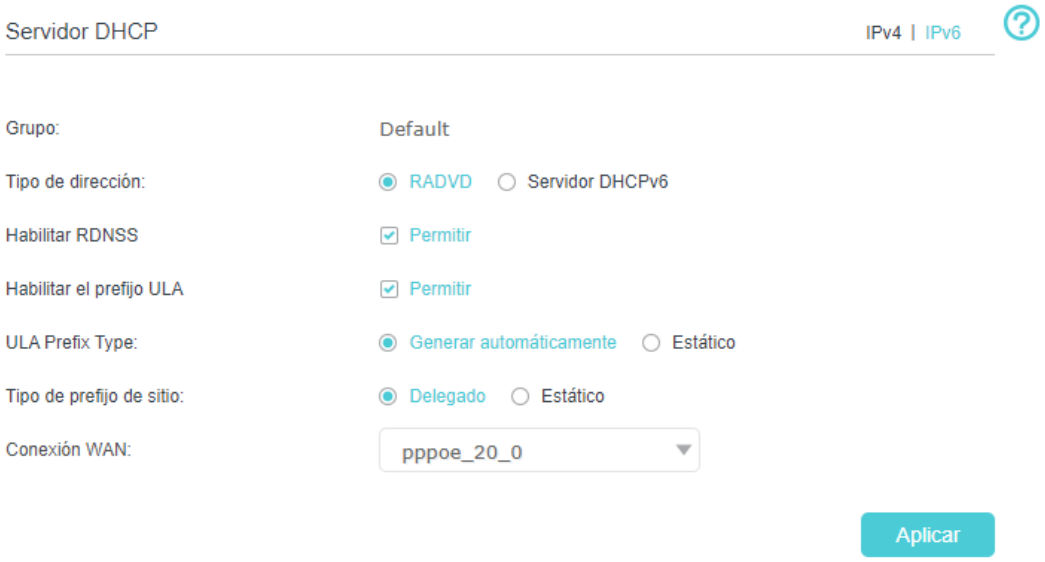
Activación y desactivación de IPV4/IPV6

Basado en el protocolo IPv6, el dispositivo proporciona dos formas de asignar direcciones LAN IPv6:

- Configurar el tipo de dirección RADVD (Dispositivo Advertisement Daemon).
- Configurar el tipo de dirección DHCPv6 Server.

1. Visita http://192.168.1.1 e inicia sesión con el usuario “user” y la contraseña que se configuro en el primer inicio.
2. Accede a la página ***Avanzado > Red > Configuración de LAN***
3. Selecciona IPv6 para configurar los parámetros de la LAN IPv6.

Configurar el tipo de dirección RADVD

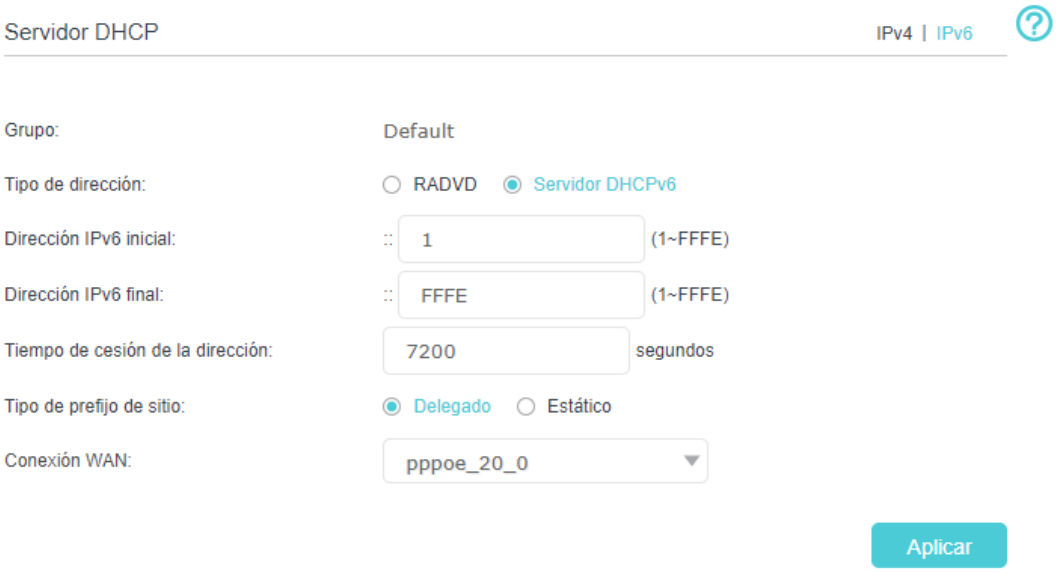


1. Selecciona “RADVD” como tipo de dirección para que el dispositivo asigne prefijos de direcciones IPv6 a los hosts.

Nota: No selecciones las casillas “Habilitar RDNSS” y “Habilitar prefijo ULA” a menos que te lo exija tu ISP, de lo contrario, es posible que no puedas acceder a la red IPv6.

2. Mantén el “Tipo de prefijo del sitio” como la configuración por defecto “Delegado”. Si tu ISP ha proporcionado un prefijo de sitio IPv6 específico, selecciona “Estático” e introduce el prefijo.
3. Mantén “Conexión WAN” como configuración por defecto.
4. Haz clic en “Aplicar” para hacer efectivos los ajustes.

Configurar el tipo de dirección del servidor DHCPv6



1. Selecciona “Servidor DHCPv6” como tipo de dirección para que el dispositivo asigne direcciones IPv6 a los hosts.
2. Especifica la dirección IPv6 inicial/final para los sufijos IPv6. El dispositivo generará direcciones IPv6 dentro del rango especificado.
3. Mantén “Tiempo de cesión de dirección” como valor por defecto.
4. Mantén “Tipo de prefijo de sitio” como valor por defecto “Delegado”. Si tu ISP ha proporcionado un prefijo de sitio IPv6 específico, selecciona “Estático” e introduce el prefijo.
5. Mantén “Conexión WAN” como valor predeterminado.
6. Haz clic en “Aplicar” para hacer efectivos los ajustes.

Configuración control parental

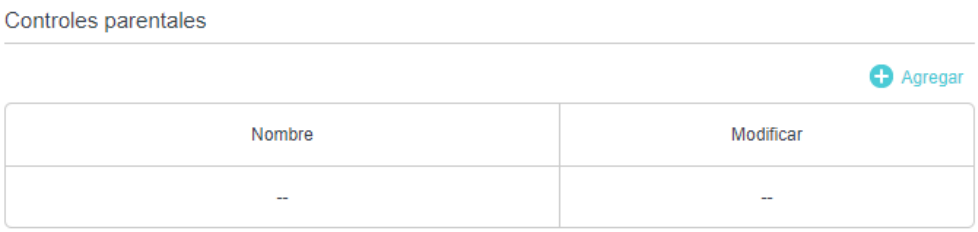
Yo quiero…

Controlar qué tipos de sitios web pueden visitar mis hijos u otros usuarios de la red doméstica y la hora del día a la que pueden acceder a Internet.

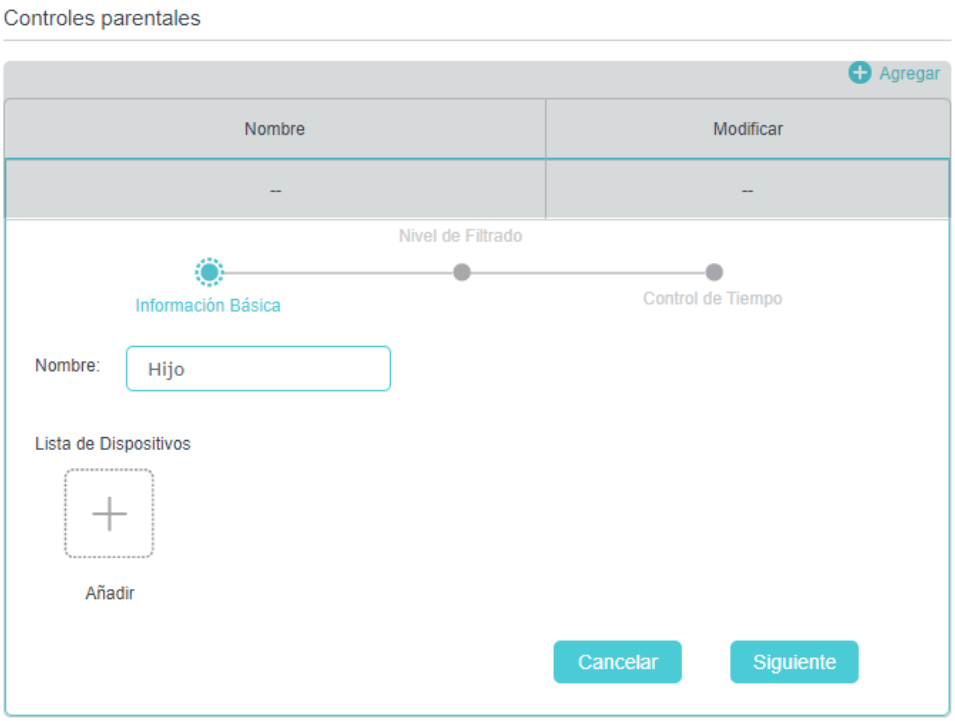
Por ejemplo, quiero permitir que los dispositivos de mis hijos (por ejemplo, un ordenador o una tableta) accedan solo a www.tp-link.com y Wikipedia.org de 18:00 (18:00) a 22:00 (22:00) los días laborables y no a otras horas.

¿Cómo puedo hacerlo?

1. Accede a la página ***Básico > Controles parentales o Avanzado > Controles parentales***



2. Haz clic en “Agregar” y a continuación, introduce un nombre manualmente. Haga clic en “Añadir” y especifica los dispositivos que pertenecen al miembro de la familia. Haz clic en “Siguiente”:

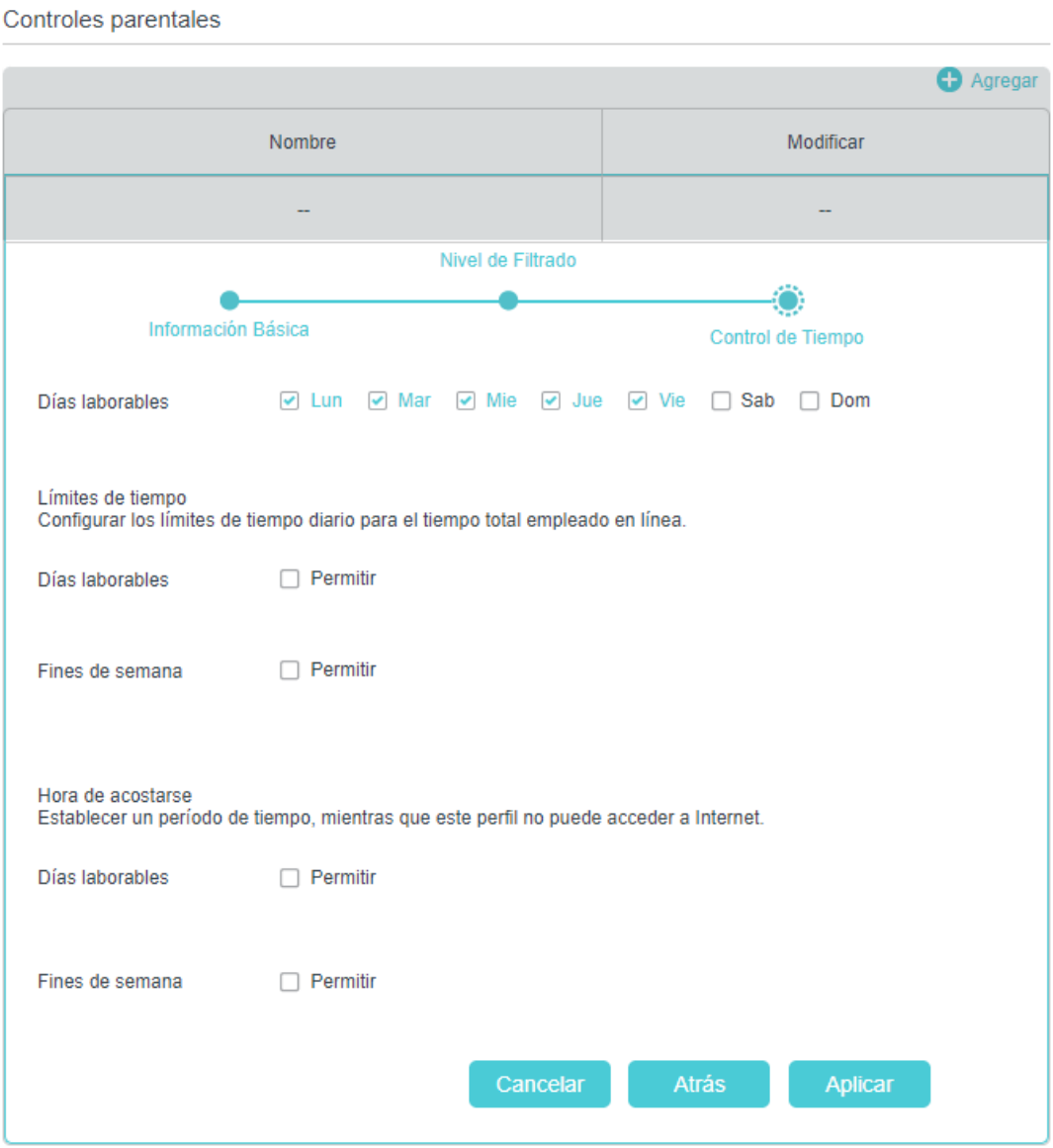


3. Selecciona un nivel de filtro basado en la edad del miembro de la familia. Los contenidos bloqueados aparecerán en la lista “Filtrar contenidos”. Haz clic en “Siguiente”:

4. Opcional: Elimina elementos de la lista “Contenido de Filtro”, añade elementos de la lista “Categorías disponibles” o haga clic en “Añadir” una nueva palabra clave para añadir una palabra clave de filtro (por ejemplo: Facebook o cualquier otra red social).

5. Activa límites de tiempo (por ejemplo: de lunes a viernes y sábados y domingos), y establece el tiempo diario permitido de conexión a Internet.

6. Activa “Hora de acostarse” en las noches de colegio (de lunes a viernes) y los fines de semana (sábado y domingo), y luego establece el periodo de tiempo durante el cual los dispositivos del perfil no pueden acceder a Internet.

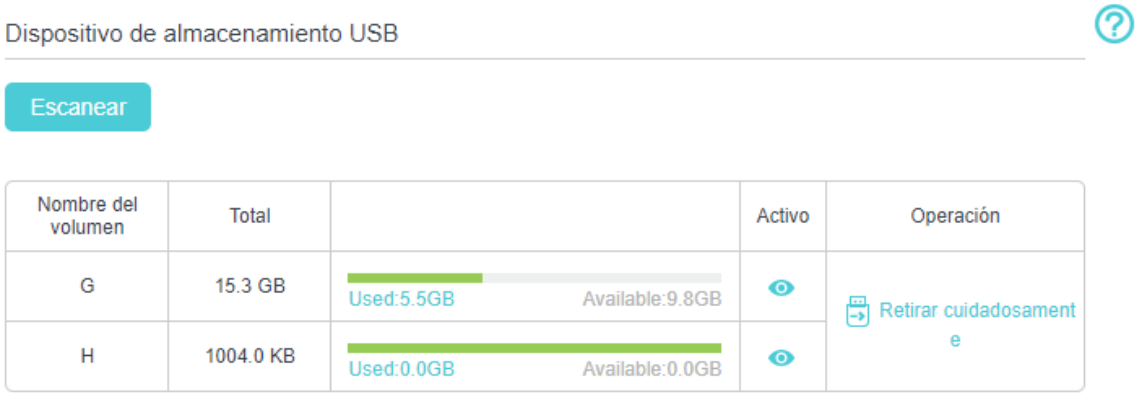


7. Por último, haz clic en “Aplicar”, ahora podrás controlar el acceso a Internet de tus hijos según tus necesidades.

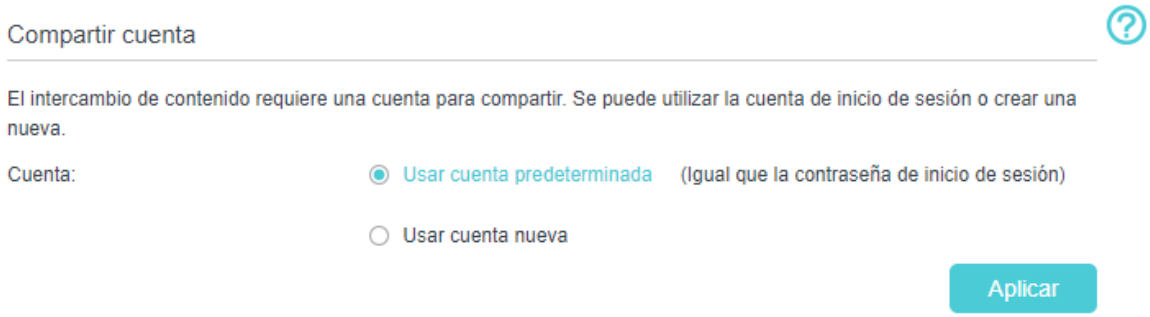
Configuración puerto USB

Inserta tu dispositivo de almacenamiento USB en el puerto USB del dispositivo y accede a los archivos almacenados en él de forma local o remota.

1. Visita http://192.168.1.1 e inicia sesión con el usuario “user” y la contraseña que se configuro en el primer inicio.
2. Accede a la página ***Avanzado > Compartir USB > Dispositivos de almacenamiento USB***
3. Comprueba que el dispositivo ha sido reconocido por el dispositivo. En la siguiente imagen de ejemplo, puedes visualizar un dispositivo USB con dos particiones:

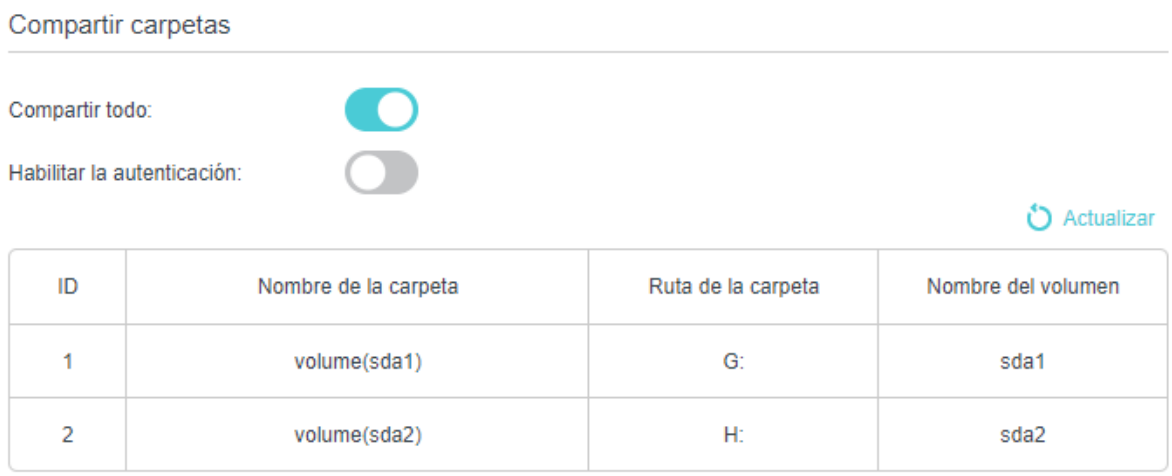


Acceso: ***Avanzado > Compartir USB > Compartir acceso > Compartir Cuenta***. Establece si quieres acceder al almacenamiento compartido con el usuario y contraseña configurados en tu dispositivo o crear una cuenta nueva.



Ajustes de compartición: Haz clic en ”Permitir” → “Vecindad de la Red” para poder acceder al almacenamiento desde tu red LAN (existen otros métodos disponibles como “Servidor Multimedia” o “FTP”) y haz clic en “Aplicar”.

Compartir carpetas: Por defecto, los volúmenes del almacenamiento estarán compartidos. Puedes habilitar la autentificación para solicitar usuario y contraseña para acceder a los mismos, de lo contrario el acceso estará permitido para cualquier dispositivo conectado a la red LAN.



ID	Nombre de la carpeta	Ruta de la carpeta	Nombre del volumen
1	volume(sda1)	G:	sda1
2	volume(sda2)	H:	sda2

User Guide

AC750 Wireless Dual Band Router

REV5.0.0 1910012397

Contents

About This Guide

This guide is a complement to Quick Installation Guide. The Quick Installation Guide provides instructions for quick internet setup, while this guide contains details of each function and demonstrates how to configure them.

When using this guide, please notice that features of the router may vary slightly depending on the model and software version you have, and on your location, language, and internet service provider. All screenshots, images, parameters and descriptions documented in this guide are used for demonstration only.

Conventions

In this guide the following conventions are used:

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

*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.
- A Technical Support Forum is provided for you to discuss our products at https://forum.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:

1. 1. Product Overview

The TP-Link router is designed to fully meet the need of Small Office/Home Office (SOHO) networks and users demanding higher networking performance. The powerful antennas ensure continuous Wi-Fi signal to all your devices while boosting widespread coverage throughout your home, and the built-in Ethernet ports supply high-speed connection to your wired devices.

Moreover, it is simple and convenient to set up and use the TP-Link router due to its intuitive web interface and the powerful Tether app.

1. 2. Panel Layout

1. 2. 1. Top View

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

LED Explanation

Name	Status	Indication
(Power)	On	The system has started up successfully.
	Flashing	The system is starting up or firmware is being upgraded. Do not disconnect or power off your router.
	Off	Power is off.

LED Explanation

Name	Status	Indication
(Wireless 2.4GHz)	On	The 2.4GHz wireless band is enabled.
	Off	The 2.4GHz wireless band is disabled.
(Wireless 5GHz)	On	The 5GHz wireless band is enabled.
	Off	The 5GHz wireless band is disabled.
(WPS)	On/Off	The light remains on for 5 minutes when a WPS connection is established, and then turns off.
	Flashing	WPS connection is in progress. This may take up to 2 minutes.
(Ethernet)	On	At least one Ethernet port is connected to a powered-on device.
	Off	No Ethernet port is connected to a powered-on device.
(Internet)	Green On	The router is connected to the internet.
	Orange On	The router's WAN port is connected, but there is no internet connection.
	Off	The router's WAN port is not connected.

1. 2. 2. The Back Panel

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

Item	Description
Power Port	For connecting the router to a power socket via the provided power adapter.
Power On/Off Button	Press this button to power on or off the router.

Item	Description
Reset Button	Press and hold this button until all the LEDs turn off to reset the router to its factory default settings.
Wi-Fi/WPS Button	Press this button, and immediately press the WPS button on your device. The WPS LED of the router should change from flashing to solid on, indicating successful WPS connection.
	Press and hold this button for about 5 seconds to turn on or off the wireless function of your router.
WAN Port	For connecting to a DSL/Cable modem, or an Ethernet port.
Ethernet Ports (1/2/3/4)	For connecting your PCs or other wired network devices to the router.
Antennas	Used for wireless operation and data transmitting. Upright them for the best Wi-Fi performance.

Chapter 2

Connect Your Router

This chapter contains the following sections:

2. 1. Position Your Router

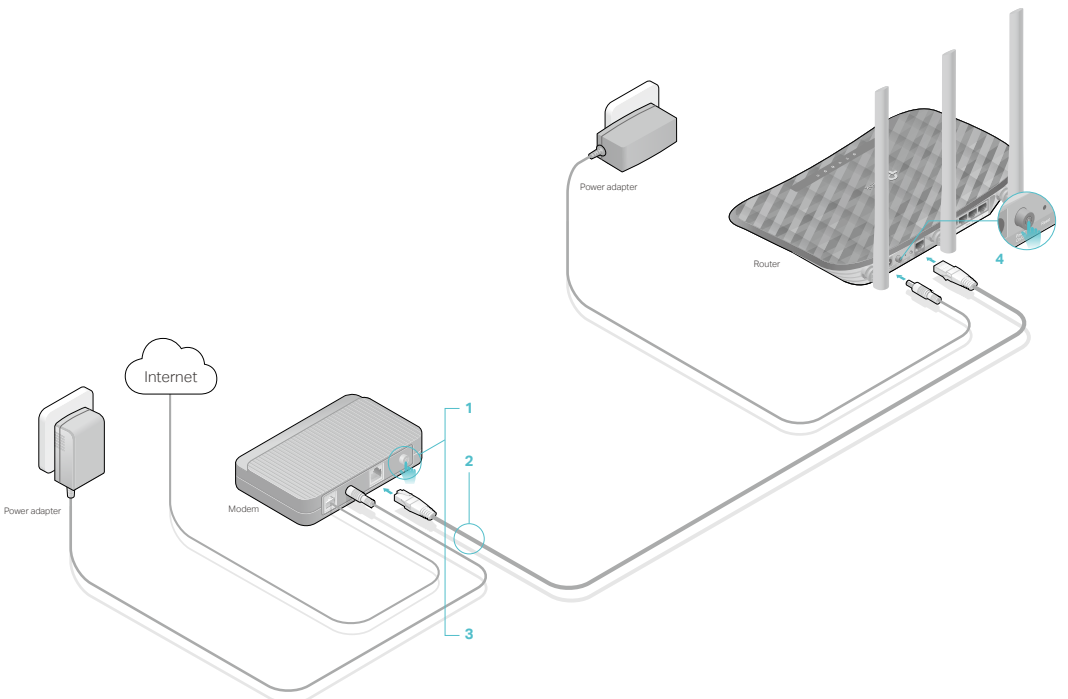
- The product should not be located in a place where it will be exposed to moisture or excessive heat.
- Place the router in a location where it can be connected to multiple devices as well as to a power source.
- Make sure the cables and power cord are safely placed out of the way so they do not create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

2. 2. Connect Your Router

This mode enables multiple users to share internet connection via ADSL/Cable Modem.

1. Follow the steps below to connect your router.

If your internet connection is through an Ethernet cable directly from the wall instead of through a DSL / Cable / Satellite modem, connect the Ethernet cable to the router's WAN port, and then follow Step 4 and 5 to complete the hardware connection.



1) Turn off the modem, and remove the backup battery if it has one.

2) Connect the modem to the **Internet port** on your router with an Ethernet cable.

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

4) Connect the power adapter to the router and turn on the router.

5) Verify that the hardware connection is correct by checking these LEDs.

Note:

If the 2.4G and 5G Wi-Fi LEDs are off, press and hold the Wi-Fi/WPS button on the rear panel for about 3 seconds, then release the button. Both LEDs will turn on.

2. Connect your computer to the router.

- **Method 1: Wired**

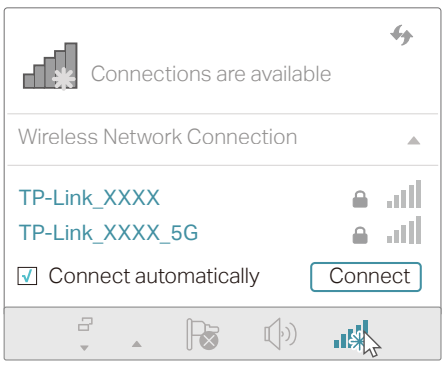
Turn off the Wi-Fi on your computer and connect the devices using an Ethernet cable.

- **Method 2: Wirelessly**

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

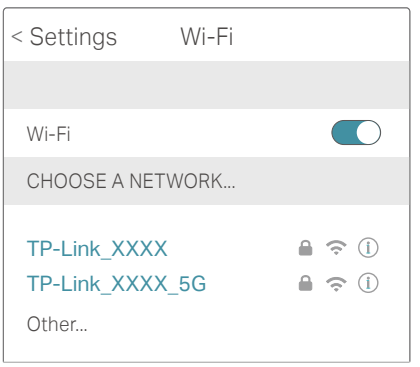
2) Click the network icon of your computer or go to Wi-Fi Settings of your smart device, and then select the SSID to join the network.

Computer



OR

Smart Device



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

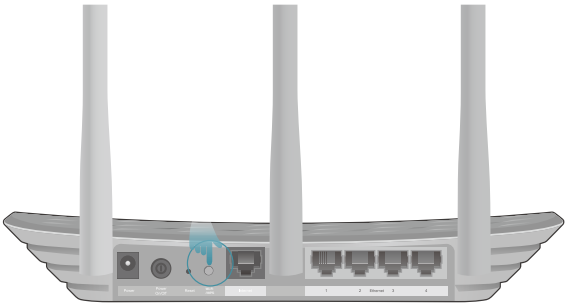
Wireless devices that support WPS, including Android phones, tablets and most USB network cards, can be connected to your router through this method (Not supported by iOS devices).

Note:

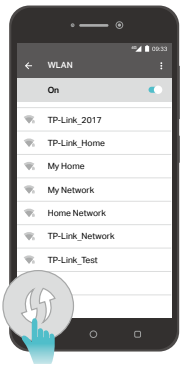
The WPS function cannot be configured if the wireless function of the router is disabled. Also, the WPS function will be disabled if your wireless encryption is WEP. Please make sure the wireless function is enabled and is configured with the appropriate encryption before configuring the WPS.

1) Tab the WPS icon on the device's screen. Here takes an Android phone as an example.

2) Immediately press the WPS button on your router.



Close to


WLAN
On
TP-Link_2017
TP-Link_Home
My Home
My Network
Home Network
TP-Link_Network
TP-Link_Test

Chapter 3

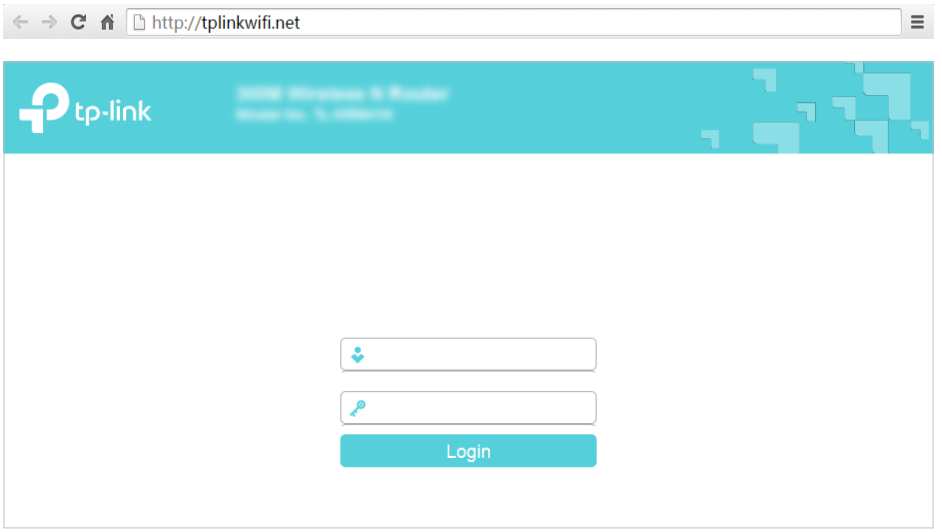
Log In

This chapter introduces how to log in to the web management page of router.

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

Follow the steps below to log in to your router.

1. Set up the TCP/IP Protocol in Obtain an IP address automatically mode on your computer.
2. Visit http://tplinkwifi.net, and log in with the 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 the FAQ section.

Chapter 4

Configure the Router

This chapter presents how to configure the various features of the router.

It contains the following sections:

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 2.4GHz/5GHz - This field displays the basic information or status of the wireless function, and you can configure them on the Wireless > Basic Settings page.

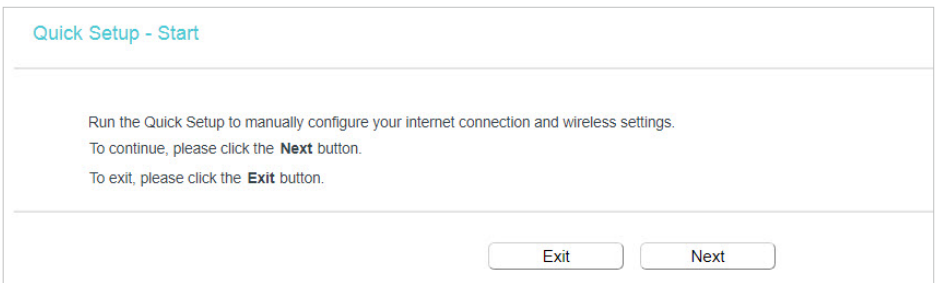
- Operation Mode - The current wireless working mode in use.
- Wireless Radio - Indicates whether the wireless radio feature of the router is enabled or disabled.
- Name(SSID) - The SSID of the Router.
- Mode - The current wireless mode which the router works on.
- Channel - The current wireless channel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

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



3. Click Next to start. Then follow the step-by-step instructions to connect your router to the internet.

4. 3. Operation Mode

The router supports three operation modes: Wireless Router mode, Access Point mode and Range Extender.

4. 3. 1. Wireless Router Mode

The default Wireless Router mode is required most commonly. In this mode, the device enables multiple users to share the internet connection via ADSL/Cable Modem.

For hardware connection, refer to Connect Your Router.

4. 3. 2. Access Point Mode

In this mode, the device can be connected to a wired network and transform the wired access into wireless one. If you already have a wired router, you can use this mode. Refer to Configure the Router in Access Point Mode session for detailed information.

4. 3. 3. Range Extender Mode

In this mode, the device can copy and reinforce the existing wireless signal to extend the coverage of the signal, especially for a large space to eliminate signal-blind corners. Refer to Configure the Router in Range Extender Mode session for detailed information.

4. 4. Network

4. 4. 1. WAN

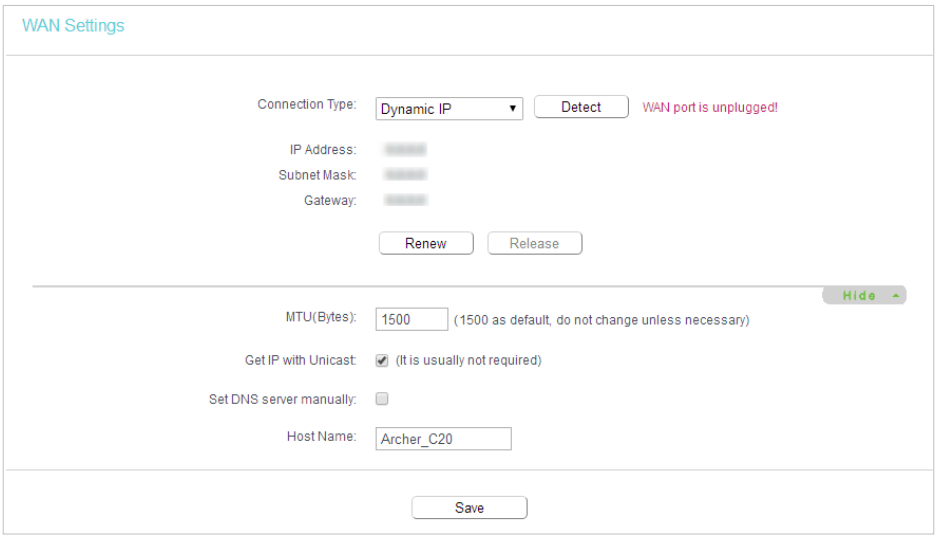
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Network > WAN.
3. Configure the IP parameters of the WAN and click Save.

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.

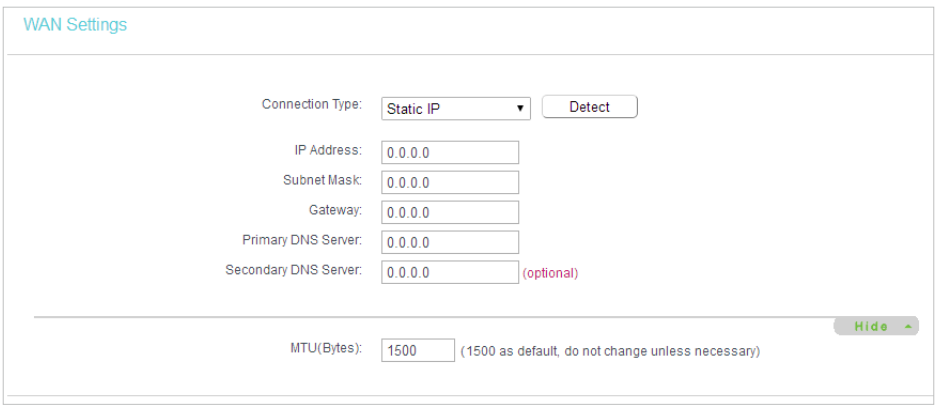
Click Release to release the IP parameters.



- 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.
- 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.

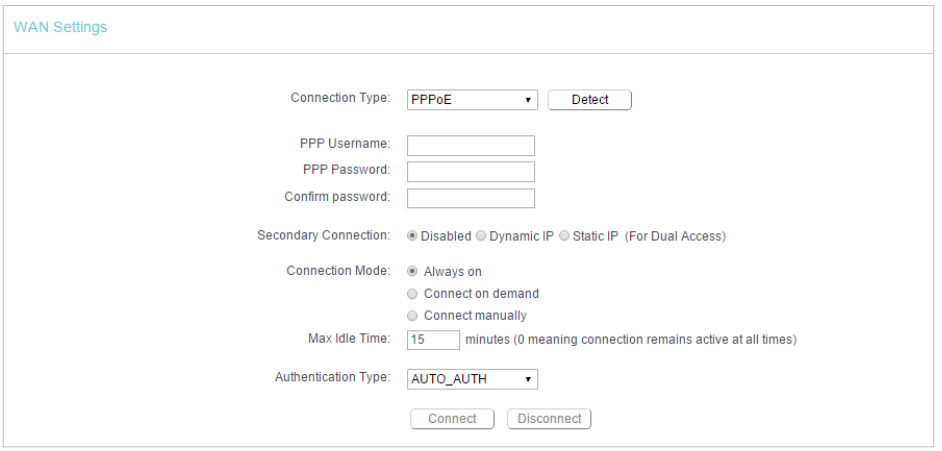


- IP Address - Enter the IP address in dotted-decimal notation provided by your ISP.
- Subnet Mask - Enter the subnet mask in dotted-decimal notation provided by your ISP. Normally 255.255.255.0 is used as the subnet mask.

- Gateway - Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- Primary/Secondary DNS Server - Enter one or two DNS addresses in dotted-decimal notation provided by your ISP. For the Secondary DSN Server, it is optional.
- 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.

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

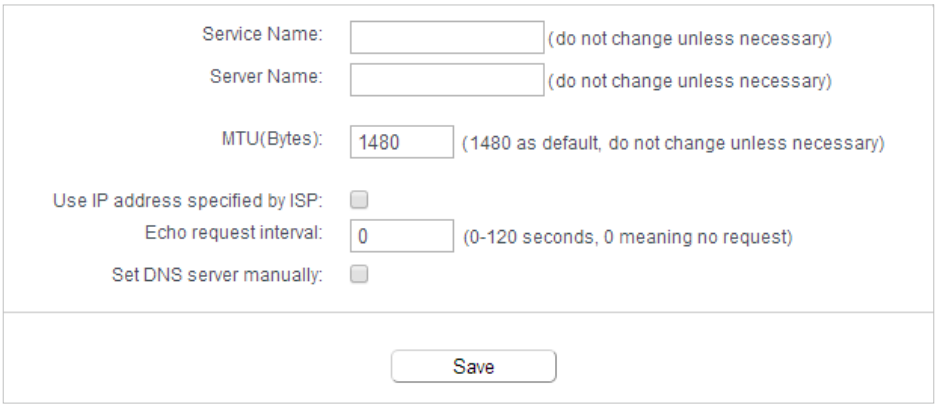
after a specified inactivity period (Max Idle Time) and not be able to re-establish when you attempt to access the internet again.

- 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.

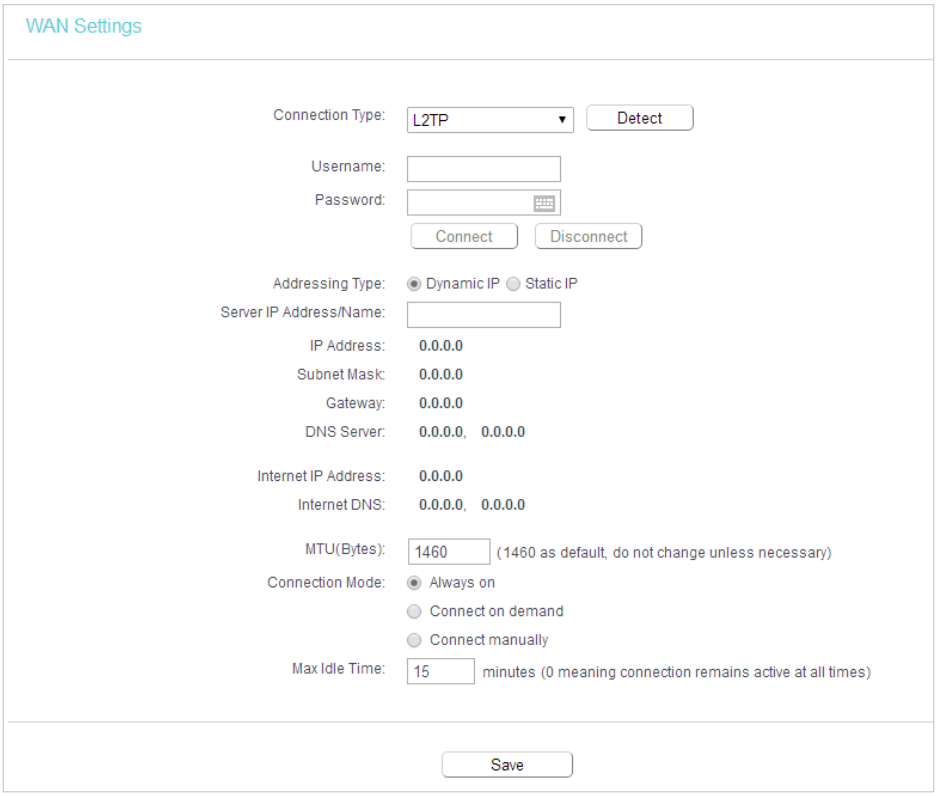
If you want to do some advanced configurations, please click Advanced.



- 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.
- 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 user name 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.
- Server IP Address/Name - Enter server IP address or domain name provided by your ISP.
- 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.
- 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

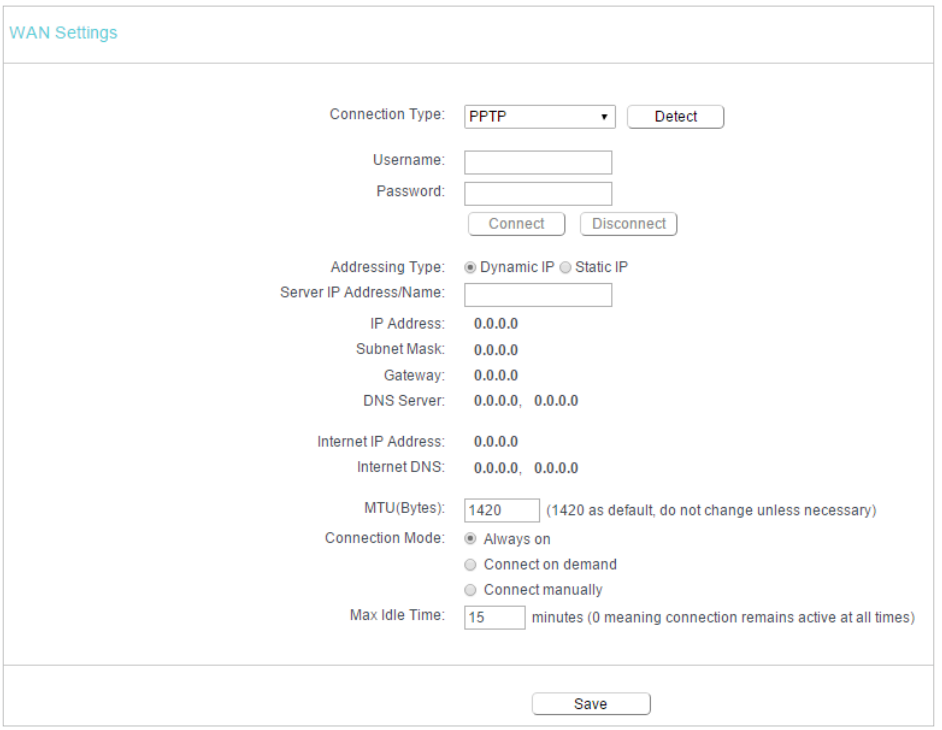
after a specified inactivity period (Max Idle Time) and not be able to re-establish when you attempt to access the internet again.

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 user name 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.
- Server IP Address/Name - Enter server IP address or domain name provided by your ISP.
- 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.
- 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.

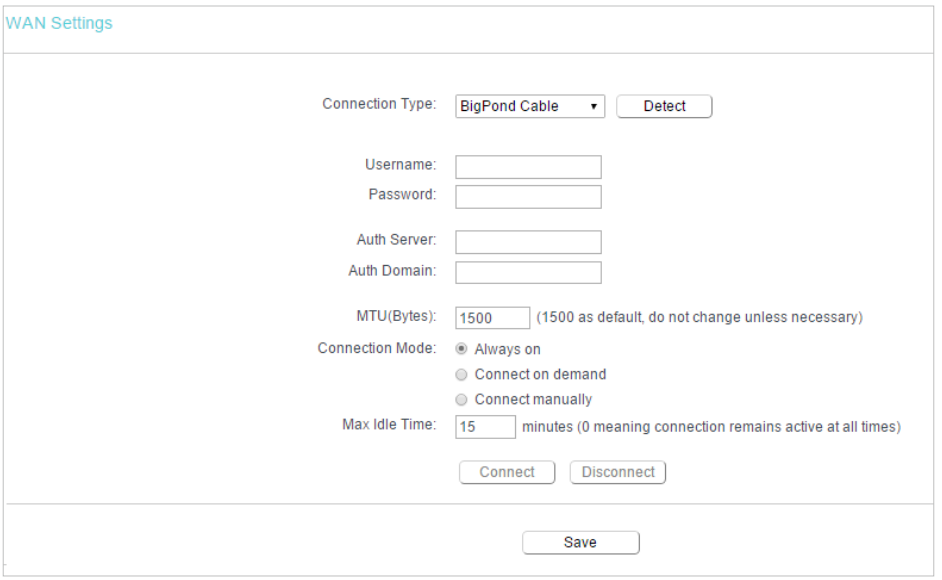
- Connect Manually - You can click Connect/Disconnect to connect/disconnect immediately. This mode also supports the Max Idle Time function as Connect on Demand mode. The internet connection can be disconnected automatically after a specified inactivity period (Max Idle Time) and not be able to re-establish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



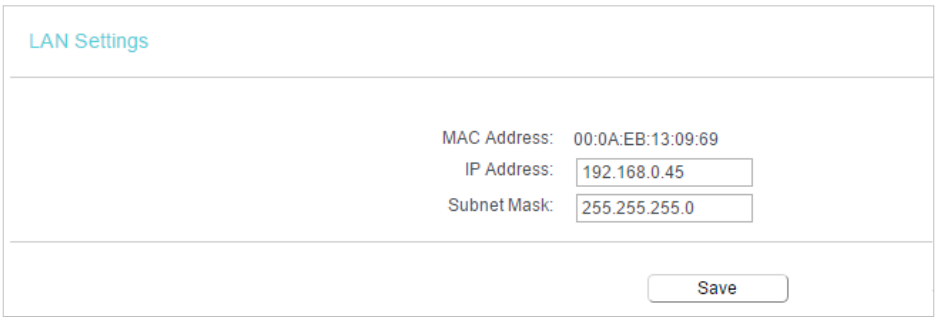
- Username/Password - Enter the use name and password provided by your ISP. These fields are case-sensitive.
- Auth Server - Enter the authenticating server IP address or host name.
- Auth Domain - Type in the domain suffix server name based on your location.
- MTU(Bytes) - The default MTU size is 1500 bytes. It is not recommended that you change the default MTU size unless required by your ISP.
- 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. 4. 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.



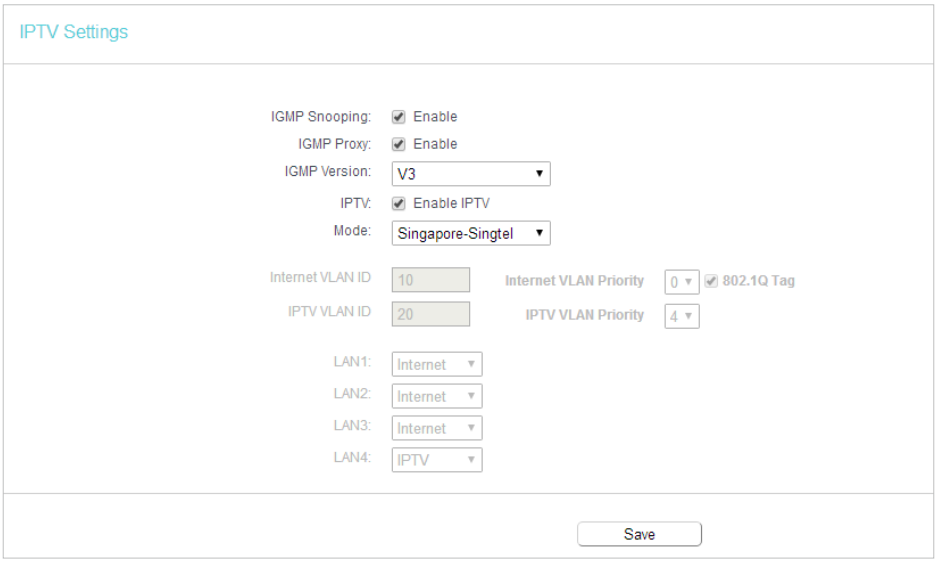
- MAC Address - The physical address of the LAN ports. The value can not be changed.
- IP Address - Enter the IP address in dotted-decimal notation of your router (factory default - 192.168.0.254).
- Subnet Mask - An address code that determines the size of the network. Normally 255.255.255.0 is used 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.

4. 4. 3. IPTV

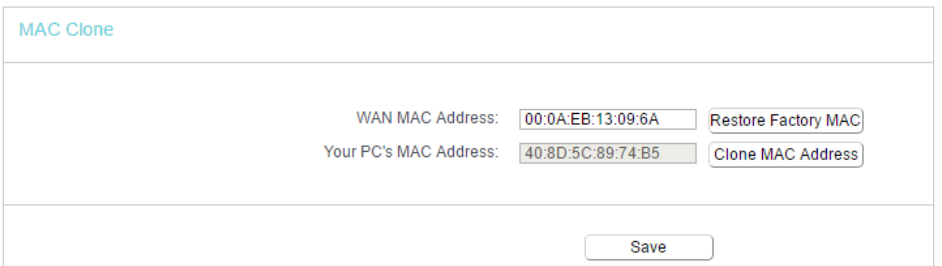
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Network > IPTV.
3. Configure the IPTV settings and click Save.



- 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.
- IGMP Proxy - Select to enable IGMP Proxy.
- IGMP Version - Select the IGMP(Internet Group Management Protocol) Proxy Version, either V2 or V3, according to your ISP.
- IPTV - Select to enable the IPTV feature.
- Mode - Select the appropriate mode according to your ISP.
- LAN 1/2/3/4 - Assign your LAN port to whether function as the Internet supplier or as the IPTV supplier.

4. 4. 4. 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.



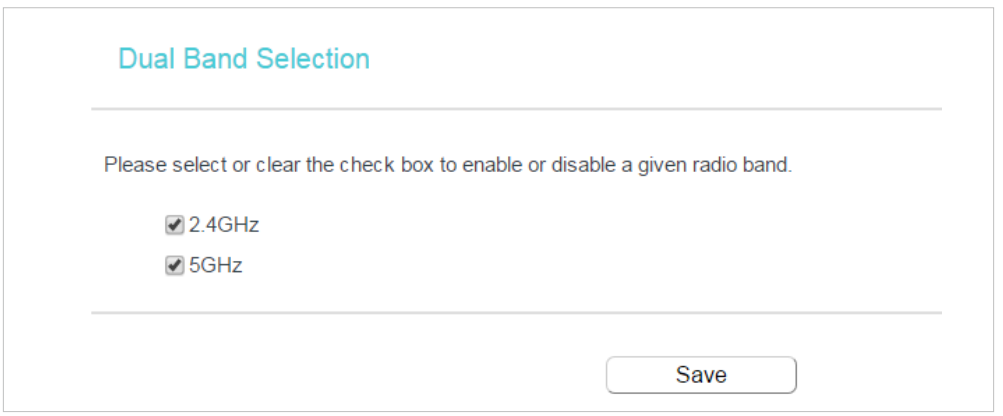
- WAN MAC Address - This field displays the current MAC address of the WAN port. If your ISP requires you to register the MAC address, please enter the correct MAC address in this field. Click Restore Factory MAC to restore the MAC address of WAN port to the factory default value.
- Your PC's MAC Address - 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. 5. Dual Band Selection

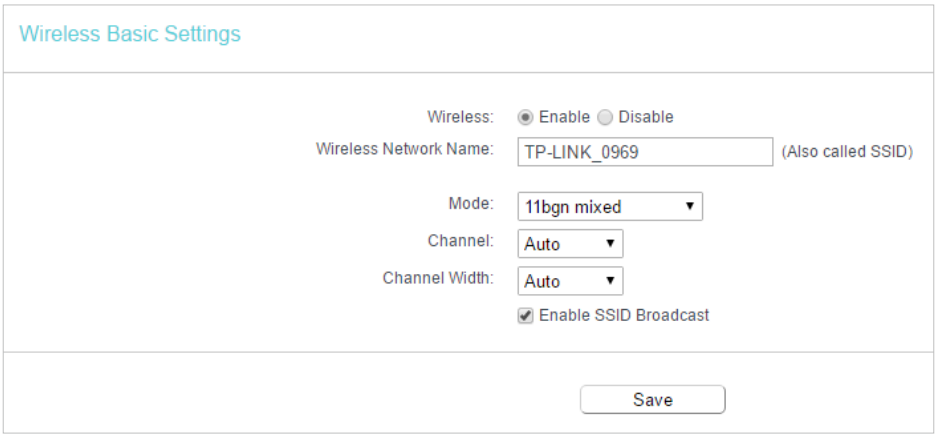
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Dual Band Selection.
3. Select the working radio band as needed and click Save.



4. 6. Wireless(2.4GHz or 5GHz)

4. 6. 1. Wireless 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. 6. 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.

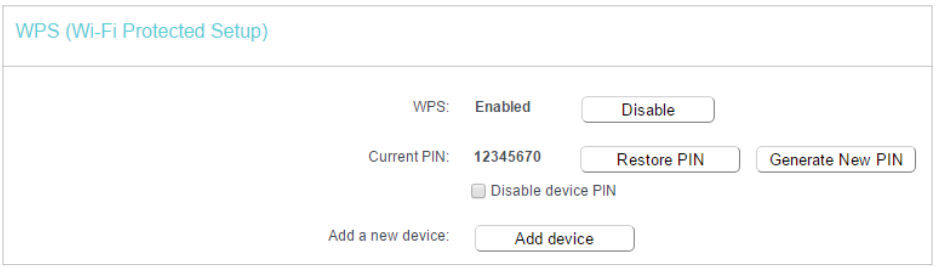
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Wireless > WPS.
3. Follow one of the following three methods to connect your client device to the router's Wi-Fi network.

Method ONE: Press the WPS Buttons on the Router and Client Device

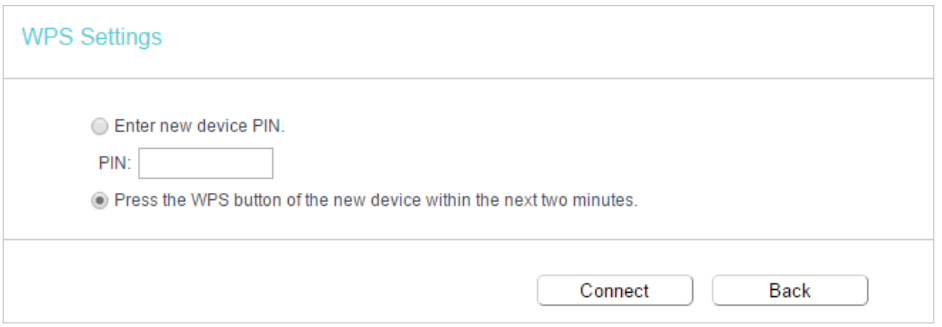
For details, refer to Method 3: Use the WPS button of Connect Your Router.

Method TWO: Press the WPS Button on Your Client Device

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



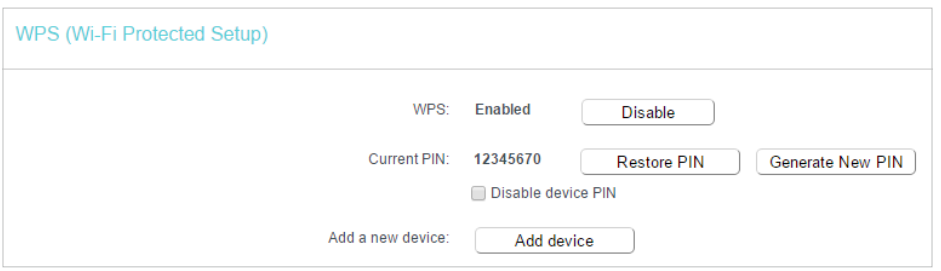
2. Select Press the WPS button of the new device within the next two minutes and click Connect.



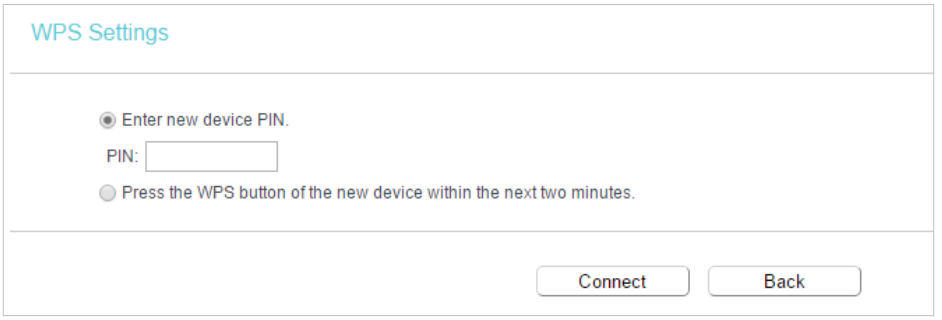
3. Within two minutes, press the WPS button on your client device.
4. A success message will appear on the WPS page if the client device has been successfully added to the router's network.

Method THREE: Enter the Client's PIN

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



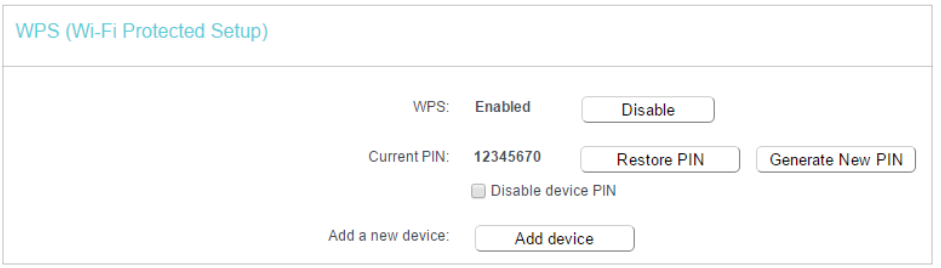
2. Select Enter new device PIN, enter your client device's current PIN in the PIN filed and click Connect.



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

Method FOUR: Enter the Router's PIN

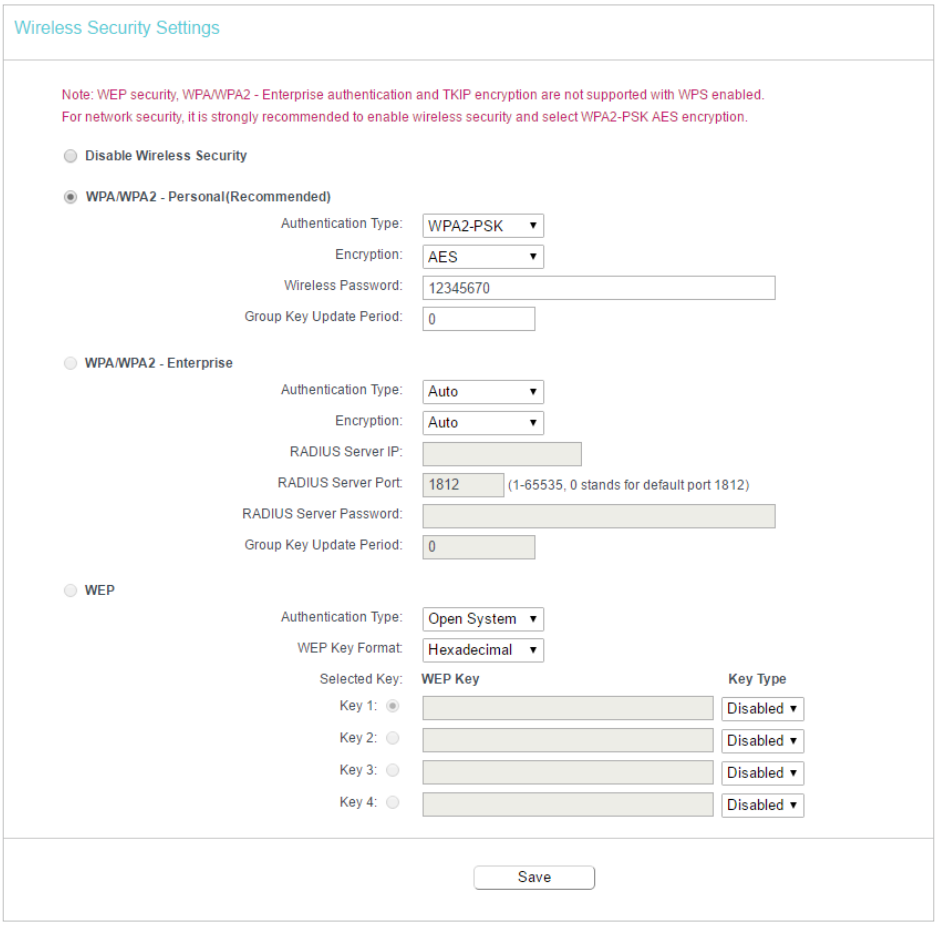
1. Keep the WPS Status as Enabled and get the Current PIN of the router.



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

4. 6. 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.
    - Authentication Type - Select Auto, WPA-PSK or WPA2-PSK.
    - Encryption - Select Auto, TKIP or AES.
    - Wireless Password - Enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters.
    - Group Key Update Period - Specify the group key update interval in seconds. The value can be 0 or at least 30. Enter 0 to disable the update.
- WPA /WPA2-Enterprise - It's based on Radius Server.
    - Authentication Type - Select Auto, WPA or WPA2.
    - Encryption - Select Auto, TKIP or AES.
    - Radius Server IP - Enter the IP address of the Radius server.

- Radius Server Port - Enter the port that Radius server used.
- Radius Server Password - Enter the password for the Radius server.
- Group Key Update Period - Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.

- WEP - It is based on the IEEE 802.11 standard.
  - Authentication Type - The default setting is Auto, which can select Shared Key or Open System authentication type automatically based on the wireless client's capability and request.
  - WEP Key Format - Hexadecimal and ASCII formats are provided here. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. ASCII format stands for any combination of keyboard characters in the specified length.
  - WEP Key (Password) - Select which of the four keys will be used and enter the matching WEP key. Make sure these values are identical on all wireless clients in your network.
  - Key Type - Select the WEP key length (64-bit or 128-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. 6. 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:

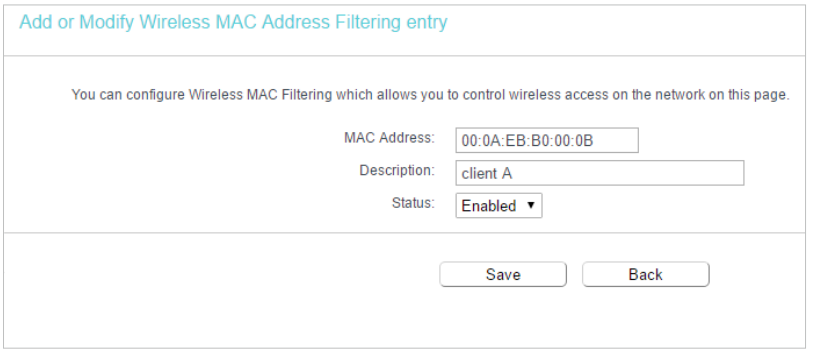
Deny or allow specific wireless client devices to access my network by their MAC addresses.

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?

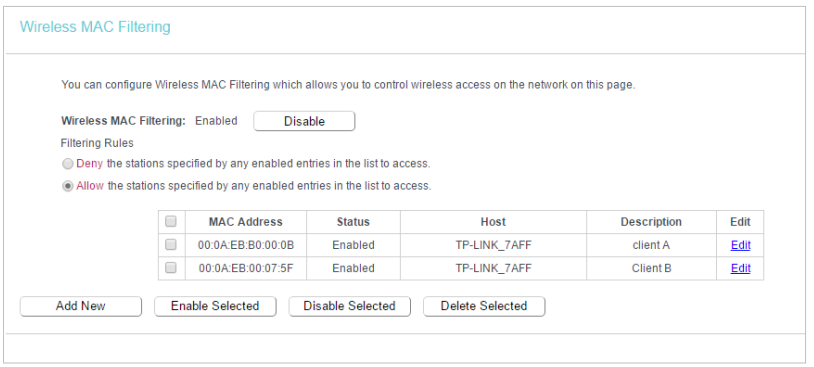
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.

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 or 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.

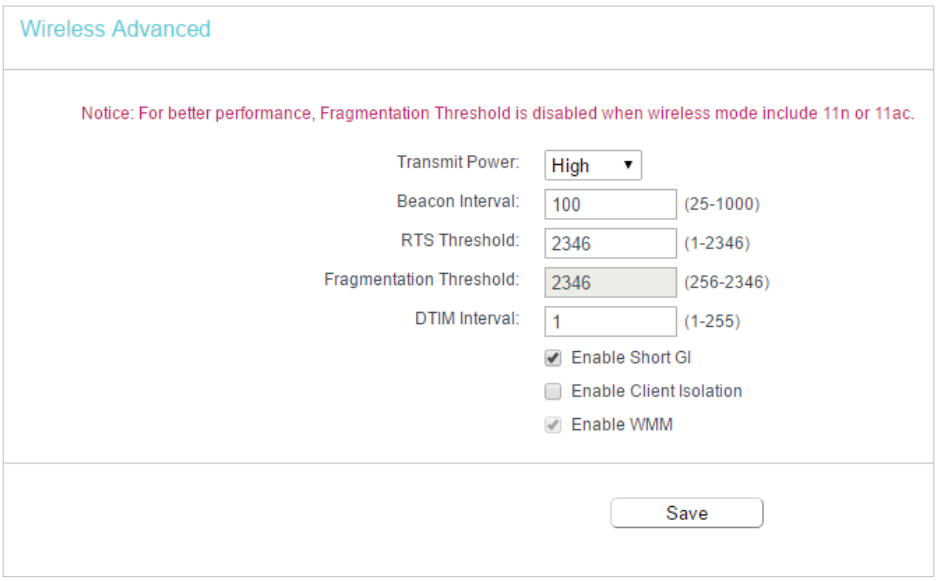
4. 6. 5. Wireless Advanced

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.

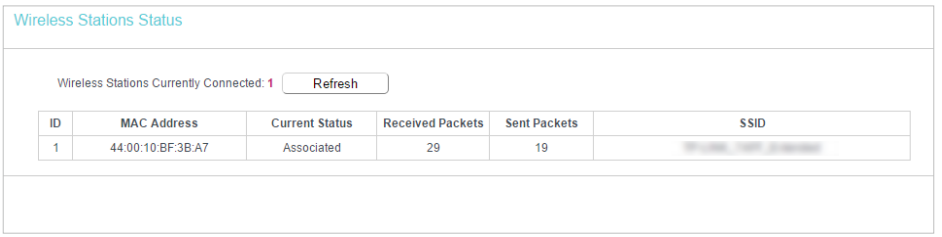


- Transmit Power - Select High, Middle or Low which you would like to specify for the router. High is the default setting and recommended.
- Beacon Interval - Enter a value between 40-1000 milliseconds for Beacon Interval here. Beacon Interval value determines the time interval of the beacons. The beacons 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.
- Enable WMM - WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended to enable this function.

4. 6. 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.



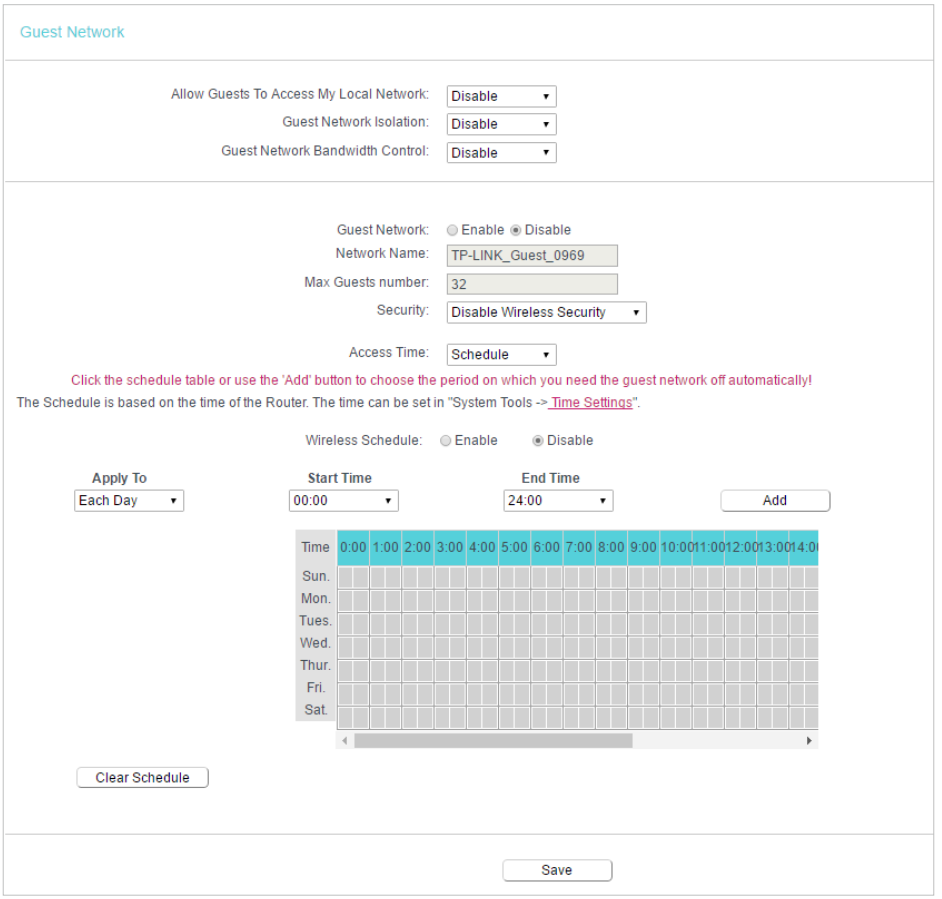
- MAC Address - The MAC address of the connected wireless client.
- Current Status - The running status of the connected wireless client.
- Received Packets - Packets received by the wireless client.
- Sent Packets - Packets sent by the wireless client.
- SSID - SSID that the station associates with.

4. 7. 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.

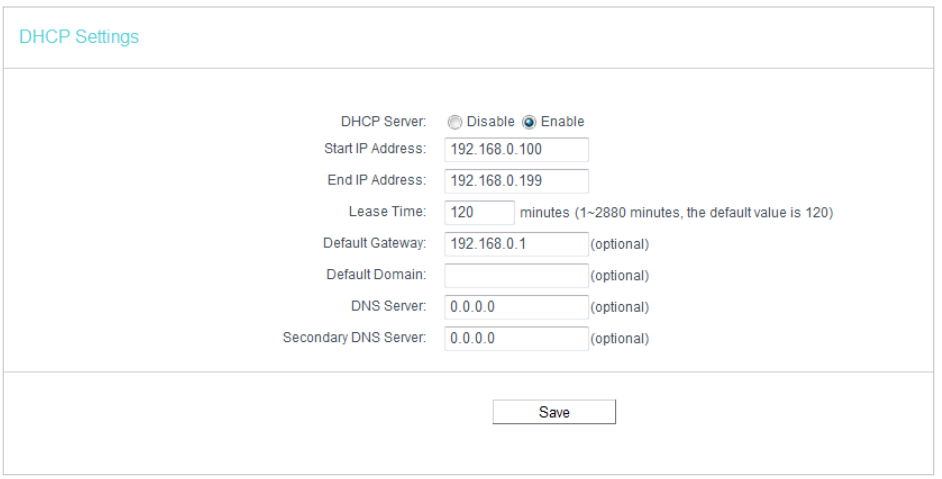
Note: The range of bandwidth for guest network is calculated according to the setting of Bandwidth Control on the Bandwidth Control page.

4. 8. 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. 8. 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.



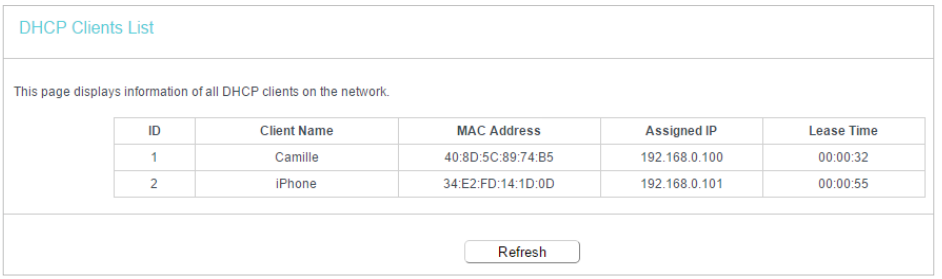
- DHCP Server - Enable or disable the DHCP server. If disabled, you must have another DHCP server within your network or else you must configure the computer manually.
- Start IP Address - Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.0.100 is the default 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. 8. 2. DHCP Client List

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



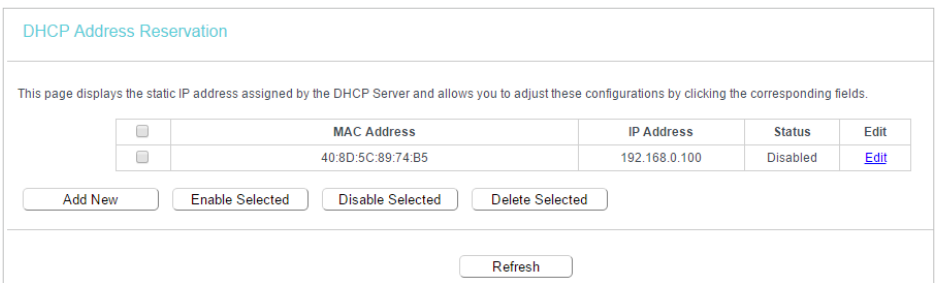
- Client Name - The name of the DHCP client.
- MAC Address - The MAC address of the DHCP client.
- Assigned IP - The IP address that the outer has allocated to the DHCP client.
- Lease Time - The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic IP address will be 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. 8. 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 blank.



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. 9. Forwarding

The router's NAT (Network Address Translation) feature makes the devices on the LAN use the same public IP address to communicate in 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. 9. 1. Virtual Server

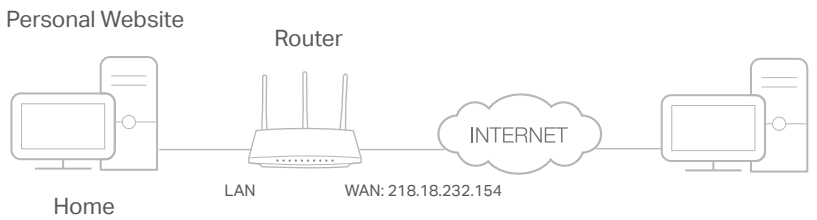
When you build up a server in the local network and want to share it on the internet, Virtual Servers can realize the service and provide it to internet users. At the same time virtual servers can keep the local network safe as other services are still invisible from the internet.

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:

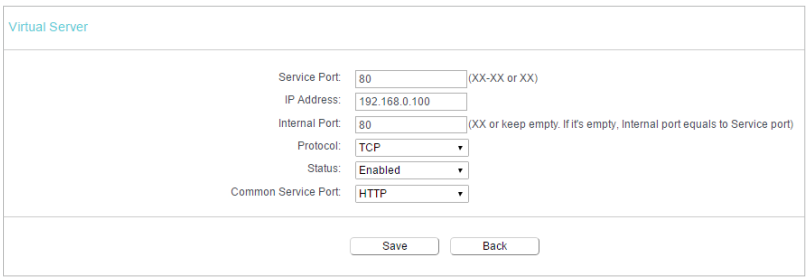
Share my personal website I've built in local network with my friends through the internet.

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.



How can I do that?

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:

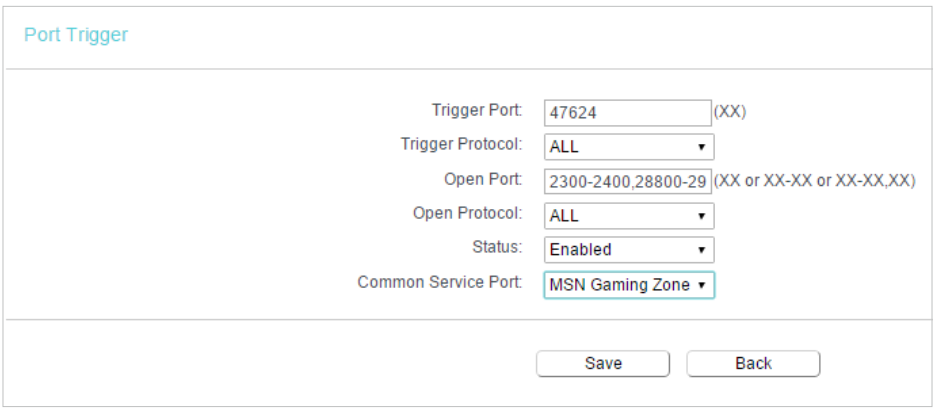
- If you have changed the default Service Port, you should use http:// WAN IP: Service Port to visit the website.
- Some specific service ports are forbidden by the ISP. If you fail to visit the website, please use another service port.

4. 9. 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 Applications list, please enter the parameters manually. You should verify the incoming 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. 9. 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.

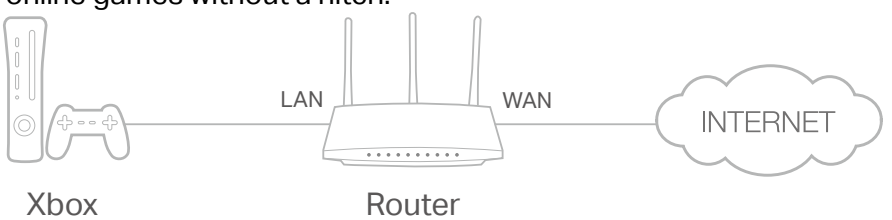
4. 9. 4. UPnP

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:

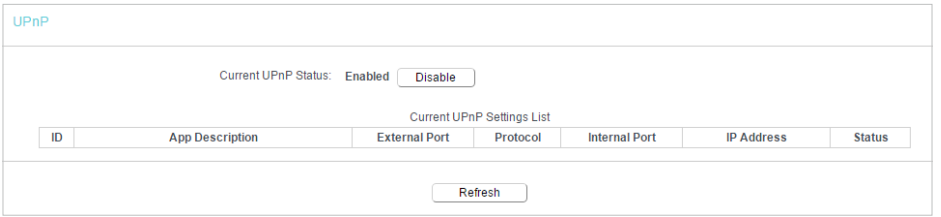
- UPnP is enabled by default in this router.
- Only the application supporting UPnP protocol can use this feature.
- UPnP feature needs the support of operating system (e.g. Windows Vista/ Windows 7/ Windows 8, etc. Some of operating system need to install the UPnP components).

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.

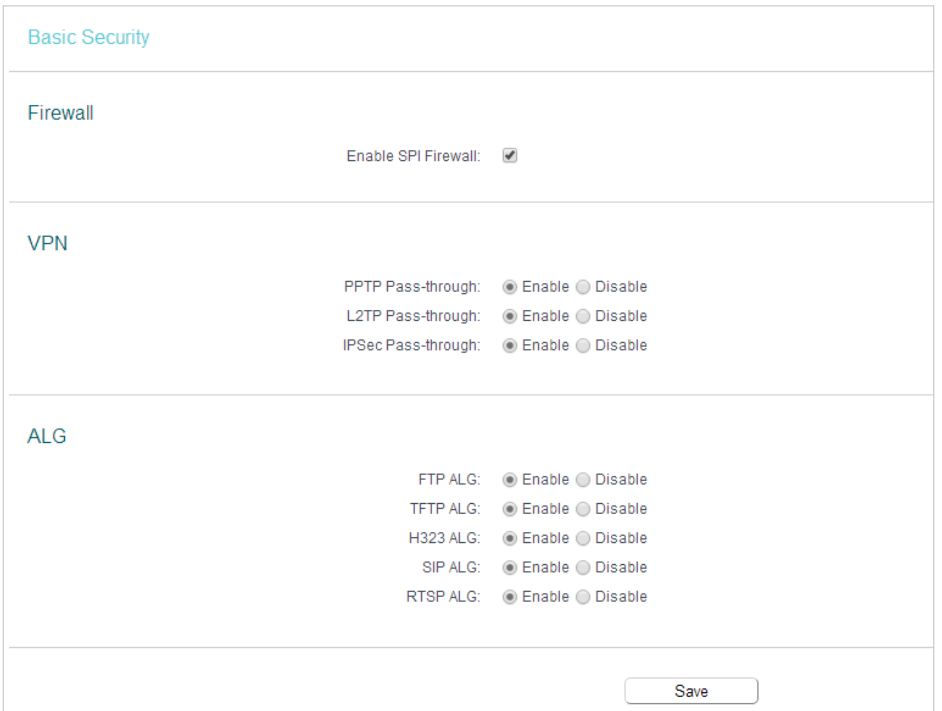


4. 10. Security

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

4. 10. 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.



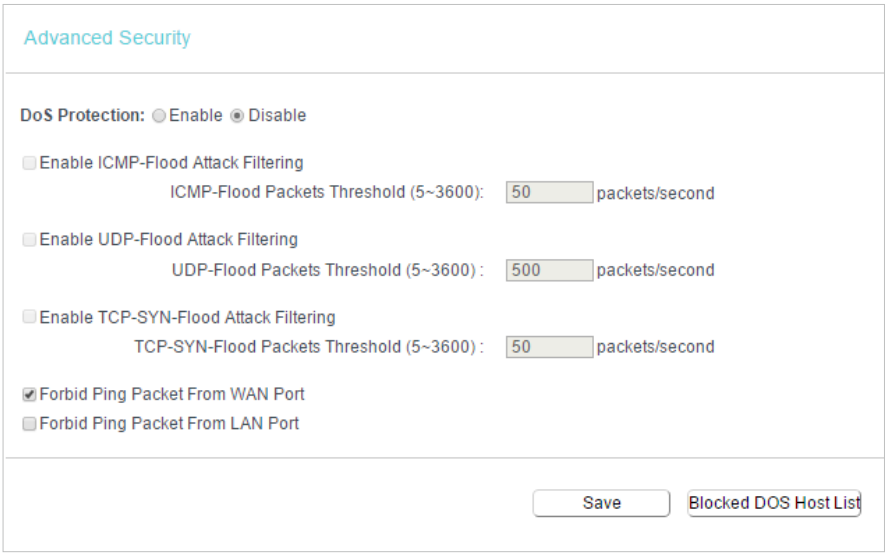
- Firewall - A firewall protects your network from internet attacks.
    - Enable SPI Firewall - SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms 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 Passthrough - 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 Passthrough - 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 Passthrough - 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. 10. 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 Tool > Statistics is enabled.

- Enable ICMP-FLOOD Attack Filtering -Check the box 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 - Check the box to enable or disable 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 -Check the box 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.
- Forbid Ping Packet From WAN Port - The default setting is enable. If disabled, the ping packet from the internet can 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.

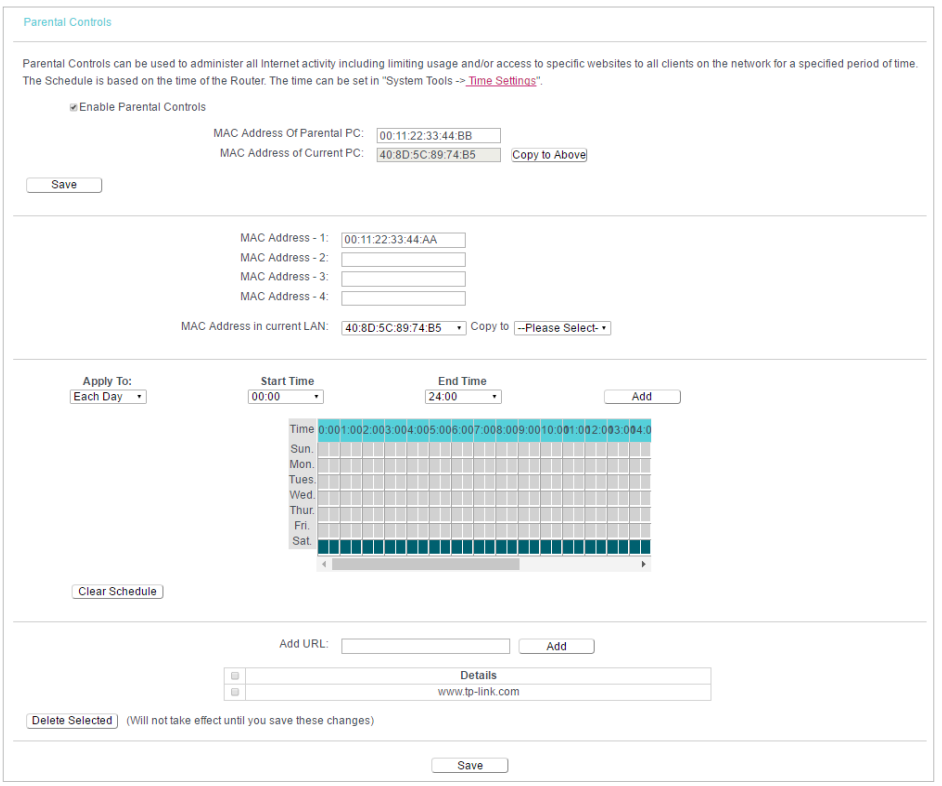
4. 11. Parental Controls

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. Check the Enable Parental Controls box and enter the MAC address 00:11:22:33:44:BB in the MAC Address of Parental PC field.
4. Enter 00:11:22:33:44:AA in the MAC Address 1 field.
5. Create a new schedule with Day is Sat and Time is all day-24 hours. Click Add
6. Enter www.tp-link.com in the Add URL field. Click Add.
7. Click Save.

Then you will see the page as shown in figure below.



4. 12. Access Control

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

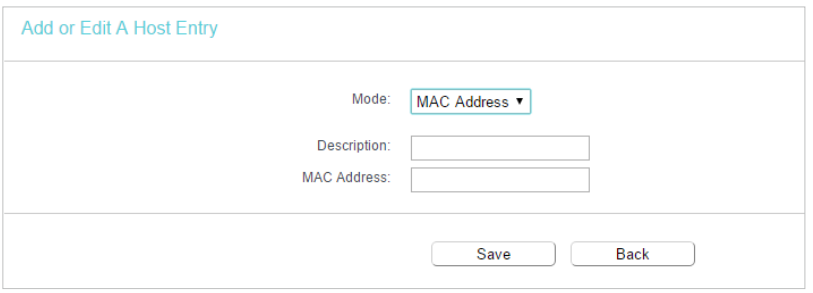
I want to:

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:

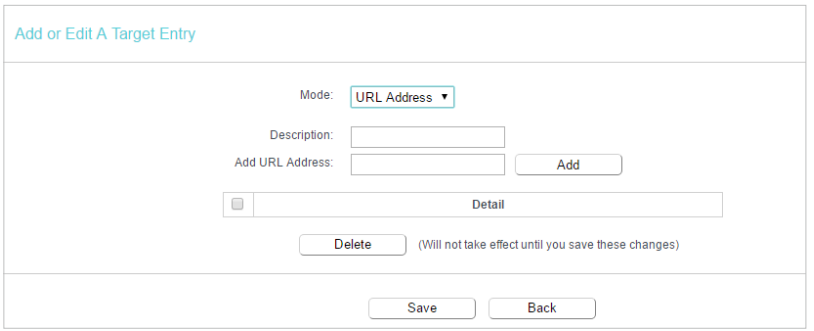
How can I do that?

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.

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

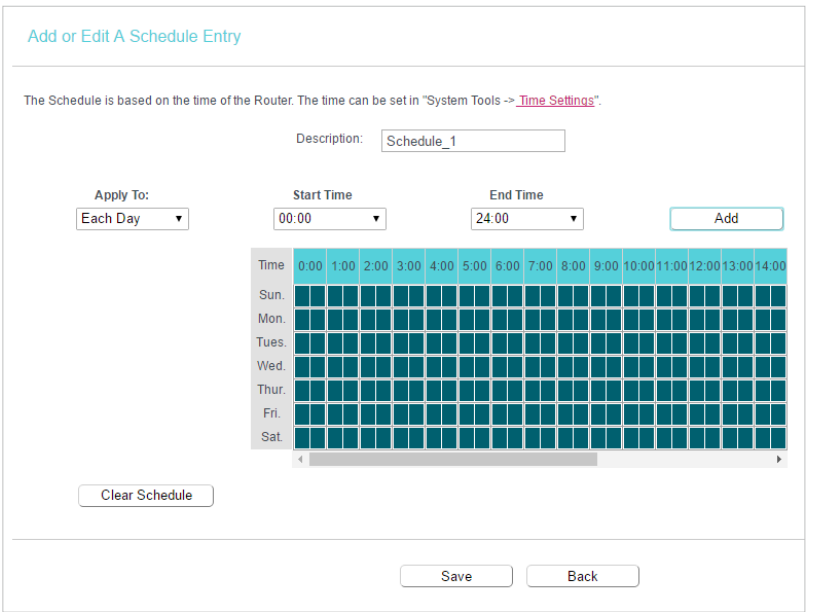


3) Click Save.

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.

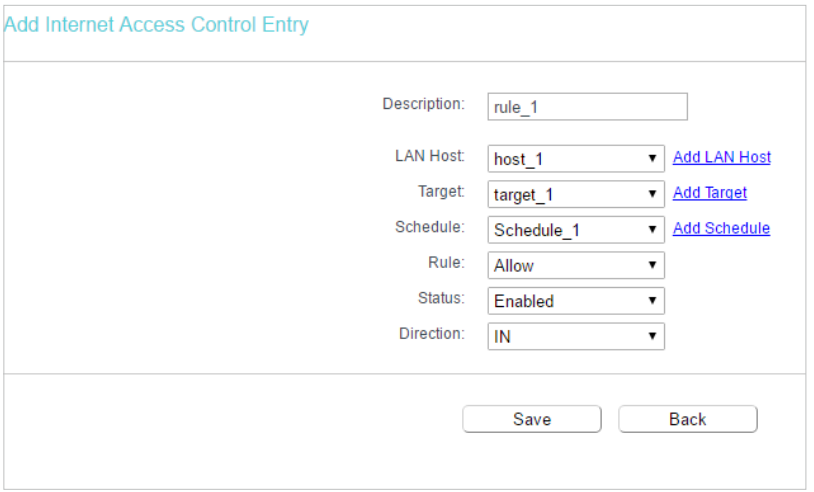


3) Click Save.

5. Go to Access Control > Rule and add a new access control rule.

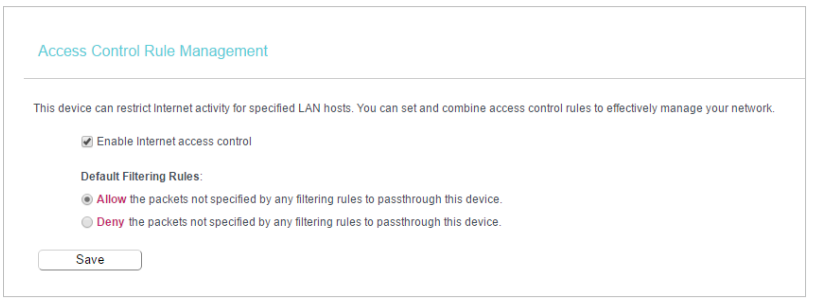
1) Click Add New.

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.

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.

4. 13. Advanced Routing

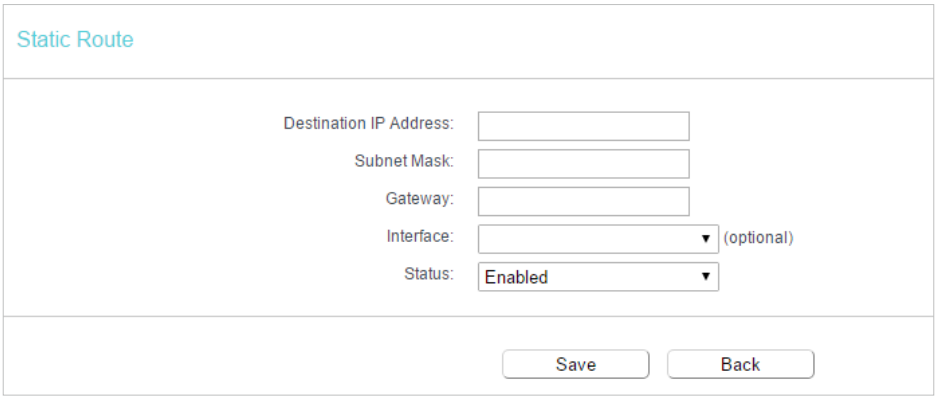
Static Routing is a form of routing that is configured manually by a network administrator or a user by adding entries into a routing table. The manually-configured routing information guides the router in forwarding data packets to the specific destination.

4. 13. 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.



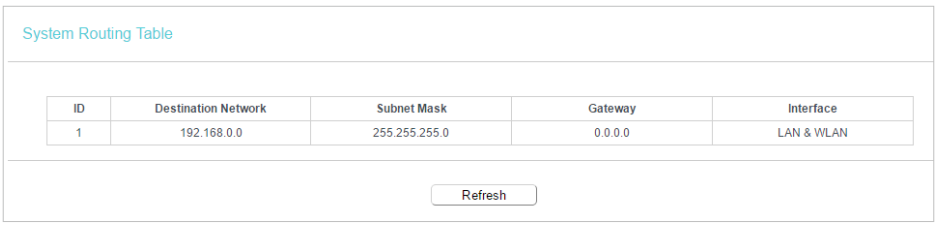
2. Enter the following information.
   - Destination IP Address - The Destination Network is the address of the network or host that you want to assign to a static route.
   - Subnet Mask - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host 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.

You can also do the following operations to modify the current settings.

- Click Delete to delete the entry.
- Click Enable Selected to enable all the entries.
- Click Disable Selected to disable all the entries.
- Click Delete Selected to delete all the entries.

4. 13. 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.

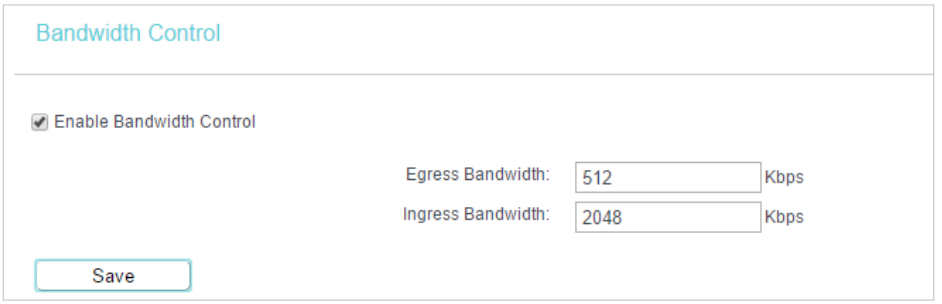


- Destination Network - The Destination Network is the address of the network or host to which the static route is assigned.
- Subnet Mask - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.
- Gateway - This is the IP address of the 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. 14. Bandwidth Control

4. 14. 1. Control Settings

1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Bandwidth Control.
3. Configure the bandwidth as needed and click Save.

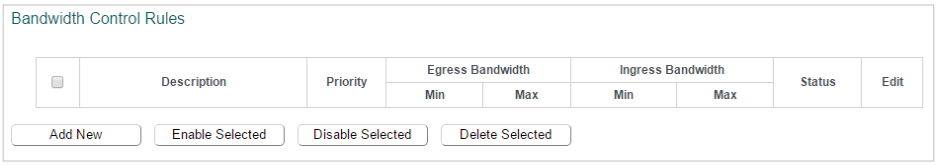


The values you configure for the Egress Bandwidth and Ingress Bandwidth should be less than 100,000Kbps. For optimal control of the bandwidth, please select the right Line Type and consult your ISP for the total egress and ingress bandwidth.

- Enable Bandwidth Control - Check this box so that the Bandwidth Control settings can take effect.
- Egress Bandwidth - The upload speed through the WAN port.
- Ingress Bandwidth - The download speed through the WAN port.

4. 14. 2. Rule List

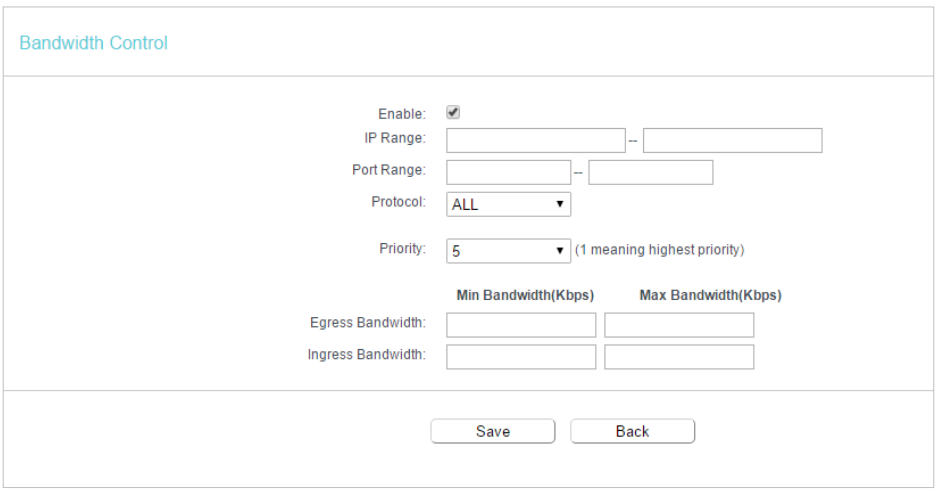
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Bandwidth Control and you can view and configure the Bandwidth Control rules.



- Description - This is the information about the rules such as address range.
- Egress Bandwidth - This field displays the max and min upload bandwidth through the WAN port. The default is 0.
- Ingress Bandwidth - This field displays the max and min download bandwidth through the WAN port. The default is 0.
- Status - This field displays the status of the rule.
- Modify - Click Modify/Delete to edit/delete the rule.

- **To add a Bandwidth control rule:**

1. Click Add New.
2. Enter the information as the figure shown below.



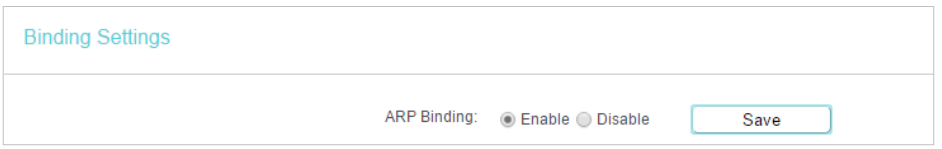
3. Click Save.

4. 15. 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. 15. 1. Binding Settings

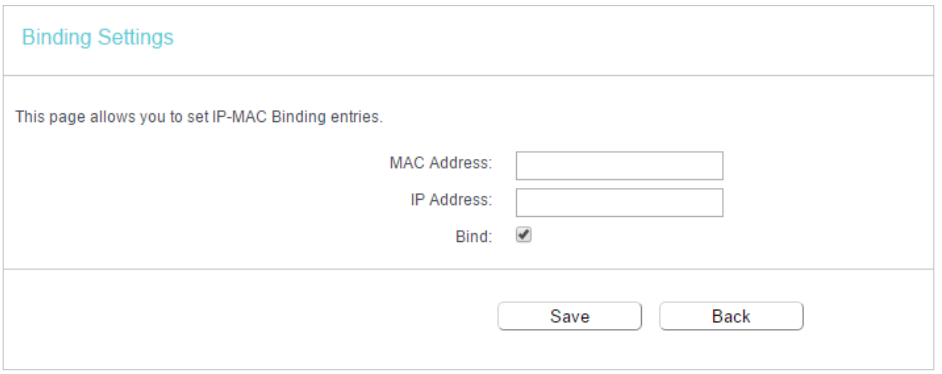
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to IP & MAC Binding > Binding Settings.
3. Select Enable for ARP Binding.



4. Click Save.

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

1. Click Add New.
2. Select the Bind checkbox.



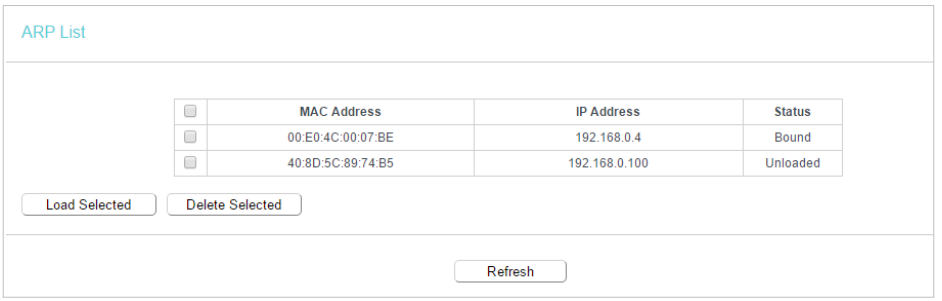
3. Enter the MAC address and IP address.
4. Click Save.

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

1. Select the desired entry in the table.
2. Click Edit or Delete Selected.

4. 15. 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.
- Configure - Load or delete an item.
    - Load - Load the item to the IP & MAC Binding list.
    - Delete - Delete the item.
- 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. Error warning will prompt as well.

4. 16. Dynamic DNS

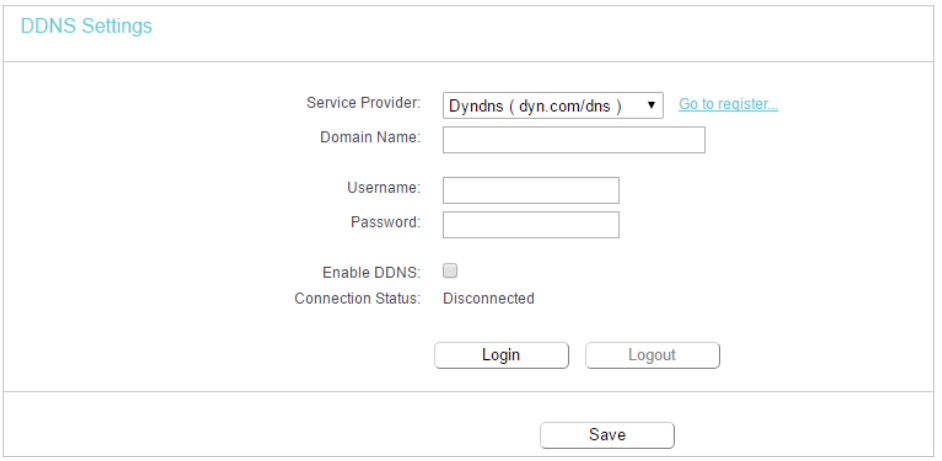
The router offers the DDNS (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address. Thus your friends can connect to your server by entering your domain name no matter what your IP 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 www.dyn.com, the following page will appear.



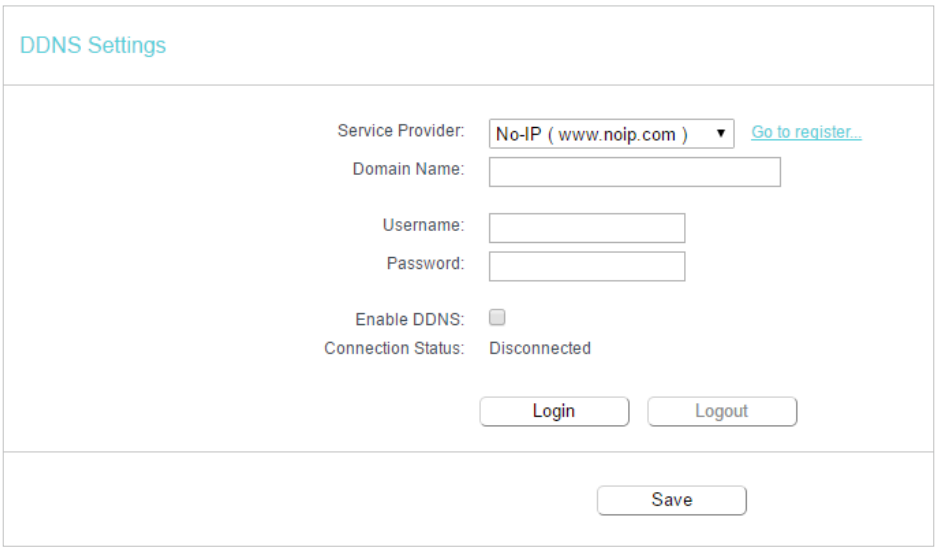
To set up for DDNS, follow these instructions:

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

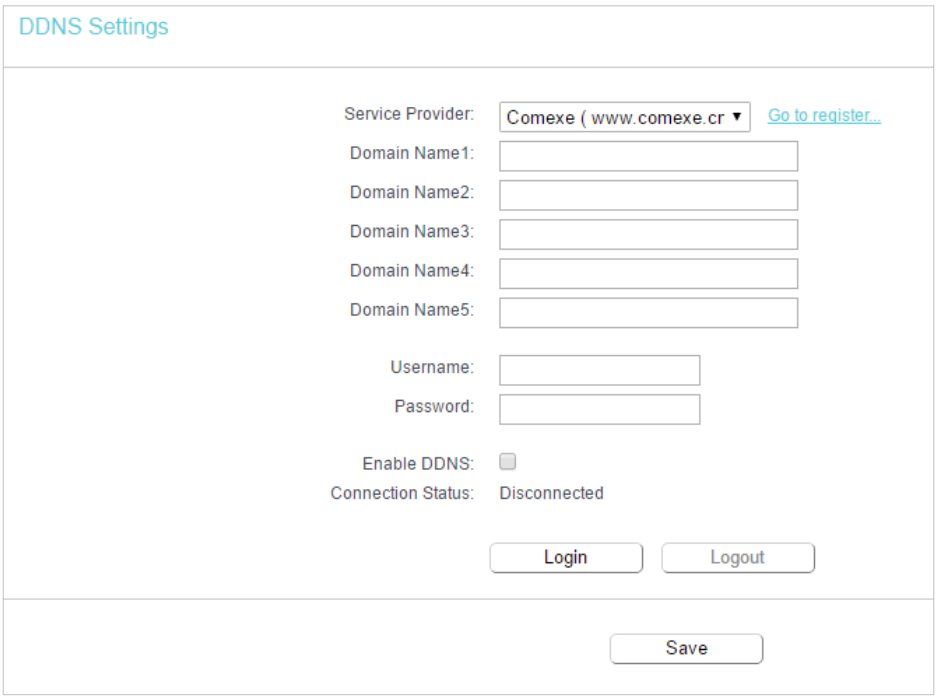
1. Enter the Domain Name you received from dynamic DNS service provider.

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.

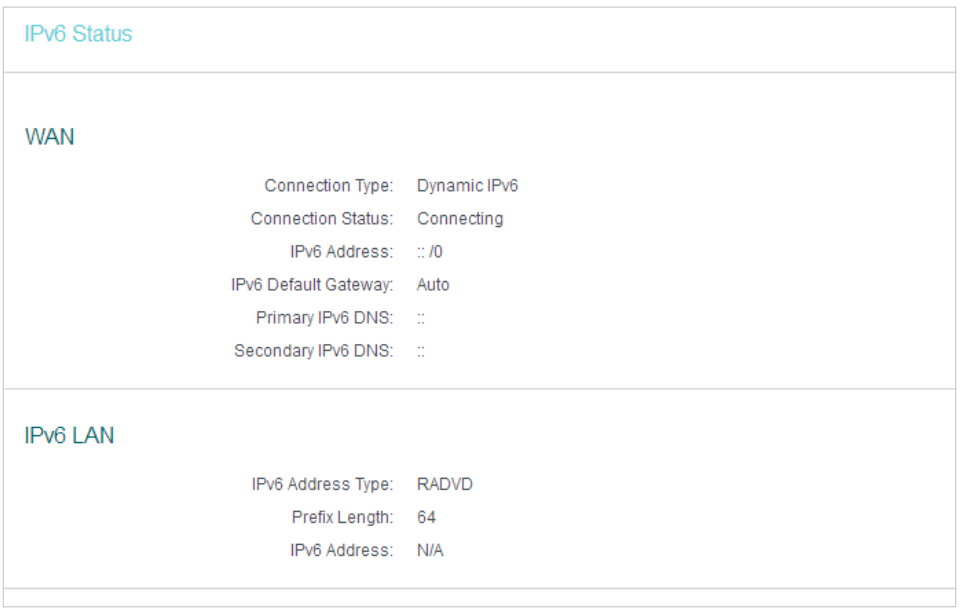
- Connection Status - The status of the DDNS service connection is displayed here.
- Logout - Click Logout to log out of the DDNS service.

4. 17. 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. 17. 1. IPv6 Status

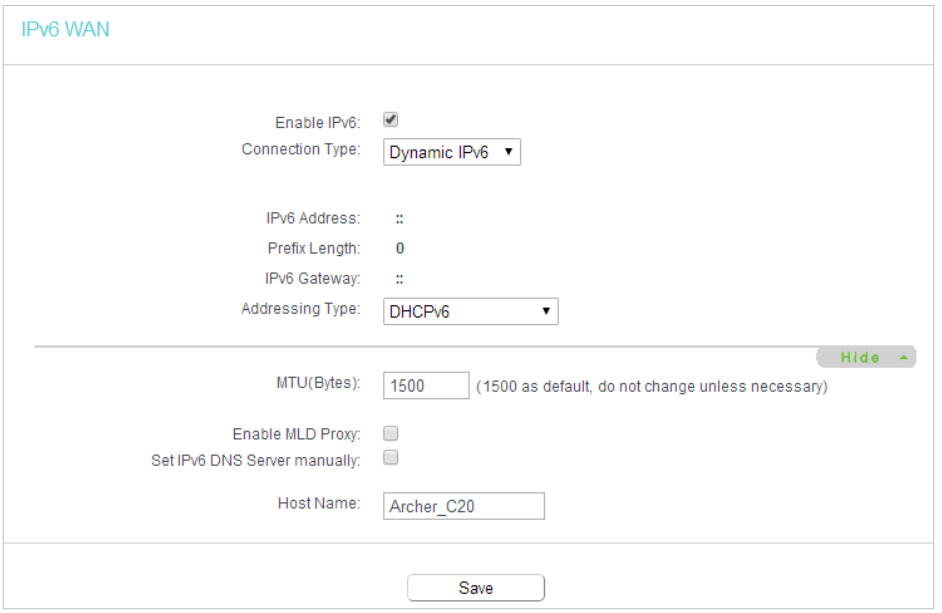
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to IPv6 > IPv6 Status, and you can view the current IPv6 status information of the router.



- WAN - This section shows the current IPv6 information of the router's WAN port, including Connection Type, IPv6 Address information, IPv6 Default Gateway, Primary IPv6 DNS and Secondary IPv6 DNS.
- IPv6 LAN - This section shows the current IPv6 information of the router's LAN port, including IPv6 Address Assign Type, IPv6 Address and Link-local Address.

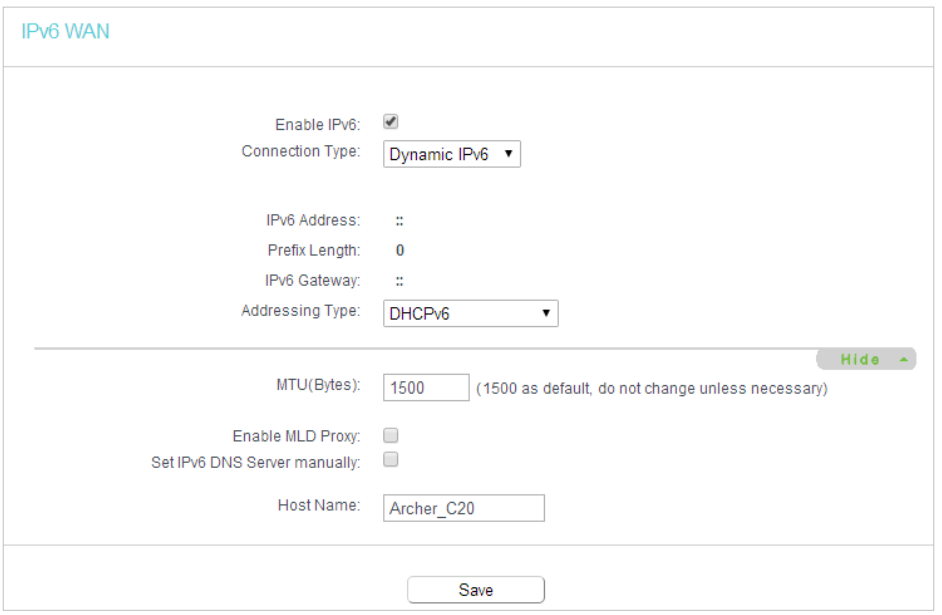
4. 17. 2. IPv6 WAN

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



3. Select the WAN Connection Type according to your ISP network topology:
   - 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.

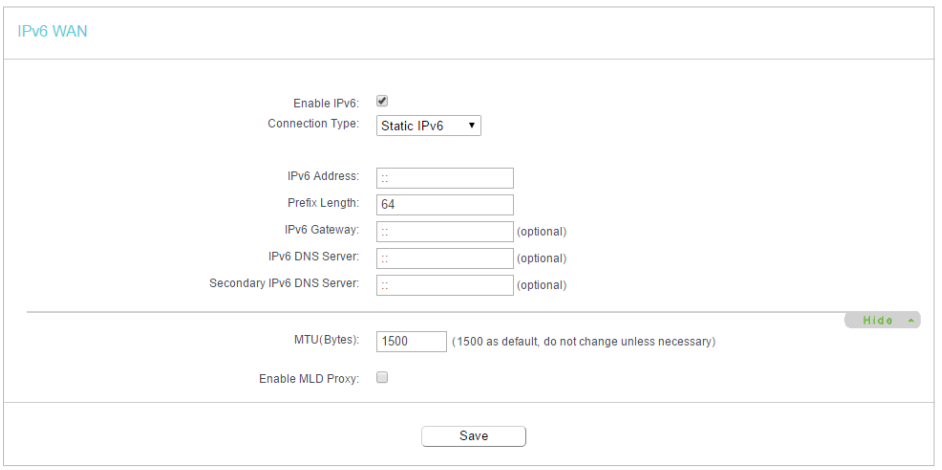
If your ISP gives you one or two DNS IPv6 addresses, select Set IPv6 DNS Server manually and enter the IPv6 DNS Server and Secondary IPv6 DNS Server into the correct fields. Otherwise, the DNS servers will be assigned from ISP dynamically.

- Enable MLD Proxy - Enable the Multicast Listener Discovery (MLD) Proxy function if you need.
- Set IPv6 DNS Server manually - Enter the DNS IPv6 address provided by your ISP.
- Secondary IPv6 DNS Server - Enter another DNS IPv6 address provided by your ISP.

Tips:

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

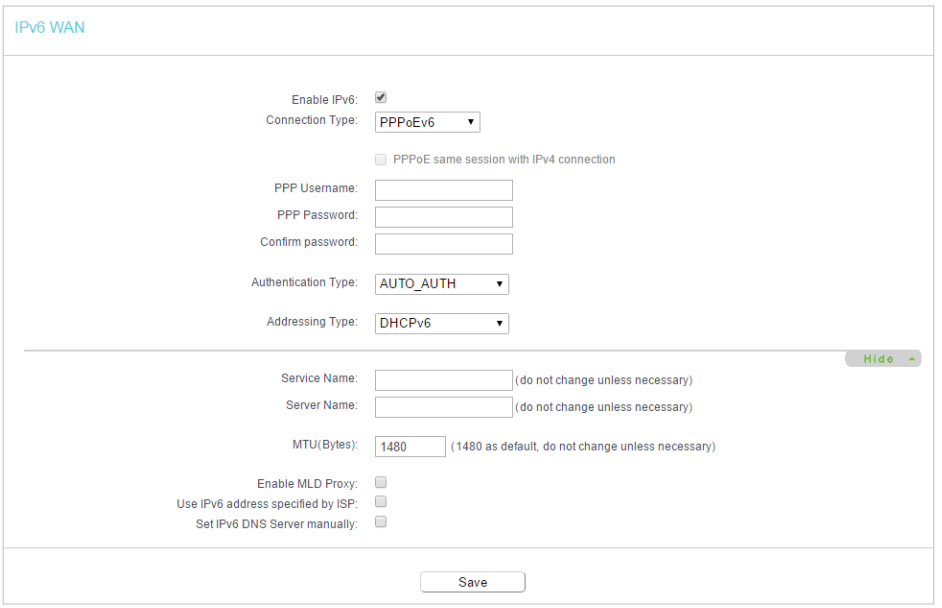
Static IPv6



- 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.

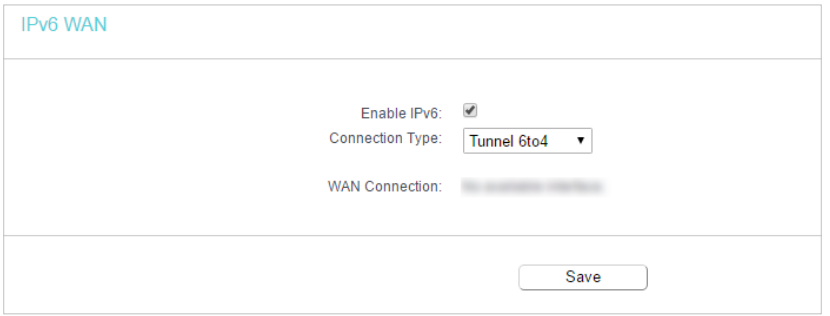
- MTU(Bytes) - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs, you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- Enable MLD Proxy - Enable the Multicast 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 1480 Bytes. It is not recommended that you change the default MTU size unless required by your ISP.
- 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

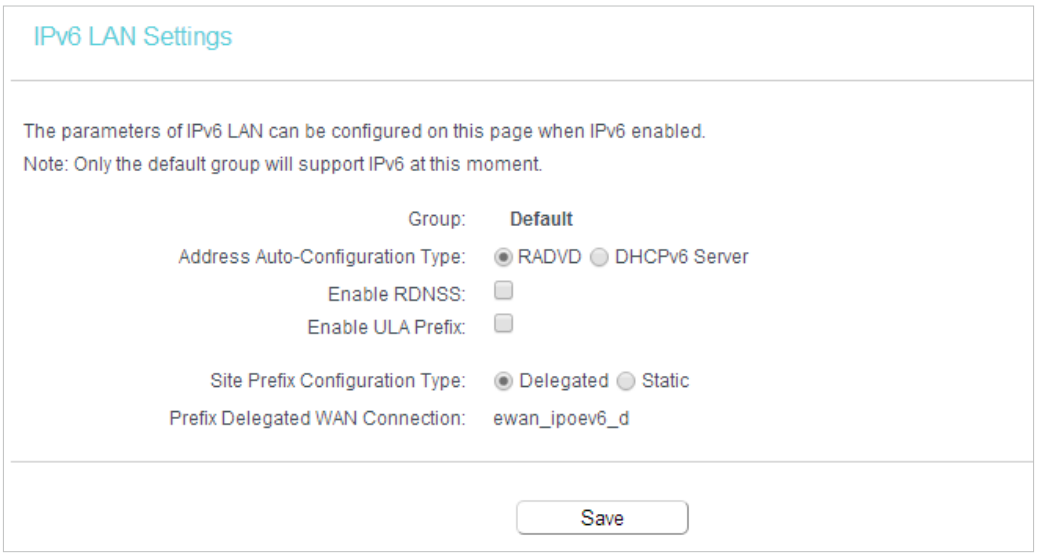


- WAN Connection - Display the available WAN connection.

4. Click Save.

4. 17. 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.



3. Select the Address Autoconfiguration Type which determines the way how the router assigns IPv6 address for PCs on the LAN:
   - Address Autoconfiguration Type - RADAD (Router Advertisement Daemon) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.
   - 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.

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

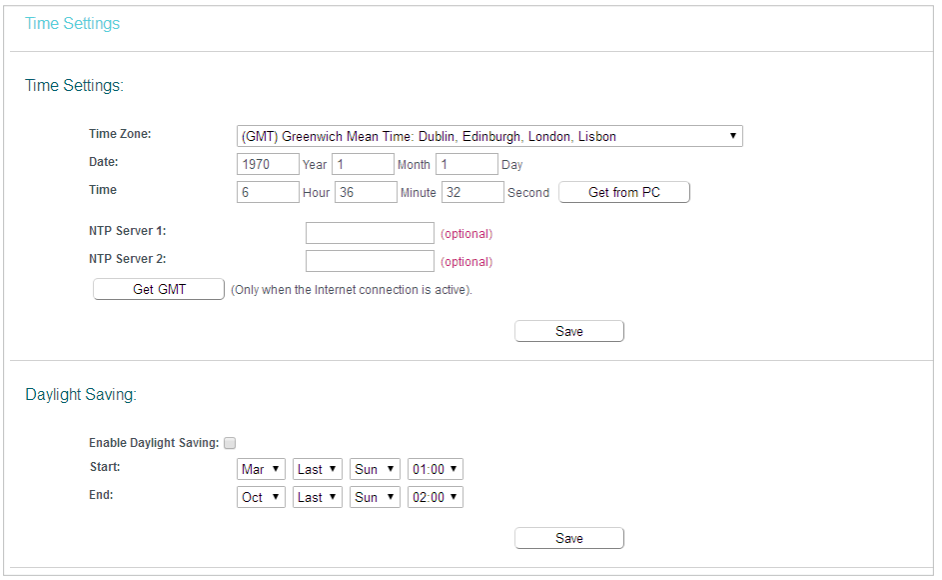
4. Click Save.

4. 18. System Tools

4. 18. 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:**

1. Select Enable DaylightSaving.
2. Select the start time from the drop-down list in the Start field.
3. Select the end time from the drop-down list in the End field.
4. Click Save.

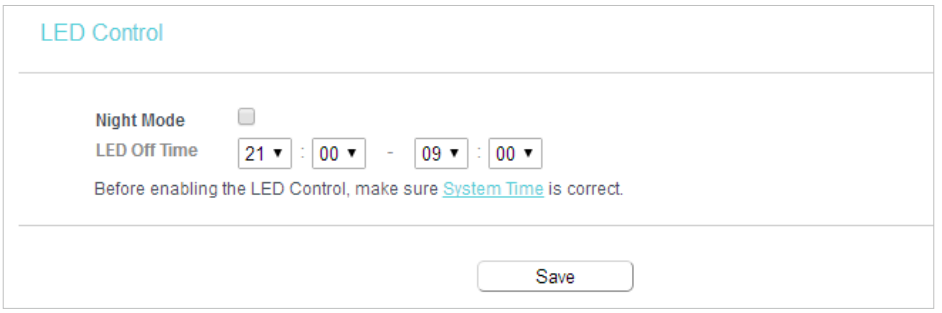
Note:

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. 18. 2. LED Control

The LED Control allows you to turn on or off the LEDs on your device according to a specific time schedule.

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

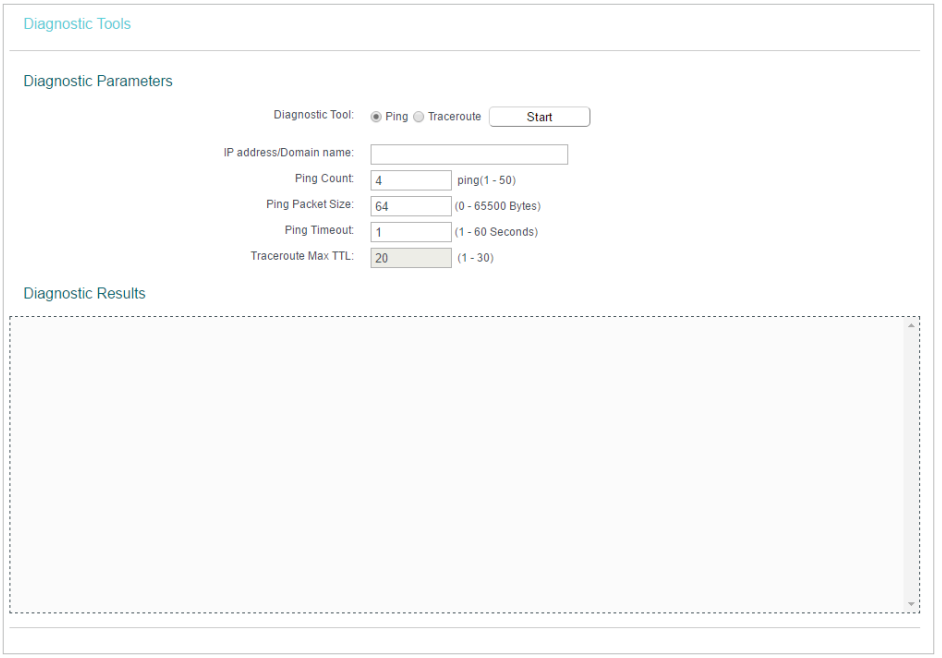


3. Enable the Night Mode.
4. Set the LED Off Time and click Save.

4. 18. 3. 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.



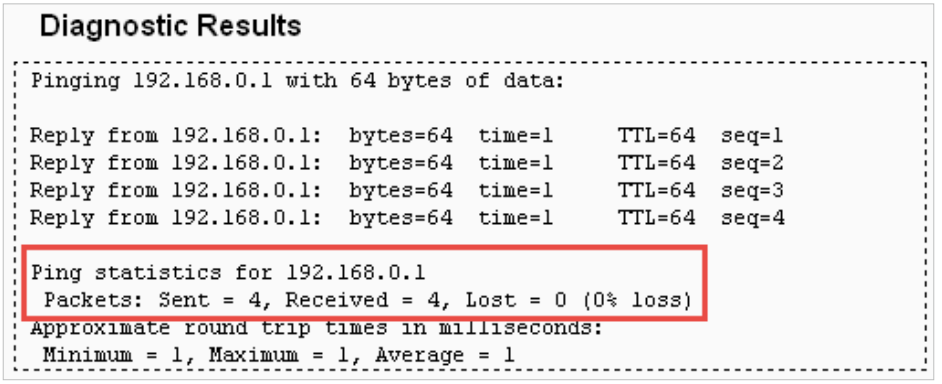
- Diagnostic Tool - Select one diagnostic tool.
  - Ping - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
  - Tracerouter - This diagnostic tool tests the performance of a connection.

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.

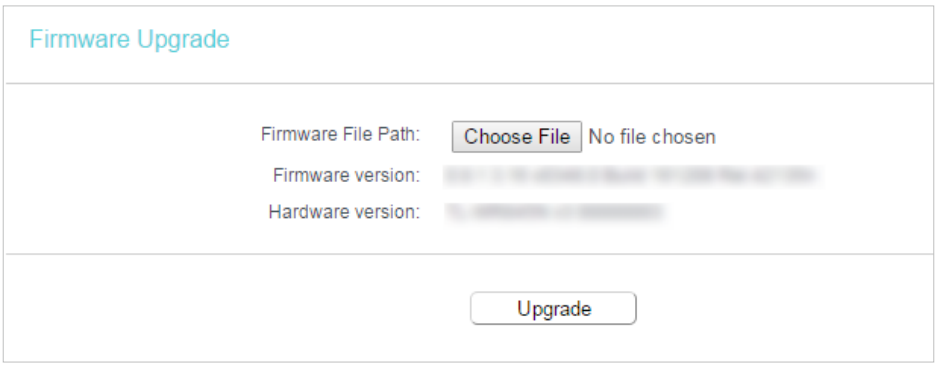


Note: Only one user can use this tool at one time. Options "Number of Pings", "Ping Size" and "Ping Timeout" are used for the Ping function. Option "Tracert Hops" is used for the Tracert function.

4. 18. 4. Firmware Upgrade

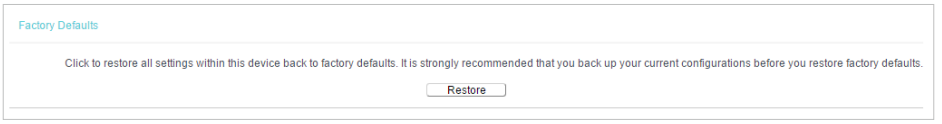
TP-Link is dedicated to improving and richening the product features, giving users a better network experience. We will release the latest firmware at TP-Link official website. You can download the latest firmware file from the Support page of our website www.tp-link.com and upgrade the firmware to the 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. 18. 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.

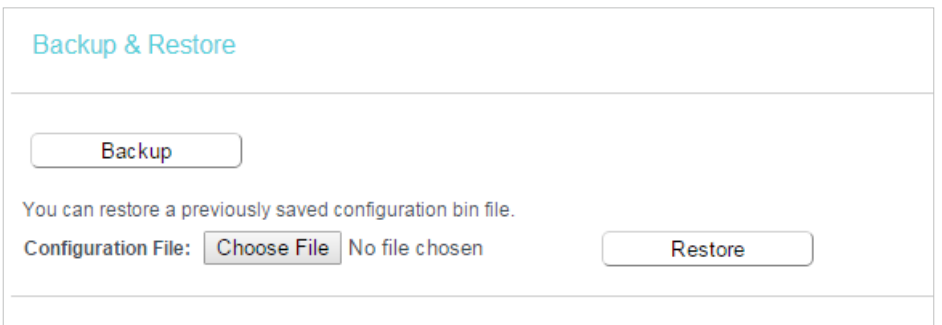


- The default Username: admin
- The default Password: admin
- The default IP Address: 192.168.0.1
- The default Subnet Mask: 255.255.255.0

4. 18. 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:**

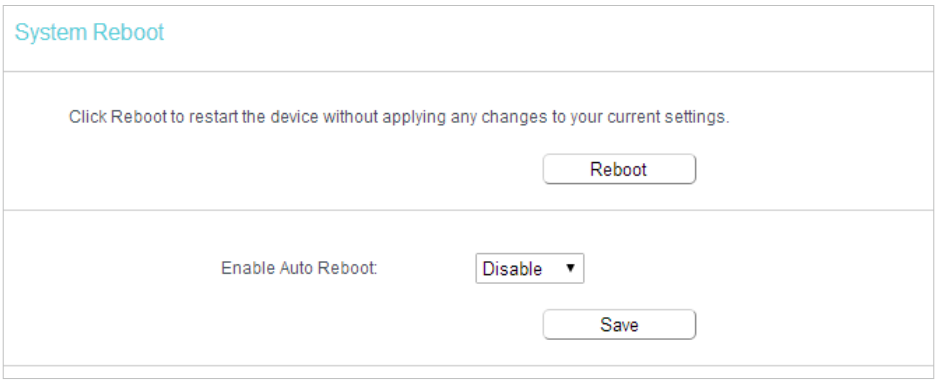
1. Click Choose File to locate the backup configuration file stored in your computer, and click Restore.
2. Wait a few minutes for the restoring and rebooting.

Note:

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

4. 18. 7. Reboot

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



3. Enable the auto reboot function as needed.
   - Disable - Disable the auto reboot function.
   - Timeout - Specify a time period(1-72 hours), then the router will reboot automatically after every this interval.
   - Schedule - The router will reboot automatically according to a specific time schedule.

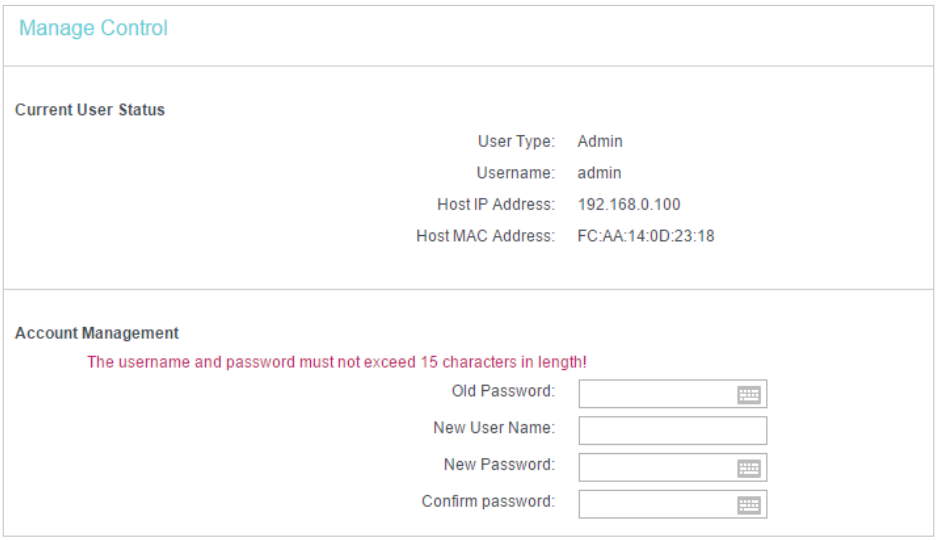
Some settings of the router will take effect only after rebooting, including:

- 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).

4. 18. 8. Administrator

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 you can change the factory default username and password of the router, and manage your router from a remote location via the internet.

- **To view and change the account settings:**



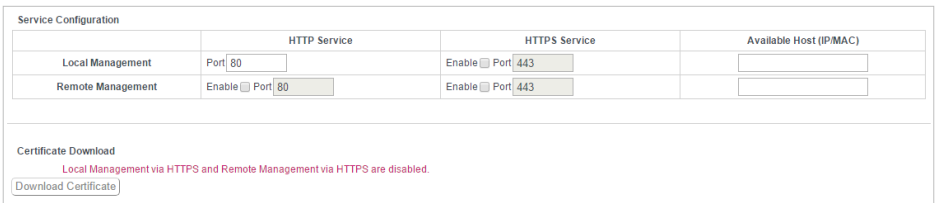
It is strongly recommended that you change the default username and password of the router, for all users that try to access the router's web management or Quick Setup will be prompted for the router's username and password.

Note:

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

- **To manage your router via the internet:**

1. Specify the management web port number and click Save.



- Port - The default management web port number is 80 for HTTP, 443 for HTTPS. For greater security, you can change the management web port to a number between 1024 and 65535 but do not use the number of any common service port. Tick Enable to enable local or remote management via HTTP or HTTPS.
- Available Host (IP/MAC) - This is the current address you will use when accessing your router from the internet.
- Certificate - A file that provides you with authentication information. Download and install the certificate for Local/Remote Management via HTTPS if you need it. Once the certificate is installed, warnings will not pop up when you access the router via HTTPS.

2. Enter your router's WAN IP address into your browser's address bar, followed by a colon and the custom port number you set in the Web Management Port box. For example, if your Router's WAN address is 202.96.12.8 and you use port number 8080, enter http://202.96.12.8:8080 in your browser.

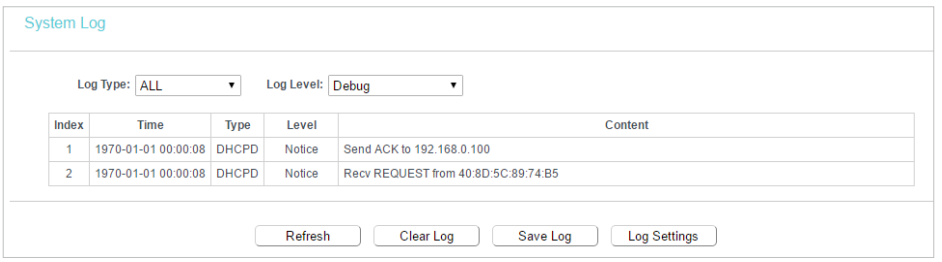
3. Enter the router's password to access the web mangement page.

Note:

- Be sure to change the router's default password to a secure password.
- If the web management port conflicts with the one used for a Virtual Server entry, the entry will be automatically disabled after the setting is saved.

4. 18. 9. System Log

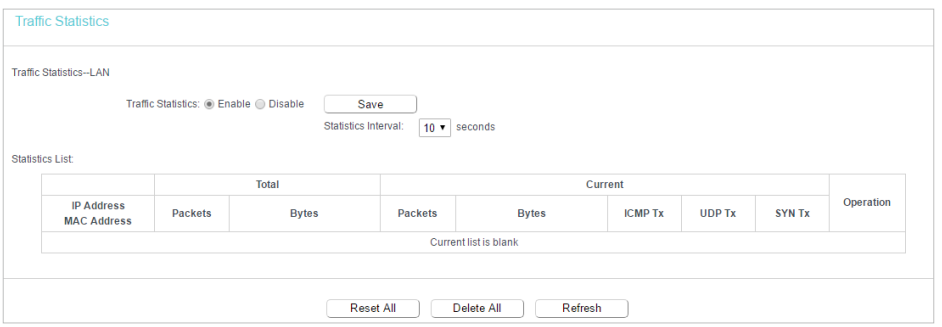
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to System Tools > System Log, and you can view the logs of the router.



- 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.

4. 18. 10. Traffic Statistics

1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to System Tools > Statistics, and you can monitor the network traffic of each device on the LAN, including total traffic and the value of the last Packets Statistic interval in seconds.



3. Enable Traffic Statistics. If it is disabled, the function of DoS protection in Security settings will be disabled.
   - Statistics Interval - The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval value indicates the time section of the packets statistic.
   - IP Address/MAC Address - The IP Address and MAC address are displayed with related statistics.
   - Total
     - Packets - The total number of packets received and transmitted by the Router.
     - Bytes - The total number of bytes received and transmitted by the Router.
   - Current
     - Packets - The number of packets received and transmitted per second at the specified Packets Statistics interval.
     - Bytes - The number of bytes received and transmitted per second at the specified Packets Statistics interval.
     - ICMP Tx - The number of ICMP packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
     - UDP Tx - The number of UDP packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
     - TCP SYN Tx - The number of TCP SYN packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
   - Operation
     - Reset - Renew the values of the entry to zero.
     - Delete - Delete the existing entry in the table.

Click the Refresh button to refresh the page.

Click the Reset All button to reset the values of all entries to zero.

Click the Delete All button to delete all entries in the table.

4. 19. Log Out

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

Chapter 5

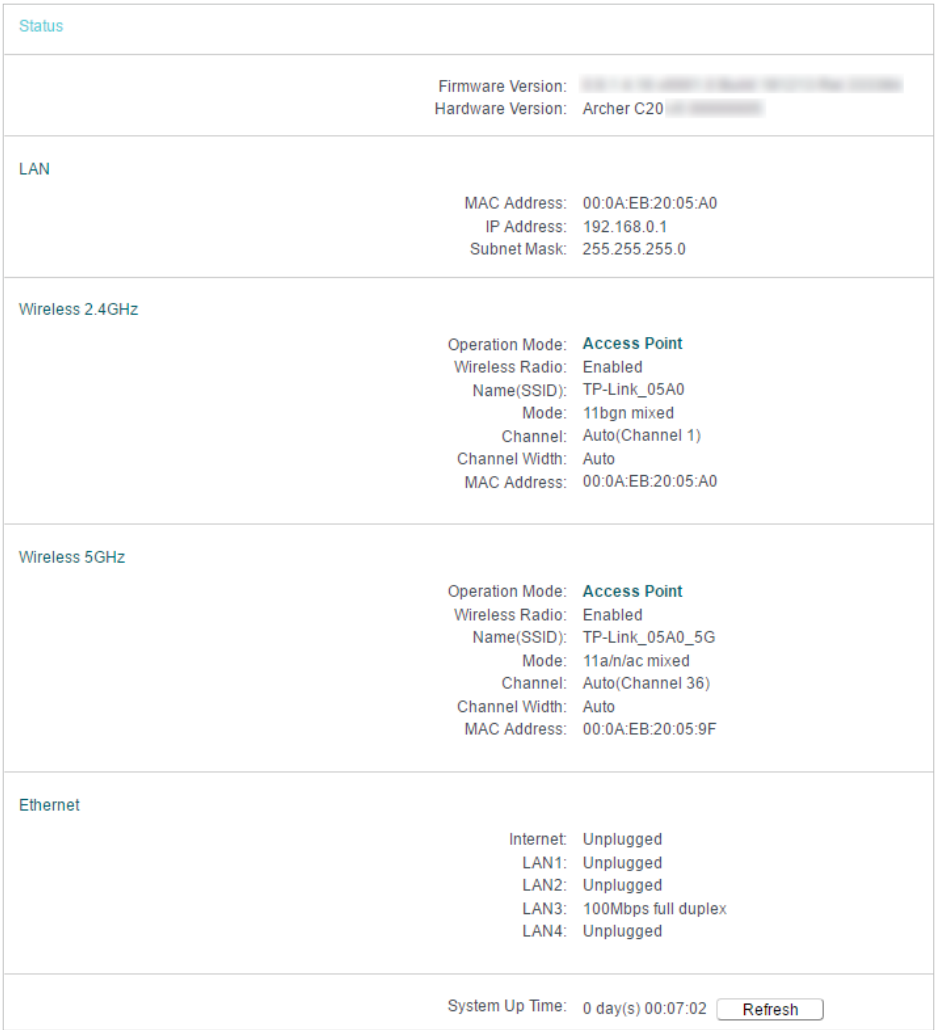
Configure the Router in Access Point Mode

This chapter presents how to configure the various features of the router in Access Point Mode.

It contains the following sections:

5. 1. Status

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



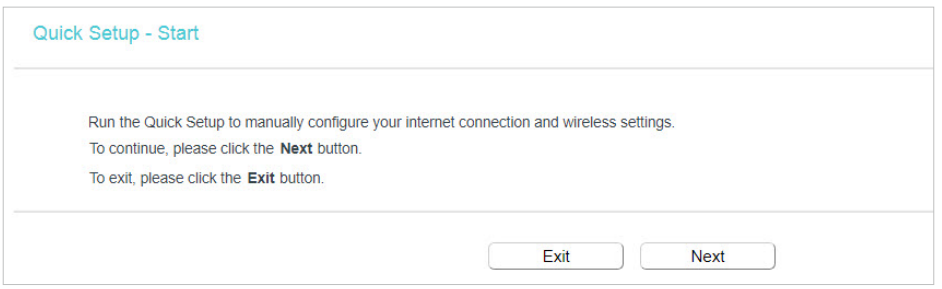
- Firmware Version - The version information of the router's firmware.
- Hardware Version - The version information of the router's hardware.
- LAN - This field displays the current settings of the LAN, and you can configure them on the Network > LAN page.
    - MAC address - The physical address of the router.
    - IP address - The LAN IP address of the router.
    - Subnet Mask - The subnet mask associated with the LAN IP address.
- Wireless 2.4GHz/5GHz - 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.

- Ethernet - Displays the current status of the Ethernet ports.
- System Up Time - The length of time since the AP was last powered on or reset. Click Refresh to get the latest status and settings of the AP.

5. 2. Quick Setup

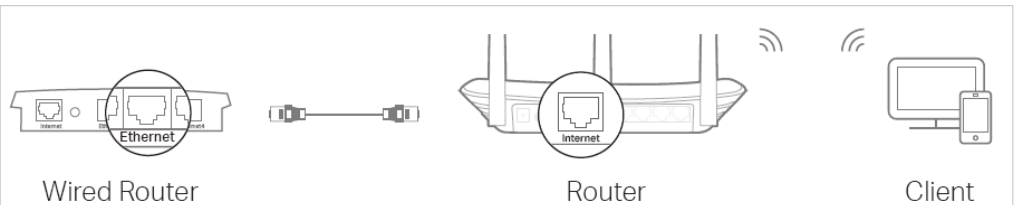
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Quick Setup.



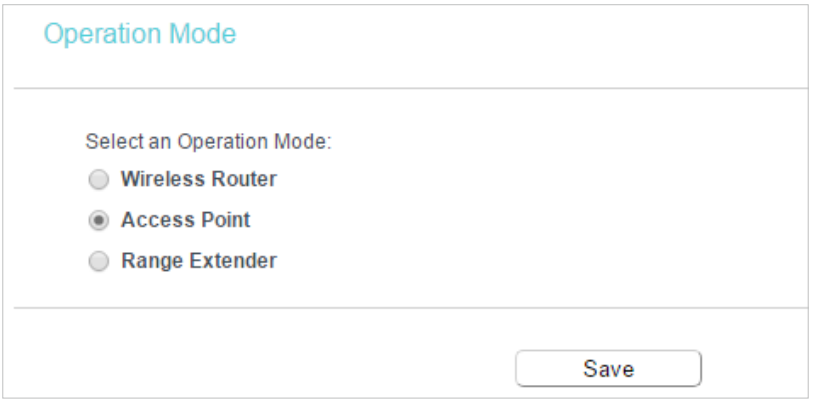
3. Click Next to start. Then follow the step-by-step instructions to connect your router to the internet.

5. 3. Operation Mode

The router supports three operation modes: Wireless Router mode, Access Point mode and Range Extender. In Access Point mode, the device can be connected to a wired network and transform the wired access into wireless one. If you already have a wired router, you can use this mode. To switch to Access Point mode:



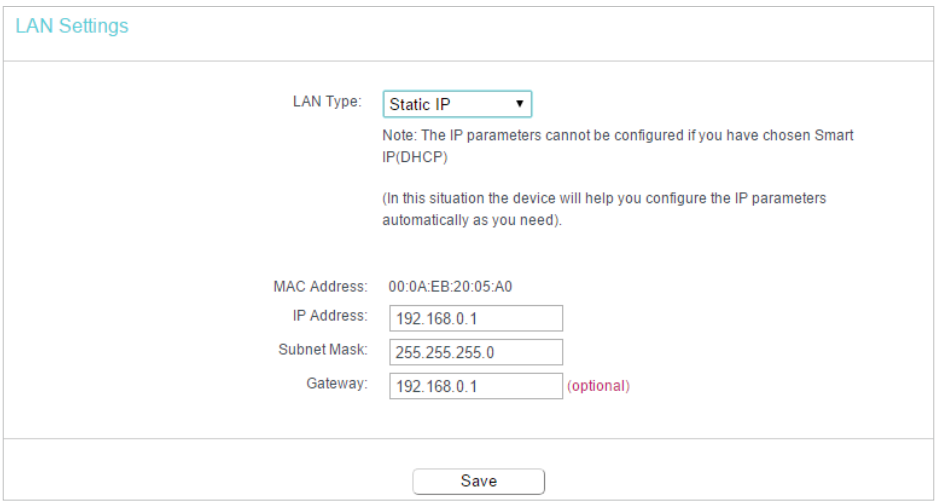
1. Find the router's Internet port, and connect it to the Ethernet port (LAN port) of your existing wired router. Then connect the power adapter and turn on the router.
2. Connect your computer to the router via an Ethernet cable or wirelessly by using the SSID (network name) and Wireless Password printed on the label at the bottom of the router.
3. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
4. Go to Operation Mode.
5. Select the Access Point mode and click Save.



5. 4. Network

5. 4. 1. LAN

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



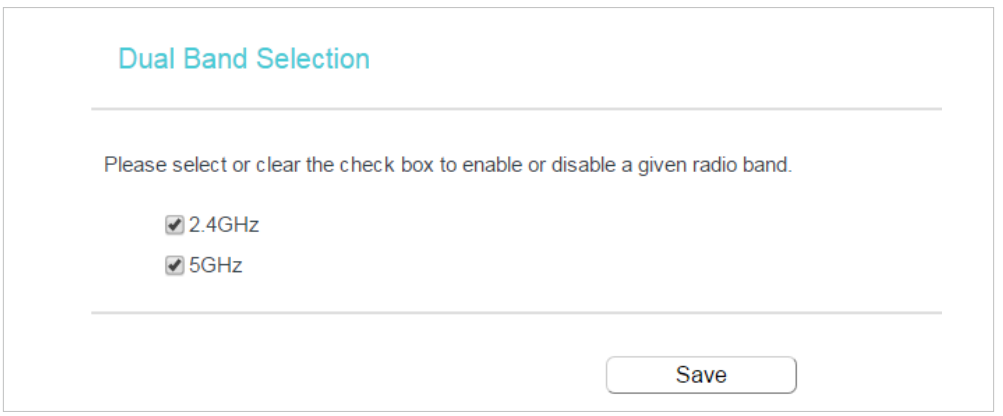
- LAN Type - Select Smart IP(DHCP) to get IP address from DHCP server, or select static IP to configure IP address manually.
- MAC Address - The physical address of the LAN ports. The value can not be changed.
- IP Address - Enter the IP address in dotted-decimal notation of your router.
- Subnet Mask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

Note:

- If you change the IP address, you must use the new IP address to login to the device.
- If you select the type of smart IP(DHCP), the DHCP server in this device will not startup.
- If the new IP address you set is not in the same subnet with the previous one, the IP Address pool in the DHCP server will be configured automatically.

5. 5. Dual Band Selection

1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Dual Band Selection.
3. Select the working radio band as needed and click Save.

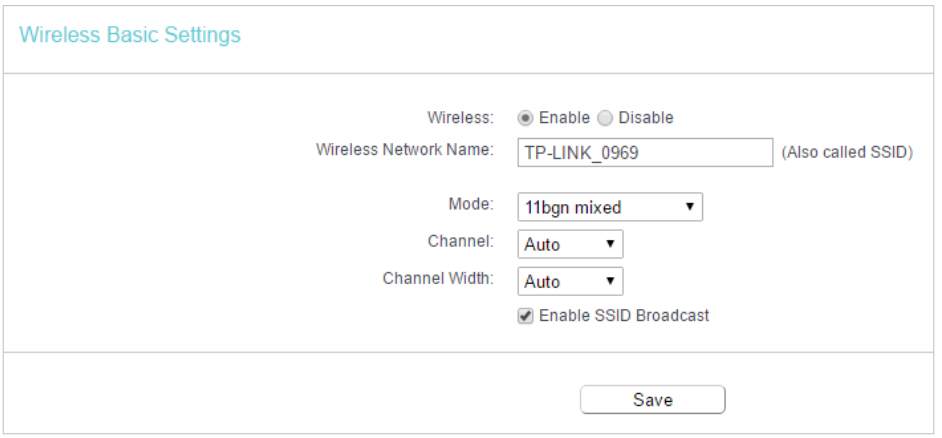


5. 6. Wireless(2.4GHz or 5GHz)

5. 6. 1. Wireless 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).

5. 6. 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.

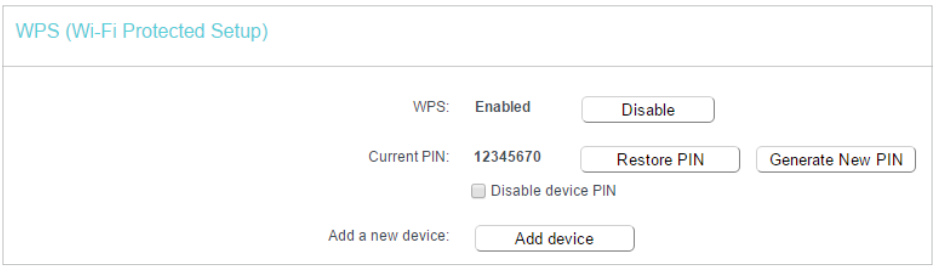
Note:

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.

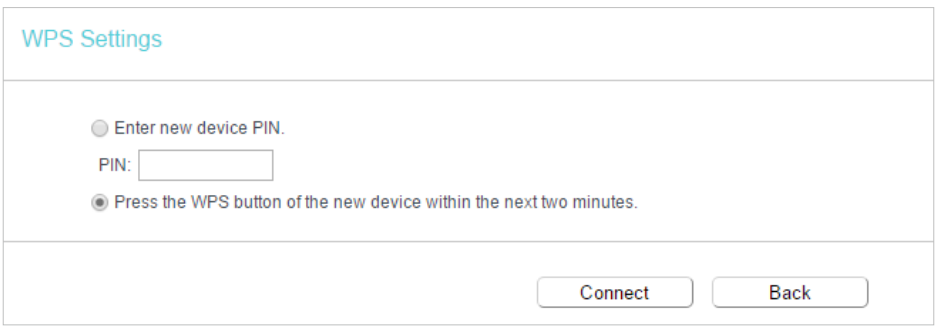
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Wireless > WPS.
3. Follow one of the following three methods to connect your client device to the router's Wi-Fi network.

Method ONE: Press the WPS Button on Your Client Device

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



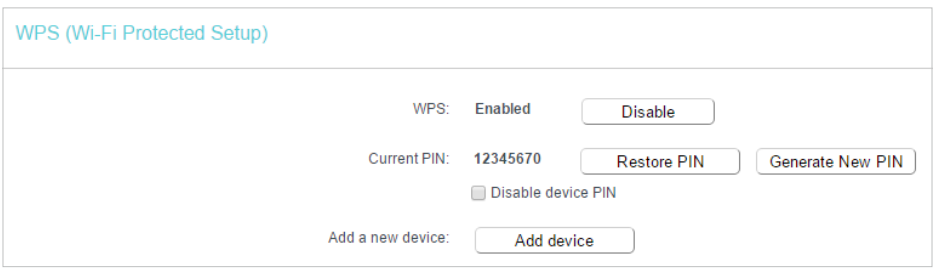
2. Select Press the WPS button of the new device within the next two minutes and click Connect.



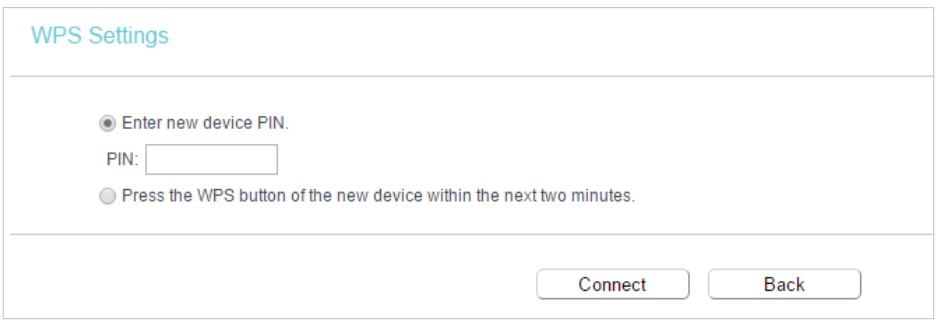
3. Within two minutes, press the WPS button on your client device.
4. A success message will appear on the WPS page if the client device has been successfully added to the router's network.

Method TWO: Enter the Client's PIN

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



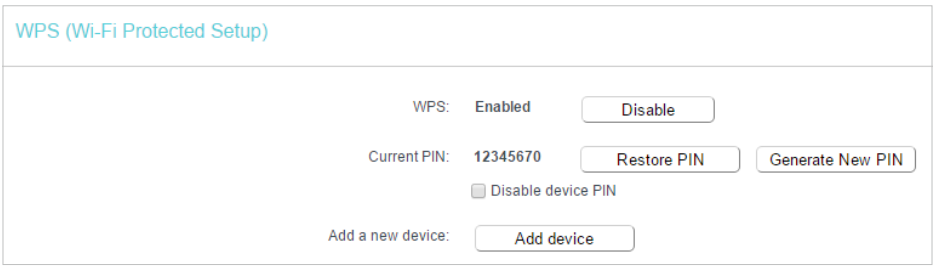
2. Select Enter new device PIN, enter your client device's current PIN in the PIN filed and click Connect.



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

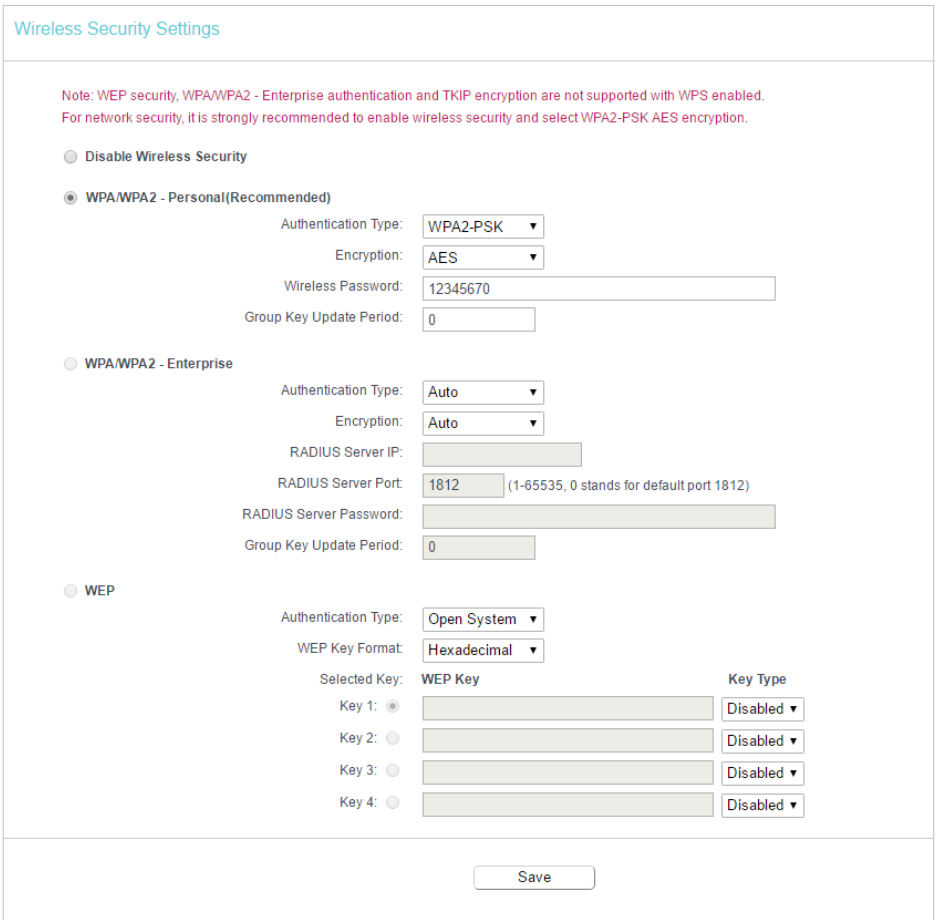
1. Keep the WPS Status as Enabled and get the Current PIN of the router.



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

5. 6. 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.
    - Authentication Type - Select Auto, WPA-PSK or WPA2-PSK.
    - Encryption - Select Auto, TKIP or AES.
    - Wireless Password - Enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters.
    - Group Key Update Period - Specify the group key update interval in seconds. The value can be 0 or at least 30. Enter 0 to disable the update.
- WPA /WPA2-Enterprise - It's based on Radius Server.
    - Authentication Type - Select Auto, WPA or WPA2.
    - Encryption - Select Auto, TKIP or AES.
    - Radius Server IP - Enter the IP address of the Radius server.
    - Radius Server Port - Enter the port that Radius server used.
    - Radius Server Password - Enter the password for the Radius server.
    - Group Key Update Period - Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.
- WEP - It is based on the IEEE 802.11 standard.
    - Authentication Type - The default setting is Auto, which can select Shared Key or Open System authentication type automatically based on the wireless client's capability and request.
    - WEP Key Format - Hexadecimal and ASCII formats are provided here. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. ASCII format stands for any combination of keyboard characters in the specified length.
    - WEP Key (Password) - Select which of the four keys will be used and enter the matching WEP key. Make sure these values are identical on all wireless clients in your network.
    - Key Type - Select the WEP key length (64-bit, 128-bit or 152-bit) for encryption. Disabled means this WEP key entry is invalid.
    - 64-bit - Enter 10 hexadecimal digits (any combination of 0-9, a-f and A-F. Null key is not permitted) or 5 ASCII characters.
    - 128-bit - Enter 26 hexadecimal digits (any combination of 0-9, a-f and A-F. Null key is not permitted) or 13 ASCII characters.

5. 6. 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.

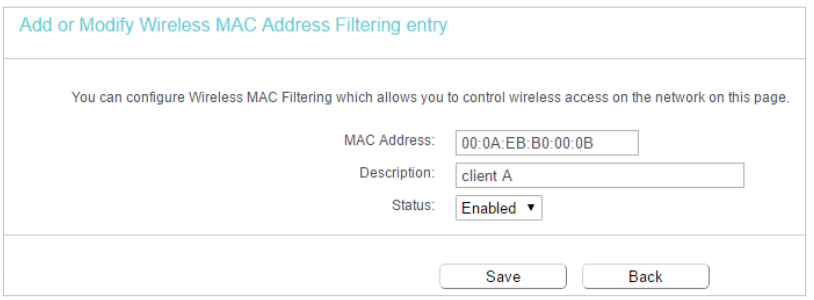
I want to:

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.

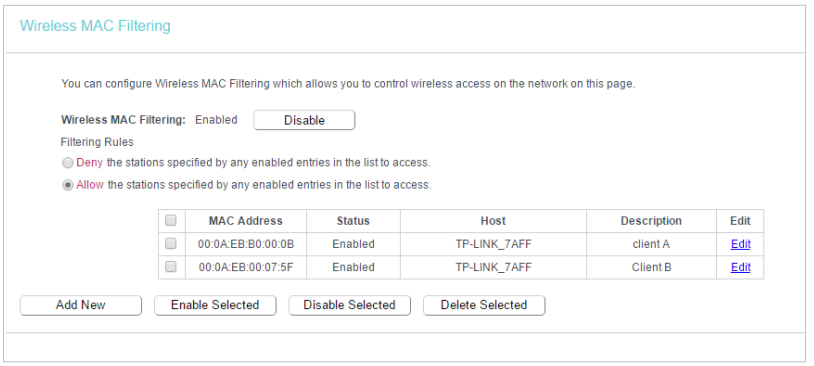
How can I do that?

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!

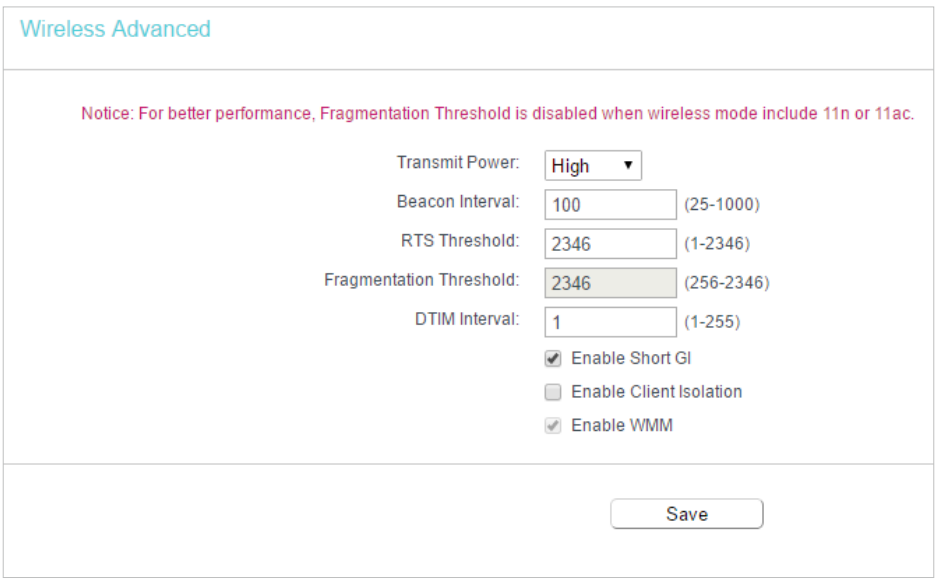
Now only client A and client B can access your network.

5. 6. 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.



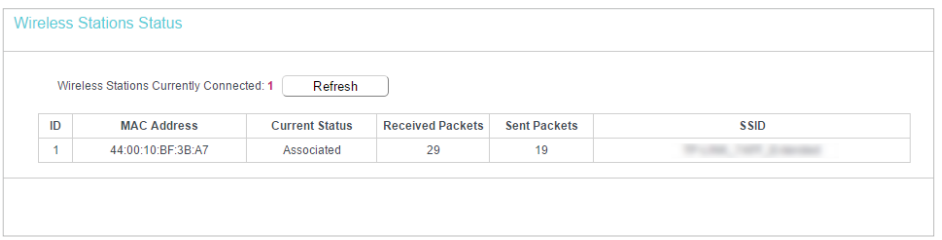
- Transmit Power - Select High, Middle or Low which you would like to specify for the router. High is the default setting and recommended.
- Beacon Interval - Enter a value between 40-1000 milliseconds for Beacon Interval here. Beacon Interval value determines the time interval of the beacons. The beacons

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.
- Enable WMM - WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended to enable this function.

5. 6. 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.

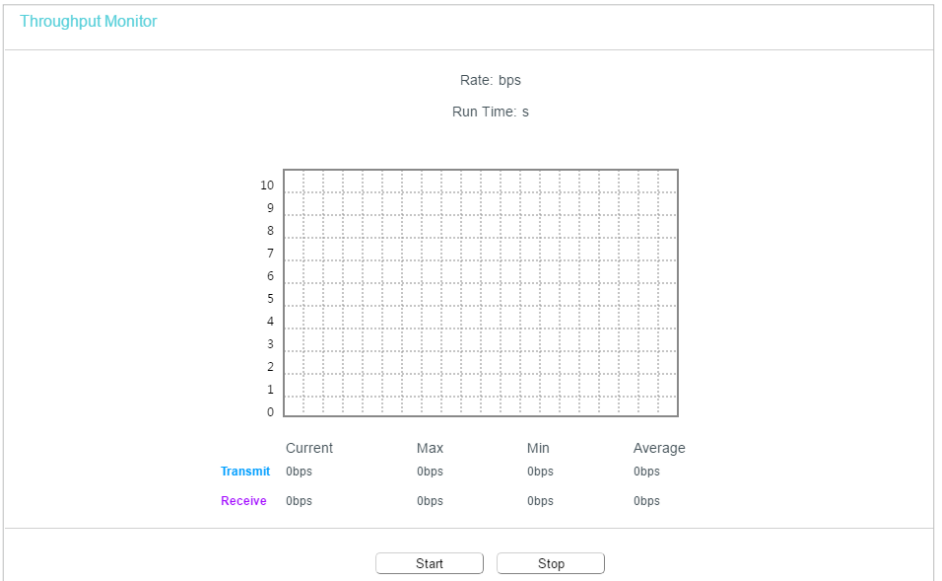


- MAC Address - The MAC address of the connected wireless client.
- Current Status - The running status of the connected wireless client.
- Received Packets - Packets received by the wireless client.
- Sent Packets - Packets sent by the wireless client.

- SSID - SSID that the station associates with.

5. 6. 7. Throughout Monitor

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



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

Click Start to start wireless throughput monitor.

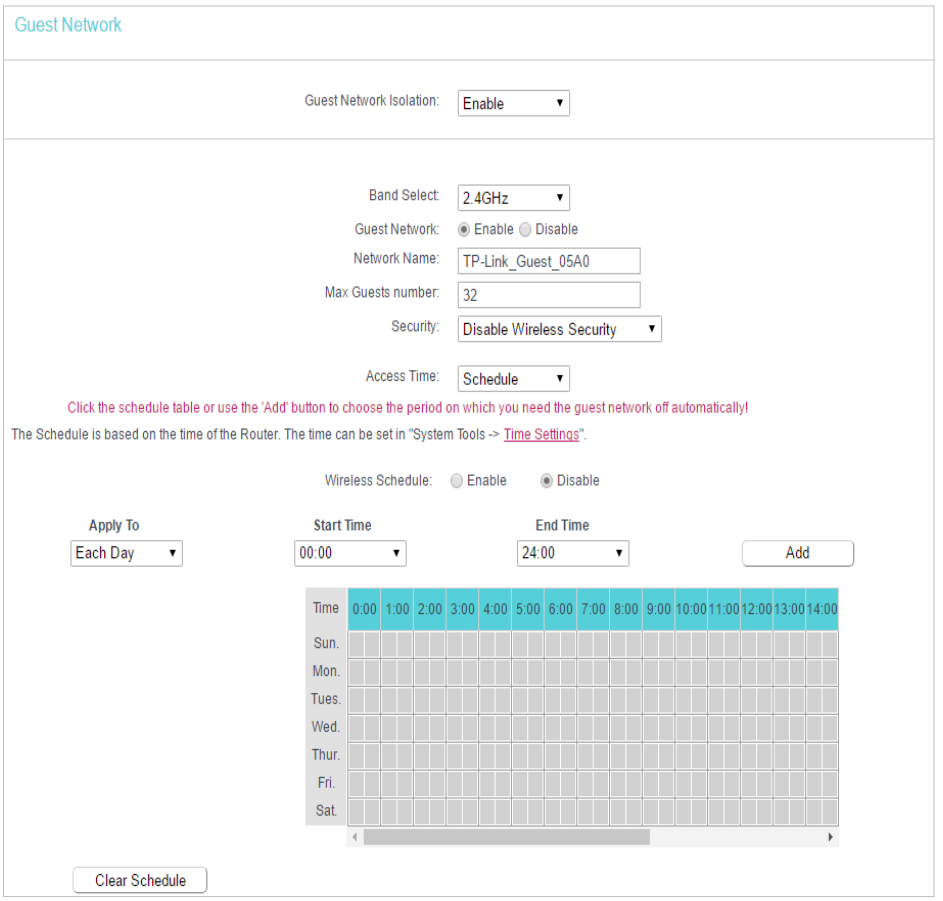
Click Stop to stop wireless throughput monitor.

5. 7. 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.

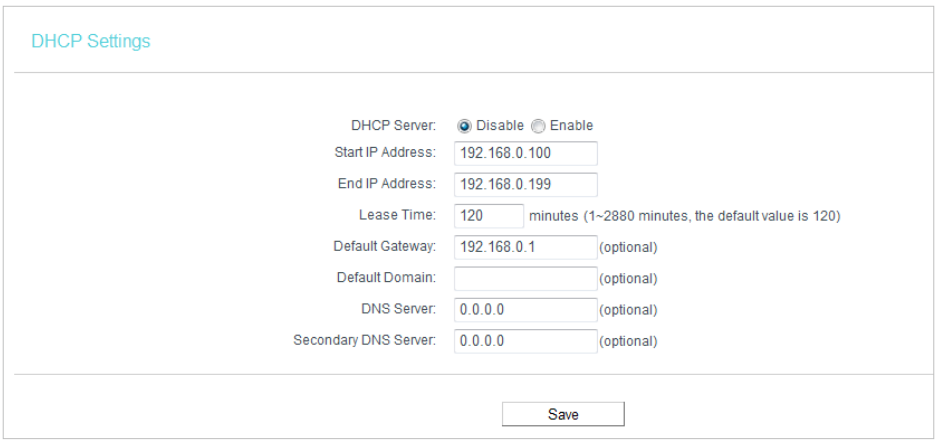
5. 8. DHCP

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. 8. 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.

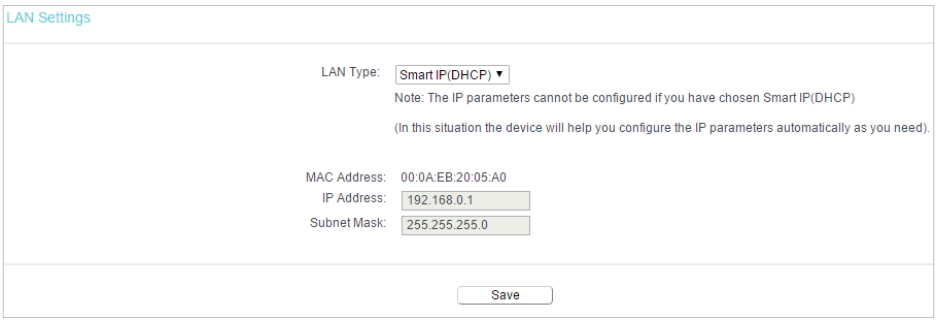
3. Specify DHCP server settings and click Save.



- 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 1.
- Default Gateway (Optional) - It is suggested to input the IP address of the LAN port of the router. The default value is 192.168.0.1.
- Default Domain (Optional) - Input the domain name of your network.
- DNS Server (Optional) - Input the DNS IP address provided by your ISP.
- Secondary DNS Server (Optional) - Input the IP address of another DNS server if your ISP provides two DNS servers.

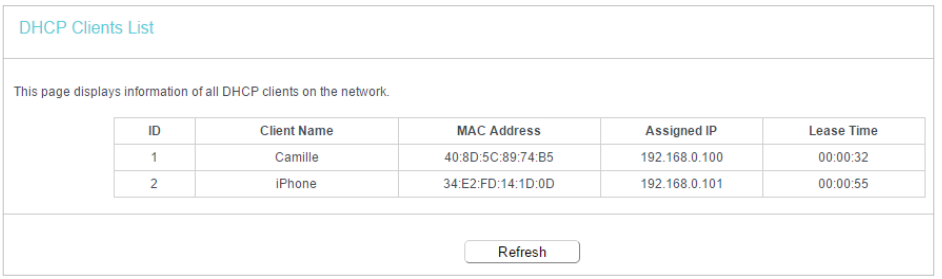
Note:

- To use the DHCP server function of the router, you must configure all computers on the LAN as Obtain an IP Address automatically.
- When you choose Smart IP (DHCP) in Network > LAN, the DHCP Server function will be disabled. You will see the page as below.



5. 8. 2. DHCP Client List

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



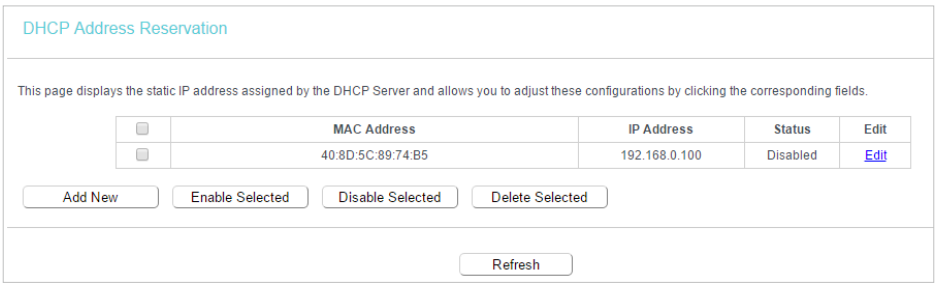
- Client Name - The name of the DHCP client.
- MAC Address - The MAC address of the DHCP client.
- Assigned IP - The IP address that the outer has allocated to the DHCP client.
- Lease Time - The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic IP address will be 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. 8. 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 blank.



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.

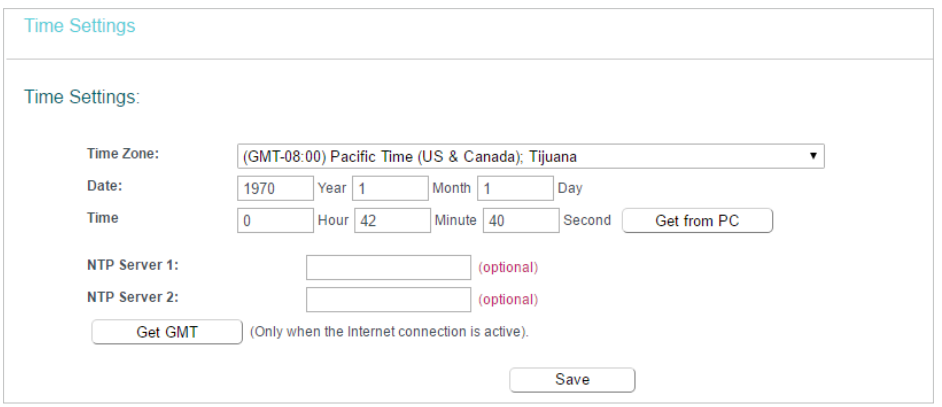
4) Click Save.

5. 9. System Tools

5. 9. 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 I or NTP Server II.
7. Click Get GMT to get time from the internet if you have connected to the internet.

- **To set Daylight Saving Time:**

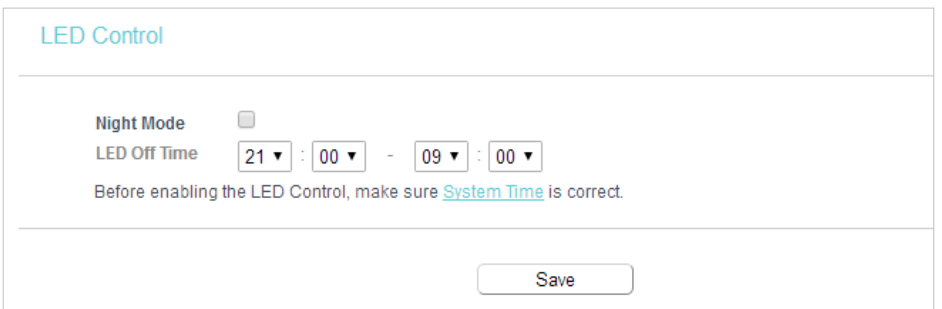
1. Select Enable DaylightSaving.
2. Select the start time from the drop-down list in the Start field.
3. Select the end time from the drop-down list in the End field.
4. Click Save.

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. 9. 2. LED Control

The LED Control allows you to turn on or off the LEDs on your device according to a specific time schedule.

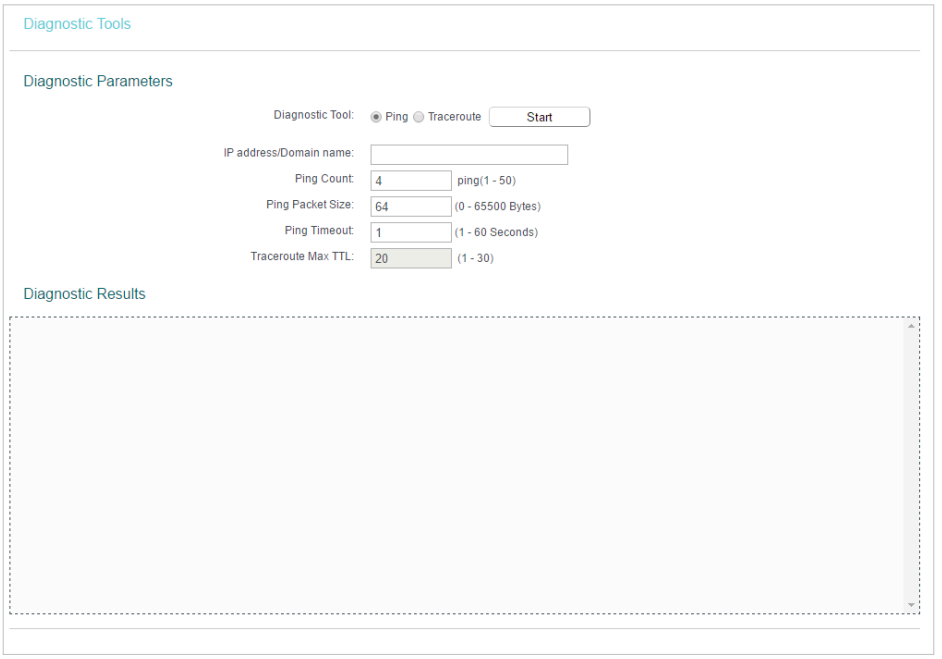
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to System Tools > LED Control.



5. 9. 3. 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.



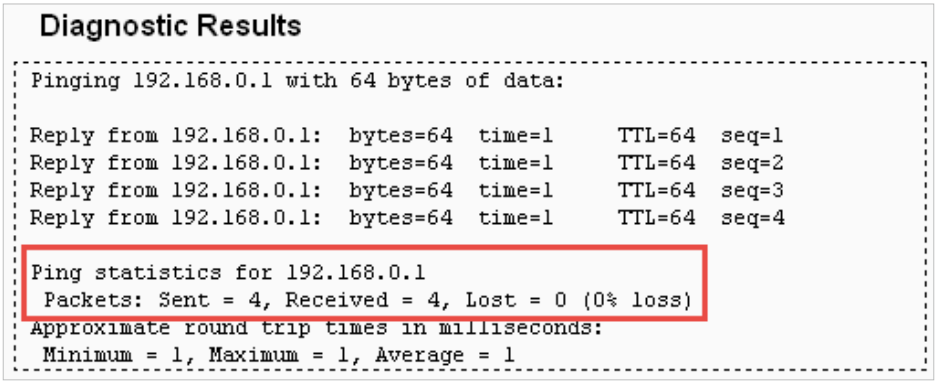
- Diagnostic Tool - Select one diagnostic tool.
  - Ping - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
  - Tracerouter - This diagnostic tool tests the performance of a connection.

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.

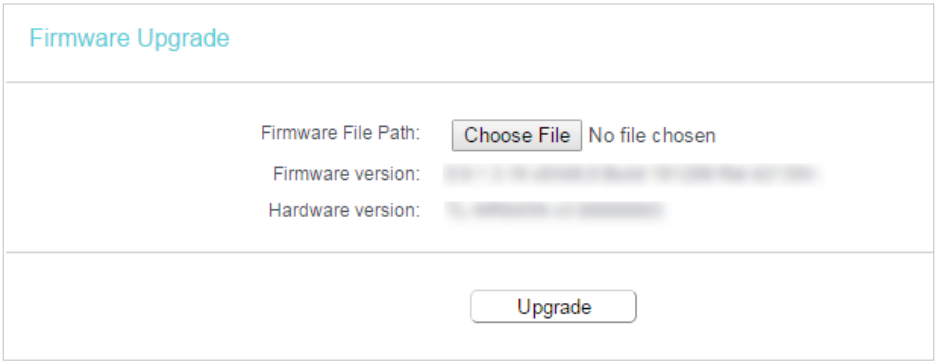


Note: Only one user can use this tool at one time. Options "Number of Pings", "Ping Size" and "Ping Timeout" are used for the Ping function. Option "Tracert Hops" is used for the Tracert function.

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

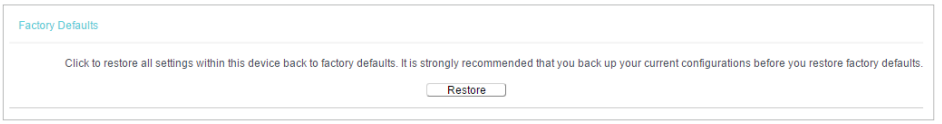
1. Download the latest firmware file for the router from our website www.tp-link.com.
2. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
3. Go to System Tools > Firmware Upgrade.
4. Click Choose File to locate the downloaded firmware file, and click Upgrade.



5. 9. 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.

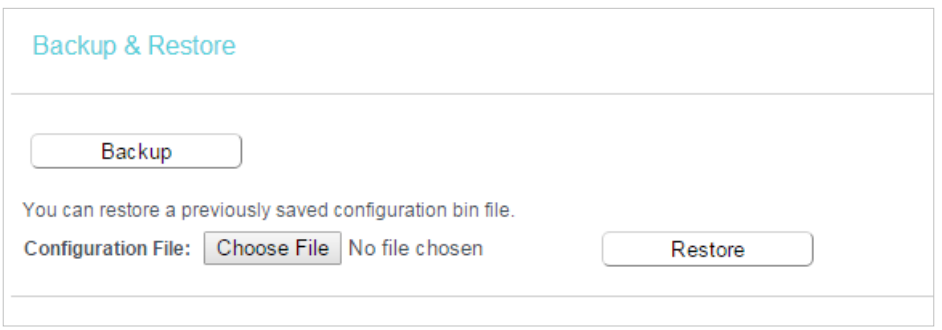


- The default Username: admin
- The default Password: admin
- The default IP Address: 192.168.0.1
- The default Subnet Mask: 255.255.255.0

5. 9. 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.

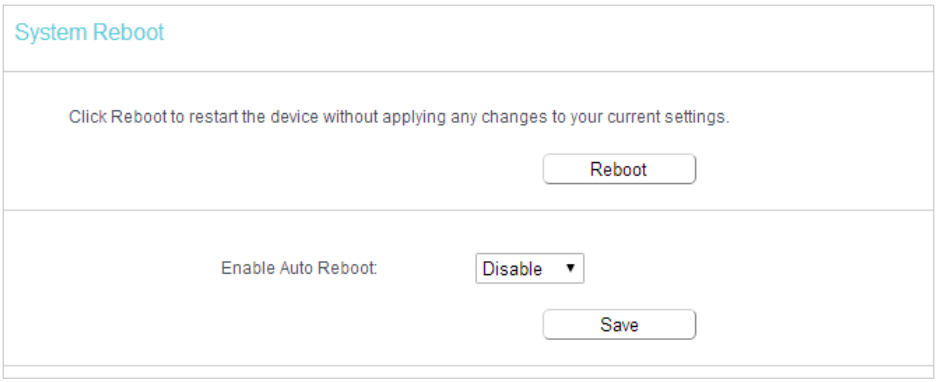
Note:

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

5. 9. 7. Reboot

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

2. Go to System Tools > Reboot, and you can restart your router.



3. Enable the auto reboot function as needed.
   - Disable - Disable the auto reboot function.
   - Timeout - Specify a time period(1-72 hours), then the router will reboot automatically after every this interval.
   - Schedule - The router will reboot automatically according to a specific time schedule.

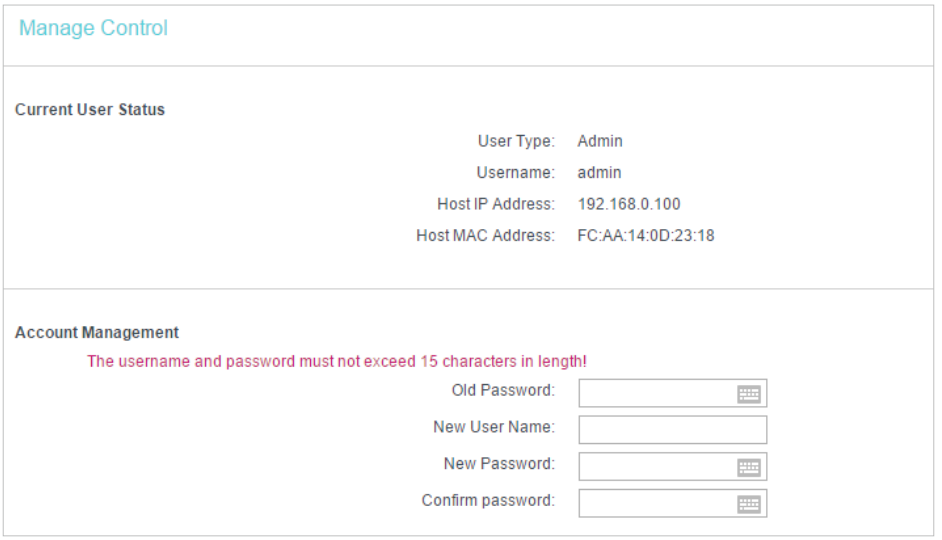
Some settings of the router will take effect only after rebooting, including:

- 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).

5. 9. 8. Administrator

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 you can change the factory default username and password of the router, and manage your router from a remote location via the internet.

- **To view and change the account settings:**



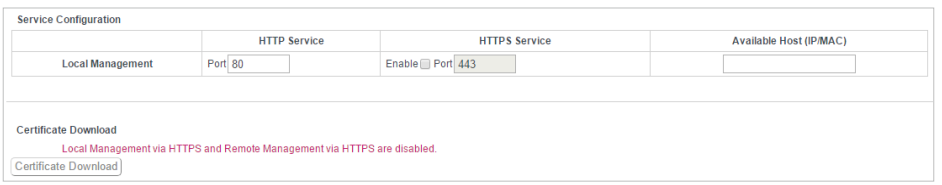
It is strongly recommended that you change the default username and password of the router, for all users that try to access the router's web mangement page or Quick Setup will be prompted for the router's username and password.

Note:

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

- **To manage your router via the internet:**

1. Specify the management web port number and click Save.



- Port - The default management web port number is 80 for HTTP, 443 for HTTPS. For greater security, you can change the management web port to a number between 1024 and 65535 but do not use the number of any common service port. Tick Enable to enable management via HTTPS.
- Available Host (IP/MAC) - This is the current address you will use when accessing your router from the internet.
- Certificate - A file that provides you with authentication information. Download and install the certificate for Local Management via HTTPS if you need it. Once the certificate is installed, warnings will not pop up when you access the router via HTTPS.

2. Enter your router's WAN IP address into your browser's address bar, followed by a colon and the custom port number you set in the Web Management Port box. For example, if your Router's WAN address is 202.96.12.8 and you use port number 8080, enter http://202.96.12.8:8080 in your browser.

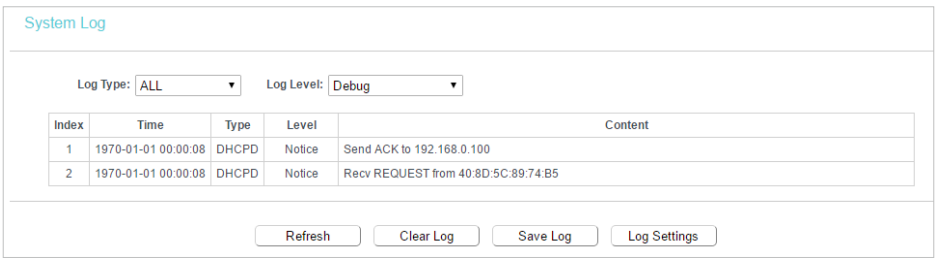
3. Enter the router's password to access the web mangement page.

Note:

- Be sure to change the router's default password to a secure password.
- If the web management port conflicts with the one used for a Virtual Server entry, the entry will be automatically disabled after the setting is saved.

5. 9. 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.

5. 10. Log Out

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

Chapter 6

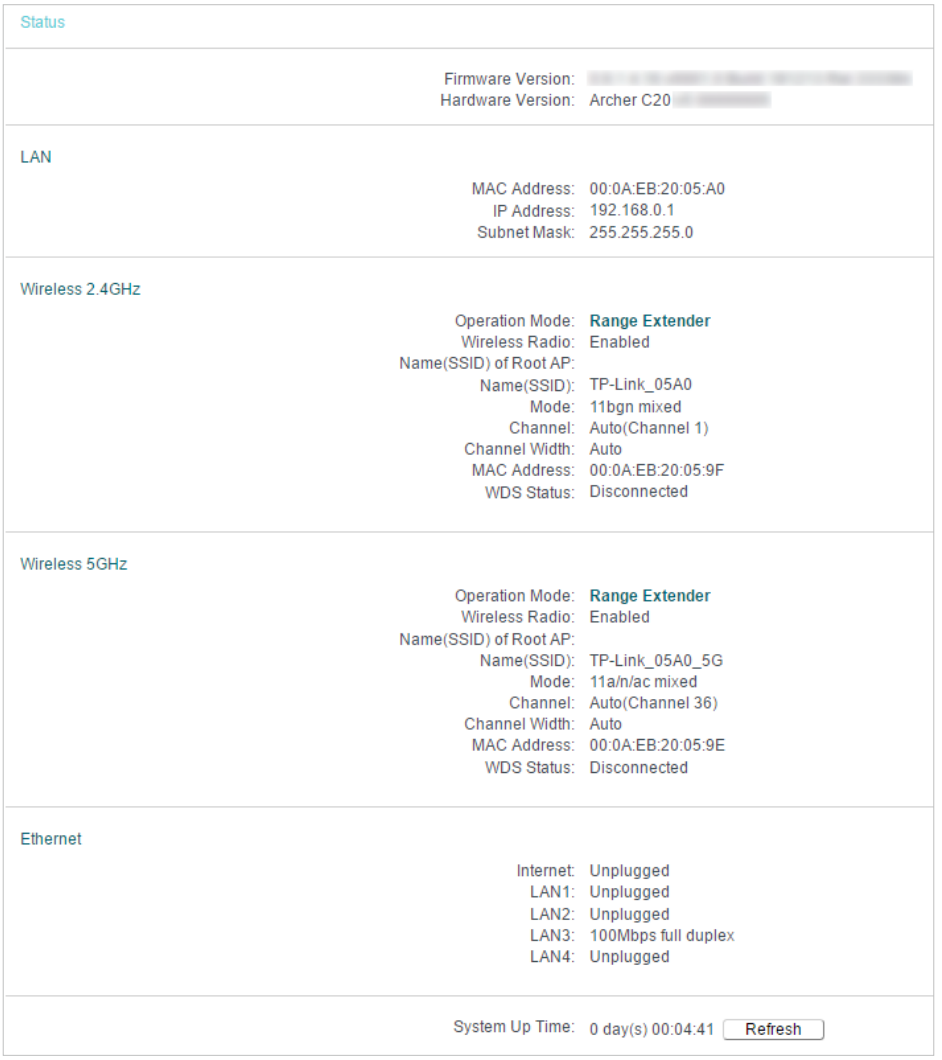
Configure the Router in Range Extender Mode

This chapter presents how to configure the various features of the router in Range Extender Mode.

It contains the following sections:

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.



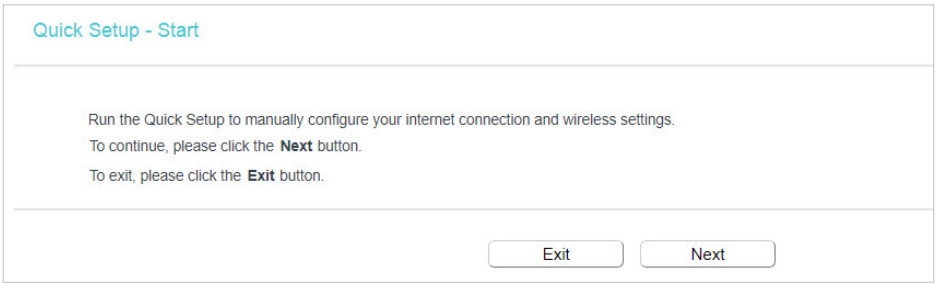
- Firmware Version - The version information of the router's firmware.
- Hardware Version - The version information of the router's hardware.
- LAN - This field displays the current settings of the LAN, and you can configure them on the Network > LAN page.
    - MAC address - The physical address of the router.
    - IP address - The LAN IP address of the router.
    - Subnet Mask - The subnet mask associated with the LAN IP address.
- Wireless 2.4GHz/5GHz - 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 time since the AP was last powered on or reset. Click Refresh to get the latest status and settings of the AP.

6. 2. Quick Setup

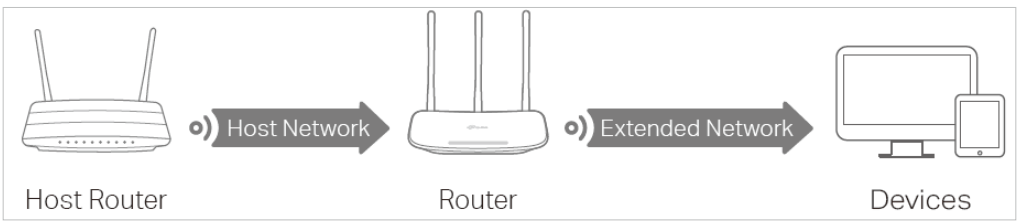
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Quick Setup.



3. Click Next to start. Then follow the step-by-step instructions to connect your router to the internet.

6. 3. Operation Mode

The router supports three operation modes: Wireless Router mode, Access Point mode and Range Extender. In Range Extender mode, the device can copy and reinforce the existing wireless signal to extend the coverage of the signal, especially for a large space to eliminate signal-blind corners. To switch to Range Extender mode:



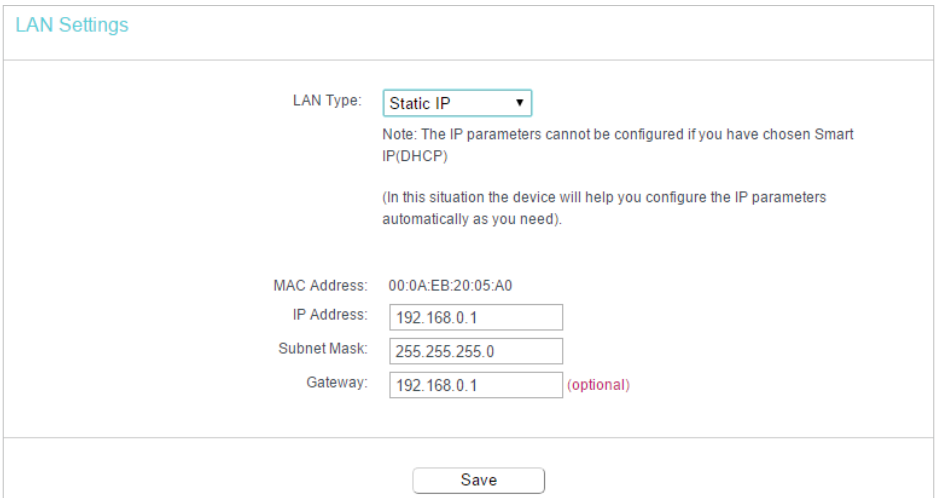
1. Place the router next to your host router and power it on.

2. Connect a computer to the router via an Ethernet cable or wirelessly by using the SSID (network name) and Wireless Password printed on the label at the bottom of the router.
3. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
4. Go to Operation Mode.
5. Select the Range Extender mode and click Save.

6. 4. Network

6. 4. 1. LAN

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



- LAN Type - Select Smart IP(DHCP) to get IP address from DHCP server, or select 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.

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

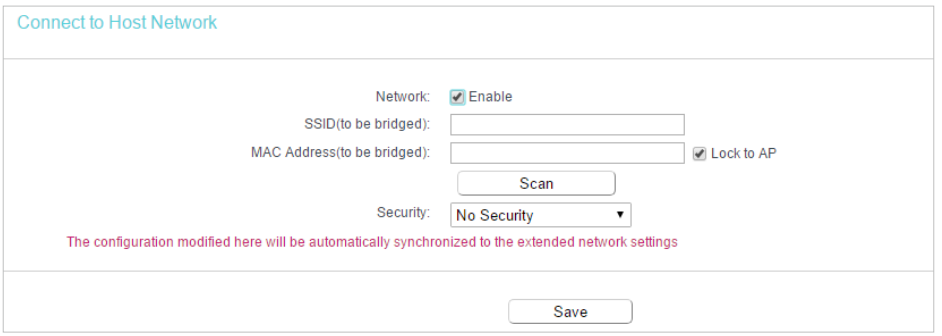
Note:

- If you change the IP address, you must use the new IP address to login to the device.
- If you select the type of smart IP(DHCP), the DHCP server in this device will not startup.
- If the new IP address you set is not in the same subnet with the previous one, the IP Address pool in the DHCP server will be configured automatically.

6. 5. Wireless(2.4GHz or 5GHz)

6. 5. 1. Connect to Host 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. Enable the Network function.
4. Configure the basic settings for the wireless network and click Save.



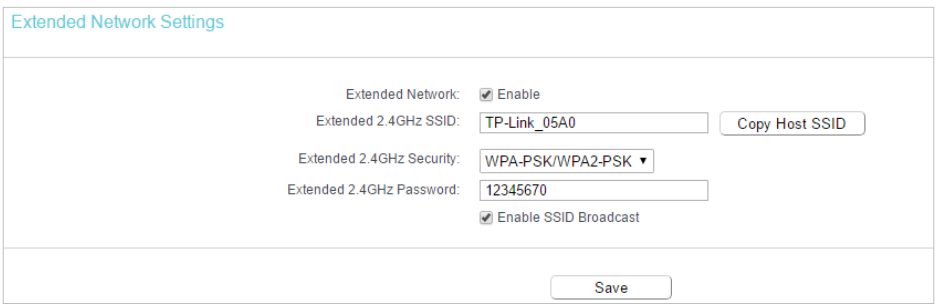
- SSID(to be bridged) - Enter the case-sensitive SSID of the host network which the extender will be connecting to, or click Scan and select a Wi-Fi network.
- MAC Address(to be bridged) - If you select Lock to AP checkbox, enter the MAC Address of the host network which the extender will be connecting to, or click Scan and select a Wi-Fi network.
- Scan - Click to scan and display all available Wi-Fi networks within range that you want the extender to connect to. Once a network is selected, the SSID and security settings of that network will automatically populate.
- Security - Select one of the security options to match with the host network.
    - No Security - This option disables the wireless security.

- WPA-PSK - This option supports implementation of the WPA (Wi-Fi Protected Access) standard. It is recommended. For Password, it should be between 8 and 63 characters.
- WPA2-PSK - This option supports implementation of the WPA2 (Wi-Fi Protected Access) standard. It is also recommended. For Password, it should be between 8 and 63 characters.
- WEP - This option is the most basic form of wireless security that can be used if your client devices can only access wireless using WEP (Wired Equivalent Privacy). Enter the matching WEP key information for your network.

6. 5. 2. Extended Network

In Range Extender mode, the device will relay data to an associated root AP. AP function is enabled meanwhile. The wireless range extender relays signal between its stations and the root AP for greater wireless range.

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



- Extended 2.4GHz SSID - Either use the Copy Host SSID button to automatically copy the main router/AP's SSID or enter a new name (up to 32 characters long). This field is case-sensitive.
- Copy Host SSID - Click to copy the Host SSID. When selected, the extended network will share the SSID of your host network.
- Extended 2.4GHz Security - Select one of the security options to set local extended wireless network.
  - No Security - This option disables the wireless security.
  - WPA-PSK/WPA2-PSK - This option supports multiple implementation of the WPA (Wi-Fi Protected Access) standard, such as WPA and WPA2.

- WEP - This option is the most basic form of wireless security that can be used if your client devices can only access wireless using WEP (Wired Equivalent Privacy).

- Enable SSID Broadcast - If you select the Enable SSID Broadcast checkbox, the wireless router will broadcast its name (SSID) on the air.

6. 5. 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.

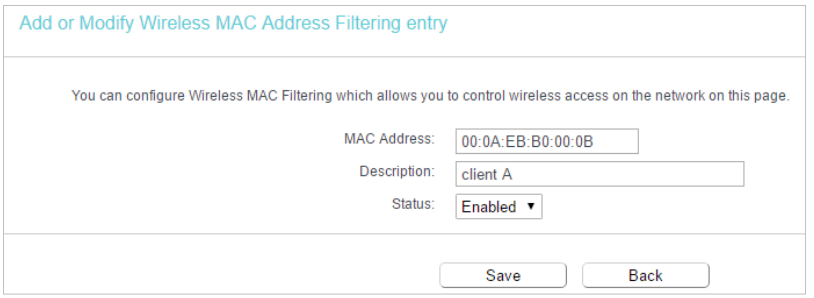
I want to:

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.

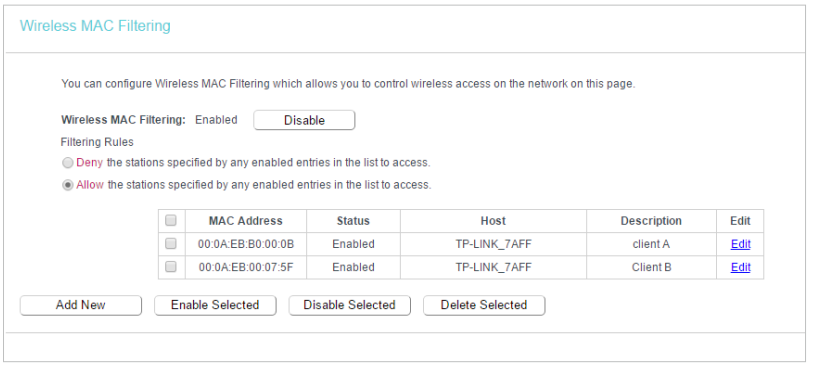
How can I do that?

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!

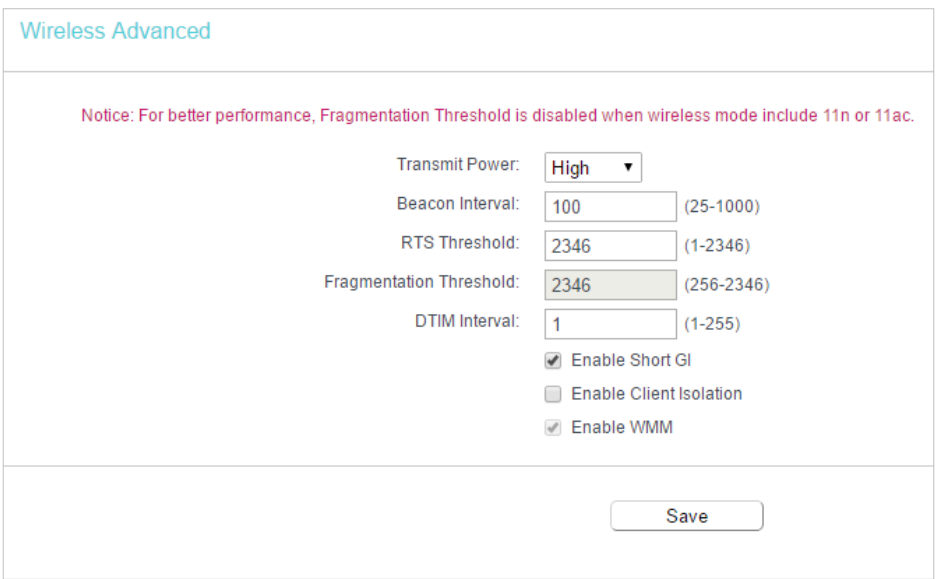
Now only client A and client B can access your network.

6. 5. 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.



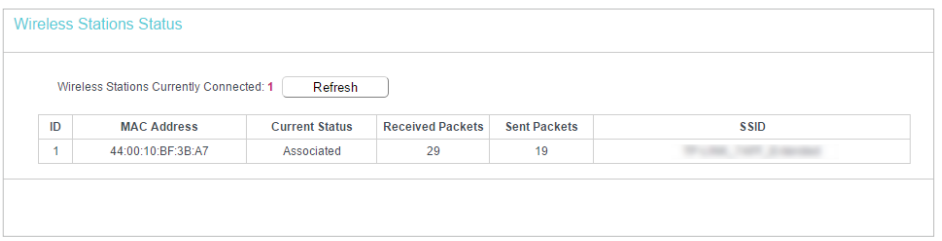
- Transmit Power - Select High, Middle or Low which you would like to specify for the router. High is the default setting and recommended.
- Beacon Interval - Enter a value between 40-1000 milliseconds for Beacon Interval here. Beacon Interval value determines the time interval of the beacons. The beacons

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.
- Enable WMM - WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended to enable this function.

6. 5. 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.

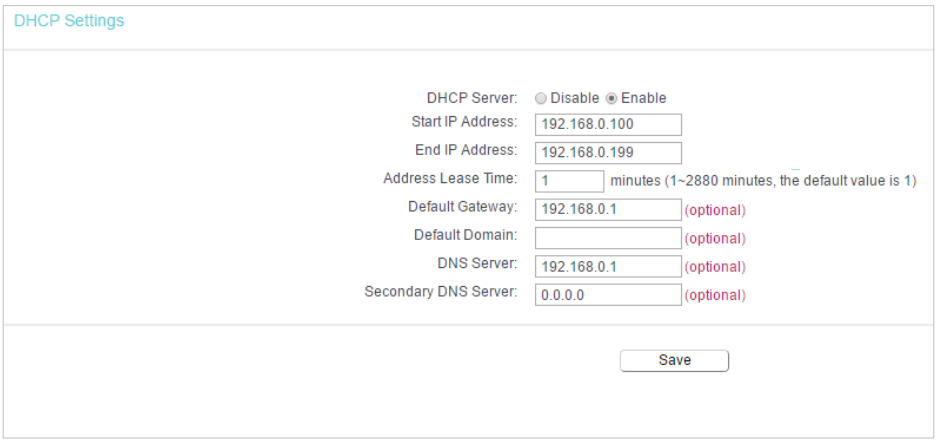
- SSID - SSID that the station associates with.

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.

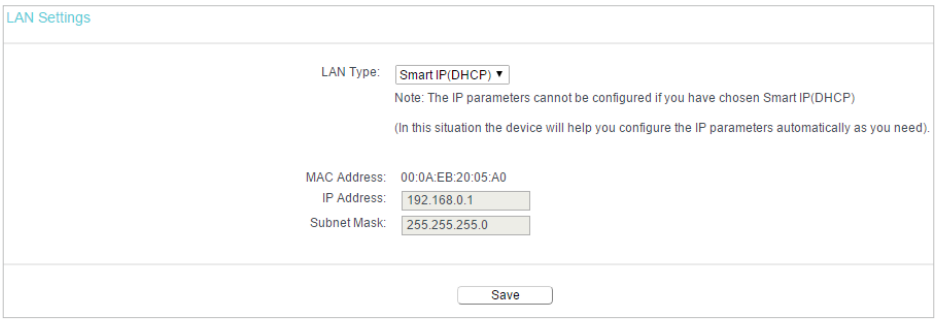


- DHCP Server - Enable or disable the DHCP server. If disabled, you must have another DHCP server within your network or else you must configure the computer manually.
- Start IP Address - Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.0.100 is the default 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 1.
- Default Gateway (Optional) - It is suggested to input the IP address of the LAN port of the router. The default value is 192.168.0.1.

- Default Domain (Optional) - Input the domain name of your network.
- DNS Server (Optional) - Input the DNS IP address provided by your ISP.
- Secondary DNS Server (Optional) - Input the IP address of another DNS server if your ISP provides two DNS servers.

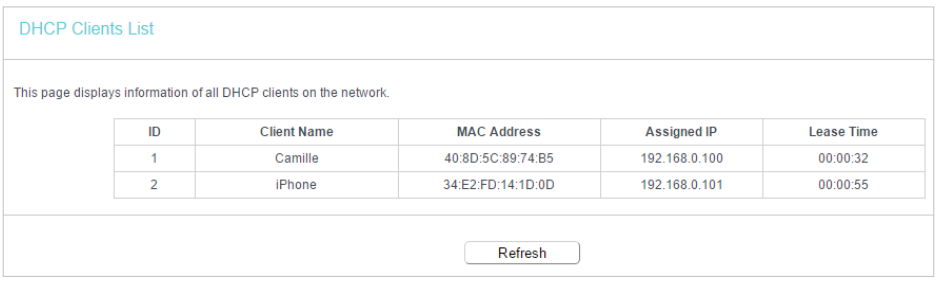
Note:

- To use the DHCP server function of the router, you must configure all computers on the LAN as Obtain an IP Address automatically.
- When you choose Smart IP (DHCP) in Network > LAN, the DHCP Server function will be disabled. You will see the page as below.



6. 6. 2. DHCP Client List

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

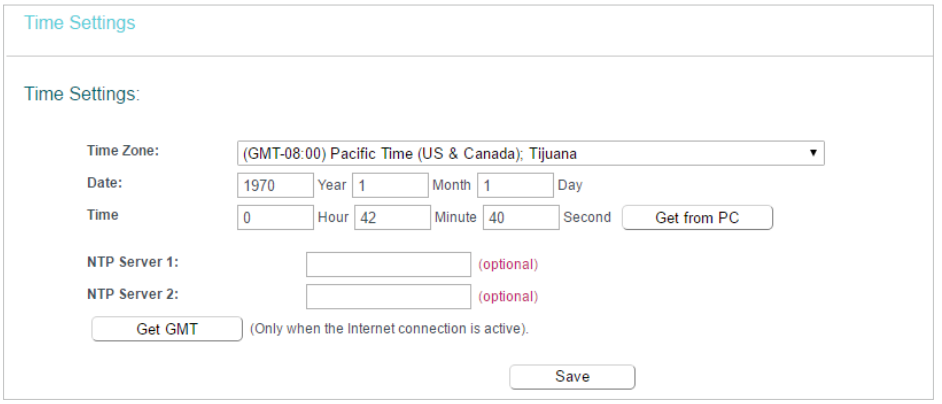
You cannot change any of the values on this page. To update this page and show the current attached devices, click Refresh.

6. 7. System Tools

6. 7. 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 I or NTP Server II.
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 DaylightSaving.
2. Select the start time from the drop-down list in the Start field.
3. Select the end time from the drop-down list in the End field.
4. Click Save.

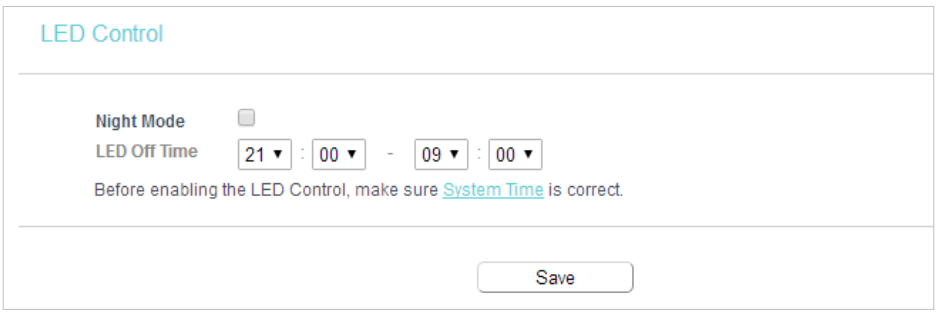
Note:

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.

6. 7. 2. LED Control

The LED Control allows you to turn on or off the LEDs on your device according to a specific time schedule.

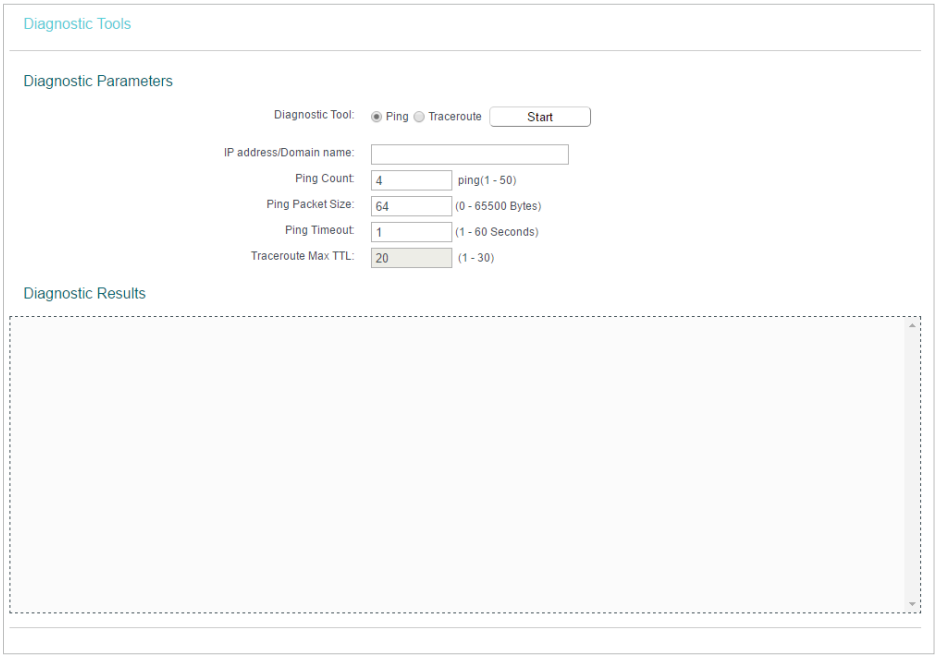
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to System Tools > LED Control.



6. 7. 3. 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.



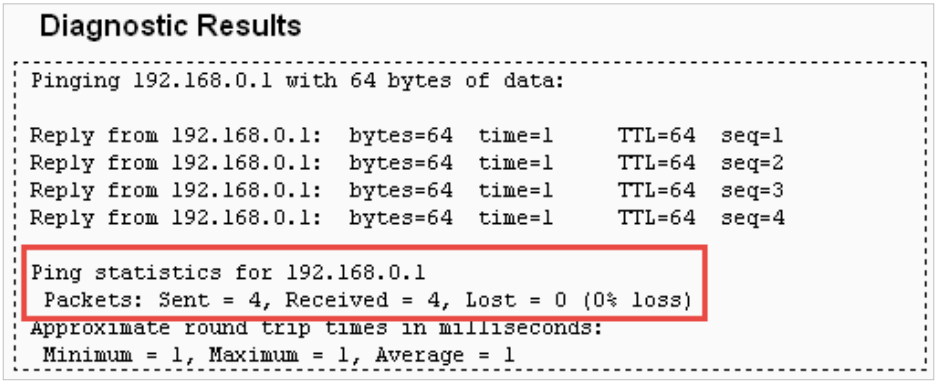
- Diagnostic Tool - Select one diagnostic tool.
  - Ping - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
  - Tracerouter - This diagnostic tool tests the performance of a connection.

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.

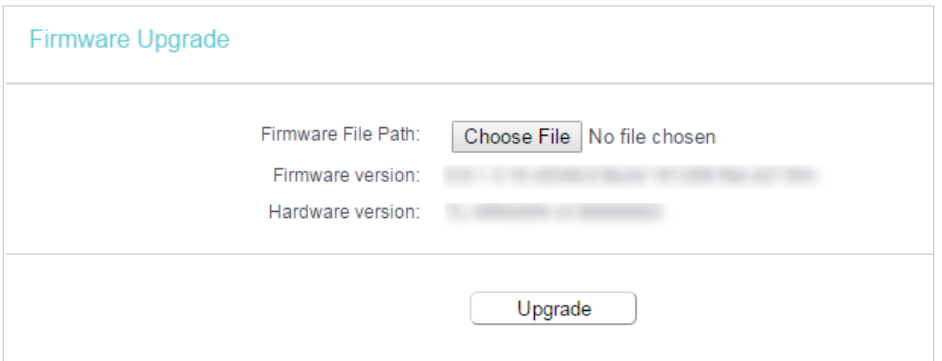


Note: Only one user can use this tool at one time. Options "Number of Pings", "Ping Size" and "Ping Timeout" are used for the Ping function. Option "Tracert Hops" is used for the Tracert function.

6. 7. 4. Firmware Upgrade

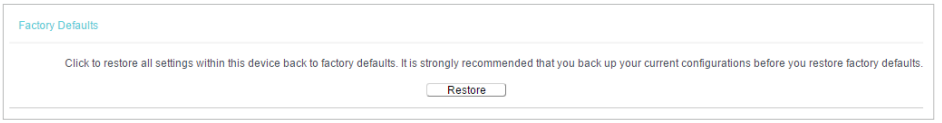
TP-Link is dedicated to improving and richening the product features, giving users a better network experience. We will release the latest firmware at TP-Link official website. You can download the latest firmware file from the Support page of our website www.tp-link.com and upgrade the firmware to the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

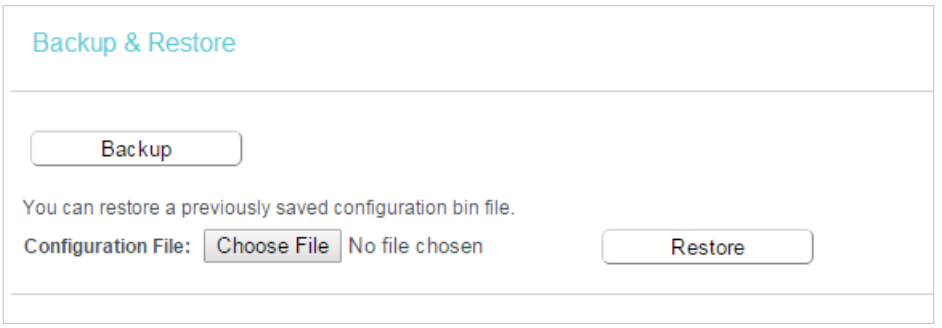


- The default Username: admin
- The default Password: admin
- The default IP Address: 192.168.0.1
- The default Subnet Mask: 255.255.255.0

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.

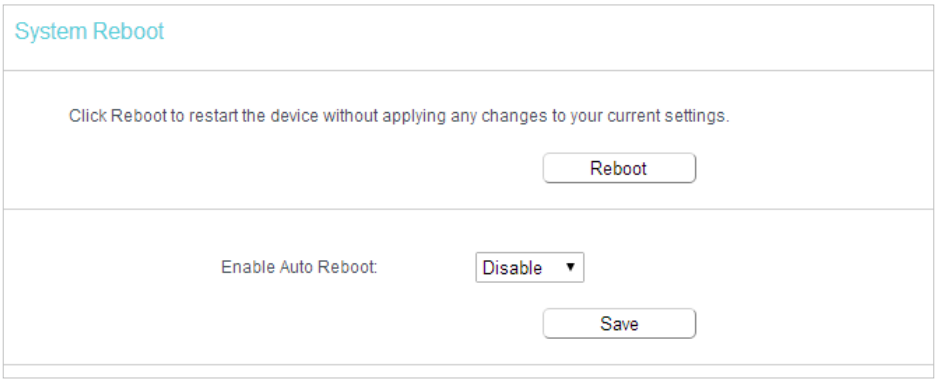
- **To restore configuration settings:**

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

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



3. Enable the auto reboot function as needed.
   - Disable - Disable the auto reboot function.
   - Timeout - Specify a time period(1-72 hours), then the router will reboot automatically after every this interval.
   - Schedule - The router will reboot automatically according to a specific time schedule.

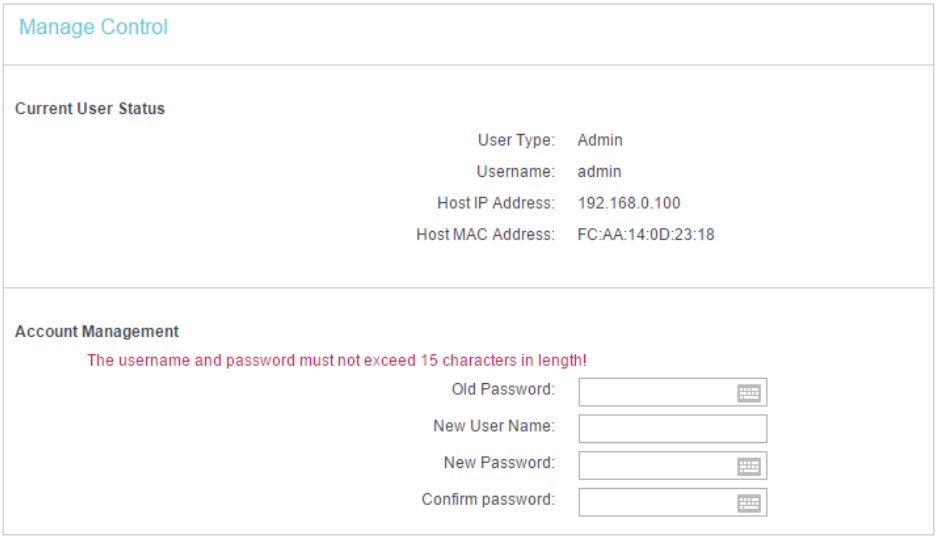
Some settings of the router will take effect only after rebooting, including:

- 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).

6. 7. 8. Administrator

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 you can change the factory default username and password of the router, and manage your router from a remote location via the internet.

- **To view and change the account settings:**



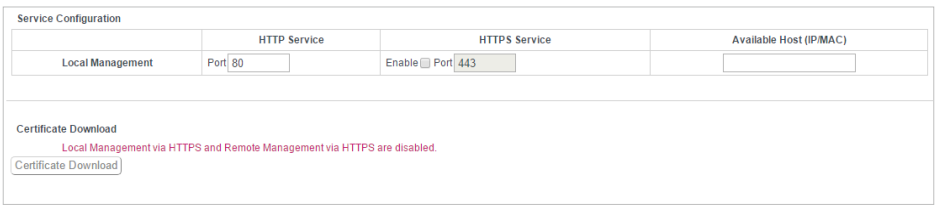
It is strongly recommended that you change the default username and password of the router, for all users that try to access the router's web mangement page or Quick Setup will be prompted for the router's username and password.

Note:

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

- **To manage your router via the internet:**

1. Specify the management web port number and click Save.



- Port - The default management web port number is 80 for HTTP, 443 for HTTPS. For greater security, you can change the management web port to a number between 1024 and 65535 but do not use the number of any common service port. Tick Enable to enable management via HTTPS.
- Available Host (IP/MAC) - This is the current address you will use when accessing your router from the internet.
- Certificate - A file that provides you with authentication information. Download and install the certificate for Local Management via HTTPS if you need it. Once the certificate is installed, warnings will not pop up when you access the router via HTTPS.

2. Enter your router's WAN IP address into your browser's address bar, followed by a colon and the custom port number you set in the Web Management Port box. For

example, if your Router's WAN address is 202.96.12.8 and you use port number 8080, enter http://202.96.12.8:8080 in your browser.

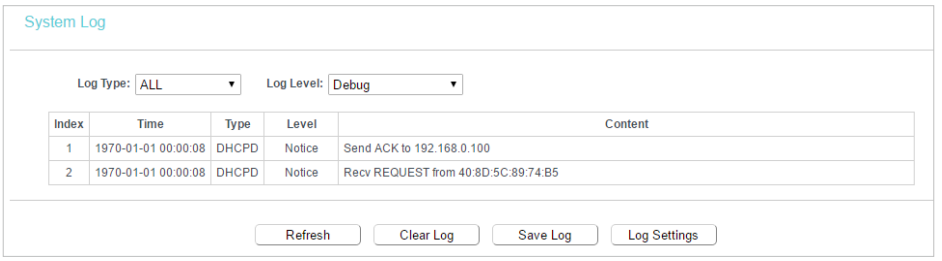
3. Enter the router's password to access the web mangement page.

Note:

- Be sure to change the router's default password to a secure password.
- If the web management port conflicts with the one used for a Virtual Server entry, the entry will be automatically disabled after the setting is saved.

6. 7. 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.

6. 8. Log Out

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

FAQ

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

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

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

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

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

If you have altered the username and password but Password Recovery is disabled:

1. Reset the router to factory default settings: press and hold the Reset button until all LEDs turn off and then release the button;
2. Visit http://tplinkwifi.net, and enter admin (in lowercase) as both username and password to log in.

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

Q3. What should I do if I cannot log in to the router's web management page?

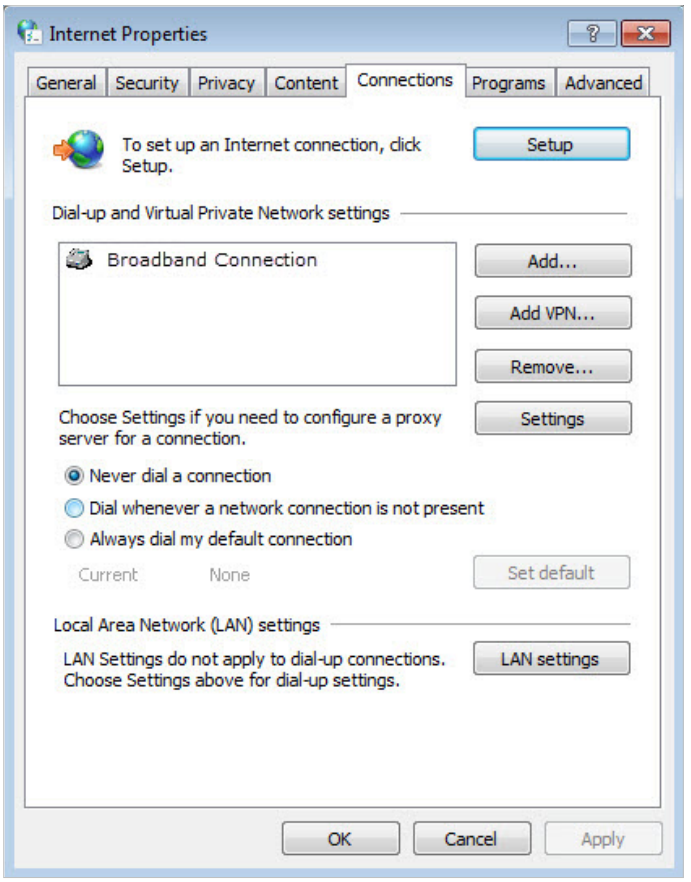
1. This can happen for a variety of reasons. Please try the methods below to log in again.

- Make sure your computer has connected to the router correctly and the corresponding LED lights up.
- Make sure the IP address of your computer is configured as Obtain an IP address automatically and Obtain DNS server address automatically.

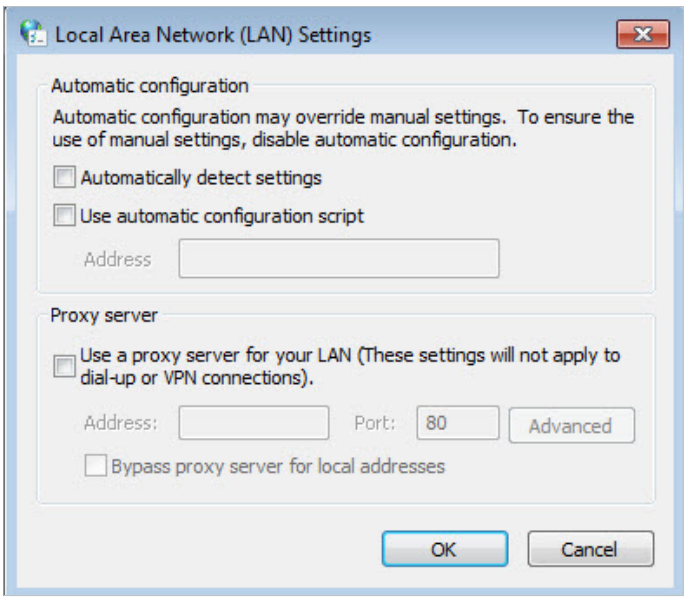
2. Make sure you enter the correct IP address to log in: http://tplinkwifi.net.

- Check your computer's settings:

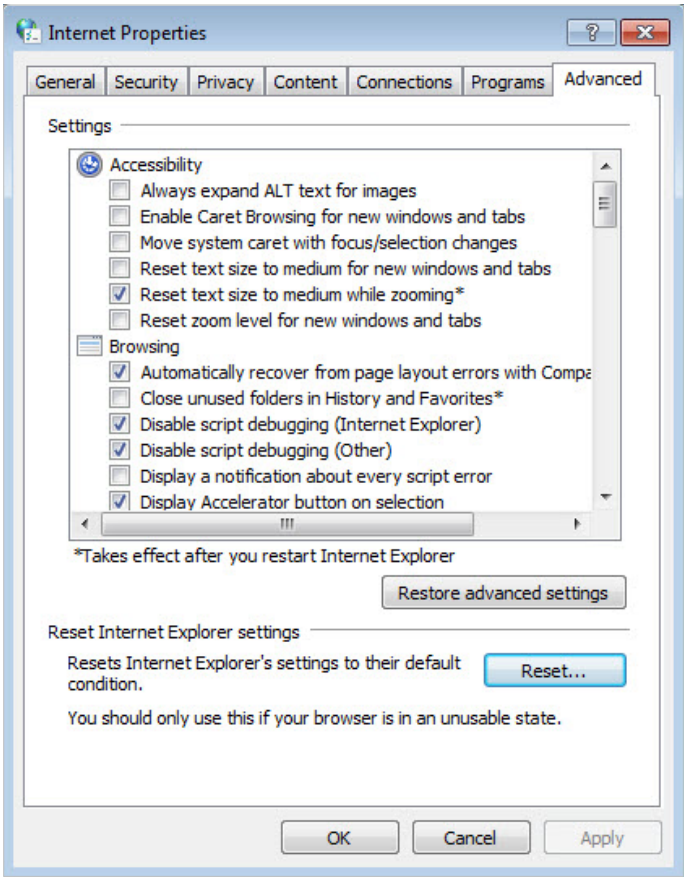
3. Go to Start > Control Panel > Network and Internet, and click View network status and tasks.
   1) Click Internet Options on the bottom left.
   2) Click Connections and select Never dial a connection.



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



4) Go to Advanced > Restore advanced settings, and click OK to save the settings.



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

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

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

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

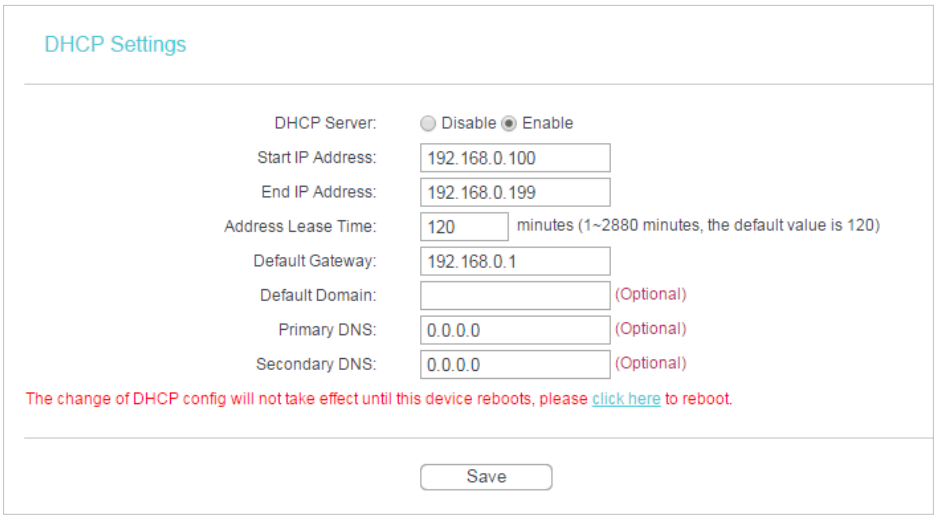
If IP Address is a valid one, please try the methods below and try again:

- Your computer might not recognize any DNS server addresses, please manually configure DNS server.

  1) Go to DHCP.

  2) Enter 8.8.8.8 as Primary DNS, and click Save.

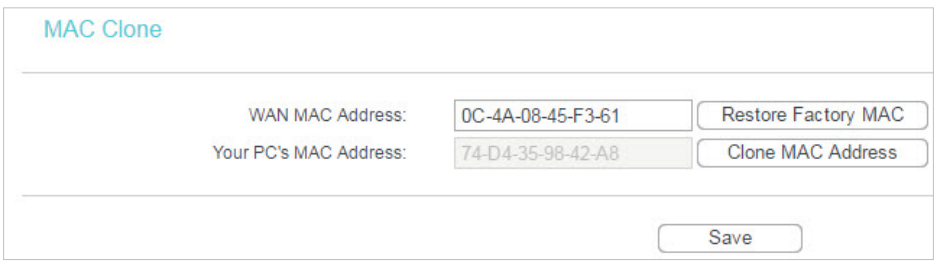
  Tips: 8.8.8.8 is a safe and public DNS server operated by Google.



- Restart the modem and the router.
  1) Power off your modem and the router, and leave them off for 1 minute.
  2) Power on your modem first, and wait about 2 minutes.
  3) Power on the router, and wait another 1 or 2 minutes and check the internet access.
- Reset the router to factory default settings and reconfigure the router.
- Upgrade the firmware of the router.
- Check the TCP/IP settings on the particular device if all other devices can get internet from the router.

If the IP Address is 0.0.0.0, please try the methods below and try again:

- Make sure the physical connection between the router and the modem is proper.
- Clone the MAC address of your computer.
  1) Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
  2) Go to Network > MAC Clone, select Clone MAC Address and click Save.



Tips:

- Some ISP will register the MAC address of your computer when you access the internet for the first time through their Cable modem, if you add a router into your network to share your internet connection, the ISP will not accept it as the MAC address is changed, so we need to clone your computer's MAC address to the router.

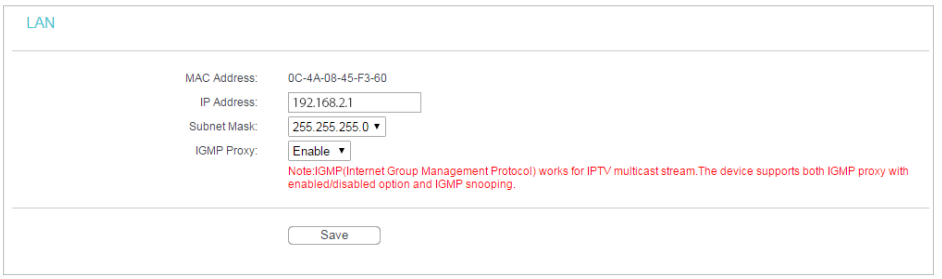
- The MAC addresses of a computer in wired connection and wireless connection are different.

- Modify the LAN IP address of the router.

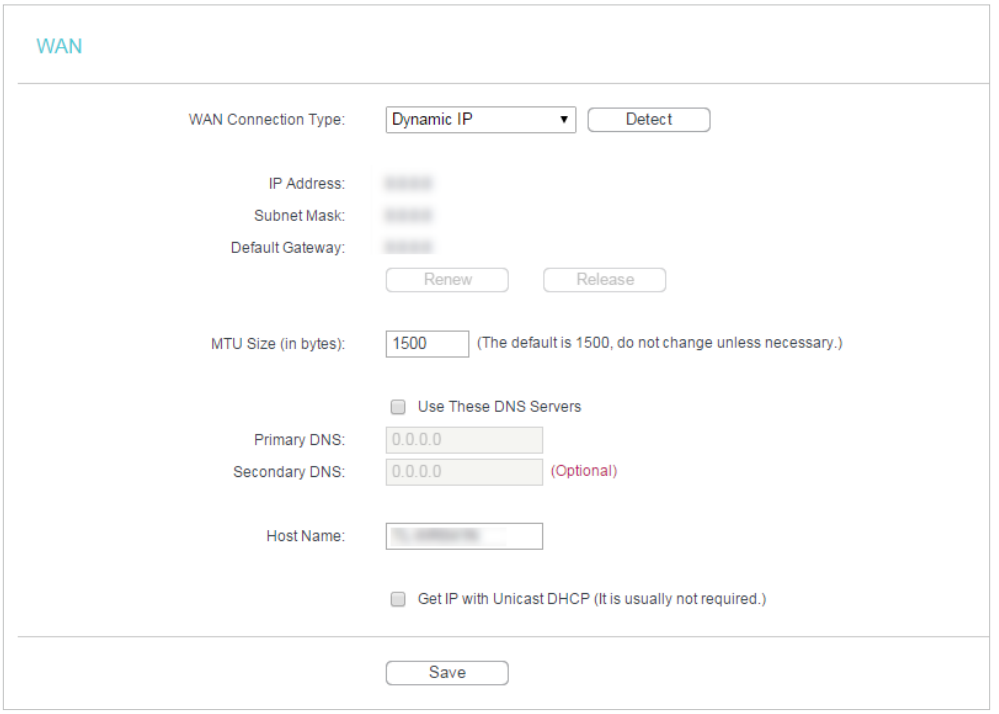
  Note:

  Most TP-Link routers use 192.168.0.1/192.168.1.1 as their default LAN IP address, it may conflict with the IP range of your existent ADSL modem/router. If so, the router is not able to communicate with your modem and cause you can't access the internet. To resolve this problem, we need to change the LAN IP address of the router to avoid such conflict, for example, 192.168.2.1.

  1) Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
  2) Go to Network > LAN.
  3) Modify the LAN IP address as the follow picture shows. Here we take 192.168.2.1 as an example.
  4) Click Save.



- Restart the modem and the router.
  1) Power off your modem and the router, and leave them off for 1 minute.
  2) Power on your modem first, and wait about 2 minutes.
  3) Power on the router, and wait another 1 or 2 minutes and check the internet access.
- Double check the internet Connection Type.
  1) Confirm your internet Connection Type, which can be learned from the ISP.
  2) Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
  3) Go to Network > WAN.
  4) Select your WAN Connection Type and fill in other parameters.
  5) Click Save.



6) Restart the modem and the router.

- Please upgrade the firmware of the router.

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

Q5. What should I do if I cannot find my wireless network or I cannot connect the wireless network?

If you fail to find any wireless network, please follow the steps below:

- Make sure the wireless function of your device is enabled if you're using a laptop with a built-in wireless adapter. You can refer to the relevant document or contact the laptop manufacturer.
- Make sure the wireless adapter driver is installed successfully and the wireless adapter is enabled.
  - **On Windows 7**

  1) If you see the message No connections are available, it is usually because the wireless function is disabled or blocked somehow.

  2) Clicking Troubleshoot and windows might be able to fix the problem by itself.
  - **On Windows XP**

  1) If you see the message Windows cannot configure this wireless connection, this is usually because windows configuration utility is disabled or you are running another wireless configuration tool to connect the wireless.

  2) Exit the wireless configuration tool (the TP-Link Utility, for example).

3) Select and right click My Computer on Desktop, and select Manage to open Computer Management window.

4) Expand Services and Applications > Services, and find and locate Wireless Zero Configuration in the Services list on the right side.

5) Right click Wireless Zero Configuration, and then select Properties.

6) Change Startup type to Automatic, click Start and make sure the Service status is Started. And then click OK.

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

- Check the WLAN LED indicator on your wireless router/modem.
- Make sure your computer/device is still in the range of your router/modem. Move closer if it is currently too far away.

If you can find your wireless network but fail to connect, please follow the steps below:

- **Authenticating problem/password mismatch:**

1) Sometimes you will be asked to type in a PIN number when you connect to the wireless network for the first time. This PIN number is different from the Wireless Password/Network Security Key. Usually you can only find it on the label of your router.

2) If you cannot find the PIN or PIN failed, you may choose Connecting using a security key instead, and then type in the Wireless Password/Network Security Key.

3) If it continues to show note of Network Security Key Mismatch, it is suggested to confirm the wireless password of your wireless router.

Note: Wireless Password/Network Security Key is case sensitive.

- **Windows unable to connect to XXXX / Can not join this network / Taking longer than usual to connect to this network:**
  - Check the wireless signal strength of your network, if it is weak (1~3 bars), please move the router closer and try again.

- Change the wireless Channel of the router to 1,6,or 11 to reduce interference from other networks.
- Re-install or update the driver for your wireless adapter of the computer.

COPYRIGHT & TRADEMARKS

FCC compliance information statement

Product Name: AC750 Wireless Dual Band Router

Model Number: Archer C20 / Archer A2

Component Name	Model
I.T.E POWER SUPPLY	T120100-2B1

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: 2019.04.03

FCC compliance information statement

Product Name: I.T.E POWER SUPPLY

Model Number: T120100-2B1

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.

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: 2019.04.03

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(the maximum transmitted power)

2400 MHz -2483.5 MHz(20dBm)

5150 MHz -5250 MHz(23dBm)

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.

National restrictions

Attention: This device may only be used indoors in all EU member states and EFTA countries.

AT	BE	BG	CH	CY	CZ	DE	DK
EE	EL	ES	FI	FR	HR	HU	IE
IS	IT	LI	LT	LU	LV	MT	NL
NO	PL	PT	RO	SE	SI	SK	UK

Canadian Compliance Statement

This device complies with Industry Canada license-exempt RSSs. Operation is subject to the following two conditions:

1) This device may not cause interference, and

2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1) l'appareil ne doit pas produire de brouillage;

2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, meme si le brouillage est susceptible d'en compromettre le fonctionnement.

Caution:

1) The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

2) For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and

The high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

Avertissement:

1) Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

2) Le gain maximal d'antenne permis pour les dispositifs avec antenne(s) amovible(s) utilisant la bande 5725-5850 MHz doit se conformer à la limitation P.I.R.E spécifiée pour l'exploitation point à point et non point à point, selon le cas.

En outre, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

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

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行；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。

4.7.9.1 應避免影響附近雷達系統之操作。

4.7.9.2 高增益指向性天線只得應用於固定式點對點系統。

BSMI Notice

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	○	○	○	○	○	○
電源適配器	—	○	○	○	○	○

備考1.“超出0.1wt%”及“超出0.01wt%”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.

EAC

Safety Information

- Keep the device away from water, fire, humidity or hot environments.
- Do not attempt to disassemble, repair, or modify the device.
- Do not use damaged charger or USB cable to charge the device.
- Do not use any other chargers than those recommended
- Do not use the device where wireless devices are not allowed.
- Adapter shall be installed near the equipment and shall be easily accessible.
-  Use only power supplies which are provided by manufacturer and in the original packing of this product. If you have any questions, please don't hesitate to contact us.

Please read and follow the above safety information when operating the device. We cannot guarantee that no accidents or damage will occur due to improper use of the device. Please use this product with care and operate at your own risk.

Explanations of the symbols on the product label

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

Hardware Connection

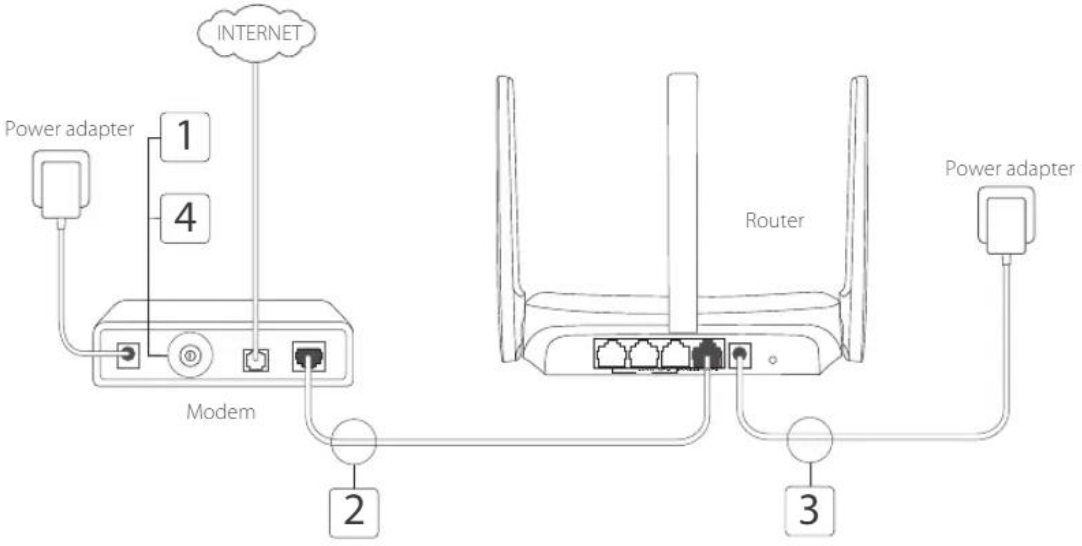


*Image may differ from actual product.

Conecte el Hardware

Conecte el hardware de acuerdo con el diagrama en el capítulo inicial de esta guía.

Si su conexión a Internet es a través de un cable Ethernet desde la pared en lugar de a través de un módem DSL / Cable / Satelital, conecte el cable Ethernet directamente al puerto WAN del router y siga el Paso 3 para completar la conexión de hardware.

1. Apague el módem y retire la batería de respaldo si tiene uno.
2. Conecte el módem al puerto WAN de su router con un cable Ethernet.
3. Encienda el router y espere a que comience.
4. Encienda el módem.

Configure el router

1. Conecte su computadora al router (con cable o inalámbrico).
   - **Alámbrico:** apague el Wi-Fi en su computadora y conecte su computadora al puerto LAN del router usando un cable Ethernet.
   - **Inalámbrico:** conecte su computadora al router de forma inalámbrica. El SSID (nombre de red) está en la etiqueta del router.
2. Inicie en un navegador web e ingrese **http://mwlogin.net** en la barra de direcciones. Crea una contraseña para futuros inicios de sesión.
   Nota: Si la ventana de inicio de sesión no aparece, consulte las Preguntas frecuentes > P1.
3. Siga las instrucciones paso a paso en la **Configuración rápida** para tener una conexión a internet y su red inalámbrica.

☺ ¡Disfruta de internet !

Nota: Si ha cambiado el SSID y la contraseña inalámbrica durante la configuración, use el nuevo SSID y la contraseña inalámbrica para unirse a la red inalámbrica.

FAQ (Preguntas Frecuentes)

Q1. ¿Qué puedo hacer si la ventana de inicio de sesión no aparece?

- Si el ordenador está configurado con una dirección Ip estática, cambie su configuración para obtener una dirección IP automática.
- Verifique que **http://mwlogin.net** está correctamente introducida en el navegador web.
- Utilice otro navegador web e inténtelo de nuevo.
- Reinicie su router e inténtelo de nuevo.
- Deshabilite y habilite otra vez el adaptador de red en uso.

Q2. ¿Qué puedo hacer si no puedo acceder a Internet?

- Compruebe si Internet está funcionando correctamente conectando un ordenador directamente al módem con un cable Ethernet. Si no es así, contacte con su proveedor de servicios de Internet.
- Reinicie su router e inténtelo de nuevo.
- Abra un navegador web, introduzca **http://mwlogin.net** e inicie otra vez la Configuración Rápida.
- Para los usuarios de cable módem, reinicie primero el módem. Si el problema persiste, inicie sesión entre la página de gestión web del router para clonar la dirección MAC.

Q3. ¿Cómo puedo restaurar el router a sus valores de fábrica por defecto?

- Con el router encendido, presione y mantenga pulsado el botón Reset en el router hasta que haya un cambio obvio en los LEDs, después suelte el botón.
- Inicie sesión en la página de gestión web del router para restaurar el router a sus valores de fábrica.

Q4. ¿Qué puedo hacer si he olvidado mi contraseña de gestión web?

- Diríjase a la FAQ > Q3 para resetear el router y después crear una contraseña para futuros accesos.

Q5. ¿Qué puedo hacer si he olvidado la contraseña de mi red inalámbrica?

- Por defecto, la red inalámbrica no tiene contraseña.
- Si ha configurado una contraseña para la red inalámbrica, inicie sesión en la página de gestión web del router para recuperar o restaurar su contraseña.

Nota: Para saber más sobre el router, por favor visite nuestra página web*http://www.mercusys.com*

MERCUSYS®

User Guide

AC1300 Wireless Dual Band Gigabit Router

AC12G

 REV2.0.0 1910080072

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 (the maximum transmitted power)

2400 MHz -2483.5 MHz (20 dBm)

5150 MHz -5250 MHz (23 dBm)

EU declaration of conformity

Mercusys hereby declares that the device is in compliance with the essential requirements and other relevant provisions of directives 2014/53/EU, 2009/125/EC, 2011/65/EU and (EU)2015/863.

The original EU declaration of conformity may be found at http://www.mercusys.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.

National Restrictions

Attention: This device may only be used indoors in all EU member states, EFTA countries and Northern Ireland.

Attention: This device may only be used indoors in Great Britain.

	AT	BE	BG	CH	CY	CZ	DE	DK
	EE	EL	ES	FI	FR	HR	HU	IE
	IS	IT	LI	LT	LU	LV	MT	NL
	NO	PL	PT	RO	SE	SI	SK	UK(NI)

	UK

UK Declaration of Conformity

Mercusys hereby declares that the device is in compliance with the essential requirements and other relevant provisions of the Radio Equipment Regulations 2017.

The original UK declaration of conformity may be found at
https://www.mercusys.com/support/ukca/

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.

Industry Canada Statement

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

Korea Warning Statements

당해 무선설비는 운용중 전파혼신 가능성이 있음.

NCC Notice

注意！

取得審驗證明之低功率射頻器材，非經核准，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及功能。

低功率射頻器材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。

前述合法通信，指依電信管理法規定作業之無線電通信。

低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾

應避免影響附近雷達系統之操作。

高增益指向性天線只得應用於固定式點對點系統。

BSMI Notice

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。
- 不要私自拆開機殼或自行維修，如產品有故障請與原廠或代理商聯繫。

設備名稱：AC1300 Wireless Dual Band Gigabit Router Equipment name						型號（型式）：AC12G Type designation (Type)
單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛 Lead (Pb)	汞 Mercury (Hg)	鎘 Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
PCB	○	○	○	○	○	○
外殼	○	○	○	○	○	○
電源供應器	—	○	○	○	○	○
天線	○	○	○	○	○	○

備考 1.〝超出 0.1 wt %〞及〝超出 0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值
Note 1: "Exceeding 0.1 wt %" and "exceeding 0.01 wt %" indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.
備考 2.〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。
Note 2: "○" indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.
備考 3.〝—〞係指該項限用物質為排除項目。
Note 3: The "–" indicates that the restricted substance corresponds to the exemption.

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

EAC

Safety Information

- Keep the device away from water, fire, humidity or hot environments.
- Do not attempt to disassemble, repair, or modify the device. If you need service, please contact us.
- Do not use damaged charger or USB cable to charge the device.
- Do not use any other chargers than those recommended
- Do not use the device where wireless devices are not allowed.
- Adapter shall be installed near the equipment and shall be easily accessible.
- Use only power supplies which are provided by manufacturer and in the original packing of this product. If you have any questions, please don't hesitate to contact us.

Please read and follow the above safety information when operating the device. We cannot

guarantee that no accidents or damage will occur due to improper use of the device. Please use this product with care and operate at your own risk.

Operating Temperature: 0°C~40°C (32°F~104°F)

This product uses radios and other components that emit electromagnetic fields. Electromagnetic fields and magnets may interfere with pacemakers and other implanted medical devices. Always keep the product and its power adapter more than 15 cm (6 inches) away from any pacemakers or other implanted medical devices. If you suspect your product is interfering with your pacemaker or any other implanted medical device, turn off your product and consult your physician for information specific to your medical device.

Explanation of the symbols on the product label

Symbol	Explanation
	DC voltage
	Class II equipment
	Polarity of d.c. power connector
	Energy efficiency Marking
	Indoor use only
	Caution
	Operator's manual
	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.

CONTENTS

Conventions

The Router, or AC12G, mentioned in this User Guide stands for AC1300 Wireless Dual Band Gigabit Router without any explanations.

Parameters provided in the pictures are just references for setting up the product, which may differ from the actual situation.

You can set the parameters according to your demand.

More Info

Specifications and the latest software can be found at the product page at the official website **http://www.mercusys.com**.

The Quick Installation Guide can be found where you find this guide or inside the package of the router.

Speed/Coverage Disclaimer

*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 1) environmental factors, including building materials, physical objects, and obstacles, 2) network conditions, including local interference, volume and density of traffic, product location, network complexity, and network overhead, and 3) client limitations, including rated performance, location, connection, quality, and client condition.

**Use of MU-MIMO requires clients to also support MU-MIMO. §Use of WPA3 requires clients to also support the corresponding feature.

***Use of WPA3 requires clients to also support the corresponding feature.

Chapter 1 Introduction

1.1 Product Overview

AC12G delivers blazing fast Wi-Fi speeds up to 1300 Mbps. Choose the 2.4 GHz band (400 Mbps) for internet browsing, email, and social media or the 5 GHz band (867 Mbps) for bandwidth-intensive tasks like HD streaming and gaming.

1.2 Product Appearance

1. 2. 1 The Front Panel

The router's LEDs are located on the front panel (View from left to right).

Name	Status	Indication
SYS	Off	Power is off or the router is not working properly.
	On	The router is working properly.
WIFI	Off	The wireless function is disabled.
	On	The wireless function is working properly.
WAN	Off	The WAN port is not connected.
	Flashing	The WAN port is transmitting/receiving data.
	On	The WAN port is connected.
LAN	Off	No LAN port is connected to a powered-on device.
	On	At least one LAN port is connected to a powered-on device.

1. 2. 2 The Rear Panel

The following items are located on the rear panel (View from left to right).

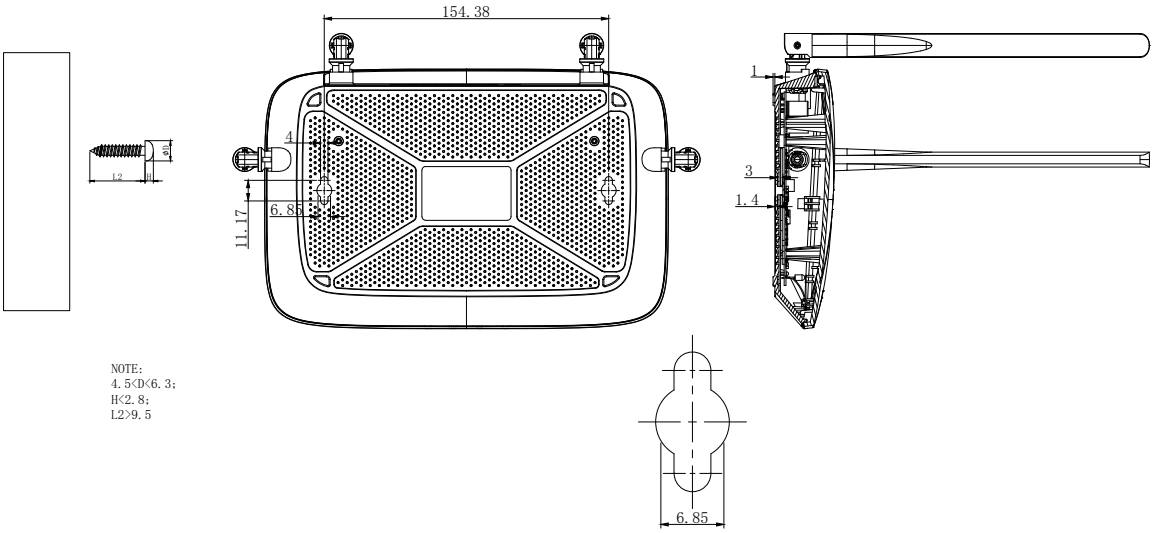
Item	Description
1-3(LAN)	These ports connect the router to the local devices.
WAN	This port is where you will connect the DSL/cable Modem, or Ethernet.
Power	The power socket is where you will connect the power adapter. Please use the power adapter provided with this router.
WPS/RESET Button	Press this button for 1 second to use WPS function. Press and hold this button for more than 5 seconds to reset the router.
Wireless Antennas	To receive and transmit the wireless data.

Chapter 2 Connect to the Internet

2. 1. Position Your Router

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

Generally, the router is placed on a horizontal surface, such as on a shelf or desktop. The device also can be mounted on the wall as shown in the following figure.



Note:

The diameter of the screw, 4.5 mm<D<6.3 mm. The distance of two screws is 154.38 mm. The screw that project from the wall need around 2.8 mm based, and the length of the screw need to be at least 9.5 mm to withstand the weight of the product.

2. 2. Connect to the Internet

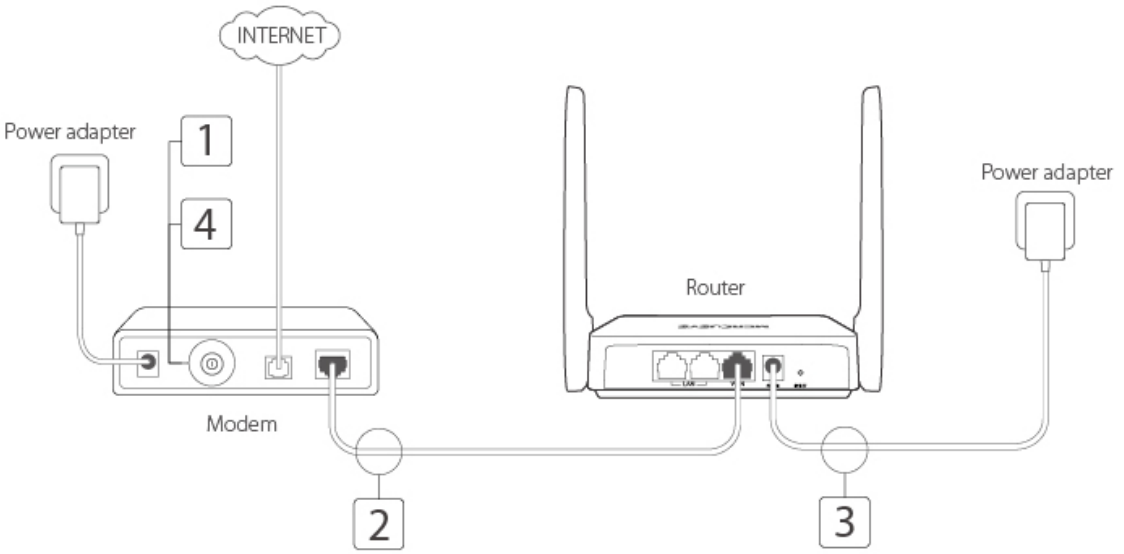
The Router provides two working modes: **Router Mode** and **Access Point Mode**. You can choose the mode to better suit your network needs and follow the guide to complete the configuration.

2. 2. 1. Router Mode

In this mode, the router can provide internet access for multiple wired and wireless devices. This mode is required most commonly.

1. Follow the steps below to connect your router.

If your Internet connection is through an Ethernet cable from the wall instead of through a DSL/Cable/Satellite modem, connect the Ethernet cable directly to the router's Internet/ WAN port, then connect the power adapter to the router.



1) Turn off the modem, and remove the backup battery if it has one.

2) Connect the modem to the router's WAN port with an Ethernet cable.

3) Connect the power adapter to the router.

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

2. Connect your computer to the router.

- **Method 1: Wired**

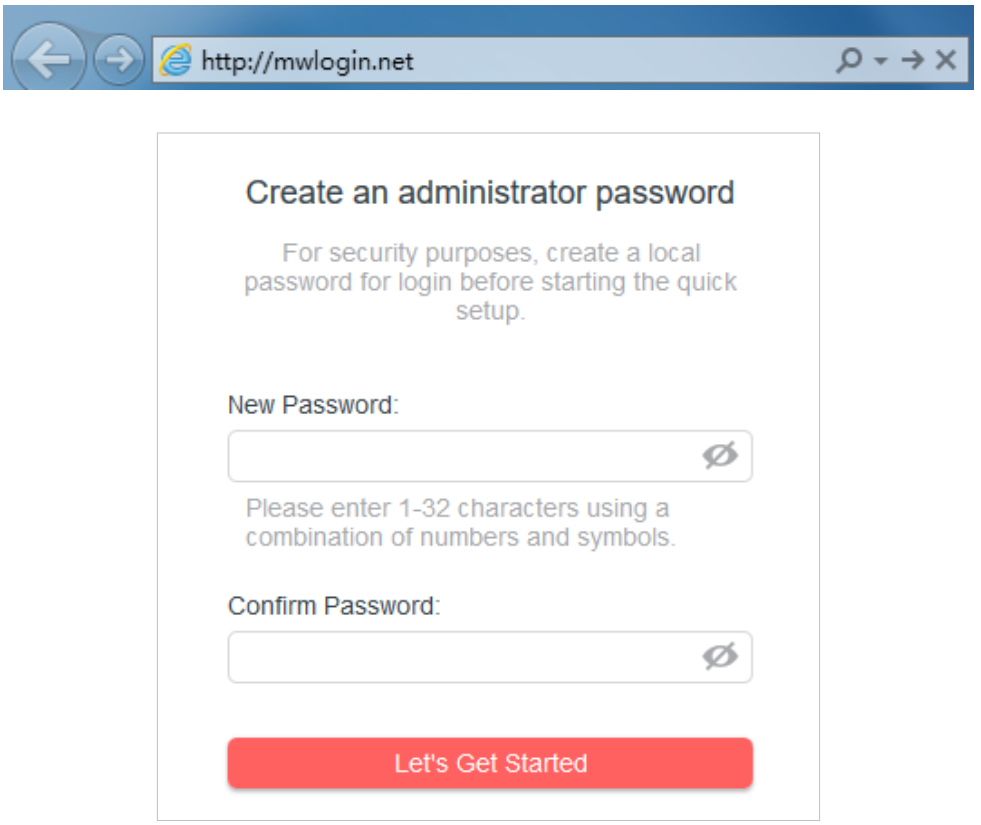
Turn off the Wi-Fi on your computer and connect the devices as shown below.

- **Method 2: Wirelessly**

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

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

3. Enter **http://mwlogin.net** in the address bar of a web browser. Create a password to log in.



Note:

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

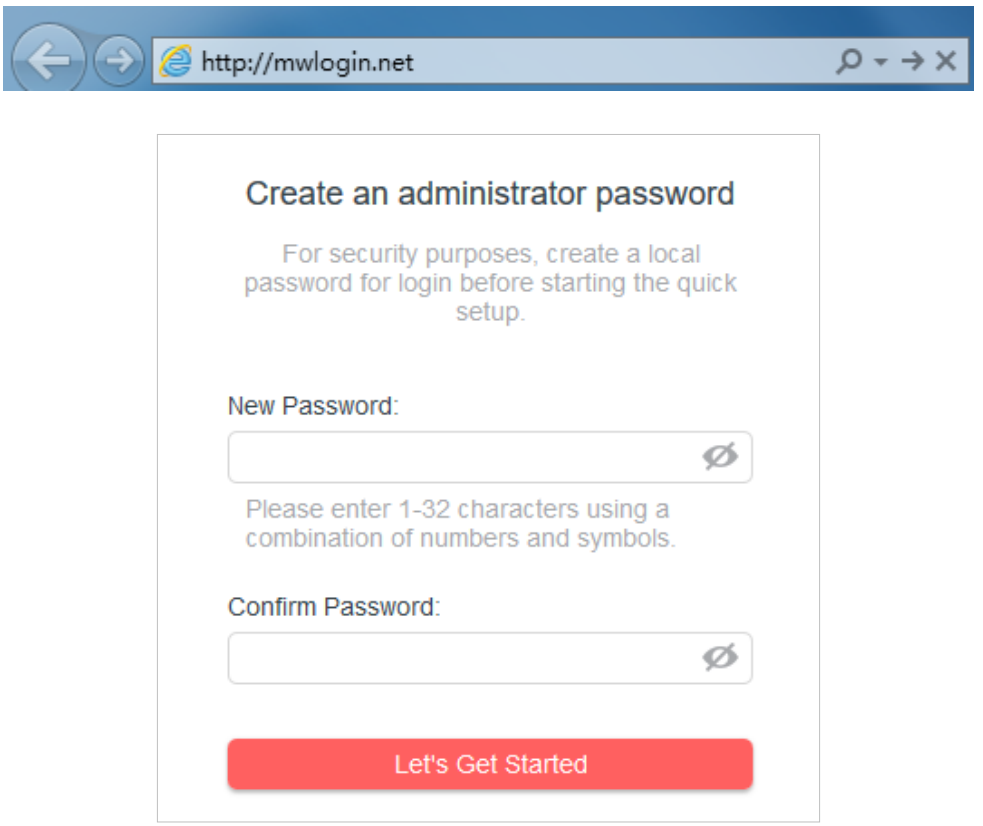
4. Follow the **Quick Setup** to set up the internet connection.
5. **Enjoy!** For wireless devices, you may have to reconnect to the wireless network if you have customized the SSID (wireless name) and password during the configuration.

2. 2. 2. Access Point Mode

In this mode, the router changes an existing wired network into a wireless one.

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

3. Connect a computer to the router via an Ethernet cable or wirelessly by using the SSID (network name) printed on the bottom label of the router.
4. Enter **http://mwlogin.net** in the address bar of a web browser. Create a password to log in.



Note:

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

5. Click **Change Mode** in the top right corner and select **Access Point Mode**. Wait for the router to reboot.
6. Follow the **Quick Setup** to set up the internet connection.
7. **Enjoy!** Connect to the wireless network by using the SSID (network name) and password of the router.

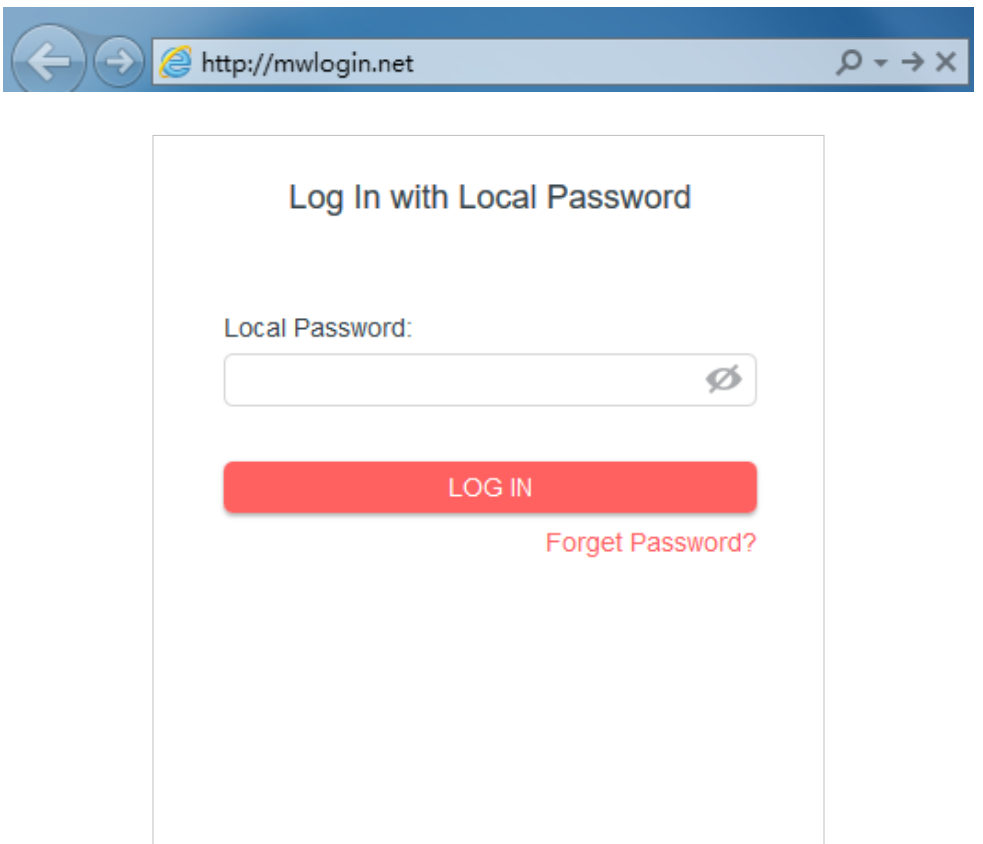
Chapter 3 Log In to the Router

This chapter introduces how to log in to the web management page of the router.

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

Follow the steps below to log in to your router.

1. Set up the TCP/IP Protocol in Obtain an IP address automatically mode on your computer.
2. Visit **http://mwlogin.net**, and log in with the password you set for the router.



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

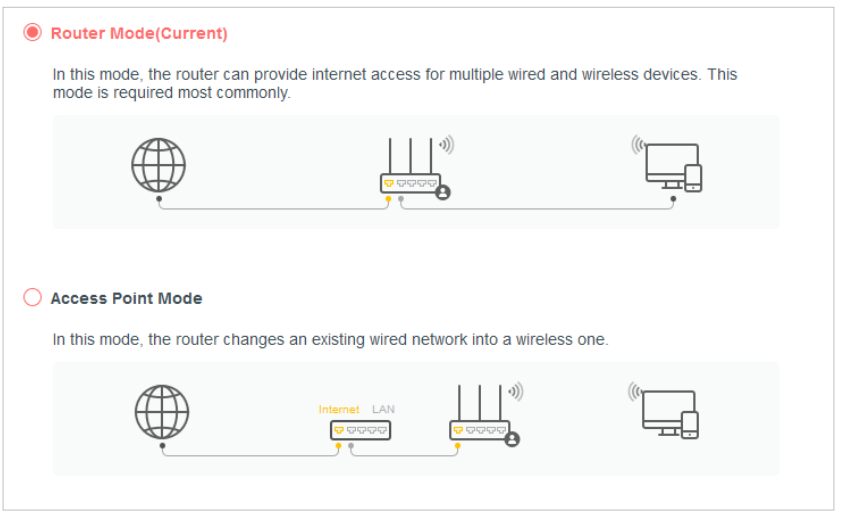
Chapter 4 Router Mode

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

It contains the following sections:

4.1 Operation Mode

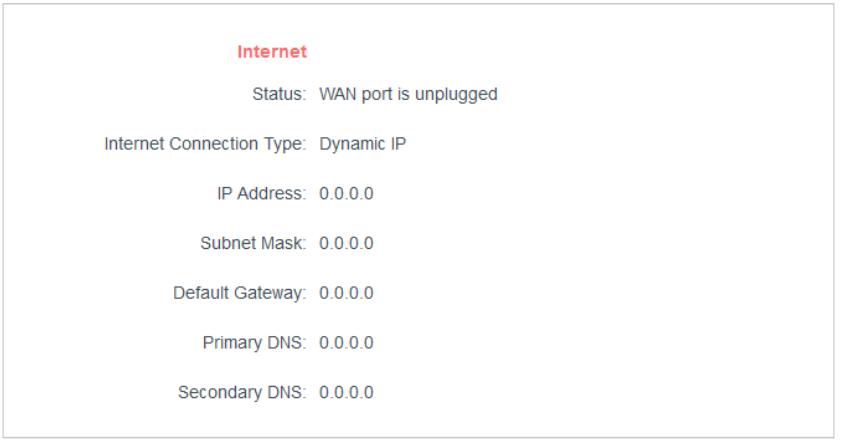
1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced** > **Operation Mode**.
3. Select the **Router Mode** and click **SAVE**.



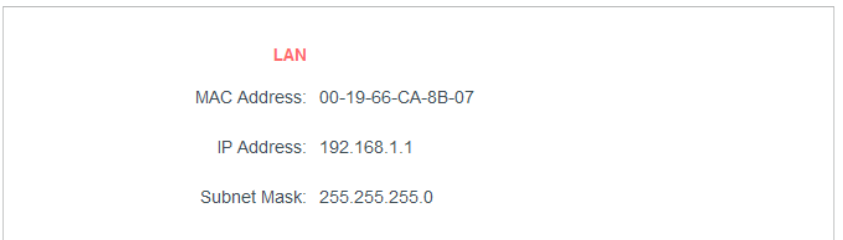
4.2 Network

4. 2. 1 Status

1. Visit **http://mwlogin.net**, and log in with password you set for the router.
2. Go to **Advanced** > **Network** > **Status**. You can view the current status information of the router.

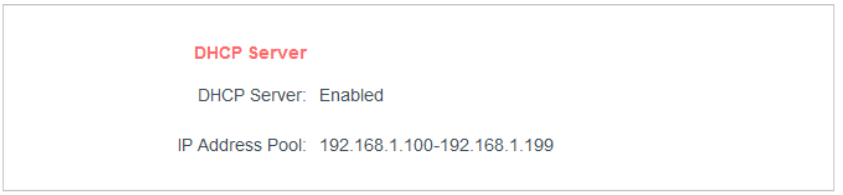


- **Internet** - This field displays the current settings of the internet, and you can configure them on the **Advanced** > **Network** > **Internet** page.
  - **Status** - Indicates whether the router has been connected to the internet.
  - **Internet Connection Type** - Indicates the way in which your router is connected to the internet.
  - **IP Address** - The WAN IP address of the router.
  - **Subnet Mask** - The subnet mask associated with the WAN IP address.
  - **Default Gateway** - The Gateway currently used is shown here.
  - **Primary & Secondary DNS** - The IP addresses of DNS (Domain Name System) server.

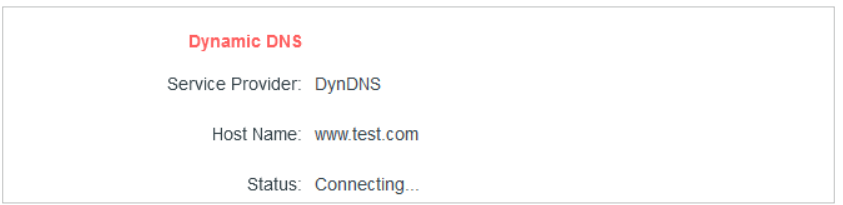


- **LAN** - This field displays the current settings of the LAN, and you can configure them on the **Advanced** > **Network** > **LAN page**.
  - **MAC Address** - The physical address of the router.
  - **IP Address** - The LAN IP address of the router.

- **Subnet Mask** - The subnet mask associated with the LAN IP address.



- **DHCP Server** - This field displays the current settings of DHCP (Dynamic Host Configuration Protocol) Server, and you can configure them on the **Network** > **DHCP Server** page.
  - **DHCP Server** - Indicates whether the DHCP server is enabled of disabled. It is enabled by default and the router acts as a DHCP server.
  - **IP Address Pool** - The IP address range for the DHCP server to assign IP addresses.



- **Dynamic DNS** - This field displays the current settings of the Dynamic DNS (Domain Name System), and you can configure them on the **Advanced** > **Network** > **Dynamic DNS** page.
  - **Service Provider** - The Dynamic DNS service provider you have signed up for.
  - **Host Name** - The Domain Name you have entered in the Dynamic DNS page.
  - **Status** - The status of the Dynamic DNS service connection.

4. 2. 2 Internet

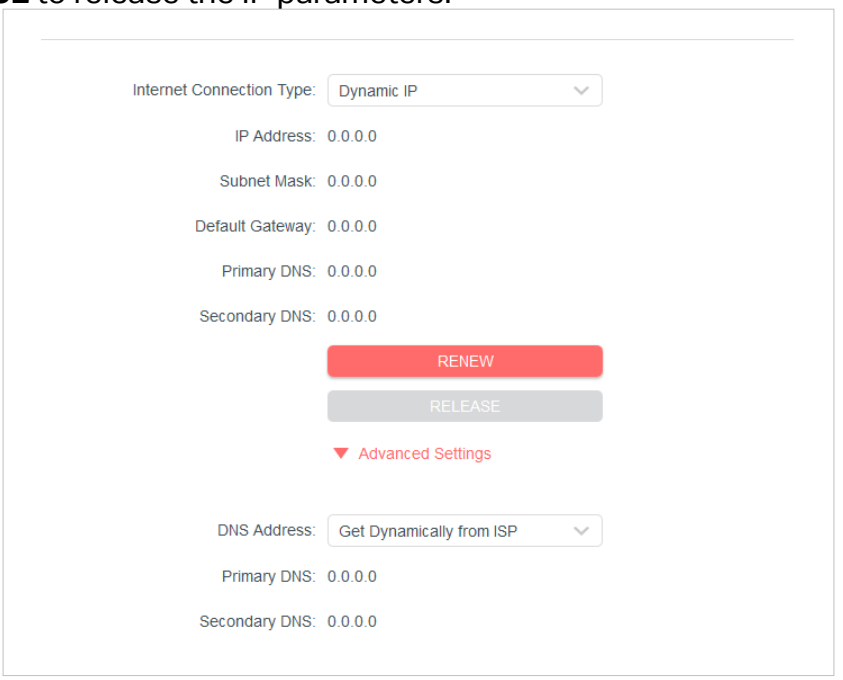
1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced** > **Network** > **Internet**.
3. Set up the internet connection and click **SAVE**.

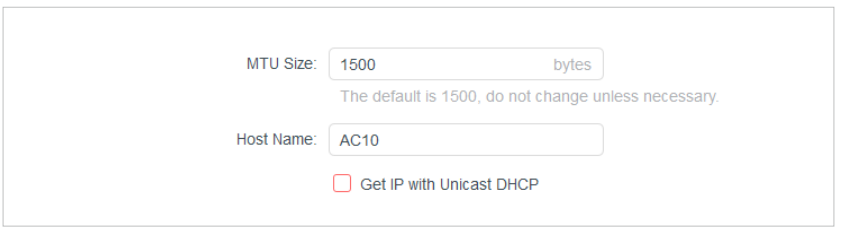
Dynamic IP

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.

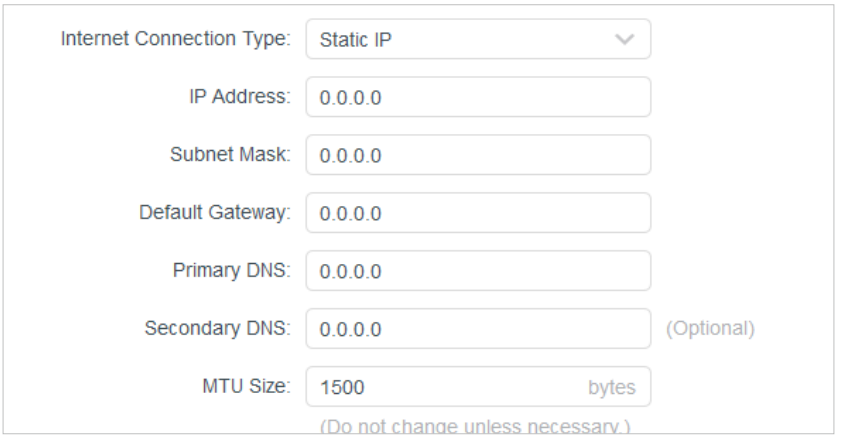




- **MTU Size** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU size unless required by your ISP.
- **Host Name** - This option specifies the name of the router.
- **Get IP with Unicast DHCP** - A few ISPs' DHCP servers do support the broadcast applications. If you cannot get the IP address normally, you can choose this option (it is rarely required).

Static IP

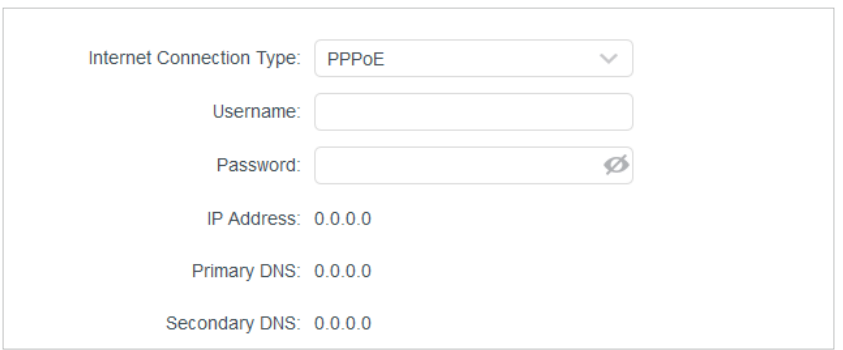
If your ISP provides a static or fixed IP address, subnet mask, default gateway and DNS setting, please select **Static IP**.



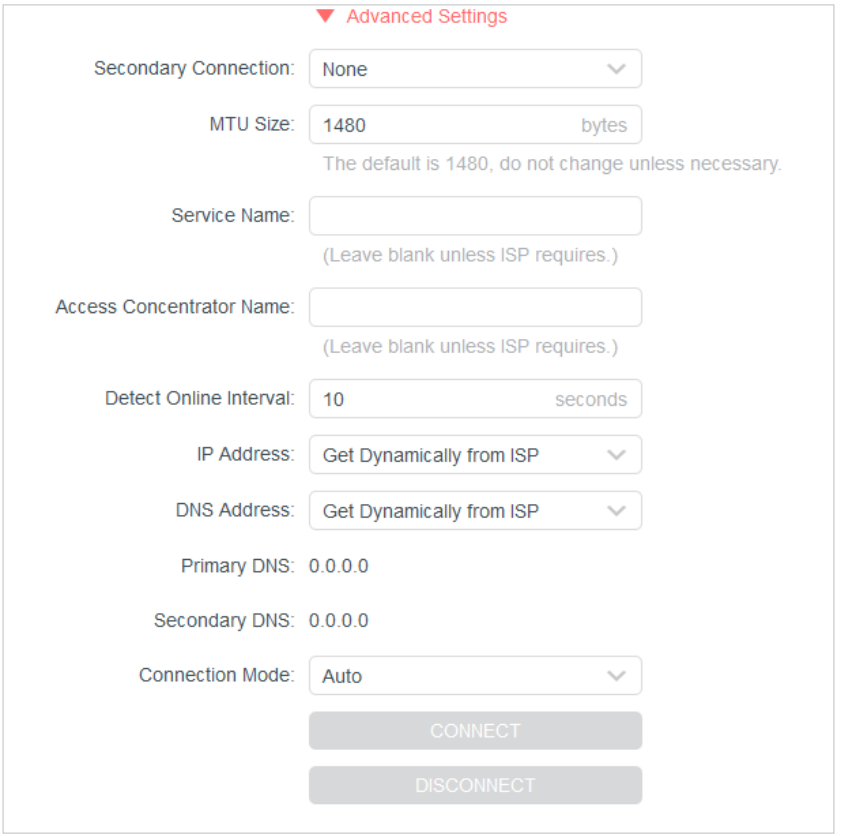
- **IP Address** - Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask** - Enter the subnet mask in dotted-decimal notation provided by your ISP. Normally 255.255.255.0 is used as the subnet mask.
- **Default Gateway** - Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- **Primary/Secondary DNS** - (Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.
- **MTU Size** - 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.

PPPoE

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



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



- **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.
- **MTU Size** - The default MTU size is 1480 bytes. It is not recommended that you change the default MTU size unless required by your ISP.
- **Service Name** - The service name should not be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank will work.
- **Access Concentrator Name** - The access concentrator name should not be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank will work.
- **Detect Online Interval** - The router will detect Access Concentrator online at every interval. The default value is 10. You can input the value between 0 and 120. The value 0 means no detect.
- **IP Address** - The default setting is to get an IP address dynamically from your ISP. If your ISP does not automatically assign IP addresses to the router, please select **Use the Following IP Address** and enter the IP address provided by your ISP in

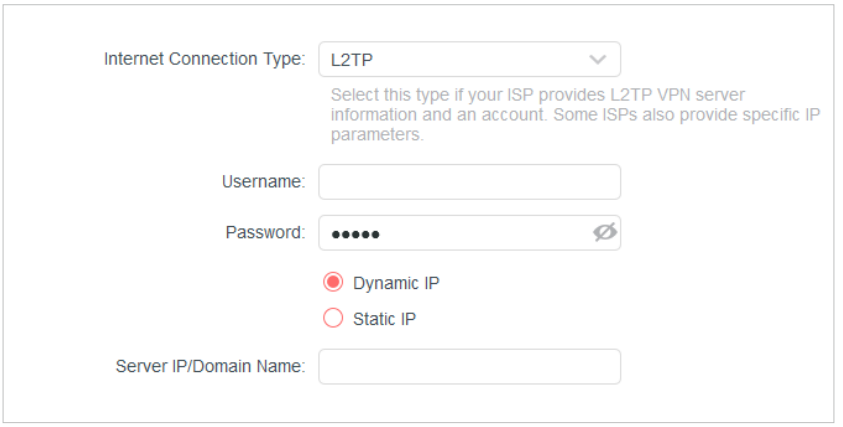
dotted-decimal notation.

- **DNS Address** - The default setting is to get an IP address dynamically from your ISP. If your ISP does not automatically assign DNS addresses to the router, please select **Use the Following DNS Addresses** 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.
- **Connection Mode** - Select an appropriate connection mode that determines how to connect to the internet.
    - **Auto** - In this mode, the internet connection reconnects automatically any it gets disconnected.
    - **On Demand** - In this mode, the internet connection will be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the internet again.
    - **Time-based** - In this mode, the internet connection is only established in a specific timeframe. If this option is selected, enter the start time and end time. Both are in HH:MM format.
    - **Manual** - In this mode, the internet connection is controlled manually by clicking the **Connect/Disconnect** button. This mode also supports the **Max Idle Time** function as **On Demand** mode. Enter a maximum time (in minutes), the internet connection can be inactive before it is terminated into the Max Idle Time. The default value is 15 minutes. If you want the internet connection remains active all the time, enter 0 (zero).

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.

L2TP

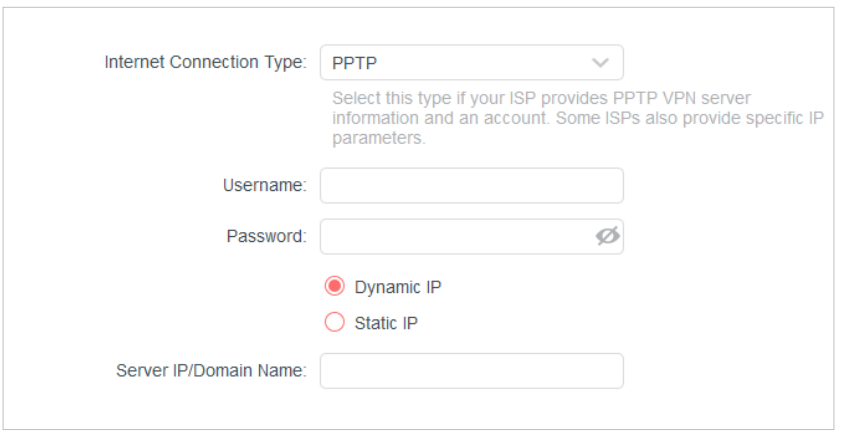
Select this type if your ISP provides L2TP VPN server information and an account. Some ISPs also provide specific IP parameters.



- **Username/Password** - Enter the username and password provided by your ISP. These fields are case-sensitive.
- **Server IP/ Domain Name** - Enter the VPN server's IP address or domain name provided by your ISP.

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.
- **Server IP/ Domain Name** - Enter the VPN server's IP address or domain name provided by your ISP.

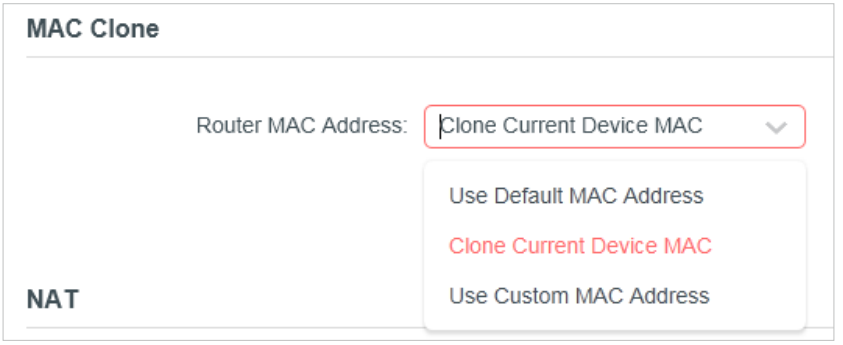
Note:

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.

4. 2. 3 MAC Clone

1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced** > **Network** > **Internet** and locate the MAC Clone section.

3. Configure **Router MAC Address** and click **SAVE**.



- **Use Default MAC Address** - Do not change the default MAC address of your router in case the ISP does not bind the assigned IP address to the MAC address.
- **Clone Current Device MAC** - Select to copy the current MAC address of the computer that is connected to the router, in case the ISP binds the assigned IP address to the MAC address.
- **Use Custom MAC Address** - Select if your ISP requires you to register the MAC address and enter the correct MAC address in this field, in case the ISP binds the assigned IP address to the specific MAC address.

Note:

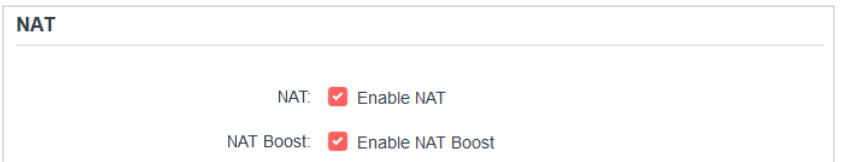
- You can only use the MAC Address Clone function for PCs on the LAN.
- If you have changed the WAN MAC address when the WAN connection is PPPoE, it will not take effect until the connection is re-established.

4. 2. 4 NAT

1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced** > **Network** > **Internet** and locate the NAT section.
3. Configure **NAT** and **NAT Boost**, then click **SAVE**.

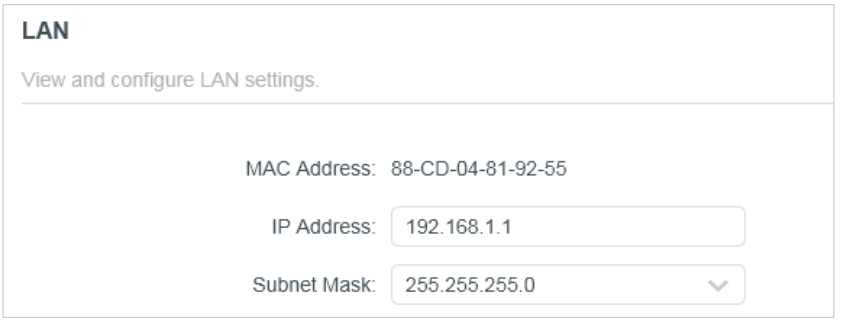
Note:

- QoS and NAT Boost cannot be enabled at the same time.



4. 2. 5 LAN

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



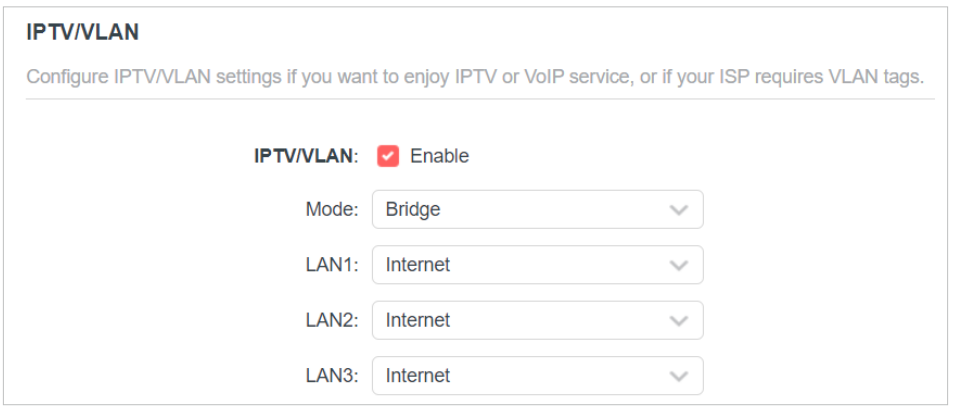
- **MAC Address** - The physical address of the LAN ports. The value can not be changed.
- **IP Address** - Enter the IP address in dotted-decimal notation of your router (the default one is 192.168.1.1).
- **Subnet Mask** - An address code that determines the size of the network. Normally 255.255.255.0 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.

4. 2. 6 IPTV/VLAN

1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced** > **Network** > **IPTV/VLAN**.
3. Configure IPTV/VLAN settings if you want to enjoy IPTV or VoIP service, or if your ISP requires VLAN tags.



- **IPTV/VLAN** - Select to enable the IPTV feature.
- **Mode** - Select the appropriate mode according to your ISP.

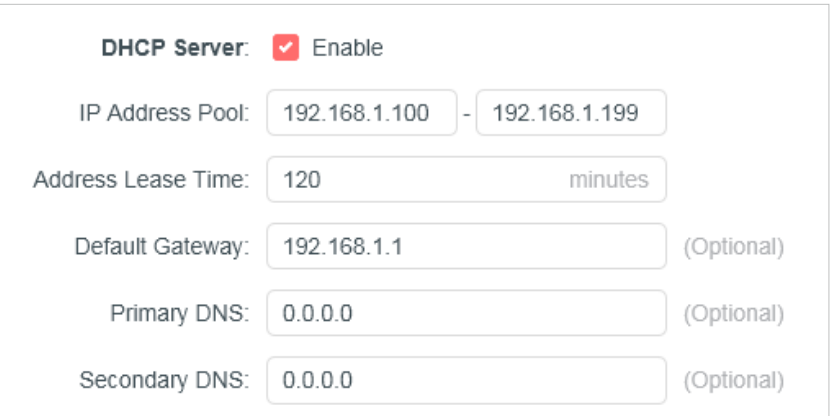
4. 2. 7 DHCP Server

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.

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

1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced** > **Network** > **DHCP Server** and locate the DHCP Server section.



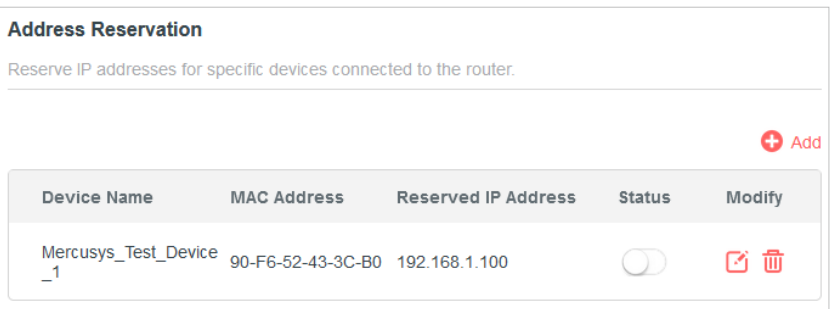
1. Tick the **Enable** checkbox.
2. Enter the starting and ending IP addresses in the **IP Address Pool**.
3. Enter other parameters if the ISP offers. The **Default Gateway** is automatically filled in and is the same as the LAN IP address of the router.
4. Click **SAVE**.

Note:

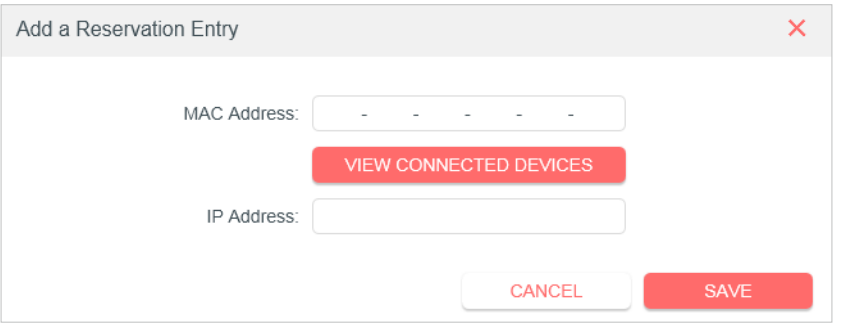
To use the DHCP server function of the router, you must configure all computers on the LAN as Obtain an IP Address automatically.

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

1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced** > **Network** > **DHCP Server** and locate the **Address Reservation** section.
3. Click **Add** in the **Address Reservation** section.



4. Click **VIEW CONNECTED DEVICES** and select the you device you want to reserve an IP for. Then the **MAC and IP Address** will be automatically filled in. You can also enter the **MAC and IP address** of the client device.



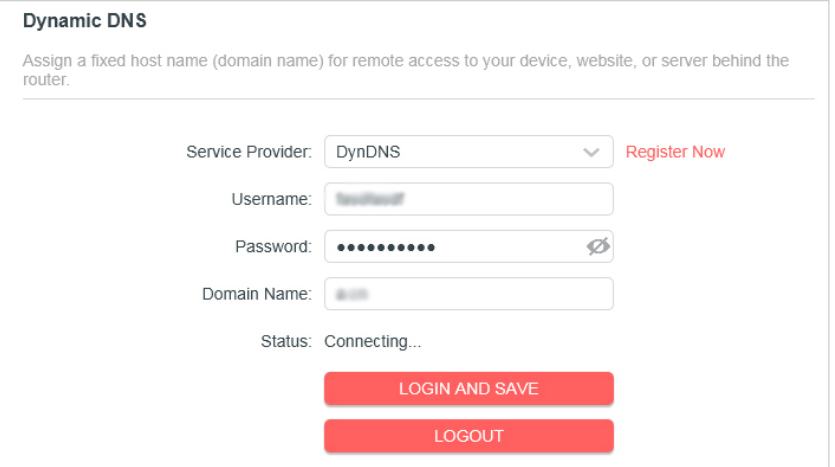
- **To check the DHCP client list:**

1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced** > **Network** > **DHCP Server** and locate the **DHCP Client List** section. You can see the device information of the list.
3. Click **Refresh** to see the current attached devices.

4. 2. 8 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://mwlogin.net**, and log in with the username and password you set for the router.
2. Go to **Advanced** > **Network** > **Dynamic DNS**.
3. Select the **DDNS Service Provider**: NO-IP or DynDNS. If you don't have a DDNS account, you have to register first by clicking **Register Now**.



4. Enter the **Username** for your DDNS account.
5. Enter the **Password** for your DDNS account.
6. Enter the **Domain Name** you received from dynamic DNS service provider here.
7. If your service provider is NO-IP, select **WAN IP binding** to ensure that the domain name is bound to the WAN IP of this router.
8. Click **LOGIN AND SAVE**.

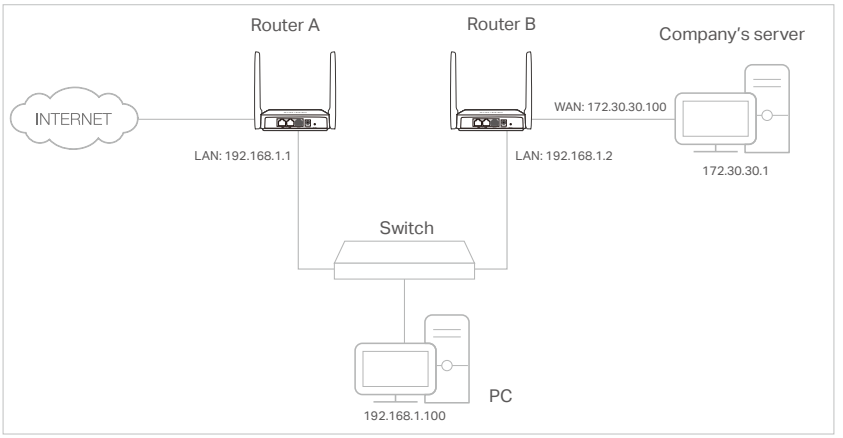
4. 2. 9 Static Routing

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.

I want to:

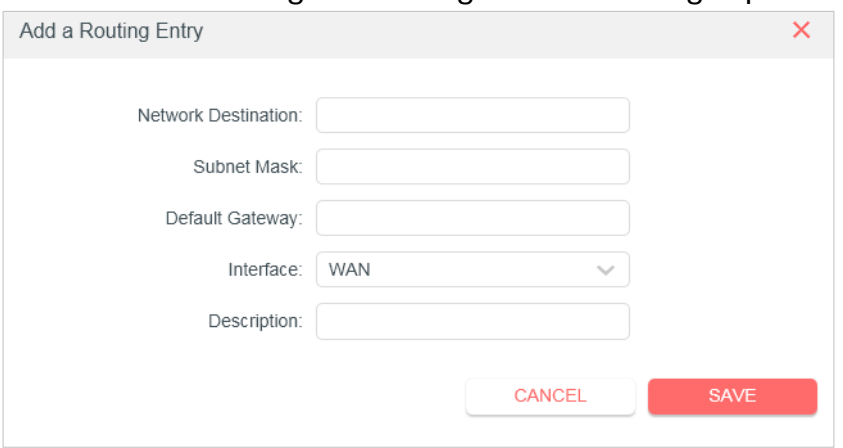
Visit multiple networks and servers at the same time.

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



How can I do that?

1. Change the routers' LAN IP addresses to two different IP addresses on the same subnet. Disable Router B's DHCP function.
2. Visit **http://mwlogin.net**, and log in with the password you set for Router A.
3. Go to **Advanced** > **Network** > **Routing** and locate the Static Routing section.
4. Click **Add** and finish the settings according to the following explanations:



- **Network Destination** - The destination IP address that you want to assign to a static route. This IP address cannot be on the same subnet with the WAN IP or LAN IP of Router A. In the example, the IP address of the company network is the destination IP address, so here enter 172.30.30.1.
- **Subnet Mask** - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.
- **Default Gateway** - The IP address of the gateway device to which the data packets will be sent. This IP address must be on the same subnet with the router's IP which sends out data. In the example, the data packets will be sent to the LAN port of Router B and then to the Server, so the default gateway

should be 192.168.1.2.

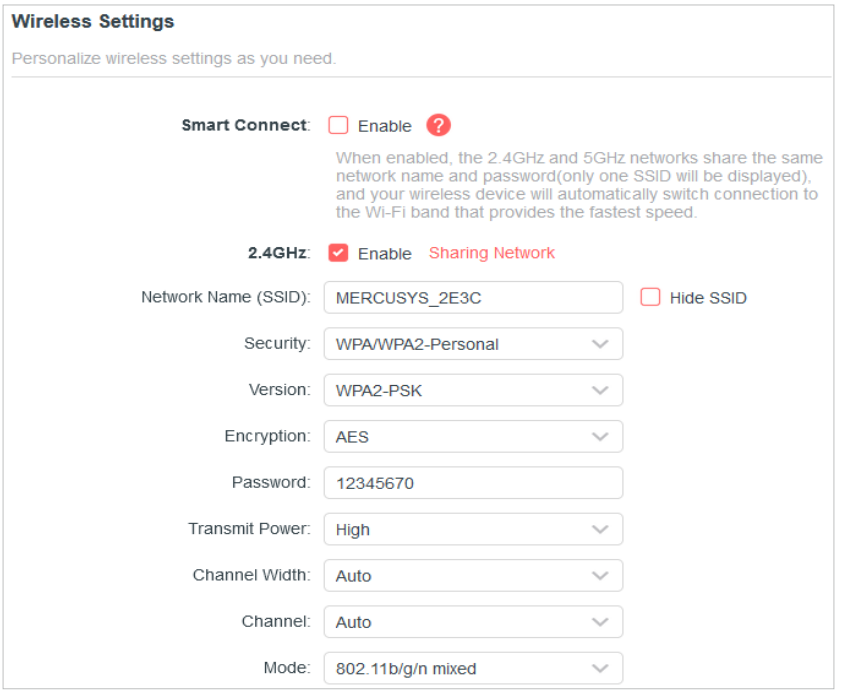
- **Interface** - Determined by the port (WAN/LAN) that sends out data packets. In the example, the data are sent to the gateway through the LAN port of Router A, so **LAN** should be selected.
- **Description** - Enter a description for this static routing entry.

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

4.3 Wireless

4. 3. 1 Wireless Settings

1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced** > **Wireless** > **Wireless Settings**.
3. Configure the wireless settings for the wireless network and click **SAVE**.



- **Smart Connect** - When enabled, the 2.4GHz and 5GHz networks share the same network name and password(only one SSID will be displayed), and your wireless device will automatically switch connection to the Wi-Fi band that provides the fastest speed.
- **2.4GHz** - Select this checkbox to enable the 2.4GHz wireless network.
- **Network Name (SSID)** - Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network.
- **Hide SSID** - Select this checkbox if you want to hide the 2.4GHz network name (SSID) from the Wi-Fi network list. In this case, you need to manually join the network.
- **Security** - Select an option from the Security drop-down list.
    - **None** - No security. It is highly recommend you enable the wireless security to protect your wireless network from unauthorized access.
    - **WPA-PSK/WPA2-Personal** - It's the WPA/WPA2 authentication type based on pre-shared passphrase. It's also the recommended security type.

- **WPA /WPA2-Enterprise** - It's based on Radius Server.

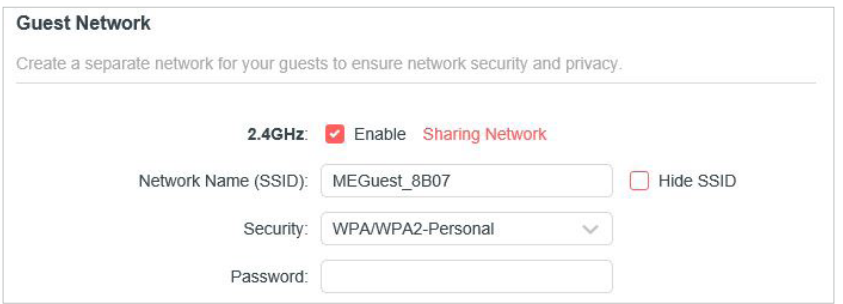
- **Version** - Keep default version value.
- **Encryption** - Select **Auto**, **TKIP** or **AES**. We recommend you keep the default settings.
- **Transmit Power** - Select **High**, **Middle** or **Low** to specify the data transmit power. The default and recommended setting is **High**.
- **Channel Width** - Select a channel width (bandwidth) for the wireless network.
- **Channel** - Select an operating channel for the wireless network. It is recommended to leave the channel to **Auto**, if you are not experiencing the intermittent wireless connection issue.
- **Mode** - You can choose the appropriate "Mixed" mode.

4. 3. 2 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.

- **Create a Guest Network**

1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to Wireless or **Advanced** > **Wireless** > **Guest Network**.
3. Enable the **Guest Network** function.

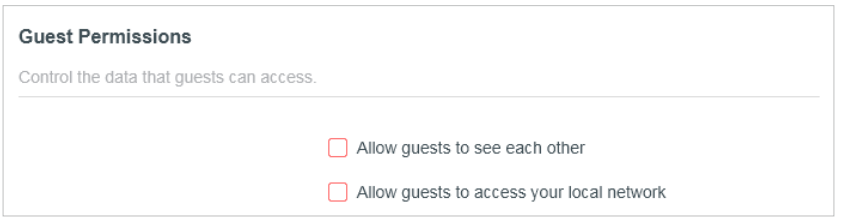


4. Create a network name for your guest network.
5. Select the **Security** type and create the **Password** of the guest network.
6. Click **SAVE**. Now you guests can access your guest network using the SSID and password you set!

- **Customize Guest Network Options**

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

2. Go to **Advanced** > **Wireless** > **Guest Network**. Locate the **Guest Permissions** section.
3. Customize guest network options according to your needs.



- **Allow guests to see each other**

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

- **Allow guests to access my local network**

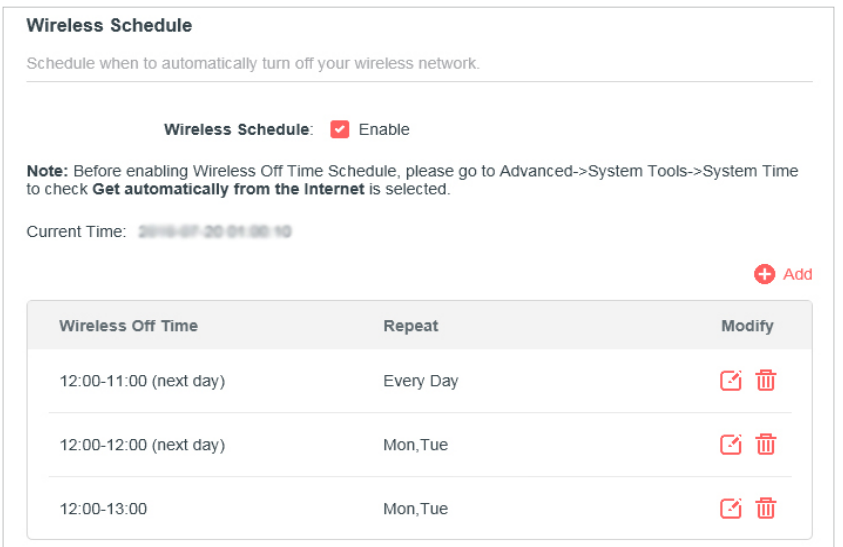
  Tick this checkbox if you want to allow the wireless clients on your guest network to communicate with the devices connected to your router's LAN ports or main network via methods such as network neighbors and Ping.

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

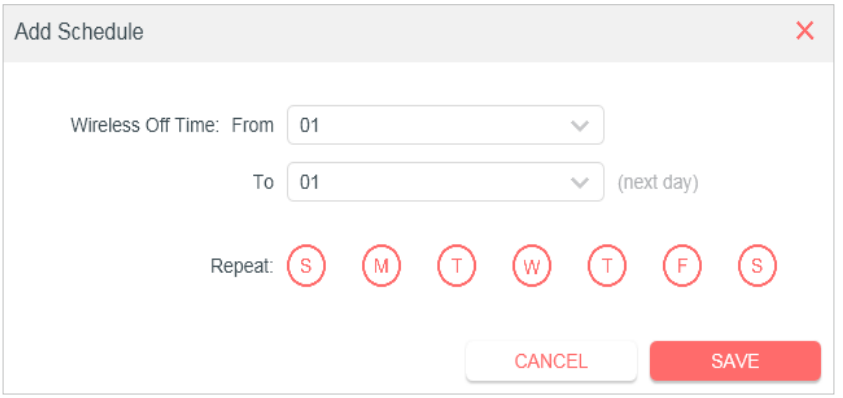
4. 3. 3 Wireless Schedule

The wireless function can be automatically off at a specific time when you do not need the wireless function.

1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced** > **Wireless** > **Wireless Schedule**.
3. Enable the **Wireless Schedule** function.



4. Click **Add** to specify a wireless off period during which you need the wireless off automatically, and click **SAVE**.



Note:

- The effective wireless schedule is based on the time of the router. You can go to **Advanced** > **System** > **Time** to modify the time.
- The wireless network will be automatically turned on after the time period you set.

4. 3. 4 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:

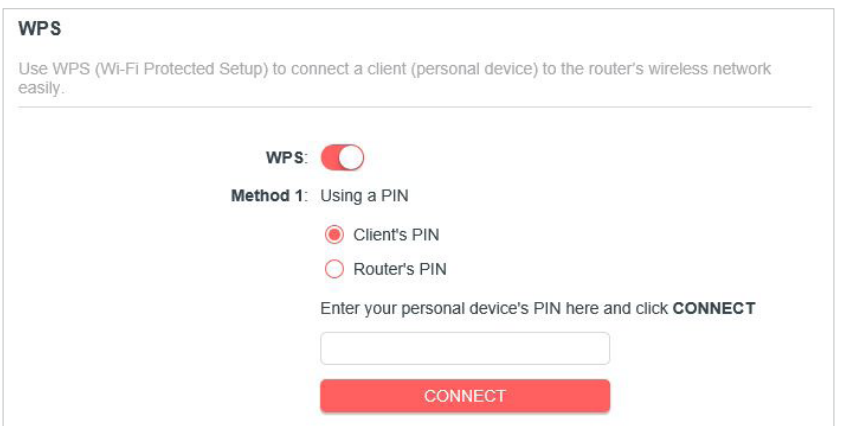
The WPS function cannot be configured if the wireless function of the router is disabled. Please make sure the wireless function is enabled before configuration.

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

Method ONE: Using a PIN

• Connects via the Client's PIN

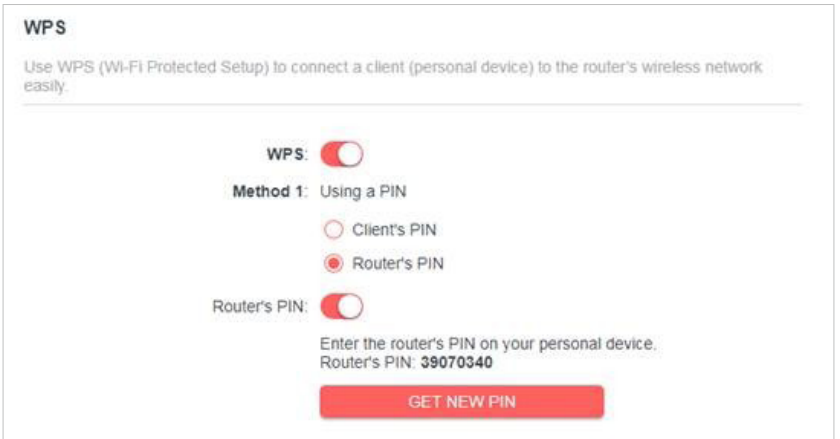
1. Keep the WPS Status as **Enabled** and select **Client's PIN**.



2. Enter the PIN of your device and click **CONNECT**. Then your device will get connected to the router.

- **Connects via the Router's PIN**

1. Keep the WPS Status as **Enabled** and select **Router's PIN**.



2. Enter the router's PIN on your personal device. You can also generate a new one.

Note:

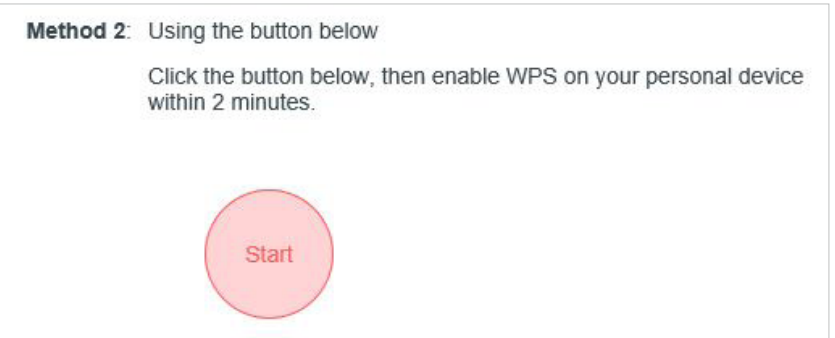
PIN (Personal Identification Number) is an eight-character identification number preset to each router. WPS supported devices can connect to your router with the PIN.

Method TWO: Push the WPS Button

Click **Start** on the screen. Within two minutes, press the WPS button on your device. A **Device-(XX-XX-XX-XX-XX-XX)** Connected message should appear on the screen and the LED should change from blinking to solid on, indicating successful WPS connection.

Note:

XX-XX-XX-XX-XX-XX is the MAC address of your device.

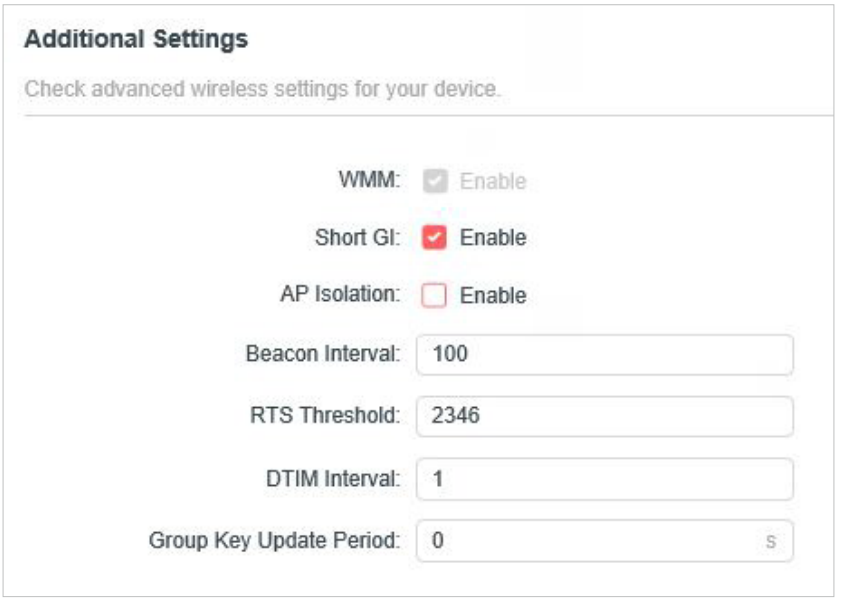


4. 3. 5 Additional Settings

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



- **Enable WMM** - WMM function can guarantee the packets with high-priority messages being transmitted preferentially.
- **Enable Short GI** - It is recommended to enable this function, for it will increase the data capacity by reducing the guard interval time.
- **AP Isolation** - This function isolates all connected wireless stations so that wireless stations cannot access each other through WLAN.
- **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.
- **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.
- **Group Key Update Period** - Enter a number of seconds (minimum 30) to control the time interval for the encryption key automatic renewal. The default value is 0,

meaning no key renewal.

4. 3. 6 WDS

WDS (Wireless Distribution System) Bridging feature allows you to bridge a router with an access point to extend the wireless network coverage.

Note:

• WDS bridging only requires configuration on the extended router;

• WDS bridging function can be enabled either in 2.4GHz frequency or 5GHz frequency. The WDS function can work at only one of the bands at one time.

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

2. Configure the router's LAN IP.

1) Go to **Advanced** > **Network** > **LAN**.

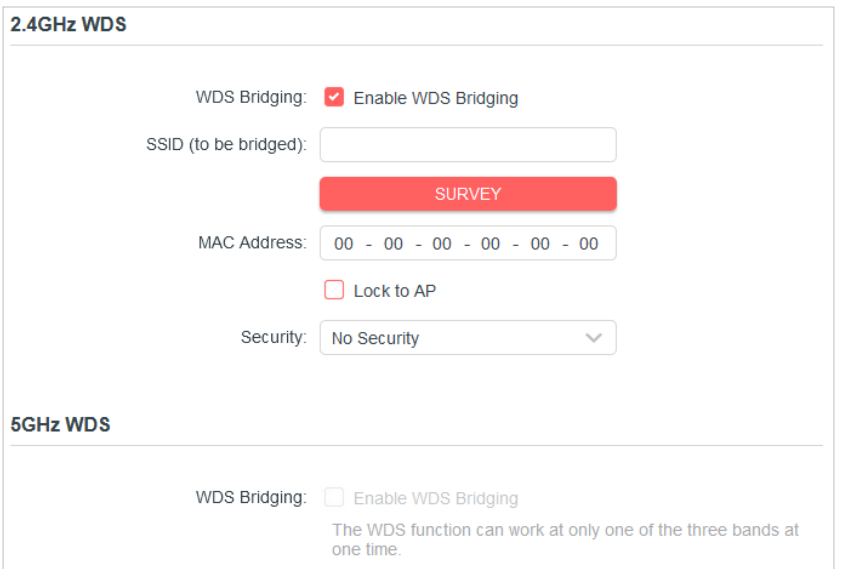
2) Set the LAN IP to be in the same subnet as the access point/router to be bridged. (For example, if your access point's LAN IP is 192.168.0.1, you can set this router's LAN IP to an address from 192.168.0.2 to 192.168.0.254.)

3) Save the settings.

3. Configure WDS Bridging.

1) Go to **Advanced** > **Wireless** > **WDS**.

2) Enable **WDS Bridging** either in 2.4GHz frequency or 5GHz frequency.



3) Click **Survey** to and choose the network to be bridged. The SSID (network name) and MAC Address will be automatically filled in. You can also manually fill in these parameters.

4) Set the **Security** type and related parameters to be the same as the network to be bridged.

5) Save the settings.

4. Go to **Advanced** > **Network** > **DHCP Server**, and disable **DHCP Server**.

4.4 NAT Forwarding

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

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

The Mercusys router includes four forwarding rules. If two or more rules are set, the priority of implementation from high to low is Port Forwarding, Port Triggering, UPNP and DMZ.

4. 4. 1 Port Forwarding

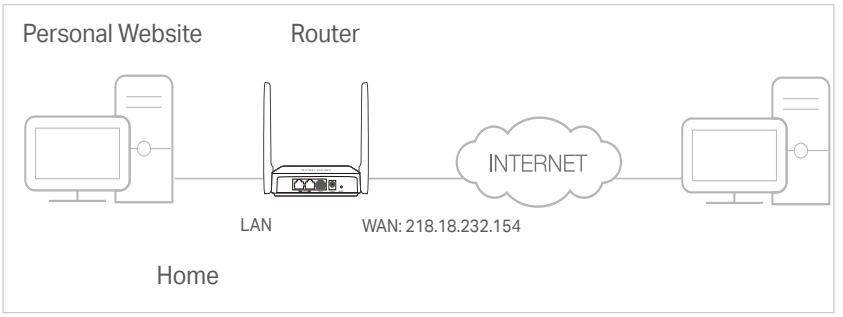
When you build up a server in the local network and want to share it on the internet, Port Forwarding can realize the service and provide it to internet users. At the same time Port Forwarding can keep the local network safe as other services are still invisible from the internet.

Port Forwarding 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.

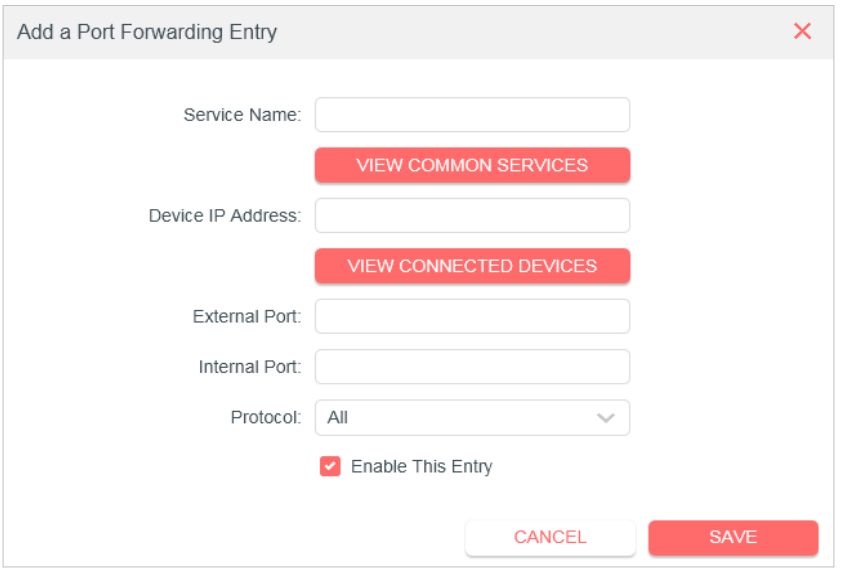
I want to:

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 (192.168.1.100). 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 192.168.1.100.
2. Visit **http://mwlogin.net**, and log in with the password you set for the router.
3. Go to **Advanced** > **NAT Forwarding** > **Port Forwarding**.
4. Click **Add**.



5. Click **VIEW COMMON SERVICES** and select **HTTP**. The **External Port**, **Internal Port** and **Protocol** will be automatically filled in.
6. Click **VIEW CONNECTED DEVICES** and select your home PC. The **Device IP Address** will be automatically filled in. Or enter the PC's IP address 192.168.1.100 manually in the **Device IP Address** field.
7. 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 Services** 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 **External Port** should not be overlapped.

Done!

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

Note:

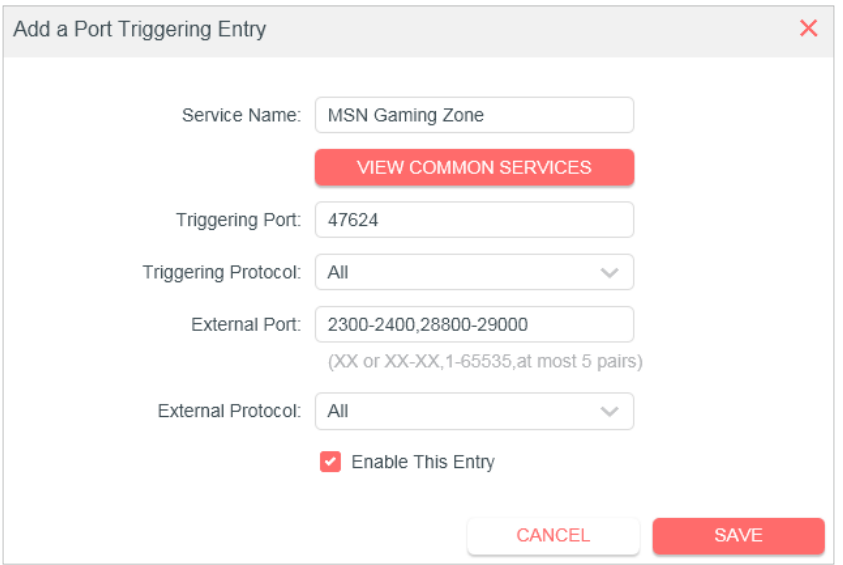
- If you have changed the default **External Port**, you should use **http:// WAN IP: External Port** to visit the website.
- The WAN IP should be a public IP address. For the WAN IP is assigned dynamically by the ISP, it is recommended to apply and register a domain name for the WAN referring to **Dynamic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

4. 4. 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://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced** > **NAT Forwarding** > **Port Triggering**.
3. Click **Add**.
4. Click **VIEW COMMON SERVICES**, and select the desired application. The Triggering Port, Triggering Protocol and External Port will be automatically filled in. The following picture takes application MSN Gaming Zone as an example.



5. 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 Services list, please enter the parameters manually. You should verify the external ports the application uses first and enter them in External Ports 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.

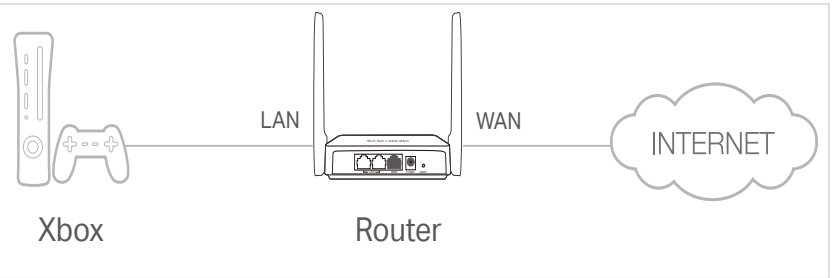
4. 4. 3 UPnP

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:

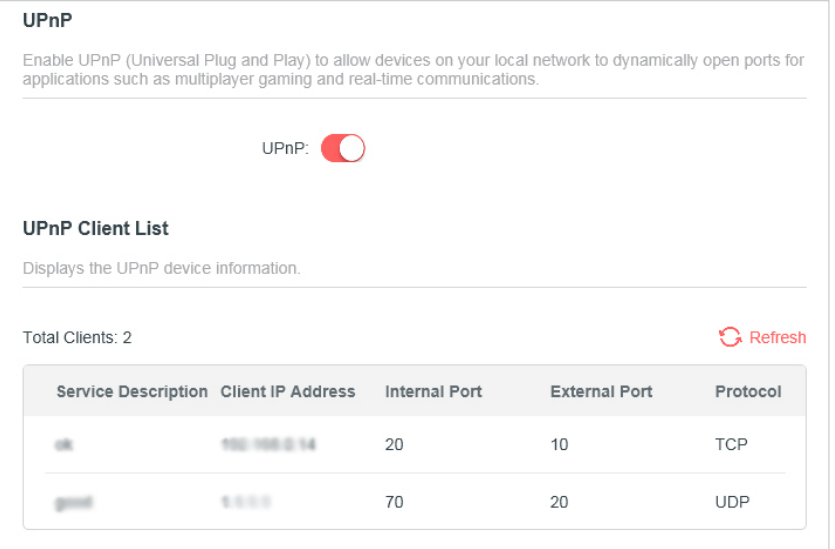
- UPnP is enabled by default in this router.
- Only the application supporting UPnP protocol can use this feature.
- UPnP feature needs the support of operating system (e.g. Windows Vista/ Windows 7/ Windows 8, etc. Some of operating system need to install the UPnP components).

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



4. 4. 4 DMZ

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

Note:

DMZ is more applicable in the situation that users are not clear about which ports to open. When it is enabled, the DMZ host is totally exposed to the internet, which may bring some potential safety hazards. If DMZ is not in use, please disable it in time.

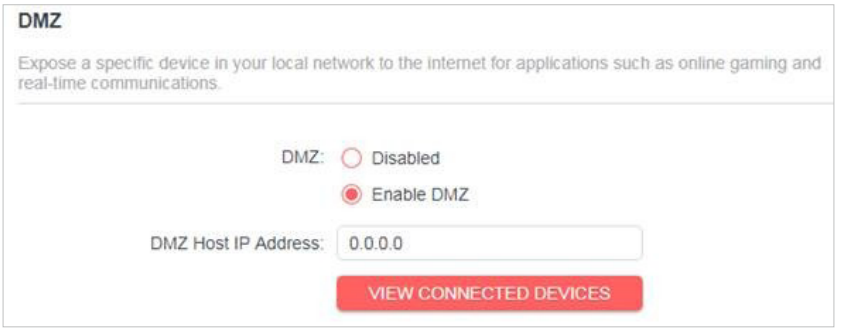
I want to:

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

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

How can I do that?

1. Assign a static IP address to your PC, for example 192.168.1.100.
2. Visit **http://mwlogin.net**, and log in with the password you set for the router.
3. Go to **Advanced** > **NAT Forwarding** > **DMZ** and select **Enable DMZ**.
4. Click **VIEW CONNECTED DEVICES** and select your PC. The DMZ Host IP Address will be automatically filled in. Or enter the PC's IP address 192.168.1.100 manually in the DMZ Host IP Address field.



5. Click **SAVE**.

Done!

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

4.5 Parental Controls

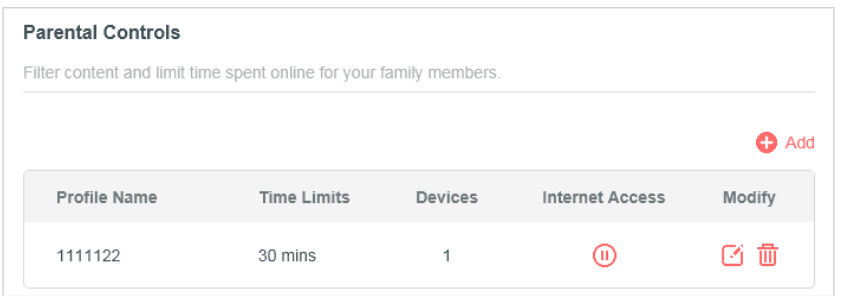
Parental Controls allows you to set up unique restrictions on internet access for each member of your family. You can block inappropriate content, set daily limits for the total time spent online and restrict internet access to certain times of the day.

I want to:

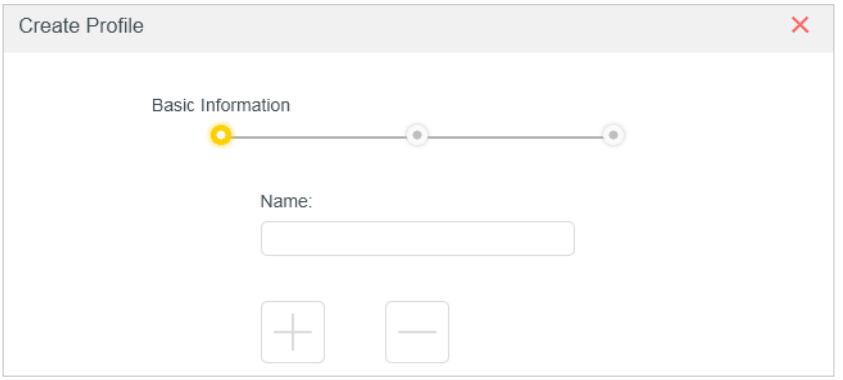
Block access to inappropriate online content for my child's devices, restrict internet access to 2 hours every day and block internet access during bed time (10 PM to 7 AM) on weekdays.

How can I do that?

1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced** > **Parental Controls**.
3. Click **Add** to create a profile for a family member.



4. Add basic profile information.



1) Enter a Name for the profile to make it easier to identify.

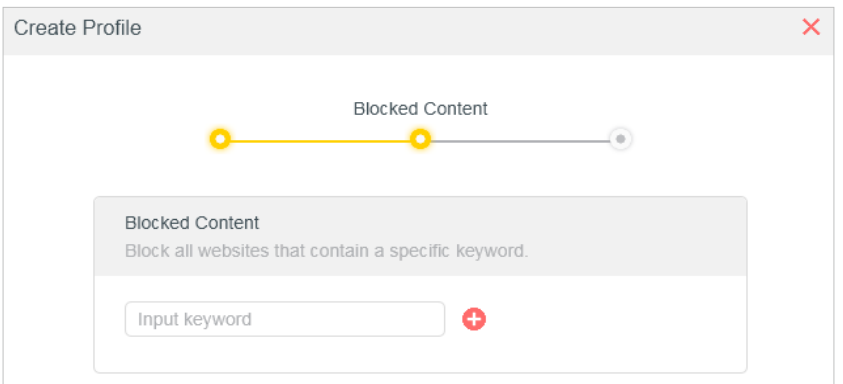
2) Under Devices, click .

3) Select the devices that belong to this family member. Access restrictions will be applied to these devices. Click **ADD** when finished.

Note: Only devices that have previously been connected to your router's network are listed here. If you are unable to find the device you want to add, connect it to your network and then try again.

4) Click **NEXT**.

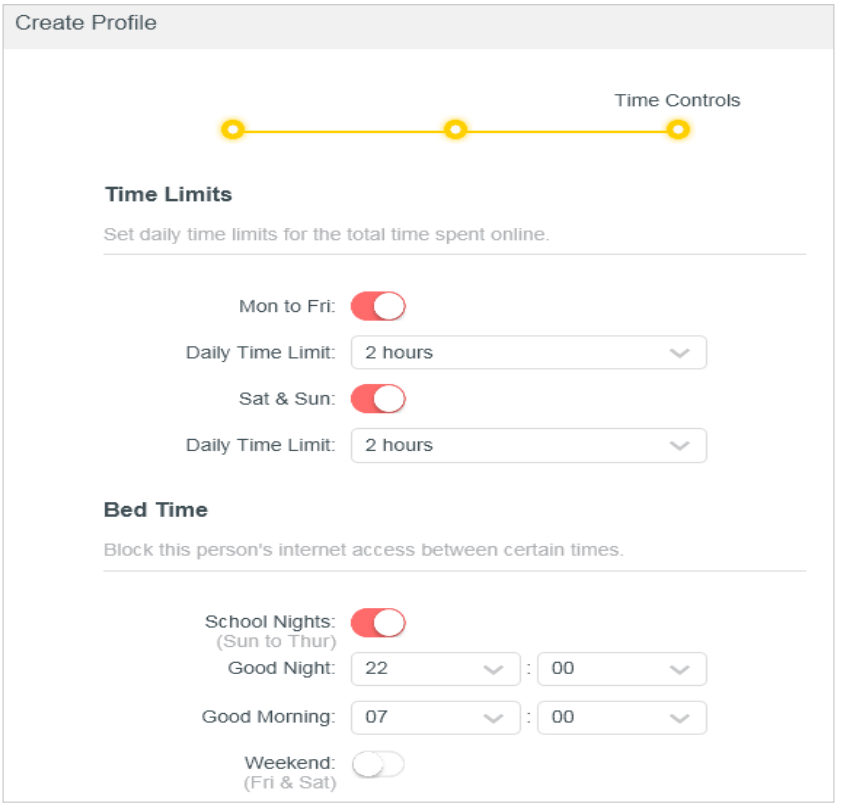
5. Block content for this profile.



1) Enter the key word of the website that you want to block. Click if want to block multiple websites.

2) Click **NEXT**.

6. Set time restrictions on internet access.



1) Enable **Time Limits** on Monday to Friday and Saturday & Sunday then set the allowed online time to 2 hours each day.

2) Enable **Bed Time** on School Nights (Sun to Thur) and use the up/down arrows or enter times in the fields. Devices under this profile will be unable to access the internet during this time period.

3) Click **SAVE**.

Note: The effective time limits are based on the time of the router. You can go to **Advanced** > **System** > **Time** to modify the time.

Done!

The amount of time your child spends online is controlled and inappropriate content is blocked on their devices.

4.6 QoS

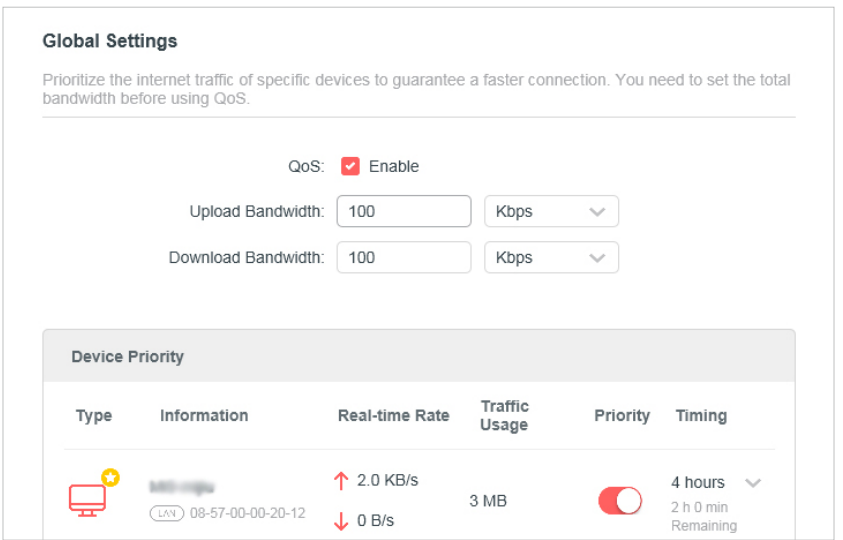
QoS (Quality of Service) is designed to ensure the efficient operation of the network when come across network overload or congestion. Devices set as high priority will be allocated more bandwidth and so continue to run smoothly even when there are many devices connected to the network.

I want to:

Ensure a fast connection of my computer while I play online games for the next 2 hours.

How can I do that

1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced** > **QoS**.
3. Tick the **Enable** checkbox of QoS.
4. Enter the maximum upload and download bandwidths provided by your internet service provider, and then click **SAVE**. 1Mbps equals to 1,000Kbps.
5. Find your computer in the **Device Priority** section and toggle on **Priority**. Select 4 hours from the drop-down list of **Timing**. Your computer will be prioritized for the next 4 hours.



Done!

You can now enjoy playing games without lag on your computer for the next 4 hours.

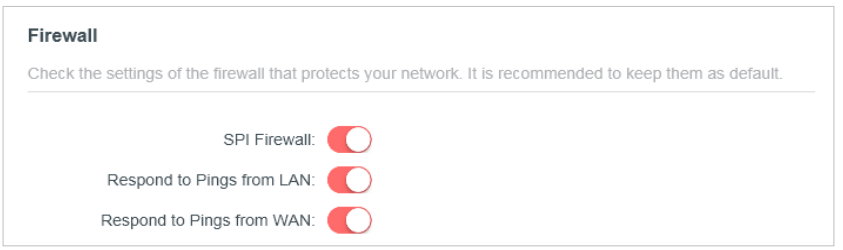
4.7 Security

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

4. 7. 1 Firewall

The SPI (Stateful Packet Inspection) Firewall protects the router from cyber attacks and validate the traffic that is passing through the router based on the protocol. This function is enabled by default.

1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced** > **Security** > **Firewall**, and configure the parameters as you need. It's recommended to keep the default settings.



4. 7. 2 Access Control

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

I want to:

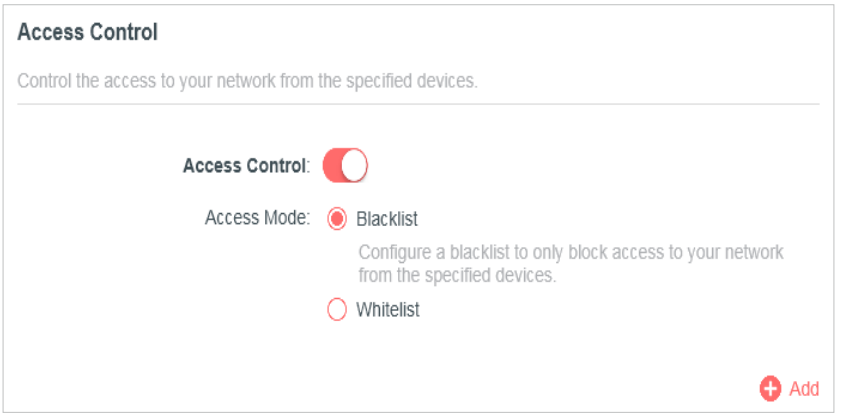
Block or allow specific client devices to access my network (via wired or wireless).

How can I do that?

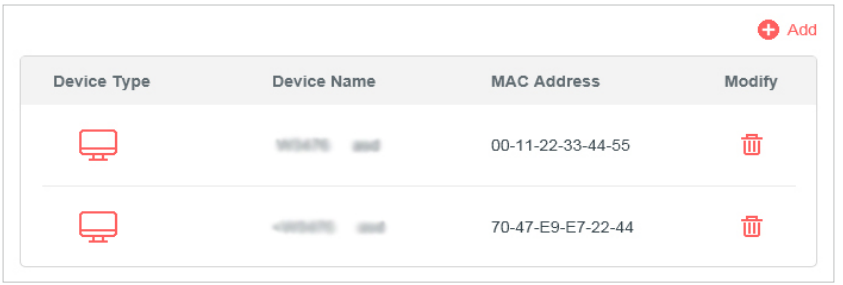
1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced** > **Security** > **Access Control**.
3. Select the access mode to either block (recommended) or allow the device(s) in the list.

   To block specific device(s):

   1) Select **Blacklist** and click **SAVE**.

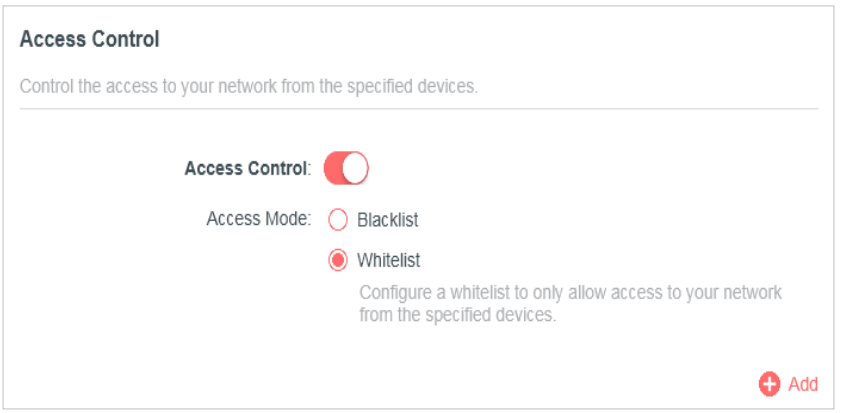


2) Click **Add** and select devices you want to be blocked. You can see the devices have been added to the blacklist.



To allow specific device(s):

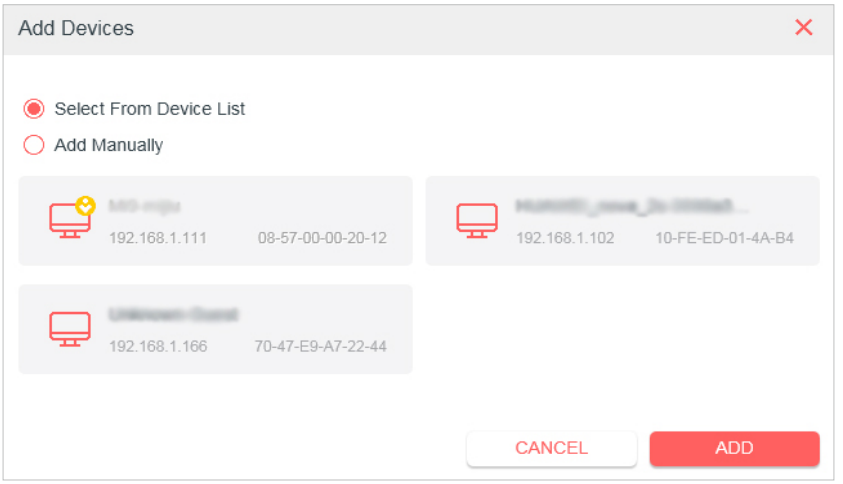
1) Select **Whitelist** and click **SAVE**.



2) Add devices to the whitelist.

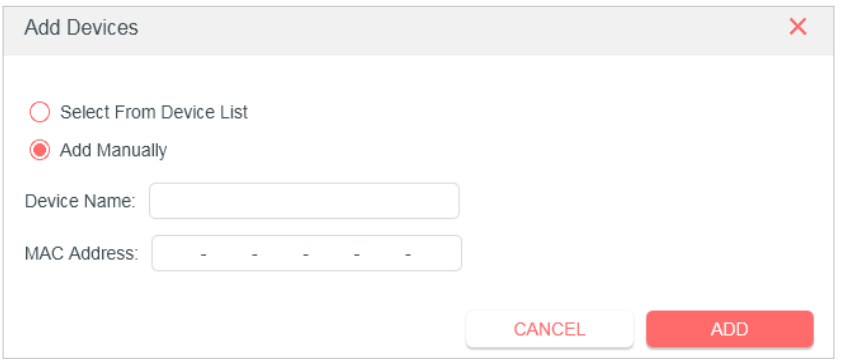
- **Add connected devices**

Click **Select From Device List** and select the devices you want to be allowed.



- **Add unconnected devices**

Click **Add Manually** and enter the **Device Name** and **MAC Address** of the device you want to be allowed.



Done!

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

4. 7. 3 IP & MAC Binding

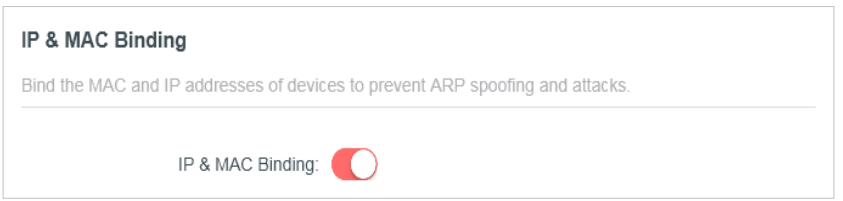
IP & MAC Binding, namely, ARP (Address Resolution Protocol) Binding, is used to bind network device's IP address to its MAC address. This will prevent ARP Spoofing and other ARP attacks by denying network access to a device with matching IP address in the Binding list, but unrecognized MAC address.

I want to:

Prevent ARP spoofing and ARP attacks.

How can I do that?

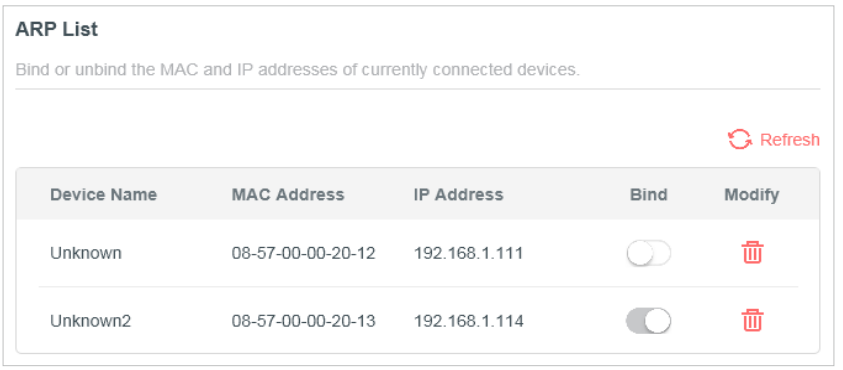
1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced** > **Security** > **IP & MAC Binding**.
3. Enable **IP & MAC Binding** and click **SAVE**.



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

To bind the connected device(s):

Locate the **ARP List** section and enable Bind to bind the IP and MAC addresses of a specific device.

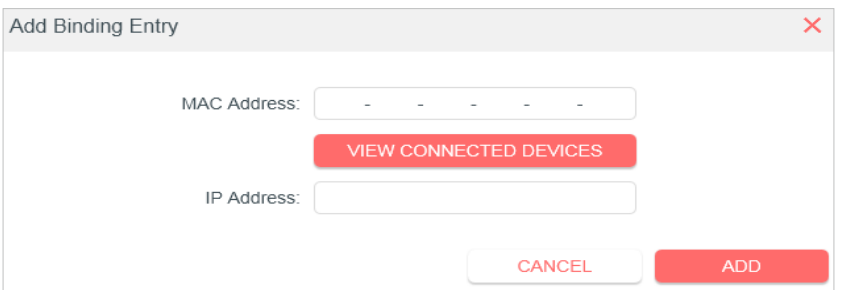


To add a binding entry:

1) Click **Add** in the **Binding List** section.

2) Click **VIEW CONNECTED DEVICES** and select the device you want to bind. Or enter the **MAC Address** and **IP Address** that you want to bind.

3) Click **ADD**.



4. 7. 4 ALG

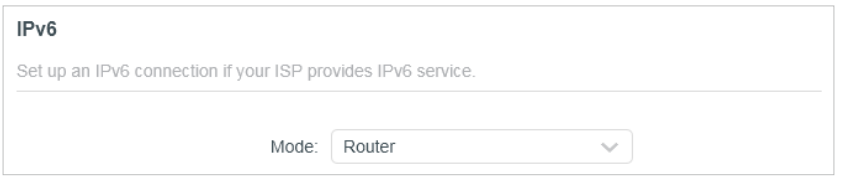
Check the ALG (Application Layer Gateway) settings. It is recommended to keep them as default.

4.8 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).

1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced** > **IPv6**, and you can view the current IPv6 status information of the router.
3. Enable **IPv6** and select the mode: **Router** or **Pass-Through (Bridge)**.

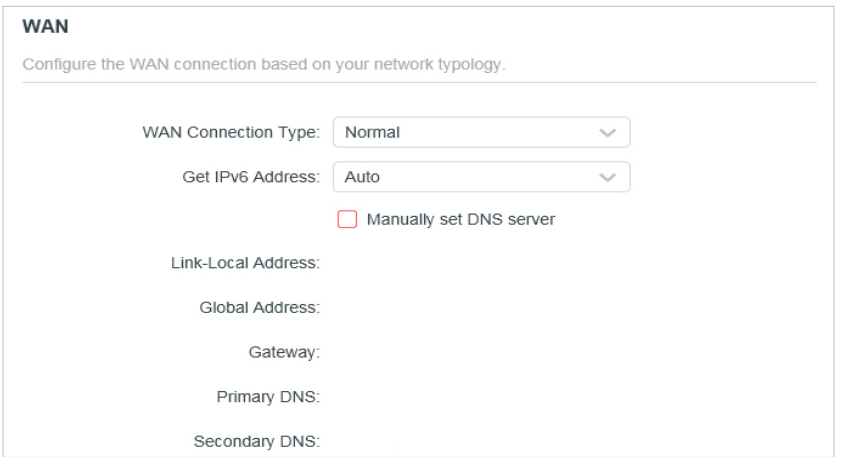
- **If you select Router:**



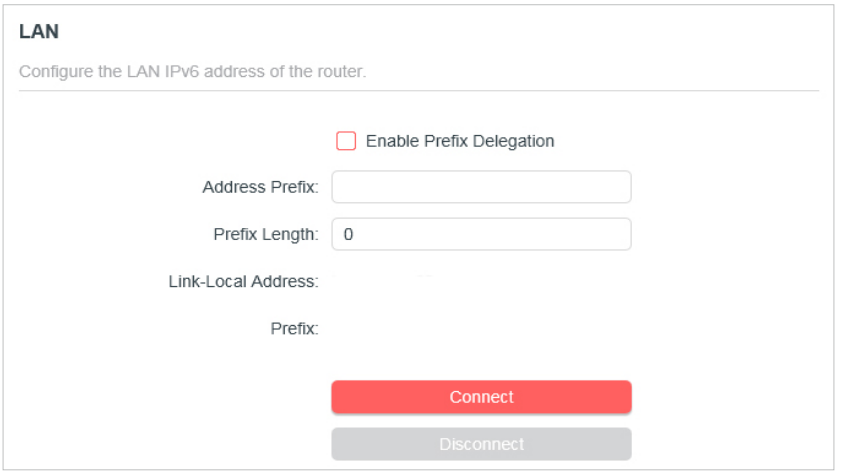
Fill in WAN and LAN information as required by different connection types.

- **Normal**: The default connection type.

1) Configure the WAN settings.



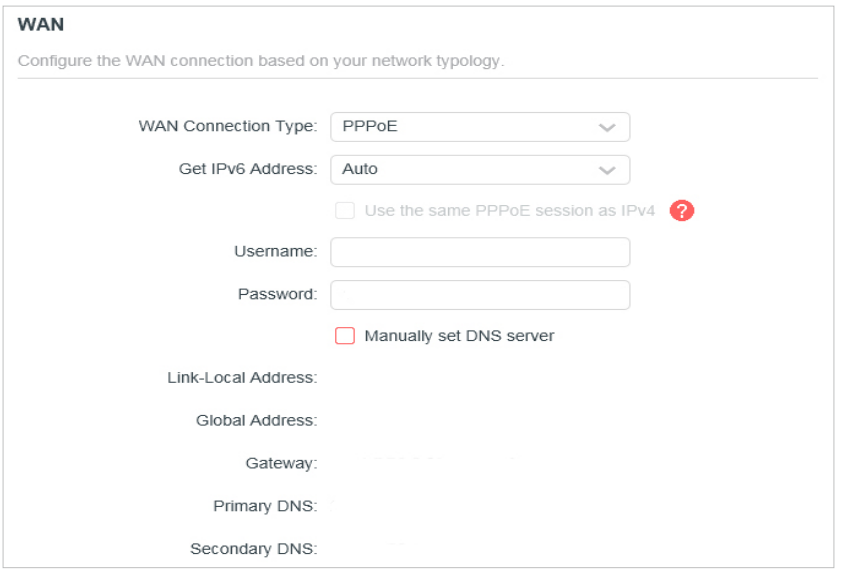
2) Configure the LAN settings. Fill in **Address Prefix** provided by your ISP.



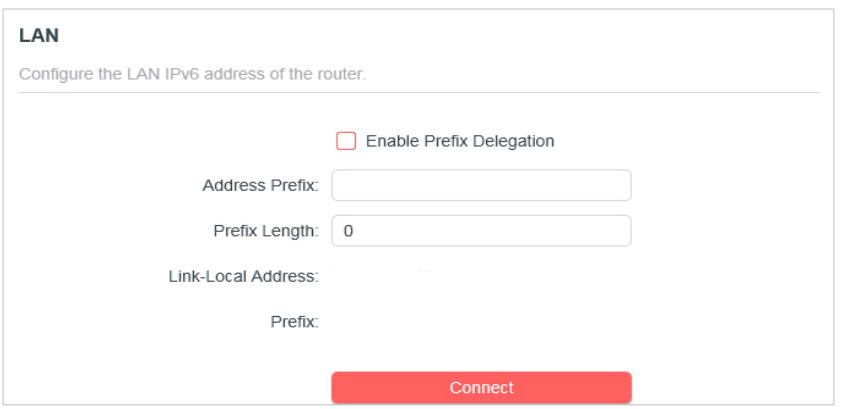
3) Click **SAVE**.

- **PPPoE**: Select this type if your ISP uses PPPoEv6, and provides a username and password.

1) Configure the WAN settings.

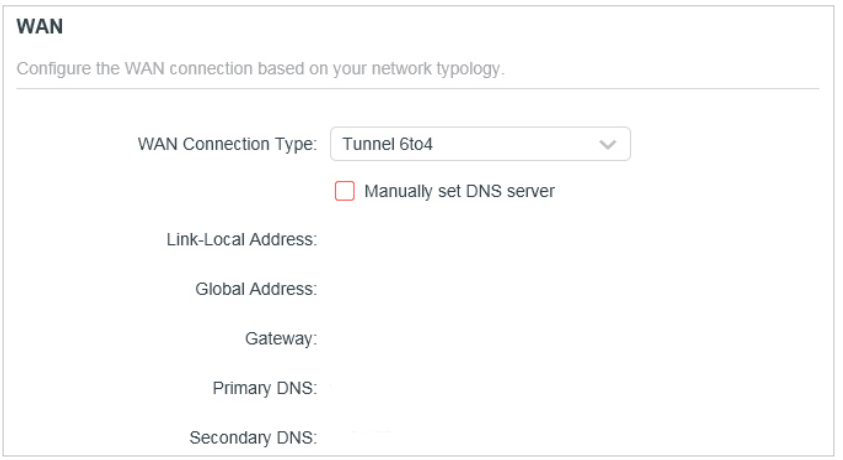


2) Configure the LAN settings. Fill in Address Prefix provided by your ISP.

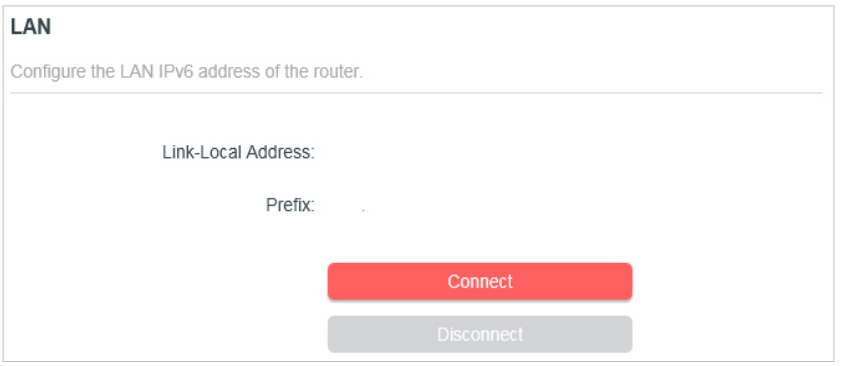


- **Tunnel 6to4**: Select this type if your ISP uses 6 to 4 deployment fort assigning address.

1) Configure the WAN settings.

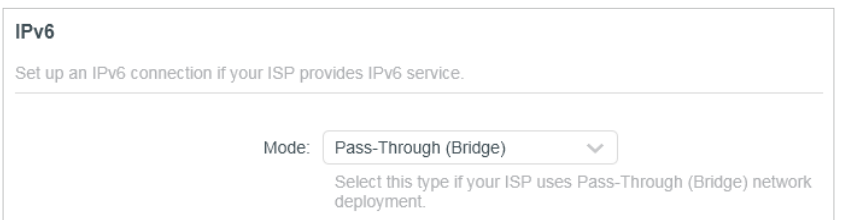


2) Configure the LAN settings.



- **If you select Pass-Through (Bridge):**

Click **SAVE**. No configuration is required.

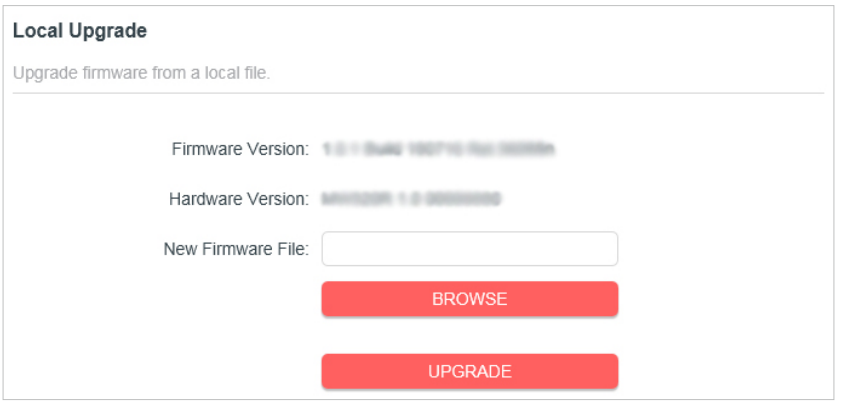


4.9 System

4. 9. 1 Firmware Upgrade

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

1. Download the latest firmware file for the router from **www.mercusys.com**.
2. Visit **http://mwlogin.net**, and log in with the password you set for the router.
3. Go to **Advanced** > **System** > **Firmware Upgrade**.
4. Click **BROWSE** to locate the downloaded firmware file, and click **UPGRADE**.



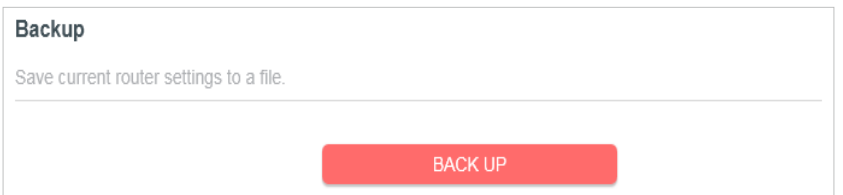
4. 9. 2 Backup & Restore

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://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced** > **System** > **Backup & Restore**.

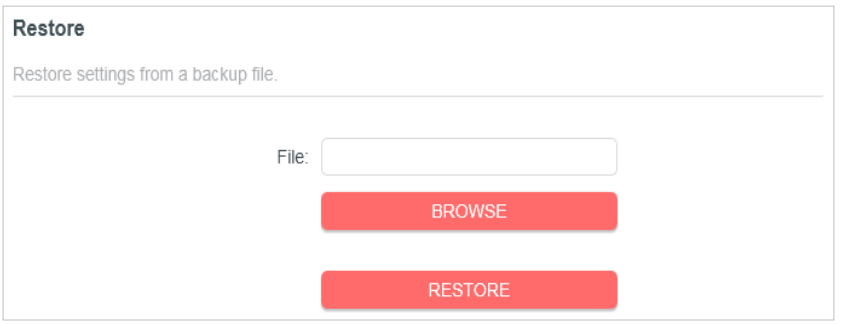
To backup configuration settings:

Click **BACK UP** 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.



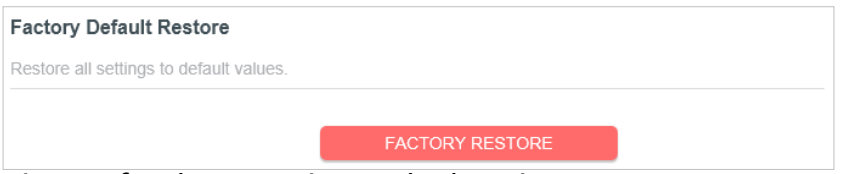
To restore configuration settings:

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



To reset the router to factory default settings:

1. Click **FACTORY RESTORE** to reset the router.



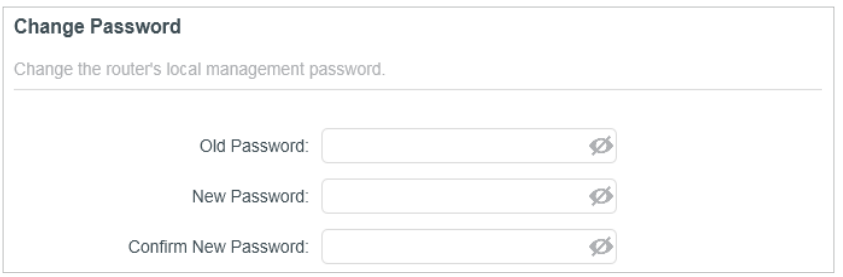
2. Wait a few minutes for the restoring and rebooting.

Note:

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

4. 9. 3 Change Password

1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced** > **System** > **Administration**, and focus on the Change Password section.



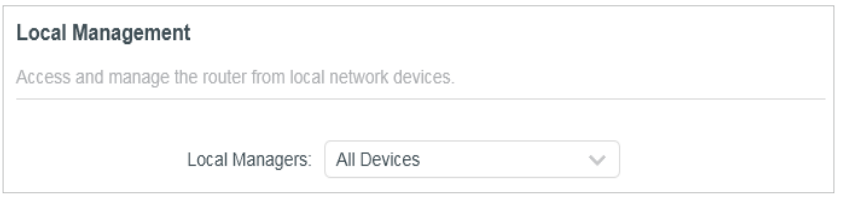
3. Enter the old password, then a new password twice (both case-sensitive). Click **SAVE**.
4. Use the new password for future logins.

4. 9. 4 Local Management

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

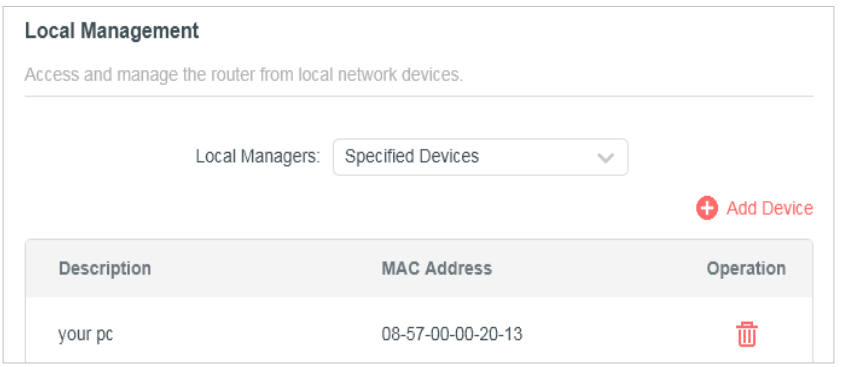
- **Allow all LAN connected devices to manage the router:**

Select **All Devices** for Local Managers.

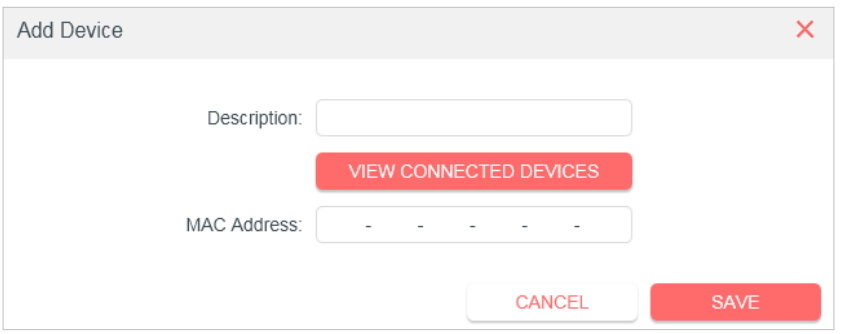


- **Allow specific devices to manage the router:**

1. Select **Specified Devices** for Local Managers and click **SAVE**.



2. Click **Add Device**.



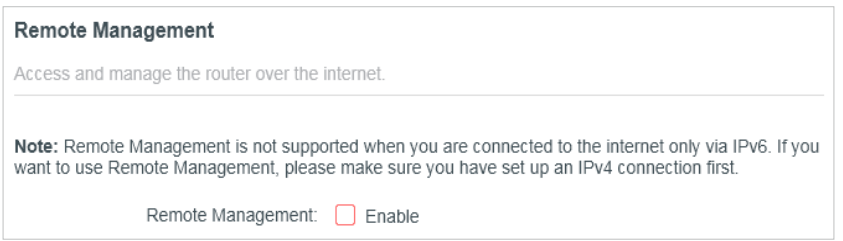
3. Click **VIEW CONNECTED DEVICES** and select the device to manage the router from the Connected Devices list, or enter the **MAC address** of the device manually.
4. Specify a **Description** for this entry.
5. Click **SAVE**.

4. 9. 5 Remote Management

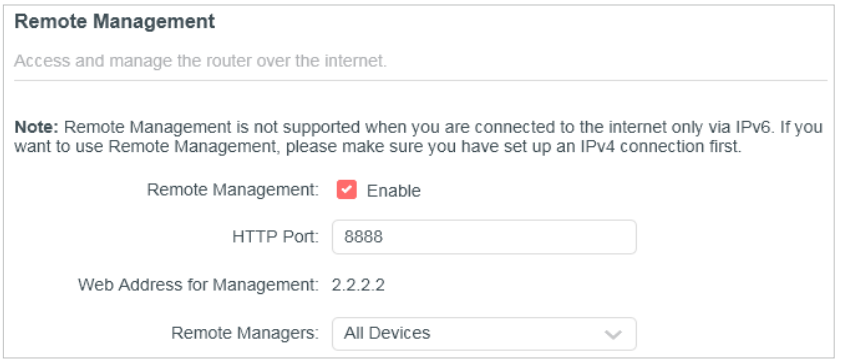
1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced** > **System** > **Administration**, and focus on the Remote Management section.

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

Do not tick the **Enable** checkbox of **Remote Management**.



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



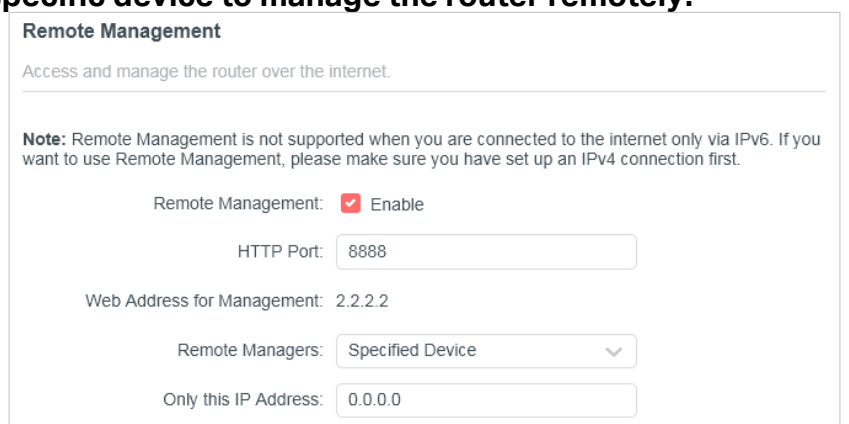
1. Tick the **Enable** checkbox of **Remote Management**.
2. Keep the HTTP port as default setting (recommended) or enter a value between 1024 and 65535.
3. Select **All Devices** for **Remote Managers**.
4. Click **SAVE**.

Devices on the internet can log in to **http://Router's WAN IP address:port number** (such as **http://113.116.60.229:1024**) to manage the router.

Tips:

- You can find the WAN IP address of the router on **Network Map** > **Internet**.
- The router's WAN IP is usually a dynamic IP. Please refer to **Dynamic DNS** if you want to log in to the router through a domain name.

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



1. Tick the **Enable** checkbox of **Remote Management**.

2. Keep the HTTP port as default setting (recommended) or enter a value between 1024 and 65535.
3. Select **Specified Device** for **Remote Managers**.
4. In the Only this IP Address field, enter the IP address of the remote device to manage the router.
5. Click **SAVE**.

Devices using this WAN IP can manage the router by logging in to **http://Router's WAN IP:port number** (such as **http://113.116.60.229:1024**).

Tips: The router's WAN IP is usually a dynamic IP. Please refer to **Dynamic DNS** if you want to log in to the router through a domain name.

4. 9. 6 HTTP Referer Head Check

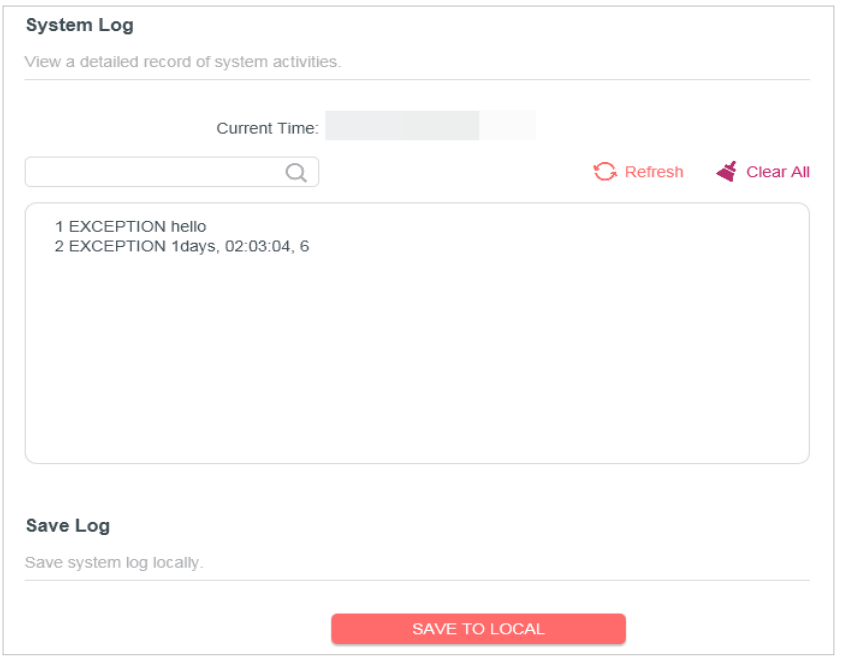
HTTP referer header check function can protect your networks against CSRF(Cross-Site Request Forgery) attacks. This function is enabled by default. You can disable this function if needed.

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

4.10 System Log

4. 10. 1 System Log

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

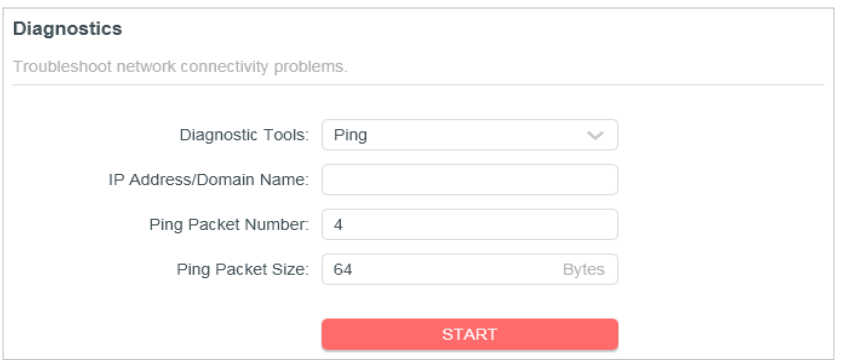


3. Click **SAVE TO LOCAL** to save the system logs to a local disk.

4. 10. 2 Diagnostics

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

1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced** > **System** > **Diagnostics**.



3. Enter the information:

1) Choose **Ping** or **Tracert** as the diagnostic tool to test the connectivity.

- **Ping** is used to test the connectivity between the router and the tested host, and measure the round-trip time.

- **Tracert** is used to display the route (path) your router has passed to reach the tested host, and measure transit delays of packets across an Internet Protocol network.

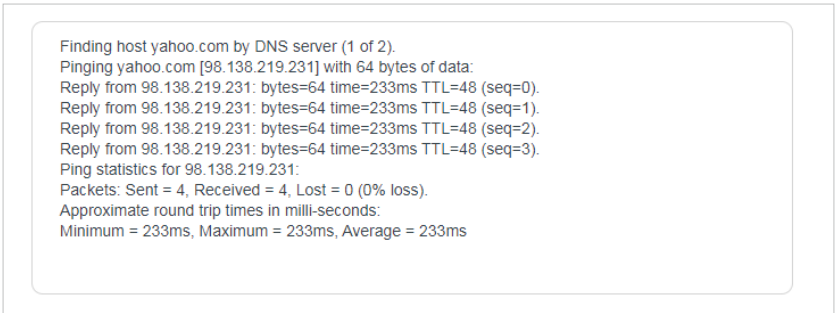
2) Enter the **IP Address** or **Domain Name** of the tested host.

3) Modify the **Ping Count** number and the **Ping Packet Size**. It's recommended to keep the default value.

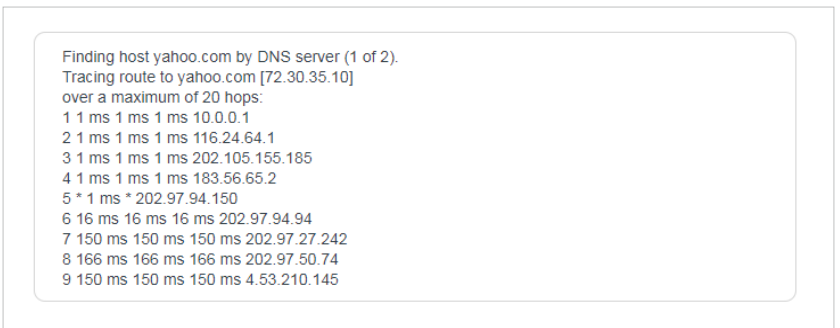
4) If you have chosen **Tracert**, you can modify the **Traceroute Max TTL**. It's recommended to keep the default value.

4. Click **START** to begin the diagnostics.

The figure below indicates the proper connection between the router and the Yahoo server (www.Yahoo.com) tested through **Ping**.



The figure below indicates the proper connection between the router and the Yahoo server (www.Yahoo.com) tested through **Tracert**.



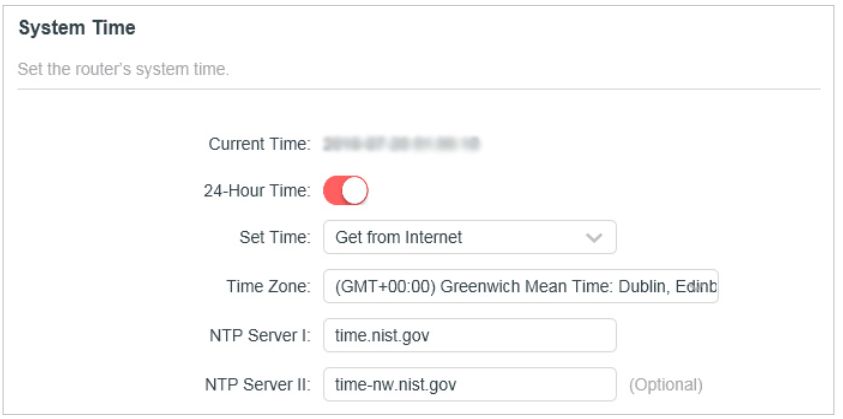
4. 10. 3 Time

This function 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://mwlogin.net**, and log in with the password you set for the router.

2. Go to **Advanced** > **System** > **Time**.

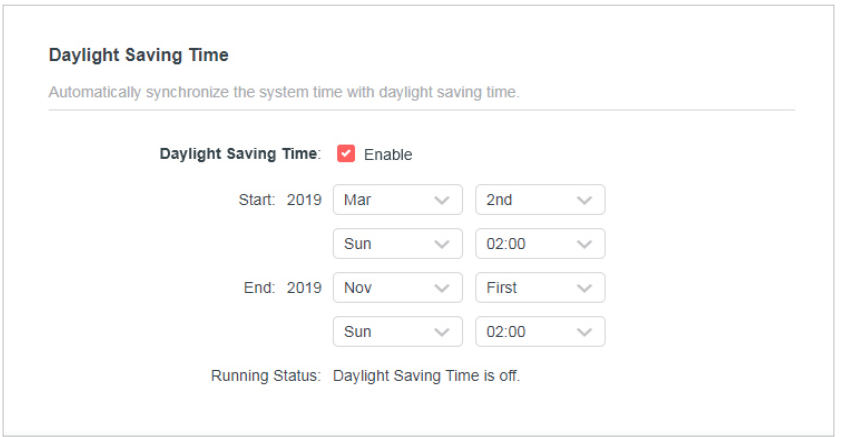
- **To set System Time:**



1. Select the way in which the router gets its time: **Get from Internet**, **Get from Managing Device**, **Manually**.
2. Select your local **Time Zone**.
3. Enter the address or domain of the **NTP Server 1** or **NTP Server 2**.
4. Click **SAVE**.

- **To set up Daylight Saving Time:**

1. Tick the **Enable** box of **Daylight Saving Time**.



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. 10. 4 Reboot

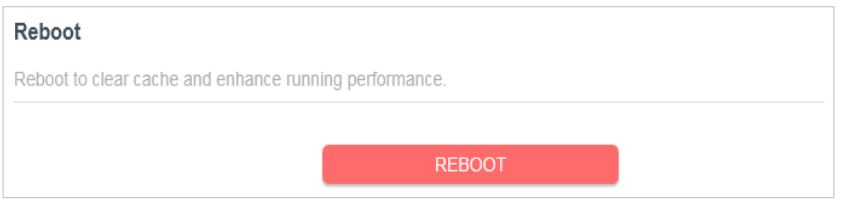
Some settings of the router will take effect only after rebooting, and the system will

reboot automatically. You can also reboot the router to clear cache and enhance running performance.

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

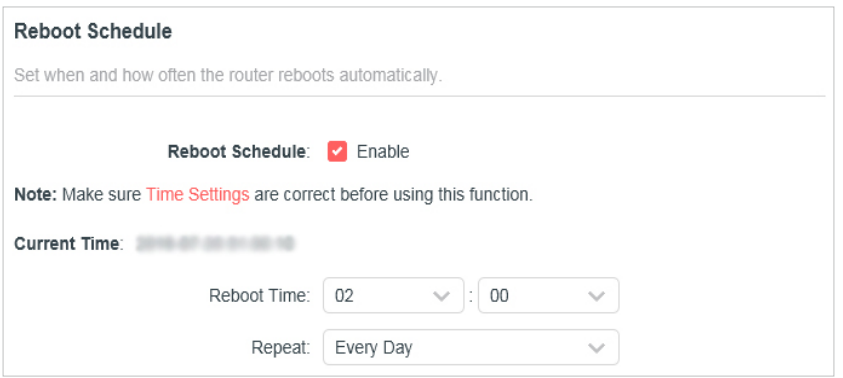
- **To reboot the router manually:**

Click **REBOOT**, and wait a few minutes for the router to reboot.



- **To set the router to reboot regularly:**

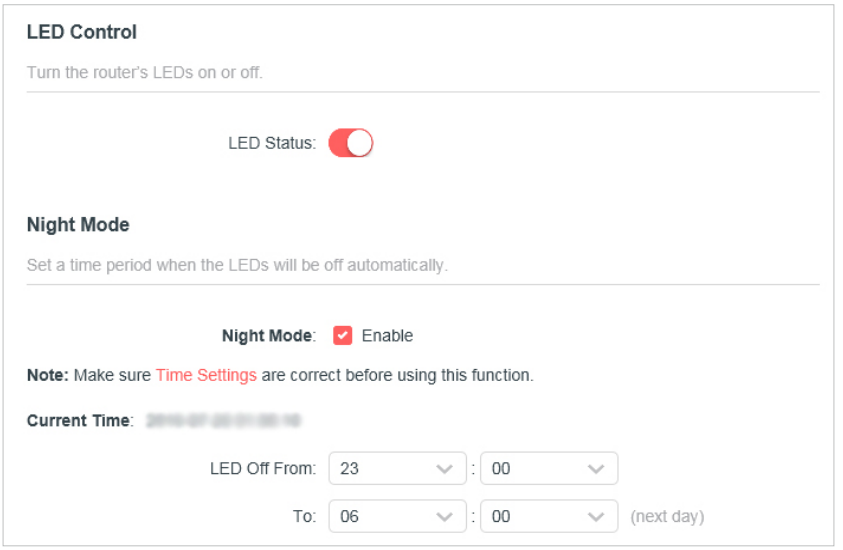
1. Tick the **Enable** box of **Reboot Schedule**.
2. Specify the **Reboot Time** when the router reboots and **Repeat** to decide how often it reboots.
3. Click **SAVE**.



4. 10. 5 LED Control

The LED of the router indicates its activities and status. You can enable the **Night Mode** feature to specify a time period during which the LED is off.

1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **Advanced** > **System** > **LED Control**.
3. Enable **Night Mode**.



4. Specify the LED off time, and the LED will be off during this period every day.

Note: The effective LED off time is based on the time of the router. You can go to **Advanced** > **System** > **Time** to modify the time.

5. Click **SAVE**.

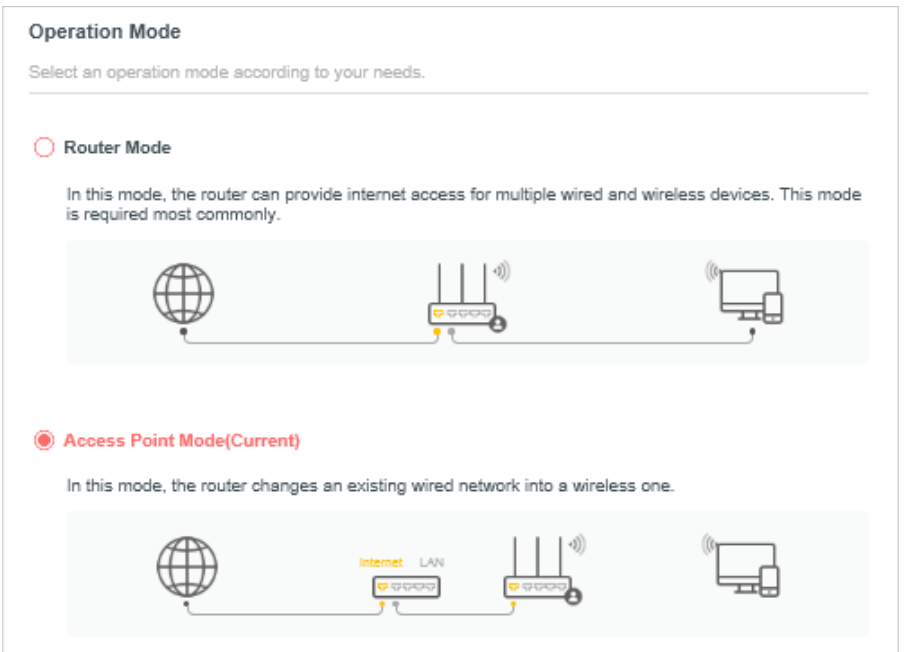
Chapter 5 Access Point Mode

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

It contains the following sections:

5.1 Operation Mode

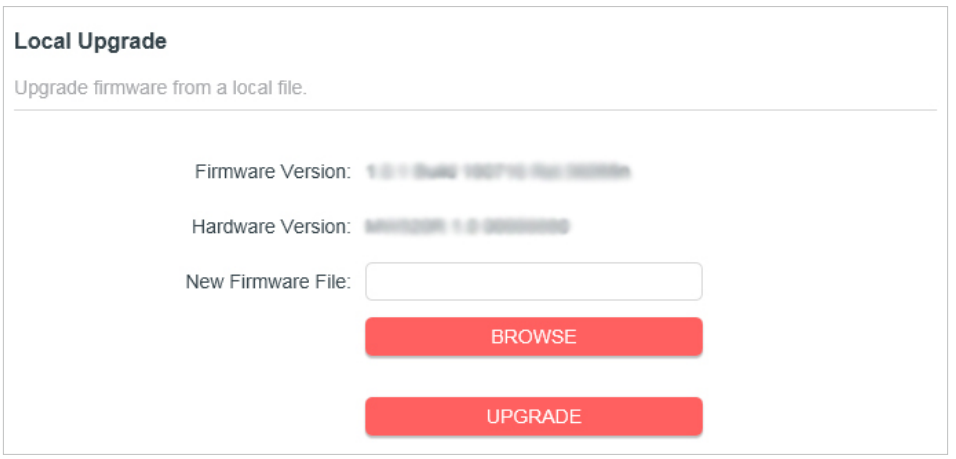
1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **System** > **Operation Mode**.
3. Select the working mode as needed and click **SAVE**.



5.2 Firmware Upgrade

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

1. Download the latest firmware file for the router from our website **www.mercusys.com**.
2. Visit **http://mwlogin.net**, and log in with the password you set for the router.
3. Go to **System** > **Firmware Upgrade**.
4. Click **BROWSE** to locate the downloaded firmware file, and click **UPGRADE**.



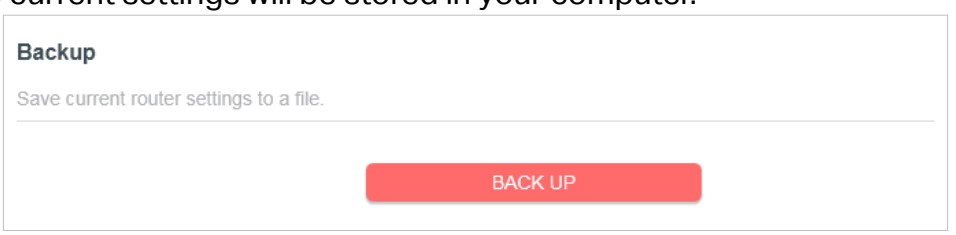
5.3 Backup & Restore

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://mwlogin.net**, and log in with the password you set for the router.
2. Go to **System** > **Backup & Restore**.

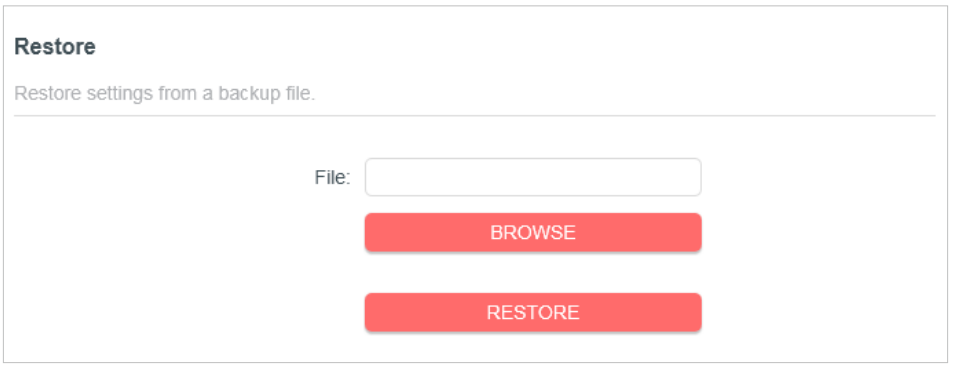
To backup configuration settings:

Click **BACK UP** 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.



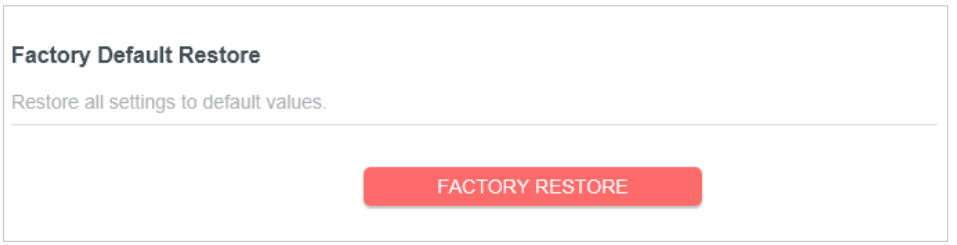
To restore configuration settings:

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



To reset the router to factory default settings:

1. Click **FACTORY RESTORE** to reset the router.



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

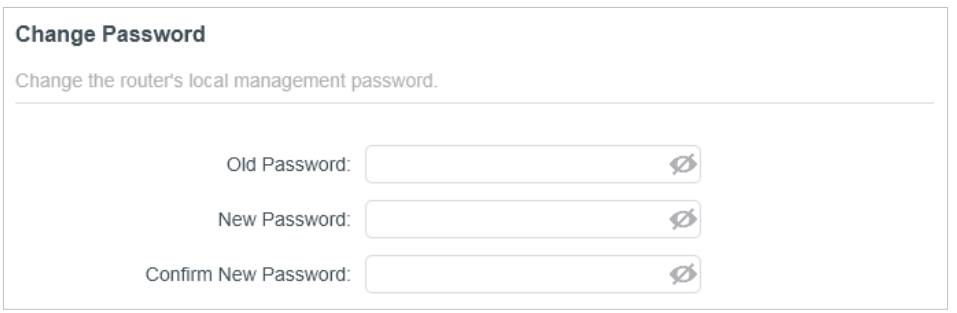
Note:

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

5.4 Administration

5. 4. 1 Change Password

1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **System** > **Administration**, and focus on the Change Password section.



3. Enter the old password, then a new password twice (both case-sensitive). Click **SAVE**.

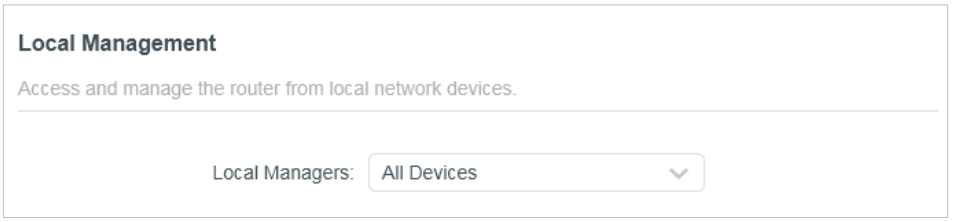
4. Use the new password for future logins.

5. 4. 2 Local Management

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

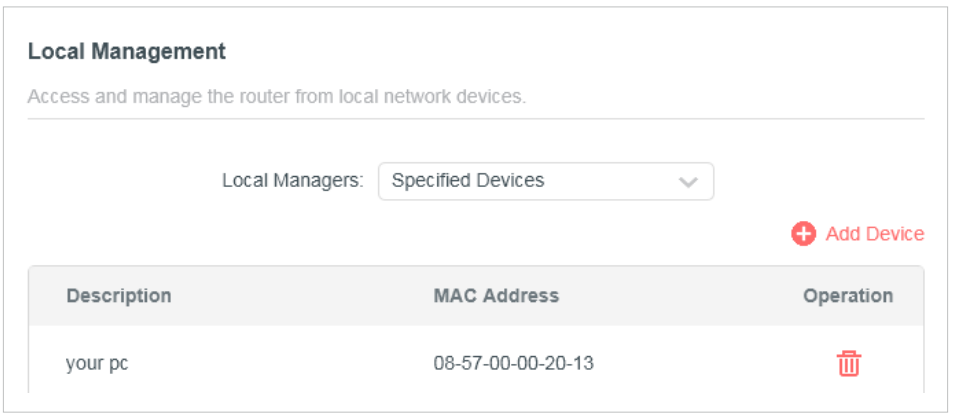
- **Allow all LAN connected devices to manage the router:**

Select **All Devices** for Local Managers.

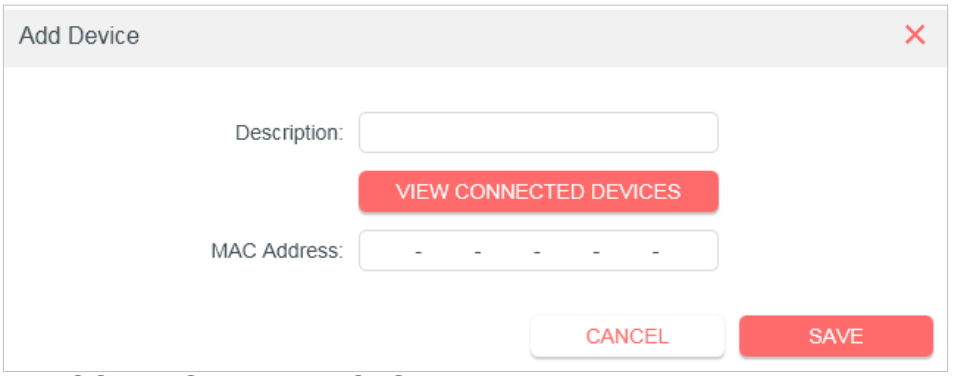


- **Allow specific devices to manage the router:**

1. Select **Specified Devices** for Local Managers and click **SAVE**.



2. Click **Add Device**.



3. Click **VIEW CONNECTED DEVICES** and select the device to manage the router from the Connected Devices list, or enter the **MAC address** of the device manually.
4. Specify a **Description** for this entry.

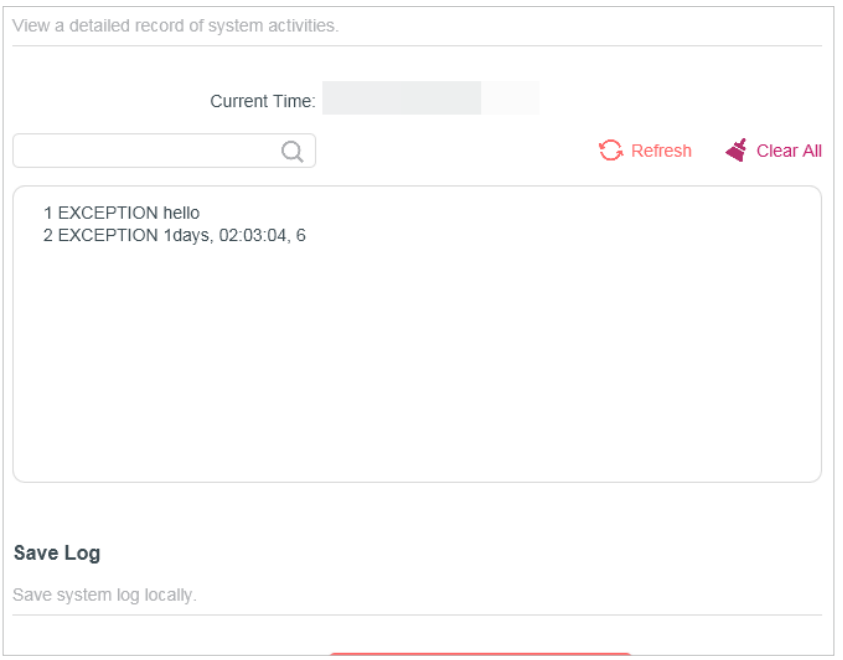
5. Click **SAVE**.

5. 4. 3 HTTP Referer Head Check

HTTP referer header check function can protect your networks against CSRF(Cross-Site Request Forgery) attacks. This function is enabled by default. You can disable this function if needed.

5.5 System Log

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

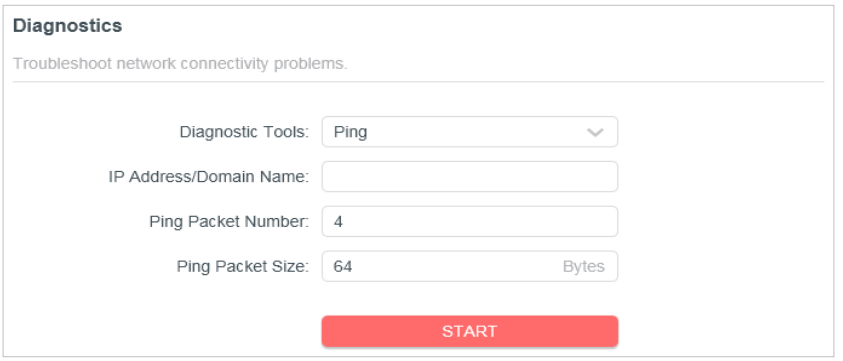


3. Click **SAVE TO LOCAL** to save the system logs to a local disk.

5.6 Diagnostics

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

1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **System** > **Diagnostics**.



3. Enter the information:

1) Choose **Ping** or **Tracert** as the diagnostic tool to test the connectivity.

- **Ping** is used to test the connectivity between the router and the tested host, and measure the round-trip time.
- **Tracert** is used to display the route (path) your router has passed to reach the tested host, and measure transit delays of packets across an Internet Protocol network.

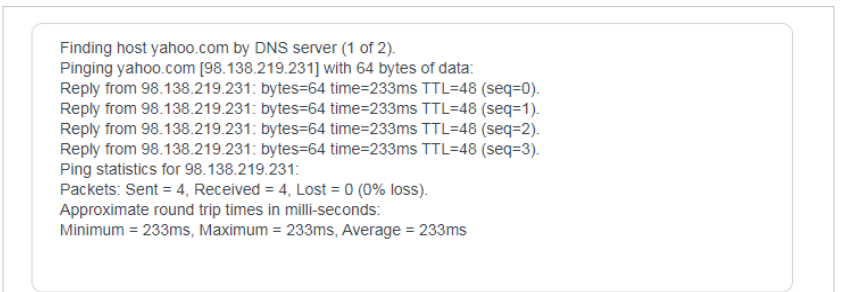
2) Enter the **IP Address** or **Domain Name** of the tested host.

3) Modify the **Ping Count** number and the **Ping Packet Size**. It's recommended to keep the default value.

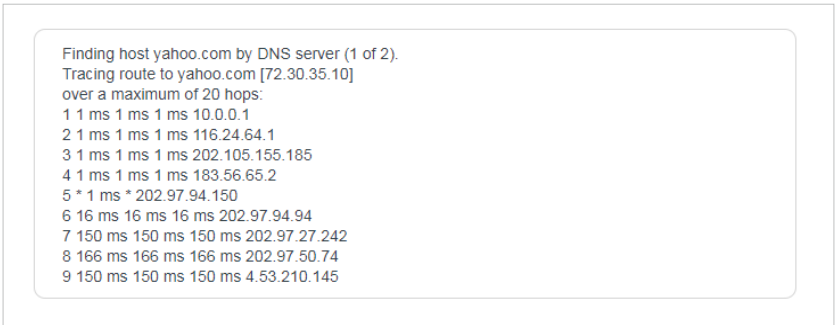
4) If you have chosen **Tracert**, you can modify the **Traceroute Max TTL**. It's recommended to keep the default value.

4. Click **START** to begin the diagnostics.

The figure below indicates the proper connection between the router and the Yahoo server (www.Yahoo.com) tested through **Ping**.



The figure below indicates the proper connection between the router and the Yahoo server (www.Yahoo.com) tested through **Tracert**.

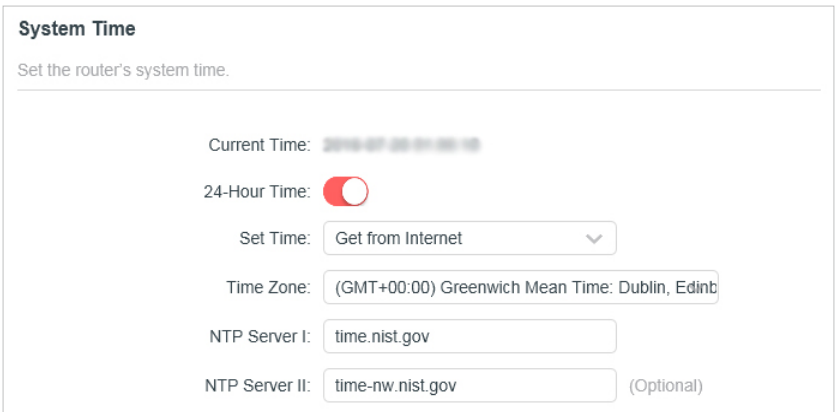


5.7 Time

This function 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://mwlogin.net**, and log in with the password you set for the router.
2. Go to **System** > **Time**.

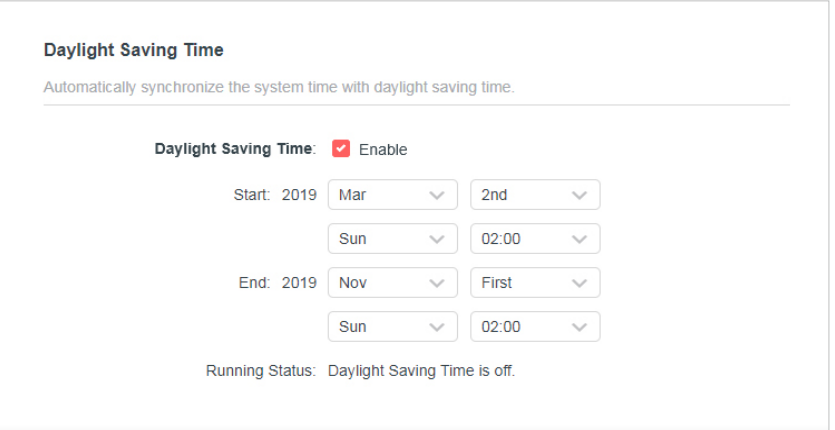
- **To set System Time:**



1. Select the way in which the router gets its time: **Get from Internet**, **Get from Managing Device**, **Manually**.
2. Select your local **Time Zone**.
3. Enter the address or domain of the **NTP Server 1** or **NTP Server 2**.
4. Click **SAVE**.

- **To set up Daylight Saving Time:**

1. Tick the **Enable** box of **Daylight Saving Time**.



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.

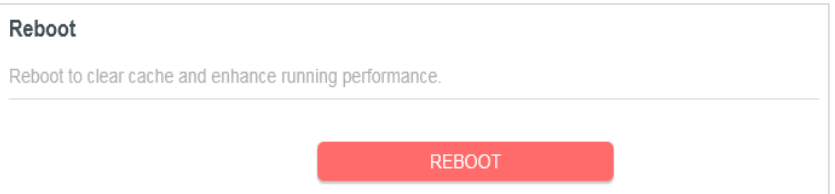
5.8 Reboot

Some settings of the router will take effect only after rebooting, and the system will reboot automatically. You can also reboot the router to clear cache and enhance running performance.

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

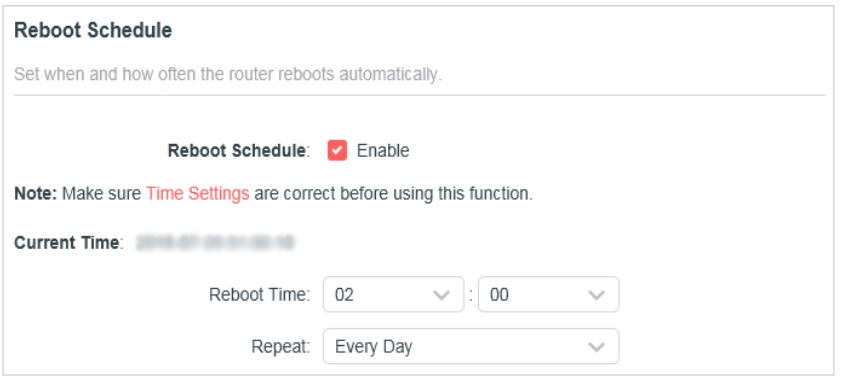
- **To reboot the router manually:**

Click **REBOOT**, and wait a few minutes for the router to reboot.



- **To set the router to reboot regularly:**

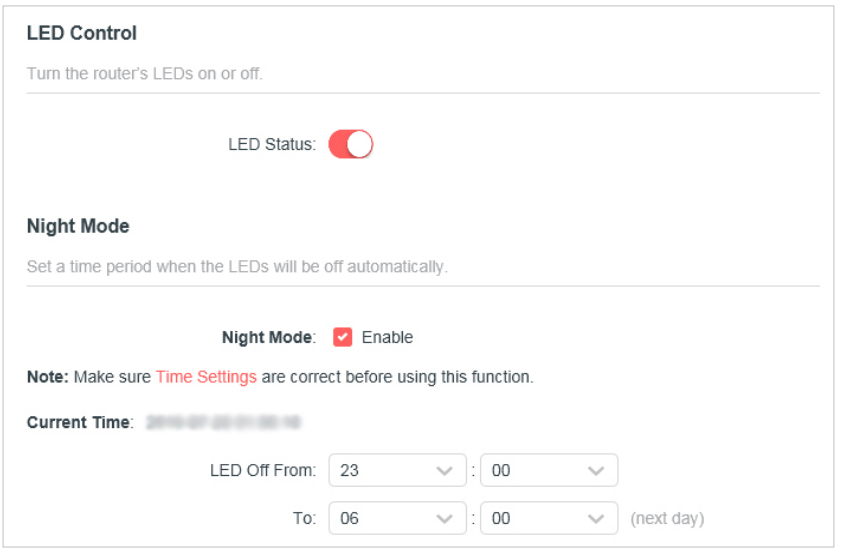
1. Tick the **Enable** box of **Reboot Schedule**.
2. Specify the **Reboot Time** when the router reboots and **Repeat** to decide how often it reboots.
3. Click **SAVE**.



5.9 LED Control

The LED of the router indicates its activities and status. You can enable the **Night Mode** feature to specify a time period during which the LED is off.

1. Visit **http://mwlogin.net**, and log in with the password you set for the router.
2. Go to **System** > **LED Control**.
3. Enable **Night Mode**.



4. Specify the LED off time, and the LED will be off during this period every day.

Note: The effective LED off time is based on the time of the router. You can go to **Advanced** > **System** > **Time** to modify the time.

5. Click **SAVE**.

Appendix A: FAQ (Frequently Asked Questions)

Q1. What can I do if the login window does not appear?

- Reboot your main router and try again.
- If the computer is set to a static IP address, change its settings to obtain an IP address automatically.
- Make sure you are accessing the web management through wireless connection.
- Verify that **http://mwlogin.net** is correctly entered in the web browser.
- Use another web browser and try again.
- Disable and enable the network adapter in use again.

Q2. What can I do if I cannot access the internet?

- Reboot your modem and main router, then try again.
- Check if the internet is working properly by connecting a computer directly to the modem via an Ethernet cable. If it is not, contact your internet service provider.
- Open a web browser, enter **http://mwlogin.net** and run the Quick Setup again.
- For cable modem users, reboot the modem first. If the problem still exists, log in to the web management page of the router to clone MAC address.

Q3. How do I restore the router to its factory default settings?

- With the router powered on, press and hold the **Reset** button on the router until there is an obvious change of the LEDs, and then release the button.
- Log in to the web management page and go to **Advanced > System tools > Factory Defaults** to restore the router to factory settings.

  NOTE:

  Once the modem router is reset, the current configuration settings will be lost and you will need to re-configure the router.

Q4. What can I do if I forgot my web management password?

Refer to FAQ >Q3 to reset the router, and then create a password for future logins.

Q5. What can I do if I forgot my wireless network password?

- By default, the wireless network has no password.
- If you have set a password for the wireless network, log in to the web management page of the router to retrieve or reset your password.

Q6. What can I do if I want to change the main router?

- Log in to **http://mwlogin.net** and go to Status.

- Choose the device you prefer and click Set as main router.
- Follow web instructions to finish the procedure.

Q7. What can I do if I want to add new Halo devices to existed mesh system?

- Log in to **http://mwlogin.net** and go to **Status > Add Device**.
- Follow web instructions to add the device to mesh network through pairing.

Q8. What if I want to add successfully-paired Halo devices to another mesh network?

- Refer to FAQ >Q3 to reset the devices.
- Log in to the web management page of the main router in mesh and go to **Status > Add Device**.
- Follow web instructions to add devices to mesh network through pairing.

Appendix B: Configuring the PC

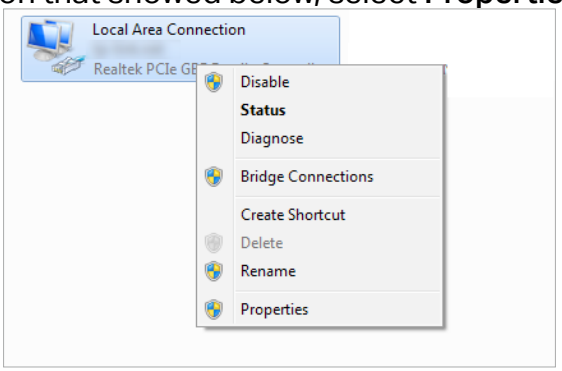
In this section, we'll introduce how to install and configure the TCP/IP correctly in Windows 7. First make sure your Ethernet Adapter is working, refer to the adapter's manual if needed.

1. **Install TCP/IP component**

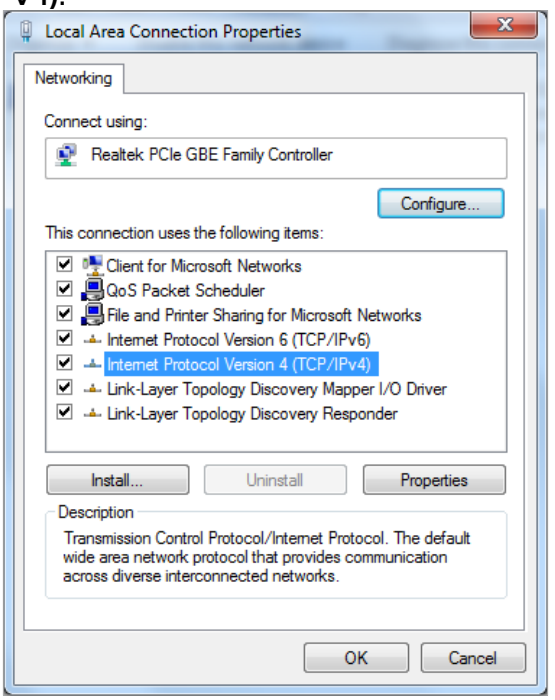
   a. On the Windows taskbar, click **Start** button, and then click **Control Panel**.

   b. Click the **Network and Internet**, and click the **Network and Sharing Center**, then click **Change adapter settings**.

   c. Right click the icon that showed below, select **Properties** on the prompt page.



   d. In the prompt page that showed below, double click on the **Internet Protocol Version 4 (TCP/IPv4)**.



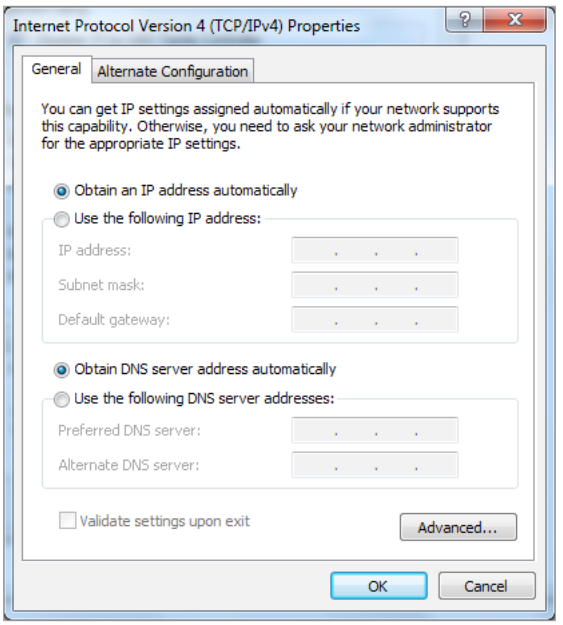
   e. The following **TCP/IP Properties** window will display and the **IP Address** tab is open on this window by default.

2. Configure the TCP/IP protocol

Now you have two ways to configure the **TCP/IP** protocol below:

- **Setting IP address automatically**

Select **Obtain an IP address automatically**, Choose **Obtain DNS server automatically**, as shown in the Figure below:



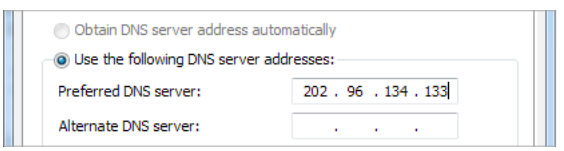
- Setting IP address manually

a. Select **Use the following IP address** radio button. And the following items available.

b. If the router's LAN IP address is 192.168.1.1, specify the IP address as 192.168.1.x (x is from 2 to 254), and **Subnet mask** is 255.255.255.0.

c. Enter the router's LAN IP address (the default IP is 192.168.1.1) in the **Default gateway** field.

d. Select **Use the following DNS server addresses** radio button. In the **Preferred DNS Server** field you can type the DNS server IP address, which has been provided by your ISP.



User Guide

300Mbps Wireless N Router
TL-WR850N

REV1.0.0 1910020829

Contents

About This Guide

This guide is a complement to Quick Installation Guide. The Quick Installation Guide provides instructions for quick Internet setup, while this guide contains details of each function and demonstrates how to configure them.

When using this guide, please notice that features of the router may vary slightly depending on the model and software version you have, and on your location, language, and Internet service provider. All screenshots, images, parameters and descriptions documented in this guide are used for demonstration only.

Conventions

In this guide the following conventions are used:

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

More Info

The latest software, management app and utility are available from the Download Center at www.tp-link.com/support.

The Quick Installation Guide can be found where you find this guide or inside the package of the router.

Specifications can be found on the product page at http://www.tp-link.com.

A Technical Support Forum is provided for you to discuss our products at http://forum.tp-link.com.

Our Technical Support contact information can be found at the Contact Technical Support page at www.tp-link.com/support.

Chapter 1

Get to Know About Your Router

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

It contains the following sections:

1. 1. Product Overview

The TP-Link router is designed to fully meet the need of Small Office/Home Office (SOHO) networks and users demanding higher networking performance. The powerful antennas ensure continuous Wi-Fi signal to all your devices while boosting widespread coverage throughout your home, and the built-in Ethernet ports supply high-speed connection to your wired devices.

Moreover, it is simple and convenient to set up and use the TP-Link router due to its intuitive web interface.

1. 2. Panel Layout

1. 2. 1. Top View

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

LED Explanation

Name	Status	Indication
(Power)	On	System initialization completes.
	Flashing	System initialization or firmware upgrade is in progress. Do not disconnect or power off the router.
	Off	Power is off.
(Wireless)	On	The wireless function is working properly.
	Off	The wireless function is disabled.
(Ethernet)	On	One of LAN ports is connected.
	Off	No LAN port is connected.
(Internet)	Blue On	The Internet is available.
	Orange On	The router's WAN port is connected, but the Internet is not available.
	Off	The router's WAN port is not connected.
(WPS)	On/Off	Turns on when WPS connection is established, and goes off about 5 minutes later.
	Flashing	A wireless device is trying to connect to the network via WPS. This process may take up to 2 minutes.

1. 2. 2. The Back Panel

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

Item	Description
Power Port	For connecting the router to a power socket via the provided power adapter.
WAN Port	For connecting to a DSL/Cable modem, or an Ethernet port.
Ethernet Ports (1/2/3/4)	For connecting your PCs or other wired network devices to the router.
WPS/Reset Button	Press and hold this button until all the LED turn on momentarily to reset the router to its factory default settings.
	To enable the WPS function, press this button about 2 seconds. If you have a WPS-supported device, you can press this button to quickly establish connection between the router and the client device and automatically configure wireless security for your wireless network.
Antennas	Used for wireless operation and data transmitting. Upright them for the best Wi-Fi performance.

Chapter 2

Connect to the Internet

This chapter contains the following sections:

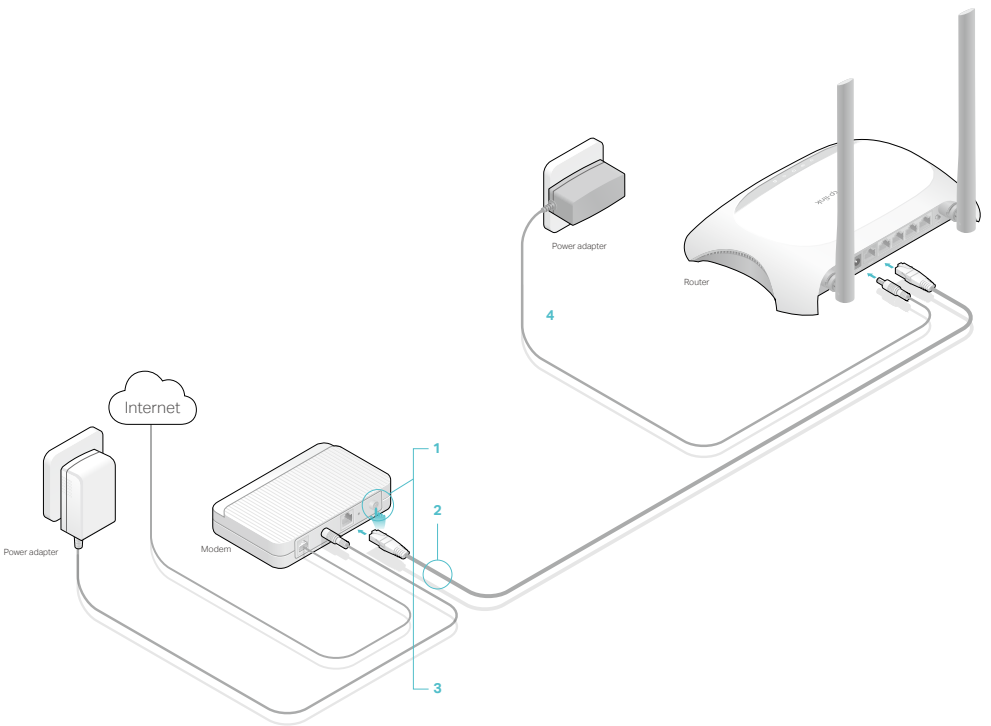
2. 1. Position Your Router

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

2. 2. Connect to the Internet

Follow the steps below to connect your router.

If your Internet connection is through an Ethernet cable from the wall instead of through a DSL / Cable / Satellite modem, connect the Ethernet cable directly to the router's WAN port, and then follow Step 4 and 5 to complete the hardware connection.



1) Turn off the modem, and remove the backup battery if it has one.

2) Connect the modem to the WAN port on your router with an Ethernet cable.

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

1) Connect the power adapter to the router and turn on the router.

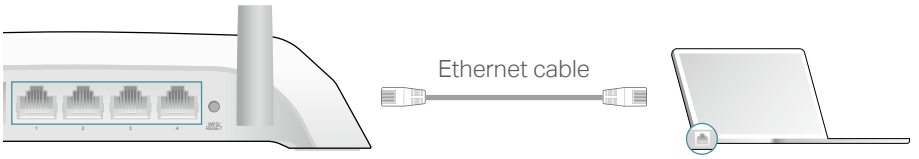
2) Verify that the hardware connection is correct by checking these LEDs.

Tips: If Wi-Fi LED is off, enable the Wi-Fi function by using a web browser.

1. Connect your computer to the router.

- **Method 1: Wired**

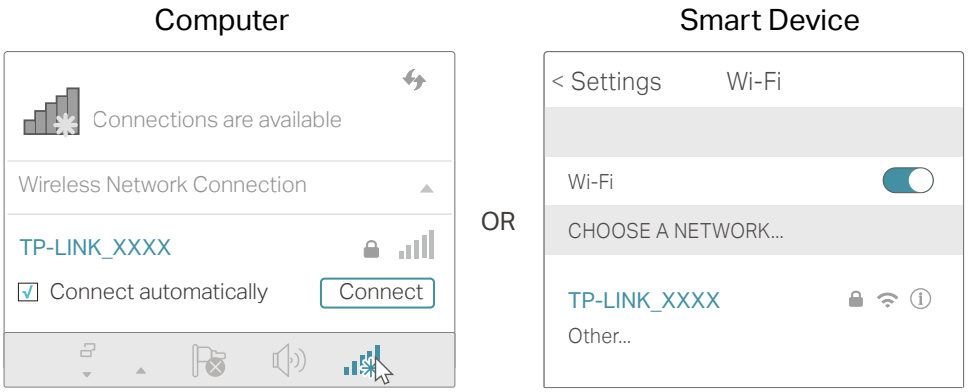
Turn off the Wi-Fi on your computer and connect the devices as shown below.



- **Method 2: Wirelessly**

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

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



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

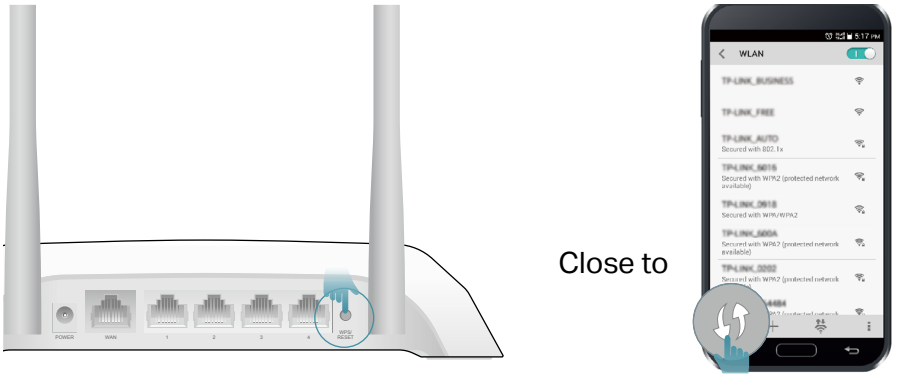
Wireless devices that support WPS, including Android phones, tablets, most USB network cards, can be connected to your router through this method (Not supported by iOS devices).

Note:

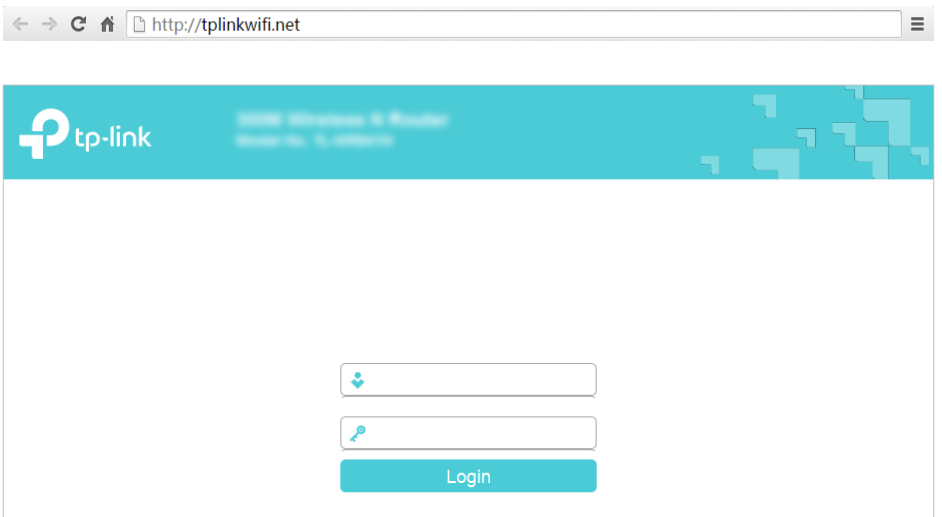
The WPS function cannot be configured if the wireless function of the router is disabled. Also, the WPS function will be disabled if your wireless encryption is WEP. Please make sure the wireless function is enabled and is configured with the appropriate encryption before configuring the WPS.

1) Tab the WPS icon on the device's screen, here takes an Android phone as an example.

2) Immediately press the WPS button on your router.



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



Note:

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

2. After successfully login, select Standard Wireless Router mode and follow Quick Setup to complete the configuration.
3. Enjoy! For wireless devices, you may have to reconnect to the wireless network if you have customized the SSID (wireless name) and password during the configuration.

Chapter 3

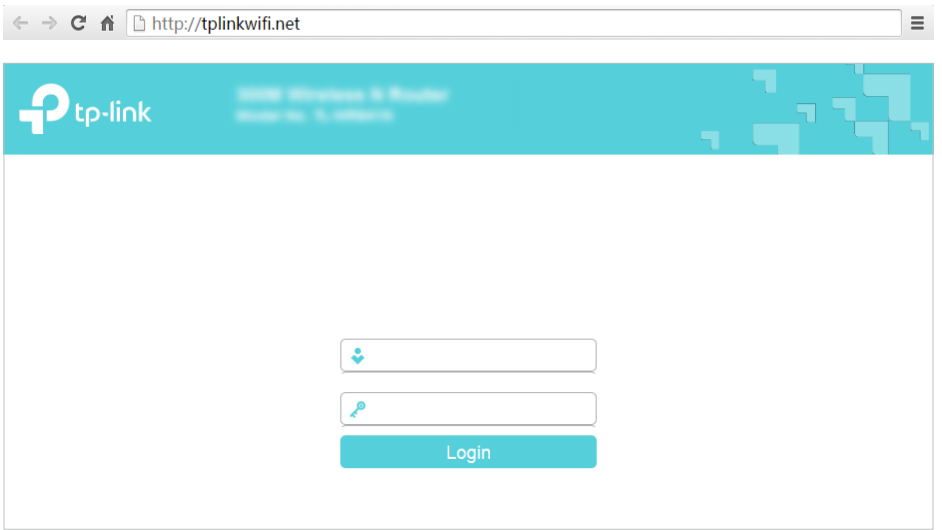
Log In

This chapter introduces how to log in to the web management page of router.

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

Follow the steps below to log in to your router.

1. Set up the TCP/IP Protocol in Obtain an IP address automatically mode on your computer.
2. Visit http://tplinkwifi.net, and log in with the 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 the "FAQ" section.

Chapter 4

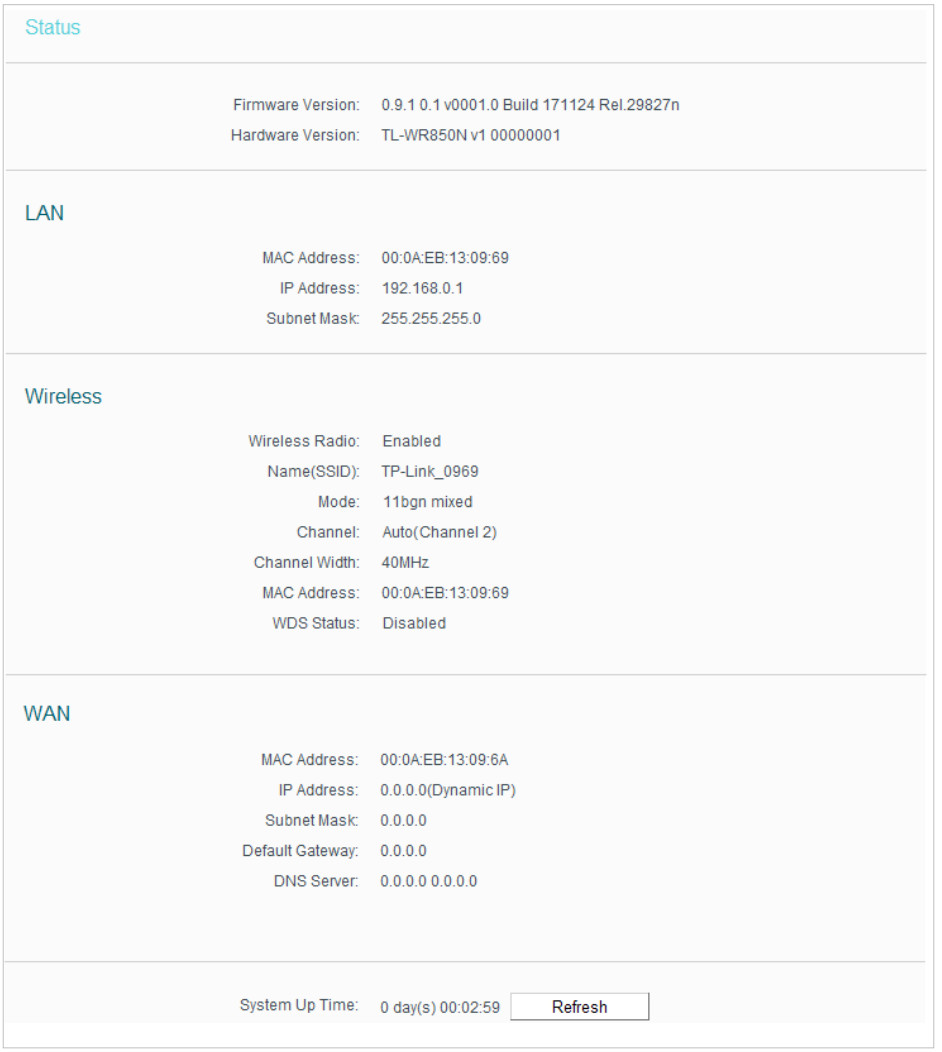
Configure the Router

This chapter presents how to configure the various features of the router.

It contains the following sections:

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 > Wireless Settings page.

- Wireless Radio - Indicates whether the wireless feature is enabled or not.
- Name (SSID) - The SSID of the router.
- Mode - The current wireless working mode in use.
- Channel Width - The current wireless channel width in use.
- Channel - The current wireless channel in use.
- MAC Address - The physical address of the router.
- WDS Status - The status of WDS connection.

- 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. Network

4. 2. 1. WAN

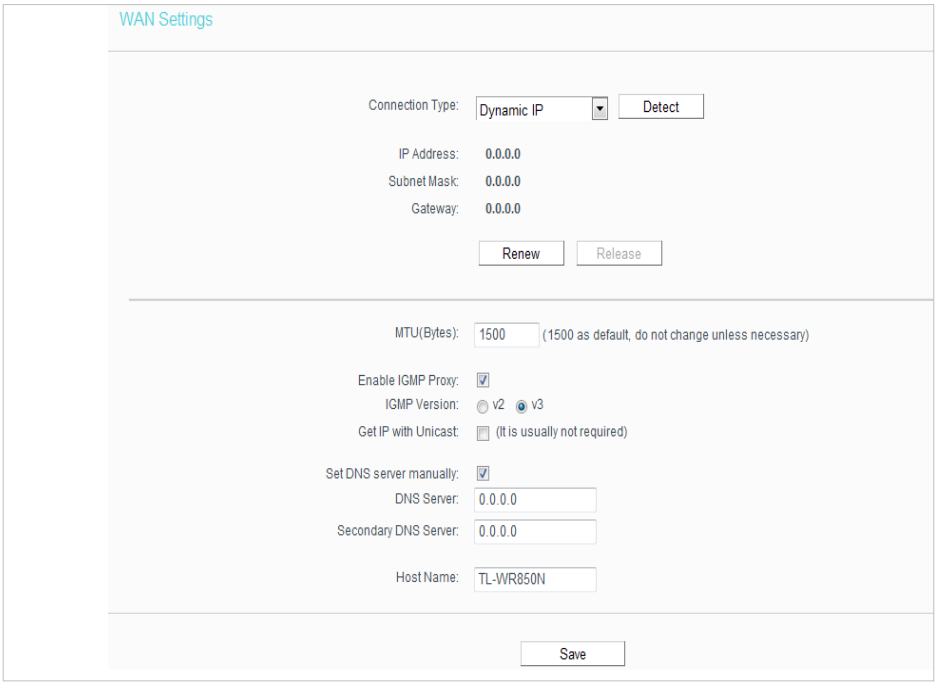
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Network > WAN.
3. Configure the IP parameters of the LAN and click Save.

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.

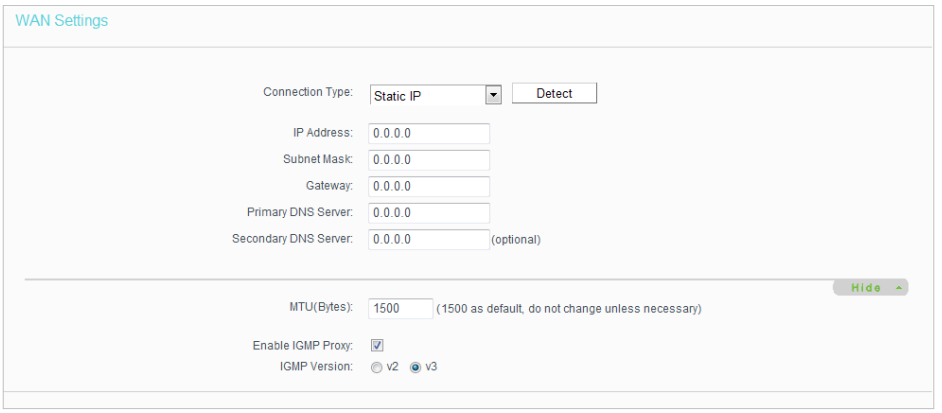
4. Click Release to release the IP parameters.Click Next to start. Then follow the step-by-step instructions to connect your router to the internet.



- MTU Size - 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.
- Set DNS server manually - If your ISP gives you one or two DNS IP addresses, select Set DNS server manually and enter the DNS Server and Secondary DNS Server into the correct fields. Otherwise, the DNS servers will be assigned from ISP dynamically.
    - Primary DNS - Enter the DNS IP address in dotted-decimal notation provided by your ISP.
    - Secondary DNS - Enter another DNS IP address in dotted-decimal notation provided by your ISP.
- Host Name - This option specifies the name of the router.
- Get IP with Unicast DHCP - 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.)

Static IP

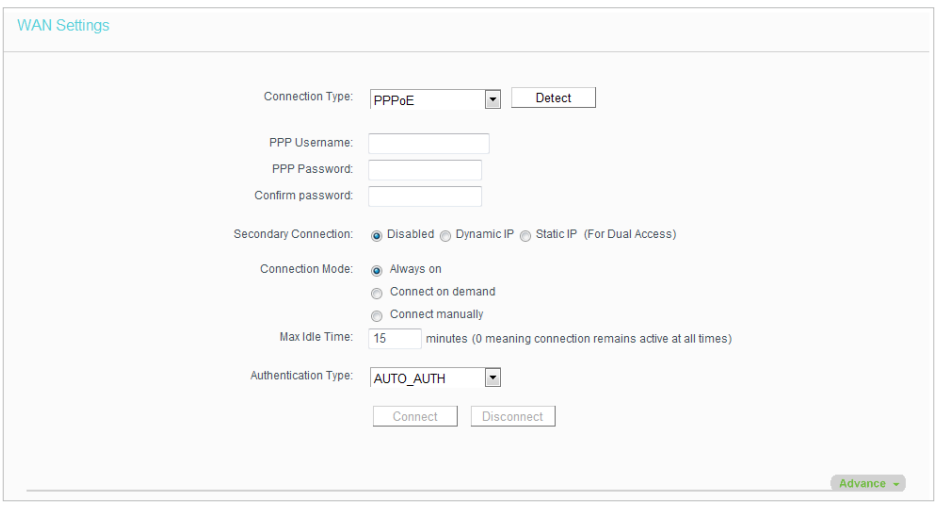
If your ISP provides a static or fixed IP address, subnet mask, default gateway and DNS setting, please select Static IP.



- 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.
- MTU Size - 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.
- Primary/Secondary DNS - (Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.

PPPoE

If your ISP provides PPPoE connection, select PPPoE.



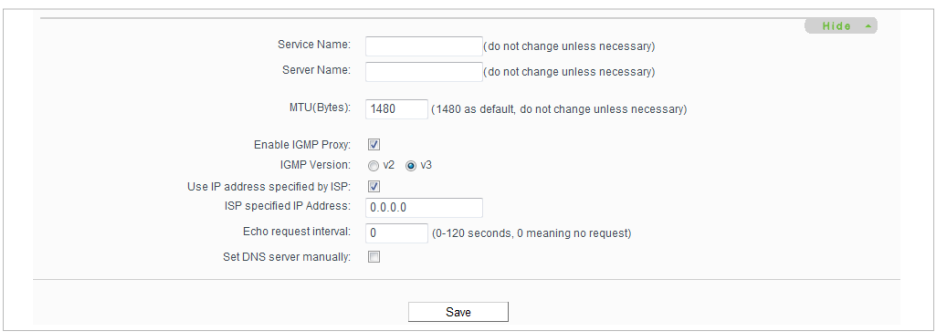
- User Name/Password - Enter the user name and password provided by your ISP. These fields are case-sensitive.

- 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 - Connect automatically after the Router is disconnected. To use this option, click the radio button.
    - Connect on demmand - You can configure the Router to disconnect your Internet connection after a specified period of the Internet connectivity (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection when you attempt to access the Internet again. If you wish to activate Connect on Demand, put a check mark in the circle. If you want your Internet connection to remain active all the times, enter 0 in the Max Idle Time field.
    - 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:

- Only when you have configured the system time on the System Tools > Time Settings page, will the time-based connecting function take effect.
- 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.

If you want to do some advanced configurations, please click Advanced.

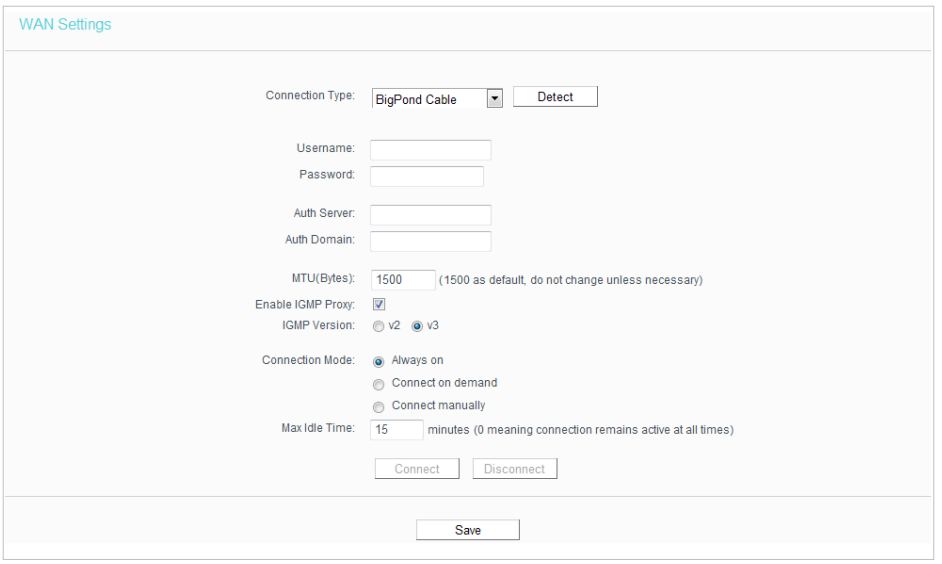


- MTU - The default MTU size is 1480 bytes. It is not recommended that you change the default MTU size unless required by your ISP.
- Service Name/Server Name - The service name and server name should not be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank will work.

- 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 request.
- Set DNS server manually - 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.

BigPond Cable

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



- User Name/Password - Enter the user name 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 - The default MTU is 1480 bytes. It is not recommended that you change the default MTU size unless required by your ISP.
- Connection Mode
    - 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.

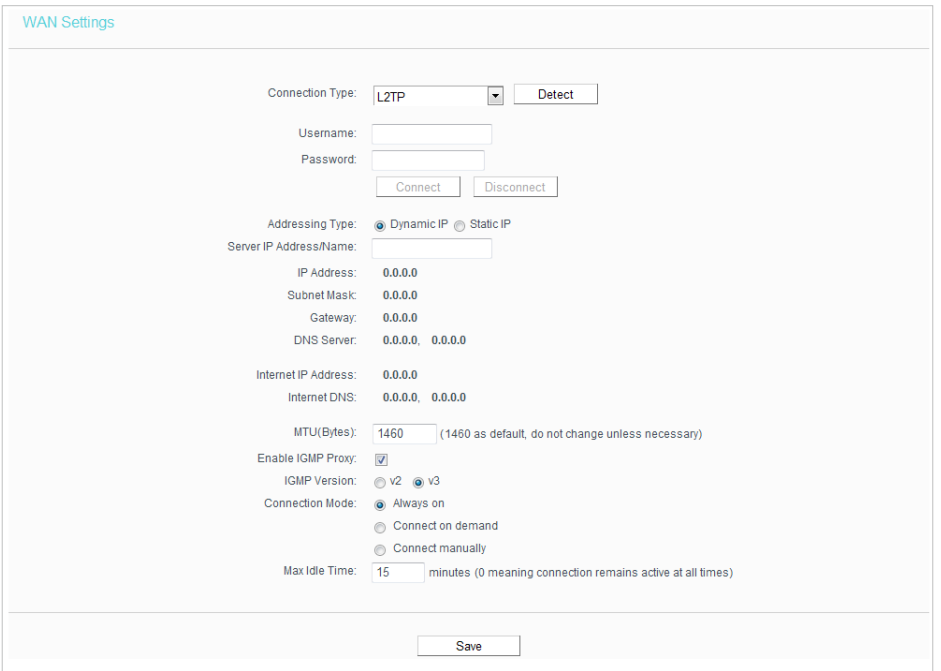
- Always on - Connect automatically after the Router is disconnected. To use this option, click the radio button.
- Connect Manually - You can click Connect/Disconnect to connect/disconnect immediately. This mode also supports the Max Idle Time function as Connect on Demand mode. The Internet connection 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.

L2TP

If your ISP provides L2TP connection, please select L2TP.



- User Name/Password - Enter the user name and password provided by your ISP. These fields are case-sensitive.
- Connect/Disconnect - Click this button to connect or disconnect immediately.
- Dynamic IP/ Static IP - Select either as required by your ISP. If Static IP is selected, please enter the IP address, subnet marsk, gateway and DNS also provided by your ISP.
- Internet IP Address/ Internet DNS - The Internet IP address and DNS server address assigned by L2TP server.

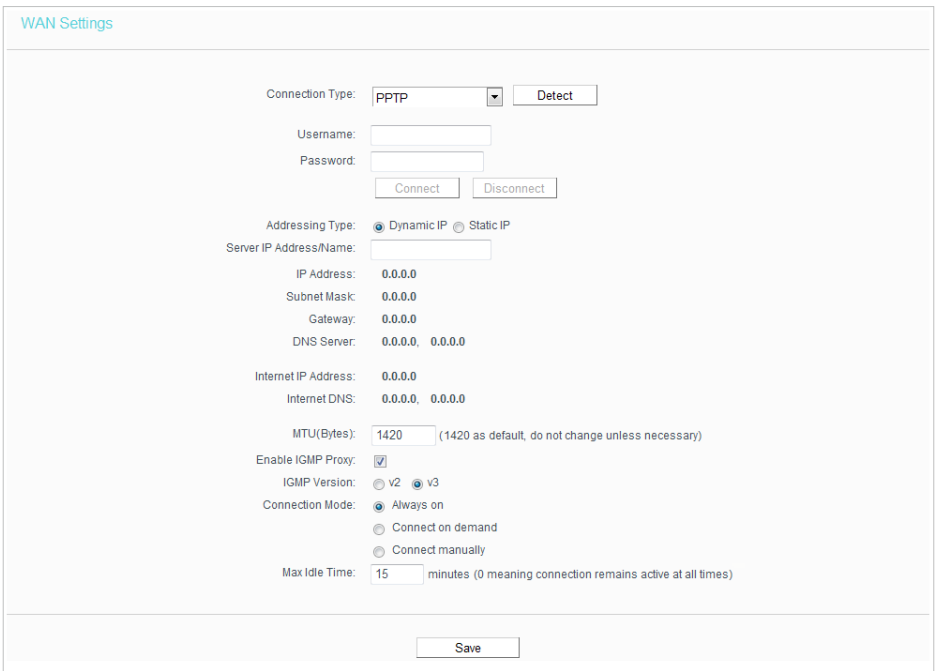
- Connection Mode
  - Connect on Demand - In this mode, the Internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the Internet again. If you want to keep your Internet connection active all the time, please enter 0 in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.
  - Always on - Connect automatically after the Router is disconnected. To use this option, click the radio button.
  - 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.



- User Name/Password - Enter the user name and password provided by your ISP. These fields are case-sensitive.
- Connect/Disconnect - Click this button to connect or disconnect immediately.

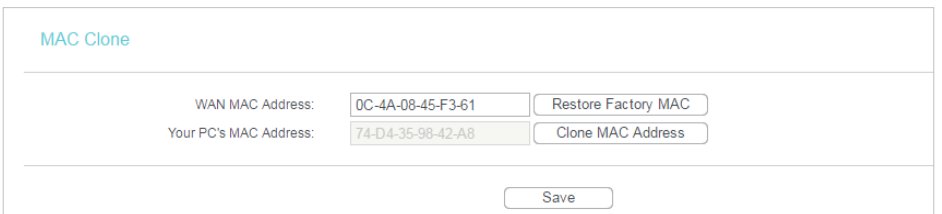
- Dynamic IP/ Static IP - Select either as required by your ISP. If Static IP is selected, please enter the IP address, subnet marsk, gateway and DNS also provided by your ISP.
- Internet IP Address/ Internet DNS - The Internet IP address and DNS server address assigned by L2TP server.
- Connection Mode
    - 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.
    - Always on - Connect automatically after the Router is disconnected. To use this option, click the radio button.
    - 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.

4. 2. 2. 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.



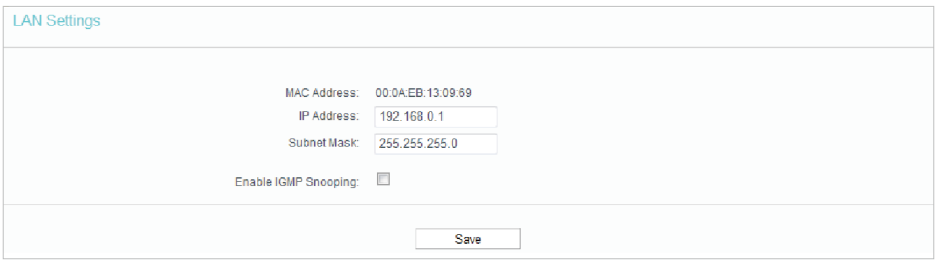
- WAN MAC Address - This field displays the current MAC address of the WAN port. If your ISP requires you to register the MAC address, please enter the correct MAC address in this field. Click Restore Factory MAC to restore the MAC address of WAN port to the factory default value.

- 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. 2. 3. 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.



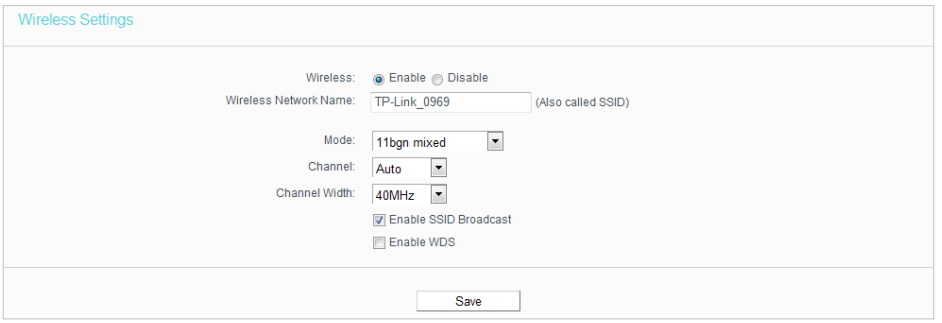
- MAC Address - The physical address of the LAN ports. The value can not be changed.
- IP Address - Enter the IP address in dotted-decimal notation of your router (factory default - 192.168.0.1).
- Subnet Mask - An address code that determines the size of the network. Normally 255.255.255.0 is used as the subnet mask.
- Enable IGMP Snooping - The Internet Group Management Protocol (IGMP) feature allow you to watch TV on IPTV-supported devices on the LAN .

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. Wireless

4. 3. 1. Wireless 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.



- Wireless Network Name - Enter a string of up to 32 characters. The default SSID is TP-LINK_XXXX (XXXX indicates the last unique four numbers of each router's MAC address). 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 - Select the desired mode. It is strongly recommended that you keep the default setting 11bgn mixed, so that all 802.11b/g/n wireless devices can connect to the router.

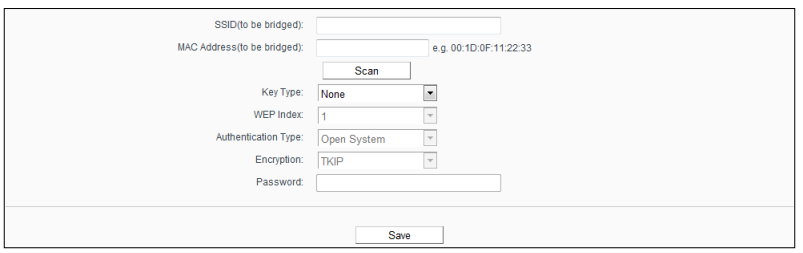
Note:

If 11bg mixed mode is selected, the Channel Width field will turn grey and the value will become 20M, and cannot be changed.

- Channel Width - Select any channel width from the drop-down list. The default setting is Auto, which can automatically adjust the channel width for your clients.
- 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.
- Enable SSID Broadcast - If enabled, the router will broadcast the wireless network name (SSID).
- Enable WDS - You can select this to enable WDS Bridging, with this function, the router can bridge two or more WLANs.

Note:

If this checkbox is selected, you had better make sure the following settings are correct.



- SSID (to be bridged) - The SSID of the AP your router is going to connect to as a client. You can also use the survey function to select the SSID to join.

- MAC Address (to be bridged) - The MAC Address of the AP your Router is going to connect to as a client. You can also use the scan function to select the MAC Address to join.
- Scan - Click this button, you can search the AP which runs currently.
- Key type - This option should be chosen according to the AP's security configuration. It is recommended that the security type is the same as your AP's security type.
- WEP Index - This option should be chosen if the key type is WEP (ASCII) or WEP (HEX). It indicates the index of the WEP key.
- Authentication Type - This option should be chosen if the key type is WEP (ASCII) or WEP (HEX).It indicates the authorization type of the Root AP.
- Password - If the AP your router is going to connect needs password, you need to fill the password in this blank.

4. 3. 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.

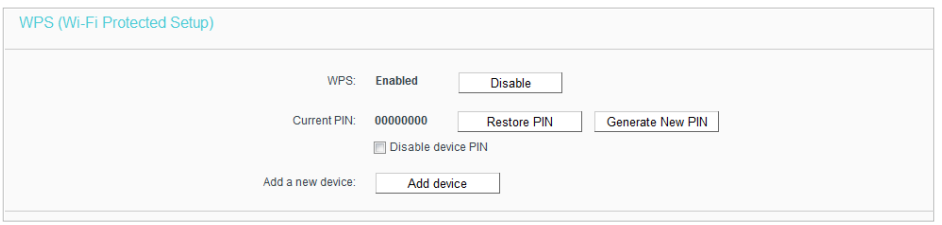
Note:

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.

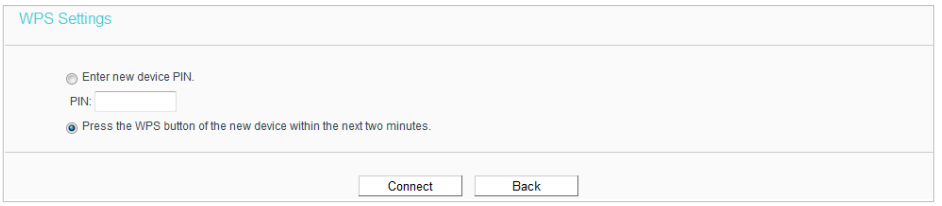
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to WPS.
3. Follow one of the following three methods to connect your client device to the router's Wi-Fi network.

Method ONE: Press the WPS Button on Your Client Device

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



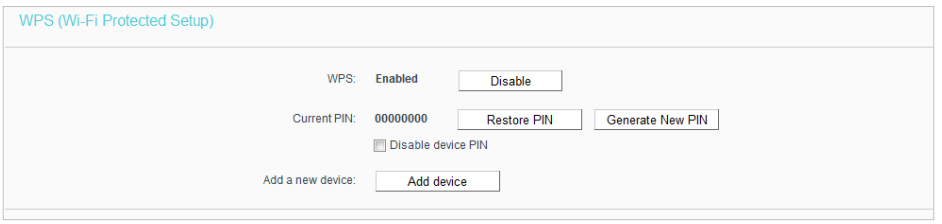
2. Select Press the WPS button of the new device in two minutes and click Connect.



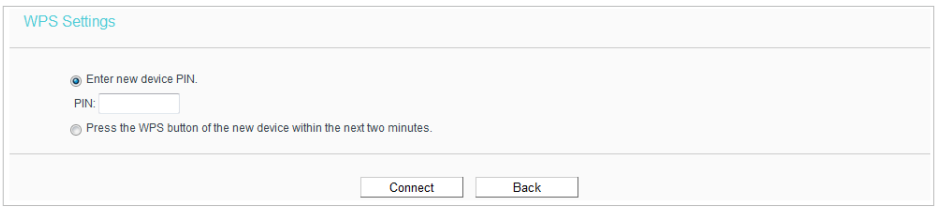
3. Within two minutes, press the WPS button on your client device.
4. A success message will appear on the WPS page if the client device has been successfully added to the router's network.

Method TWO: Enter the Client's PIN

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



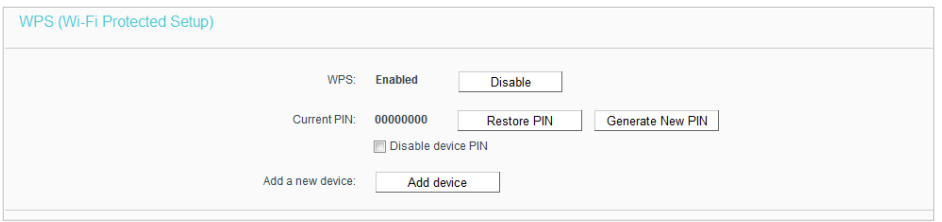
2. Select Enter the new device's PIN, enter your client device's current PIN in the PIN filed and click Connect.



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

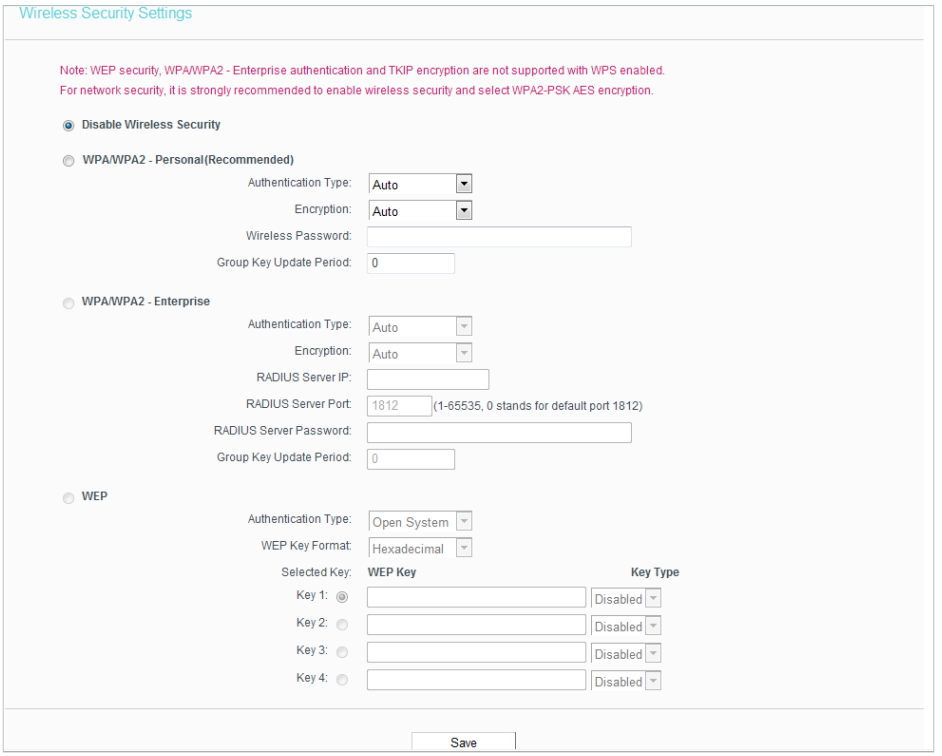
1. Keep the WPS Status as Enabled and get the Current PIN of the router.



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

4. 3. 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 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.
    - Authentication Type - Select Automatic, WPA-PSK or WPA2-PSK.
    - Encryption - Select Automatic, TKIP or AES.
    - Wireless Password - Enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters.
    - Group Key Update Period - Specify the group key update interval in seconds. The value can be 0 or at least 30. Enter 0 to disable the update.

- WPA /WPA2-Enterprise - It's based on Radius Server.
  - Authentication Type - Select Automatic, WPA or WPA2.
  - Encryption - Select Automatic, TKIP or AES.
  - Radius Server IP - Enter the IP address of the Radius server.
  - Radius Port - Enter the port that Radius server used.
  - Radius 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 Automatic, which can select Shared Key or Open System authentication type automatically based on the wireless client's capability and request.
  - WEP Key Format - Hexadecimal and ASCII formats are provided here. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. ASCII format stands for any combination of keyboard characters in the specified length.
  - WEP Key (Password) - Select which of the four keys will be used and enter the matching WEP key. Make sure these values are identical on all wireless clients in your network.
  - Key Type - Select the WEP key length (64-bit, 128-bit or 152-bit) for encryption. Disabled means this WEP key entry is invalid.
  - 64-bit - Enter 10 hexadecimal digits (any combination of 0-9, a-f and A-F. Null key is not permitted) or 5 ASCII characters.
  - 128-bit - Enter 26 hexadecimal digits (any combination of 0-9, a-f and A-F. Null key is not permitted) or 13 ASCII characters.
  - 152-bit - Enter 32 hexadecimal digits (any combination of 0-9, a-f and A-F. Null key is not permitted) or 16 ASCII characters.

4. 3. 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.

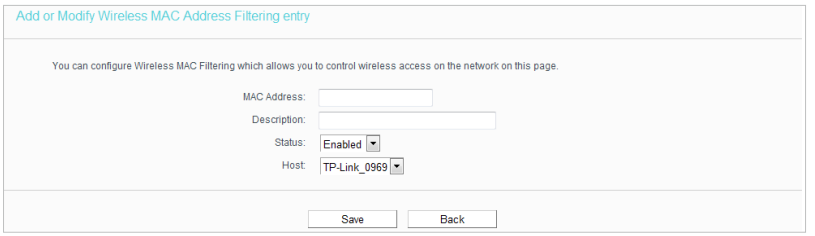
I want to:

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.

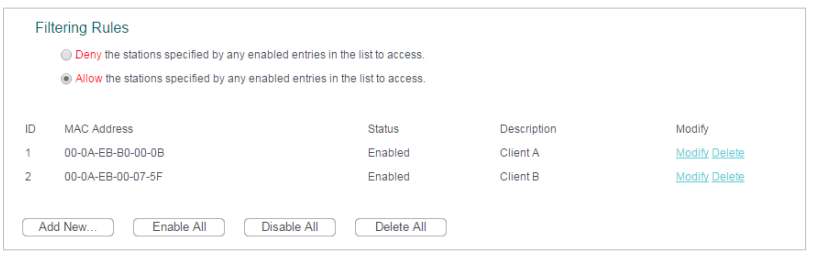
How can I do that?

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 or disable all entries if there are any entries already.
6. Click Add New and fill in the blanks.



   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) Leave the status as Enabled.
   4) Click Save and click Back.

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



Done!

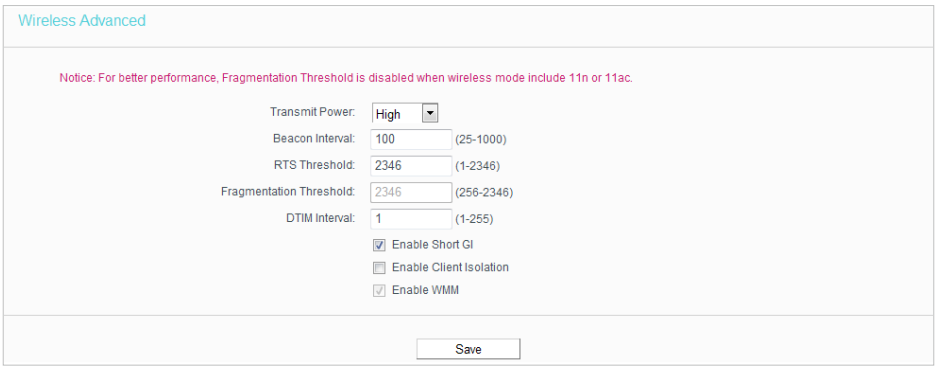
Now only client A and client B can access your network.

4. 3. 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:

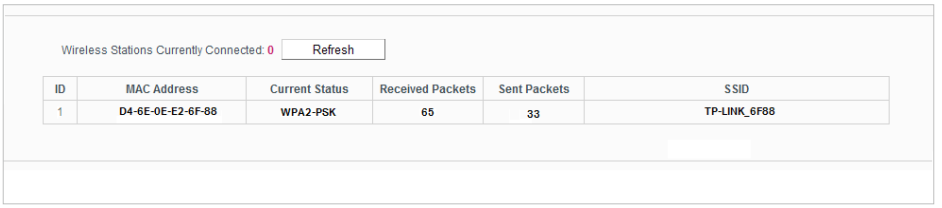
- If you are not familiar with the setting items on this page, it's strongly recommended to keep the provided default values; otherwise it may result in lower wireless network performance.



- 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 WMM - WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended to enable this function.
- Enable Short GI - It is recommended to enable this function, for it will increase the data capacity by reducing the guard interval time.
- Enable AP 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.

4. 3. 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.



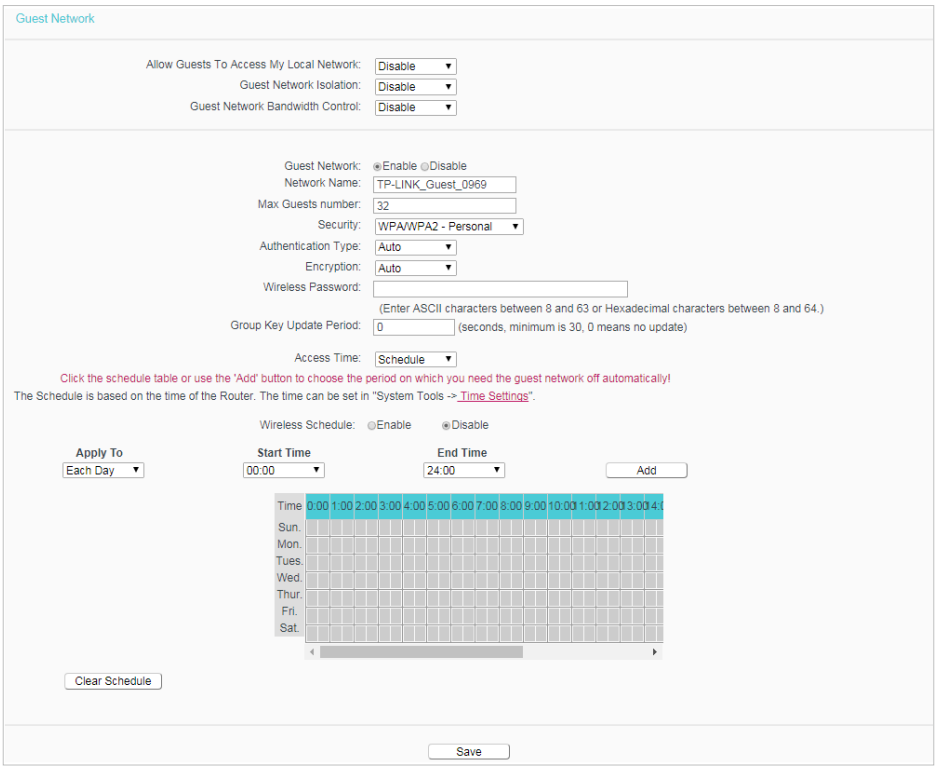
- MAC Address - The MAC address of the connected wireless client.
- Current Status - The running status of the connected wireless client.
- Received Packets - Packets received by the wireless client.
- Sent Packets - Packets sent by the wireless client.
- SSID - SSID that the station associates with.

4. 4. Guest Network

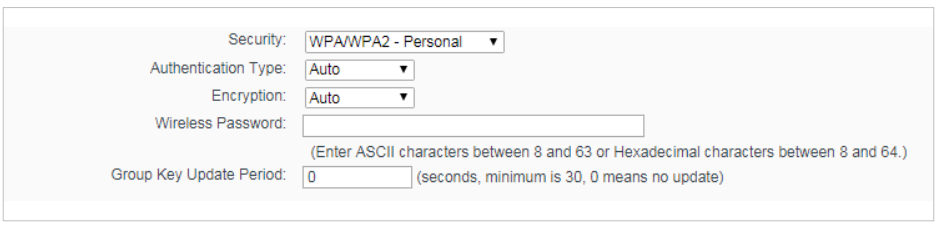
Guest Network allows you to provide Wi-Fi access for guests without disclosing your host network. When you have guests in your house, apartment, or workplace, you can create a guest network for them. In addition, you can customize guest network permissions to ensure network security and privacy.

If you run a small shop, you can set up Facebook Wi-Fi. It allows customers to easily connect to your Wi-Fi by redirecting them to your company's Facebook page. Here, they are encouraged to check in and like your page before receiving free web access. This raises the profile of your business on Facebook and increases customer engagement with promotional content on your page.

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. Configure the Security type.
   - To configure a secure network, select WPA/WPA2 - Personal and create a password for the guest network.



6. Select Schedule from the Access Time drop-down list and customize it for the guest network.
7. Customize guest network permissions.
   - 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 > Control Settings page.

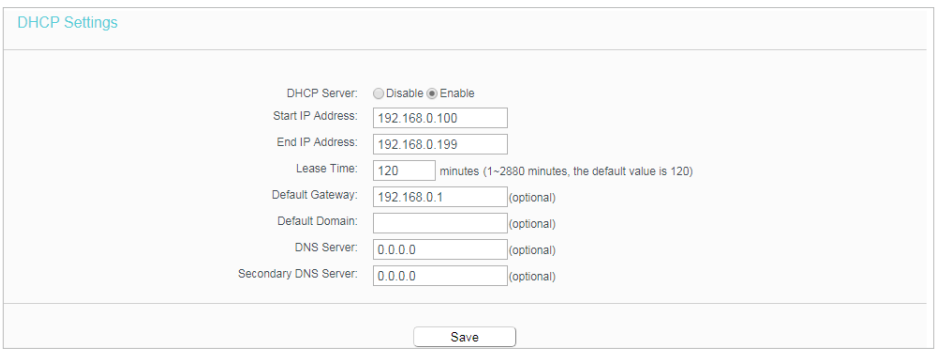
8. Click Save.

4. 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.

4. 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.
- End IP Address - Specify an IP address for the DHCP Server to end with when assigning IP addresses.
- 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.
- Default Gateway (Optional) - It is suggested to input the IP address of the LAN port of the router.

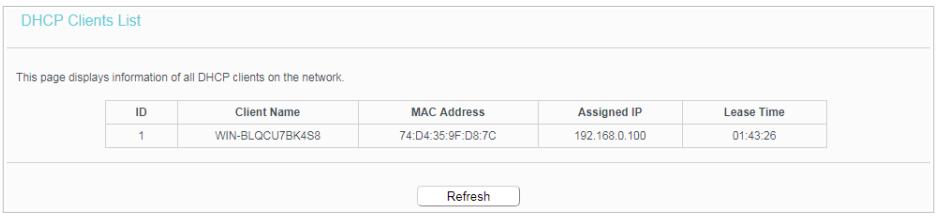
- Default Domain (Optional) - Input the domain name of your network.
- DNS Server (Optional) - Input the DNS IP address provided by your ISP.
- Secondary DNS Server (Optional) - Input the IP address of another DNS server if your ISP provides two DNS servers.

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. 5. 2. DHCP Client List

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



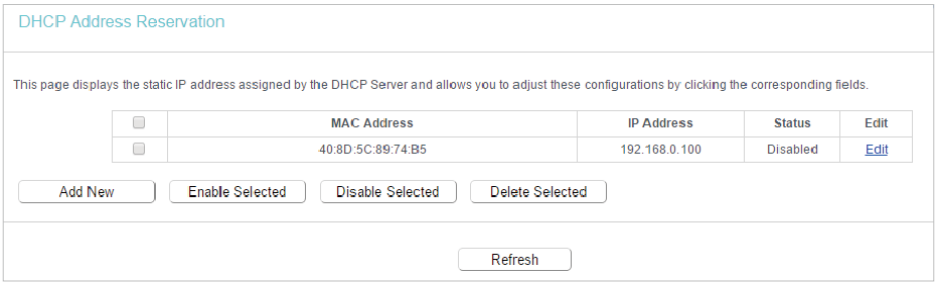
- Client Name - The name of the DHCP client.
- MAC Address - The MAC address of the DHCP client.
- Assigned IP - The IP address that the outer has allocated to the DHCP client.
- Lease Time - The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic IP address will be 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. 5. 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 blank.



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. 6. Forwarding

The router's NAT (Network Address Translation) feature makes the devices on the LAN use the same public IP address to communicate in 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.

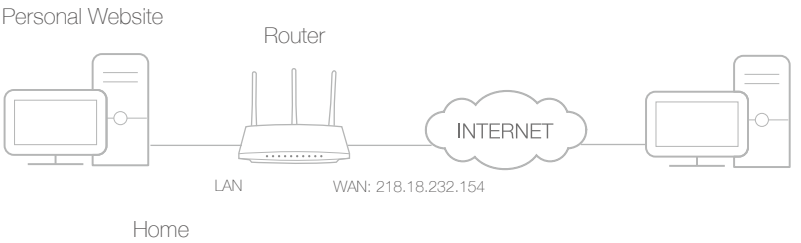
4. 6. 1. Virtual Server

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.

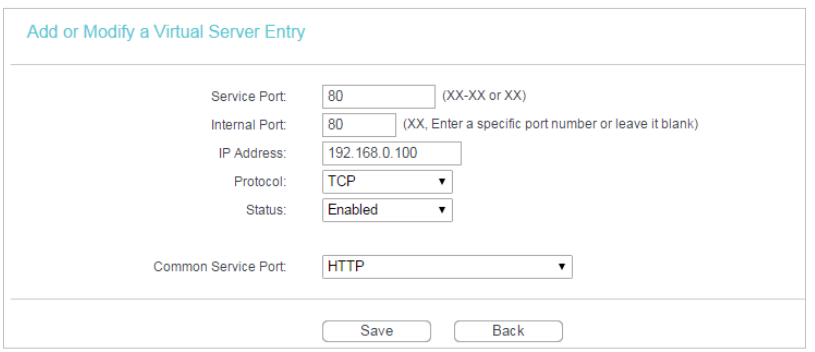
Virtual Servers can be used to set up public services in your local network, such as HTTP, FTP, DNS, POP3/SMTP and Telnet. Different service uses different service port. Port 80 is used in HTTP service, port 21 in FTP service, port 25 in SMTP service and port 110 in POP3 service. Please verify the service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

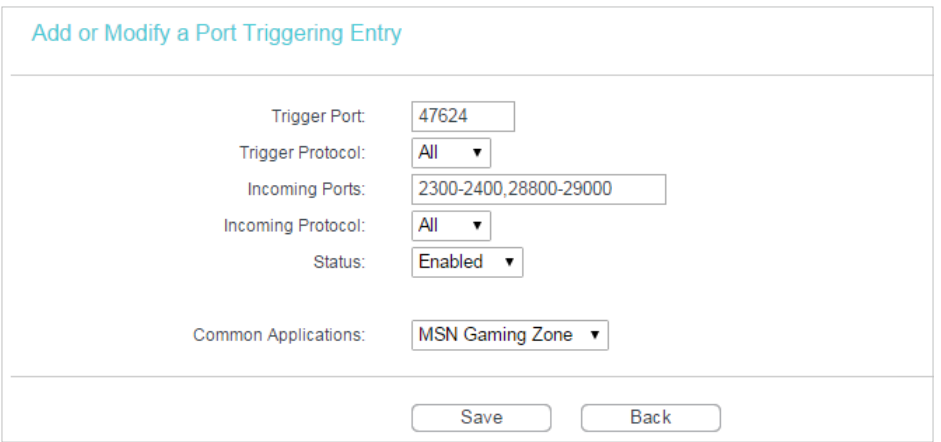
- Some specific service ports are forbidden by the ISP, if you fail to visit the website, please use another service port.

4. 6. 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 Applications list, please enter the parameters manually. You should verify the incoming ports the application uses first and enter them in Incoming Ports 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. 6. 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!

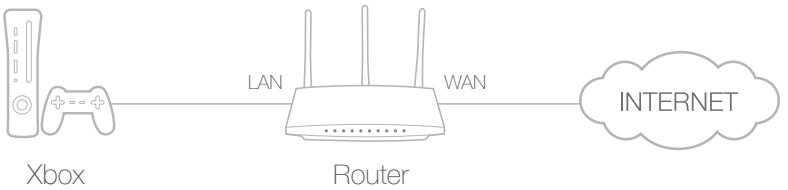
You've set your PC to a DMZ host and now you can make a team to game with other players.

4. 6. 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.

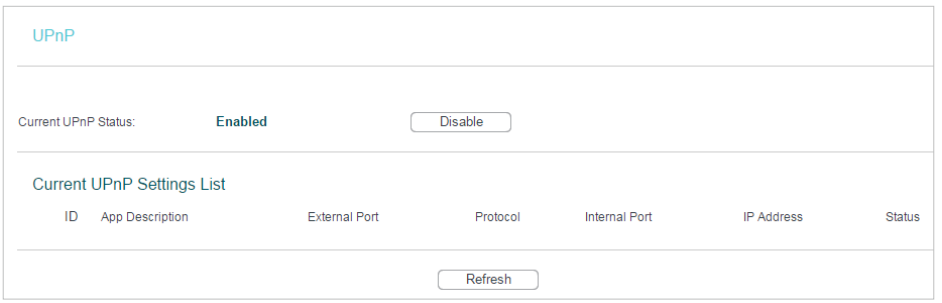
Tips:
- UPnP is enabled by default in this router.
- Only the application supporting UPnP protocol can use this feature.
- UPnP feature needs the support of operating system (e.g. Windows Vista/ Windows 7/ Windows 8, etc. Some of operating system need to install the UPnP components).

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.

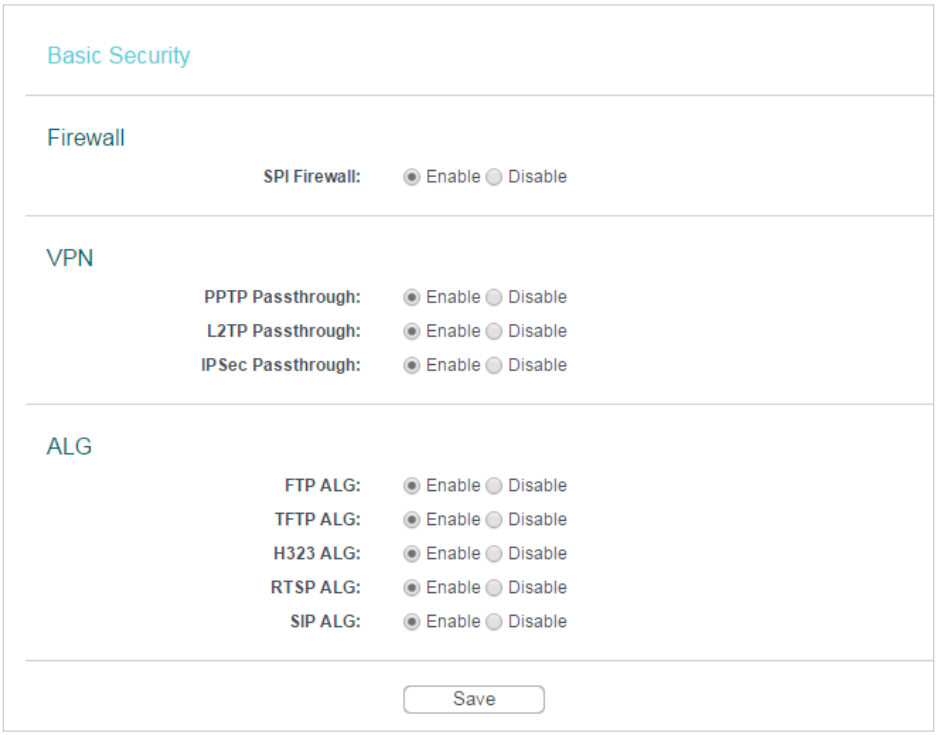


4. 7. Security

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

4. 7. 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.



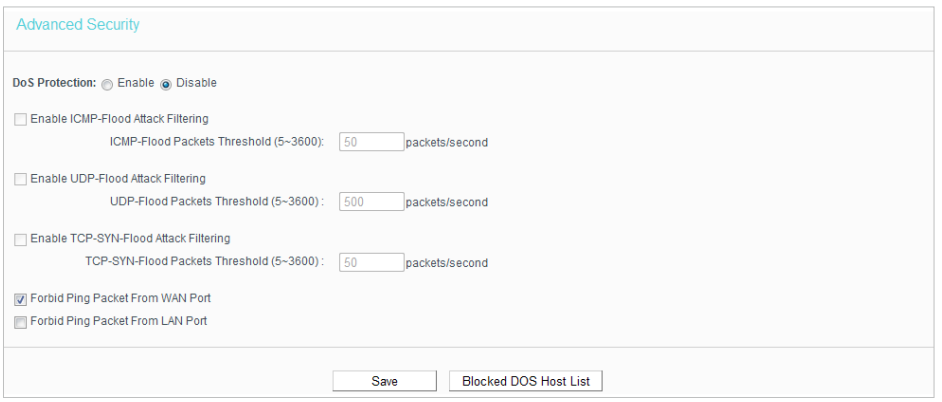
- Firewall - A firewall protects your network from Internet attacks.
    - SPI Firewall - SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the 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 Passthrough - 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 Passthrough - 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 Passthrough - 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.
- RTSP ALG - To allow some media player clients to communicate with some streaming media servers across NAT, click Enable.
- SIP ALG - To allow some multimedia clients to communicate across NAT, click Enable.

3. Click Save.

4. 7. 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 Tool > Statistics is enabled.

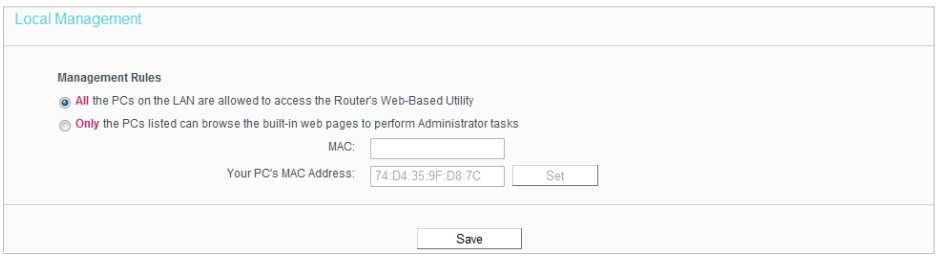
- Enable ICMP-FLOOD Attack Filtering -Check the box to enable or disable this function.
- ICMP-FLOOD Packets Threshold (5~3600) - The default value is 50. Enter a value between 5 ~ 3600. When the number of the current ICMP-FLOOD packets is beyond the set value, the router will startup the blocking function immediately.
- Enable UDP-FLOOD Filtering - Check the box to enable or disable 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 -Check the box 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.
- Forbid Ping Packet From WAN Port - Enable or Disable Forbid Ping Packet From WAN Port. The default setting is enabled. The ping packet from WAN cannot access the Router. (Defends against some viruses).
- 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. 7. 3. Local Management

1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Security > Local Management, and you can block computers in LAN from accessing the router.



For example, if you want to allow PCs with specific MAC addresses to access the router's web management page locally from inside the network, please follow the instructions below:

1) Select Only the PCs listed can browse the built-in web pages to perform Administrator tasks.

2) Enter the MAC address of each PC separately. The format of the MAC address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). Only the PCs with the listed

MAC addresses can use the password to browse the built-in web pages to perform administrator tasks.

3) Click Add, and your PC's MAC address will also be listed.

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.

4. 7. 4. Remote Management

1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Security > Remote Management, and you can manage your router from a remote device via the Internet.

- Web Management Port - Web browser access normally uses the standard HTTP service port 80. This router's default remote management web port number is 80. For higher security, you can change the remote management web port to a custom port by entering a number between 1 and 65534 but do not use the number of any common service port.
- Remote Management IP Address - This is the address you will use when accessing your router via a remote device. This function is disabled when the IP address is set to the default value of 0.0.0.0. To enable this function, change 0.0.0.0 to a valid IP address. If it is set to 255.255.255.255, then all the remote devices can access the router from the Internet.

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.

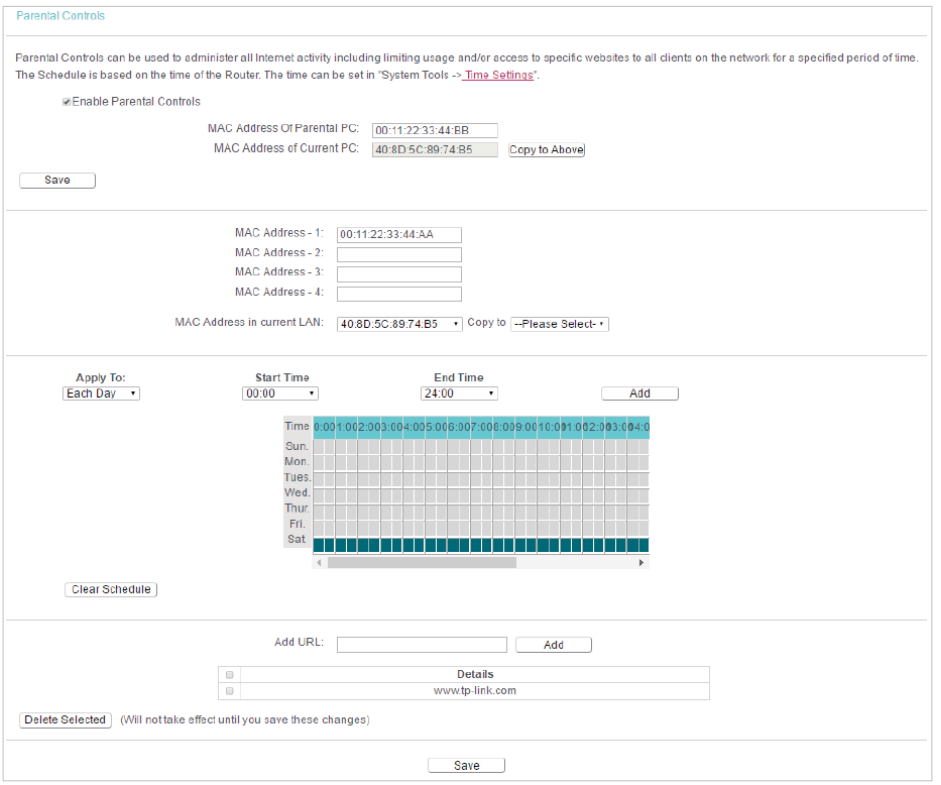
4. 8. Parental Controls

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. Check the Enable Parental Controls box and enter the MAC address 00:11:22:33:44:BB in the MAC Address of Parental PC field.
4. Enter 00:11:22:33:44:AA in the MAC Address 1 field.
5. Create a new schedule with Day is Sat and Time is all day-24 hours. Click Add
6. Enter www.tp-link.com in the Add URL field. Click Add.
7. Click Save.

Then you will see the page as shown in figure below.



4. 9. Access Control

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

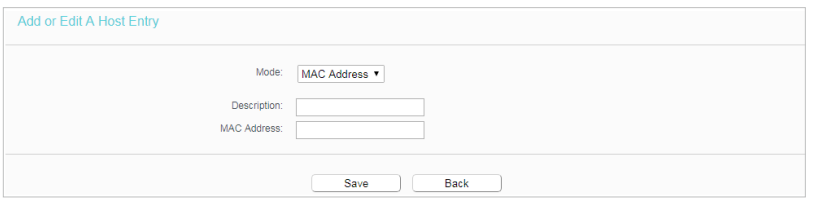
I want to:

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?

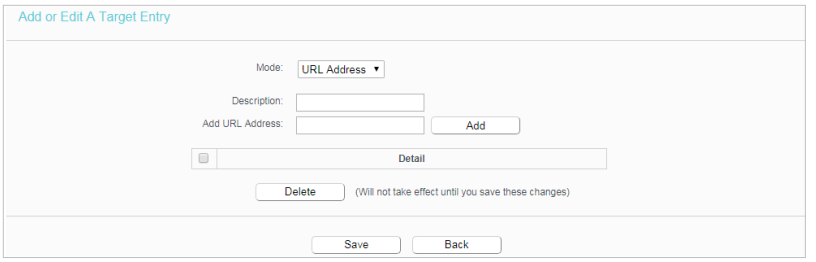
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Access Control > Host and configure the host settings:
   1) Click Add New.
   2) Select MAC Address as the mode type. Create a unique description (e.g. host_1) for the host in the Description field 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.

   Note:

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

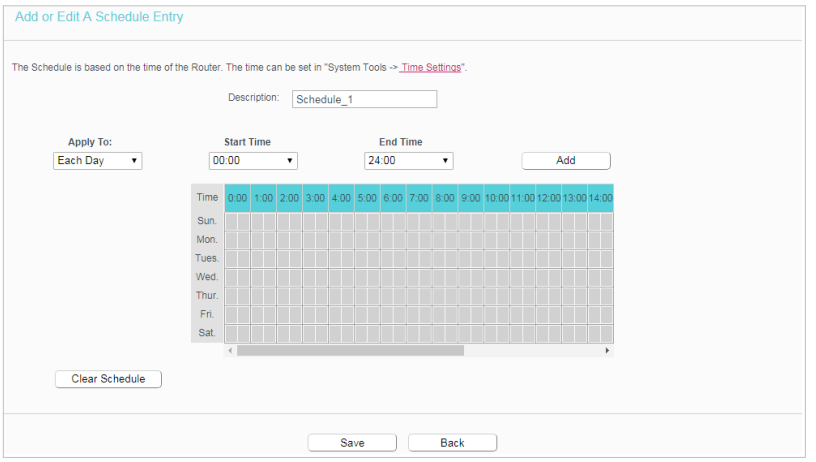


3) Click Save.

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.

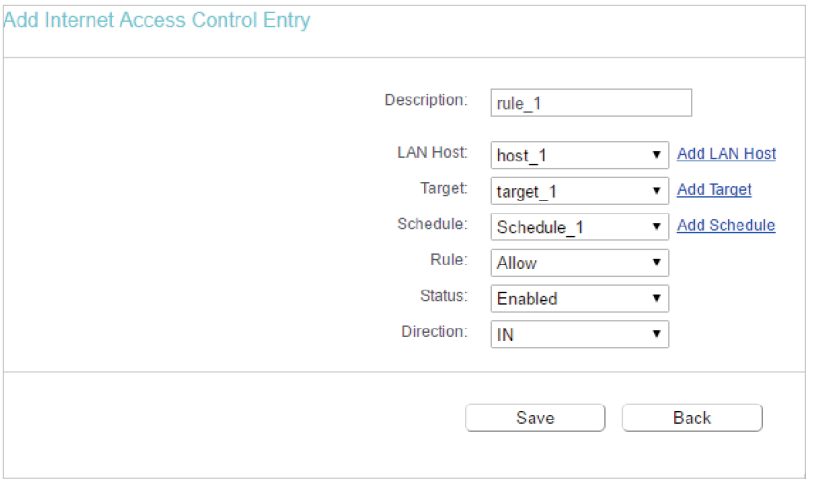


3) Click Save.

5. Go to Access Control > Rule and add a new access control rule.

1) Click Add New.

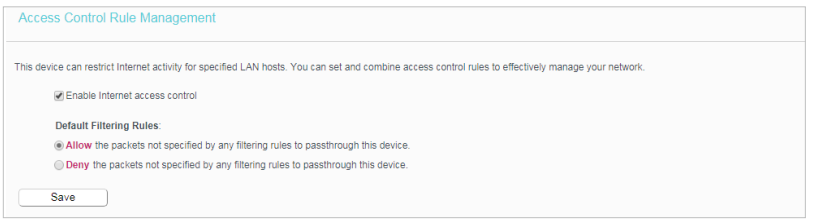
2) Give a name for the rule in the Description field. Select host_1 from the LAN host drop-down list; select target_1 from the target drop-down list; select schedule_1 from the schedule drop-down list.



3) Leave the status as Enabled as click Save.

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.

4. 10. Advanced Routing

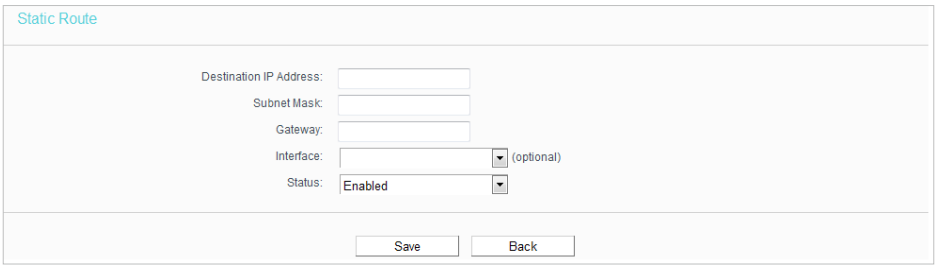
Static Routing is a form of routing that is configured manually by a network administrator or a user by adding entries into a routing table. The manually-configured routing information guides the router in forwarding data packets to the specific destination.

4. 10. 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.



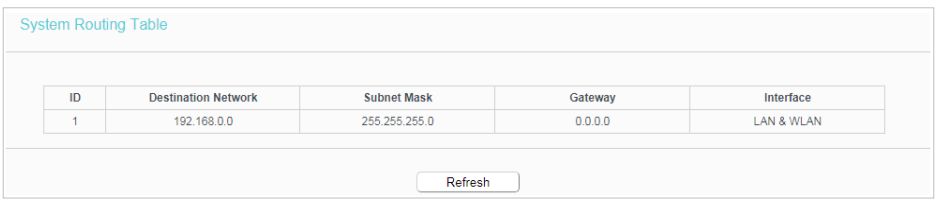
2. Enter the following information.
   - Destination IP Address - The Destination Network is the address of the network or host that you want to assign to a static route.
   - Subnet Mask - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host 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.

You can also do the following operations to modify the current settings.

- Click the Enable Selected button to enable selected entries..
- Click the Disable Selected button to disable selected entries.
- Click the Delete Selected button to delete selected entries.

4. 10. 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.



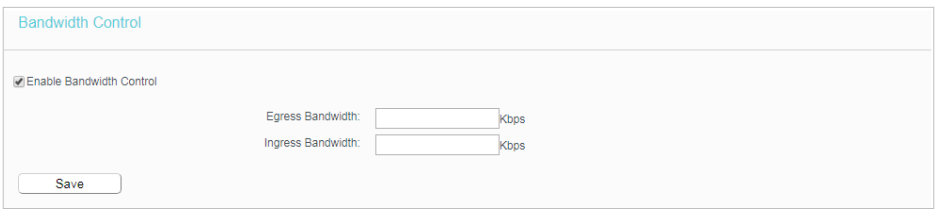
- Destination Network - The Destination Network is the address of the network or host to which the static route is assigned.
- Subnet Mask - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.

- 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. 11. Bandwidth Control

4. 11. 1. Control Settings

1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Bandwidth Control.
3. Configure the bandwidth as needed and click Save.

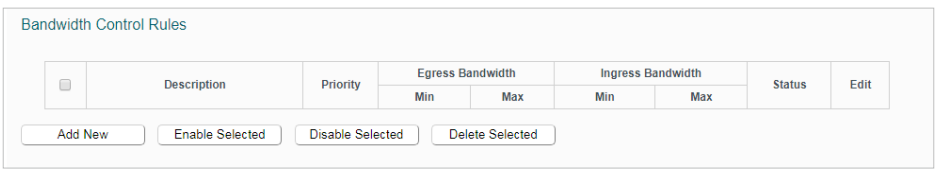


The values you configure for the Egress Bandwidth and Ingress Bandwidth should be less than 100,000Kbps. For optimal control of the bandwidth, please select the right Line Type and consult your ISP for the total egress and ingress bandwidth.

- Enable Bandwidth Control - Check this box so that the Bandwidth Control settings can take effect.
- Egress Bandwidth - The upload speed through the WAN port.
- Ingress Bandwidth - The download speed through the WAN port.

4. 11. 2. Rule List

1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to Bandwidth Control and you can view and configure the Bandwidth Control rules.

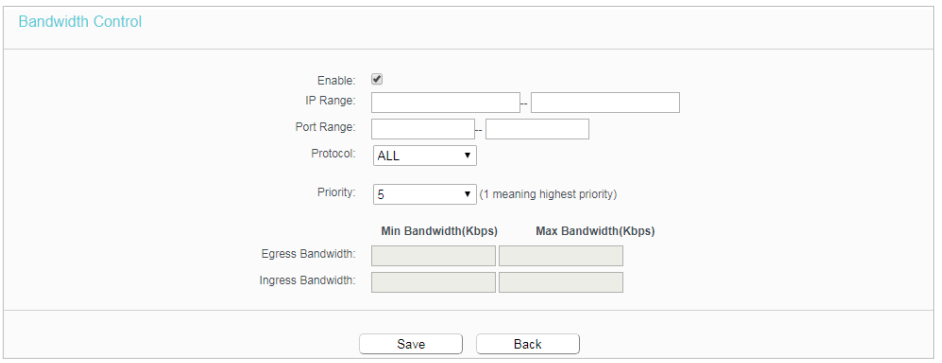


- Description - This is the information about the rules such as address range.

- Egress Bandwidth - This field displays the max and min upload bandwidth through the WAN port. The default is 0.
- Ingress Bandwidth - This field displays the max and min download bandwidth through the WAN port. The default is 0.
- Status - This field displays the status of the rule.
- Modify - Click Modify/Delete to edit/delete the rule.

➢ **To add a Bandwidth control rule:**

1. Click Add New.
2. Enter the information as the figure shown below.



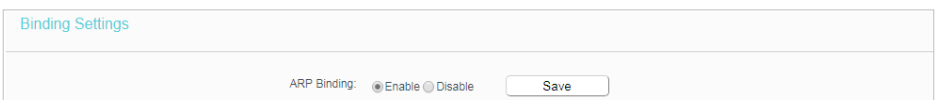
3. Click Save.

4. 12. 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. 12. 1. Binding Settings

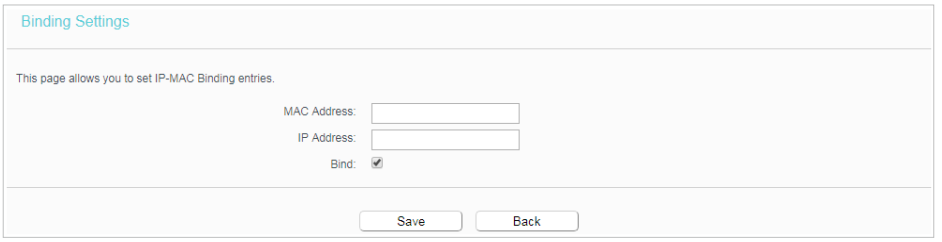
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to IP & MAC Binding > Binding Settings.
3. Select Enable for ARP Binding.



4. Click Save.

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

1. Click Add New.
2. Select the Bind checkbox.



3. Enter the MAC address and IP address.
4. Click Save.

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

1. Select the desired entry in the table.
2. Click Edit or Delete Selected.

4. 12. 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. Error warning will prompt as well. Likewise, Load All only loads the items without interference to the IP & MAC Binding list.

4. 13. Dynamic DNS

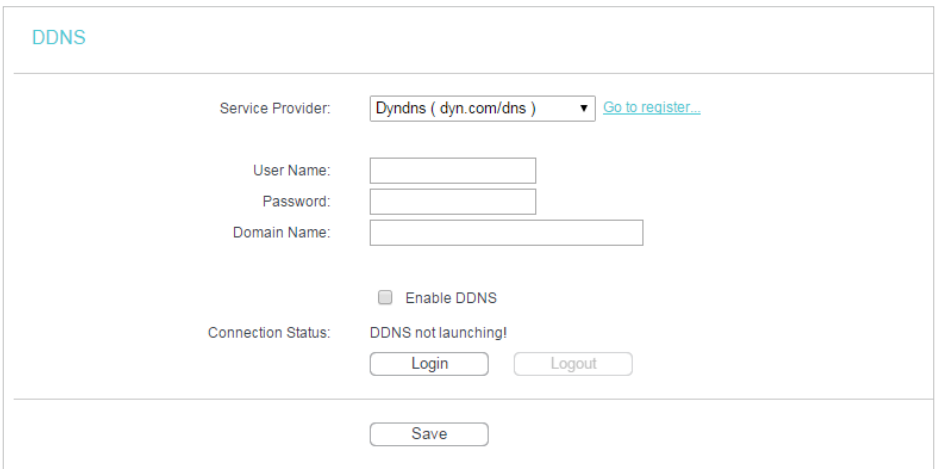
The router offers the DDNS (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address. Thus your friends can connect to your server by entering your domain name no matter what your IP 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:

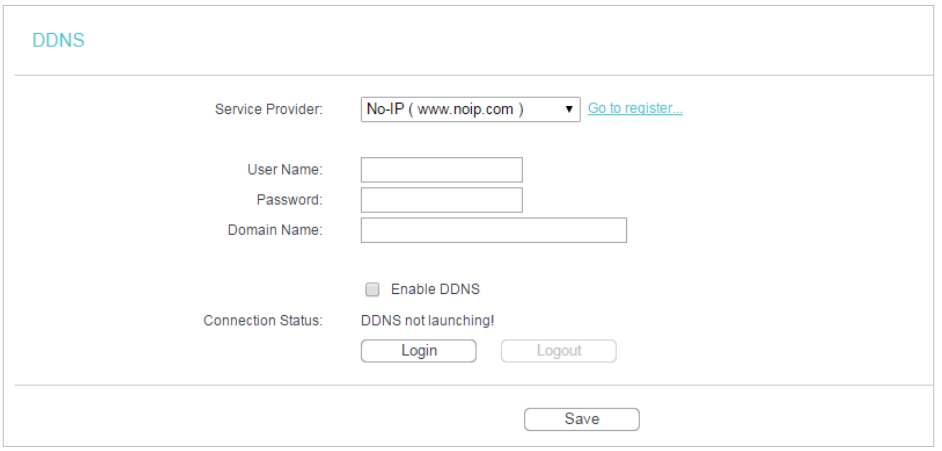
1. Enter the User Name for your DDNS account.
2. Enter the Password for your DDNS account.
3. Enter the Domain Name you received from dynamic DNS service provider here.
4. Select Enable DDNS.
5. Click Login.
6. Click Save.

- 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.



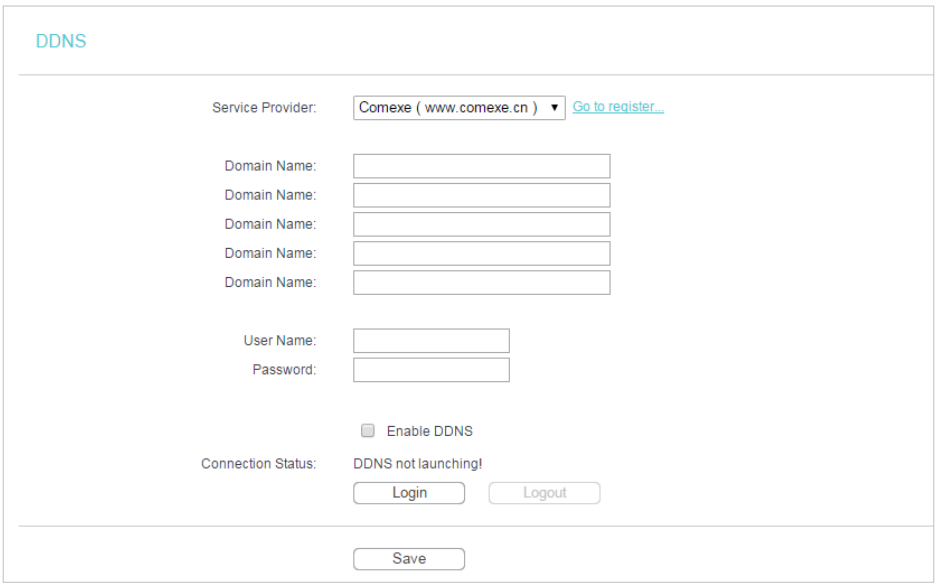
To set up for DDNS, follow these instructions:

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.

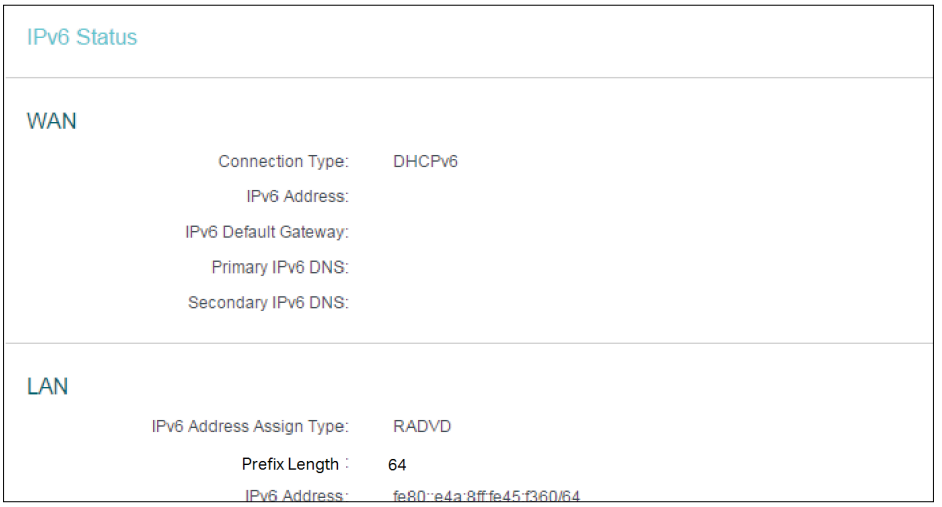
- Connection Status - The status of the DDNS service connection is displayed here.
- Logout - Click Logout to log out of the DDNS service.

4. 14. 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. 14. 1. IPv6 Status

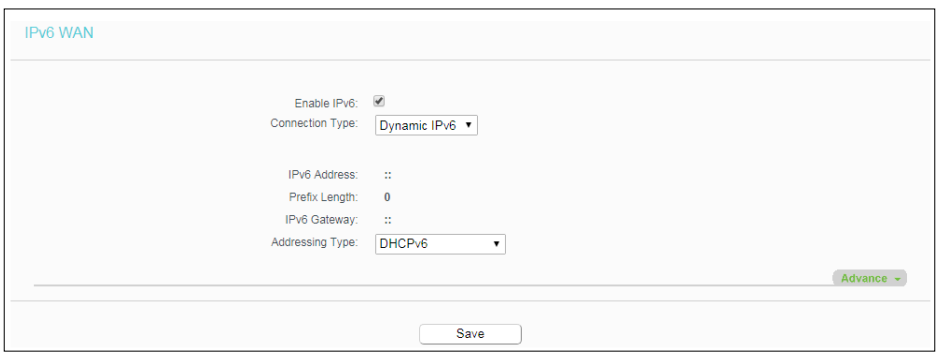
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to IPv6 > IPv6 Status, and you can view the current IPv6 status information of the router.



- WAN - This section shows the current IPv6 information of the router's WAN port, including Connection Type, IPv6 Address information, IPv6 Default Gateway, Primary IPv6 DNS and Secondary IPv6 DNS.
- LAN - This section shows the current IPv6 information of the router's LAN port, including IPv6 Address Assign Type, IPv6 Address and Prefix Length.

4. 14. 2. IPv6 WAN

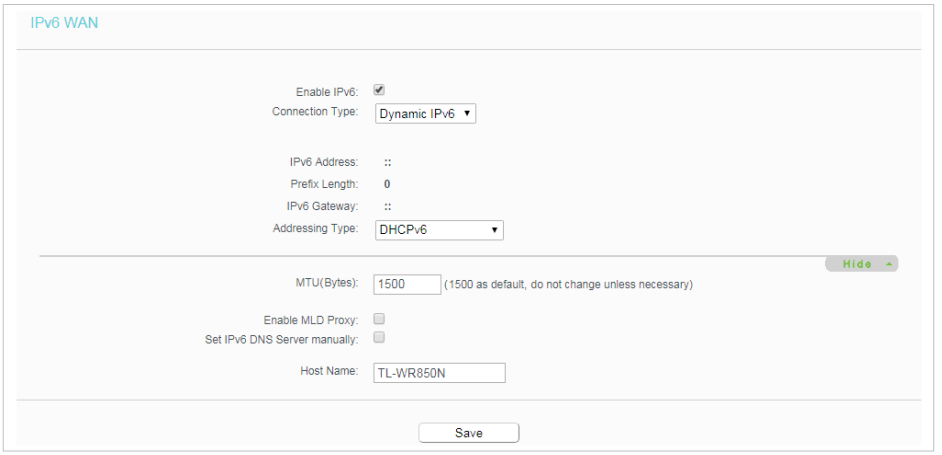
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to IPv6 > IPv6 WAN.
3. Eanble IPv6.



4. Select the WAN Connection Type according to your ISP network topology:
   - 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.

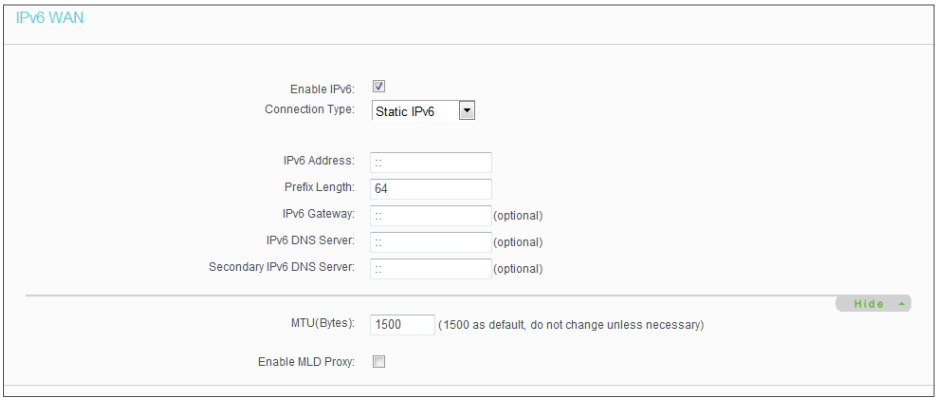
If your ISP gives you one or two DNS IPv6 addresses, select Set IPv6 DNS Server manually and enter the IPv6 DNS Server and Secondary IPv6 DNS Server into the correct fields. Otherwise, the DNS servers will be assigned from ISP dynamically.

- Enable MLD Proxy - Enable the Multicast Listener Discovery (MLD) Proxy function if you need.
- Primary IPv6 DNS - Enter the DNS IPv6 address in colon-hexadecimal notation provided by your ISP.
- Secondary IPv6 DNS - Enter another DNS IPv6 address in colon-hexadecimal notation provided by your ISP.

Note:

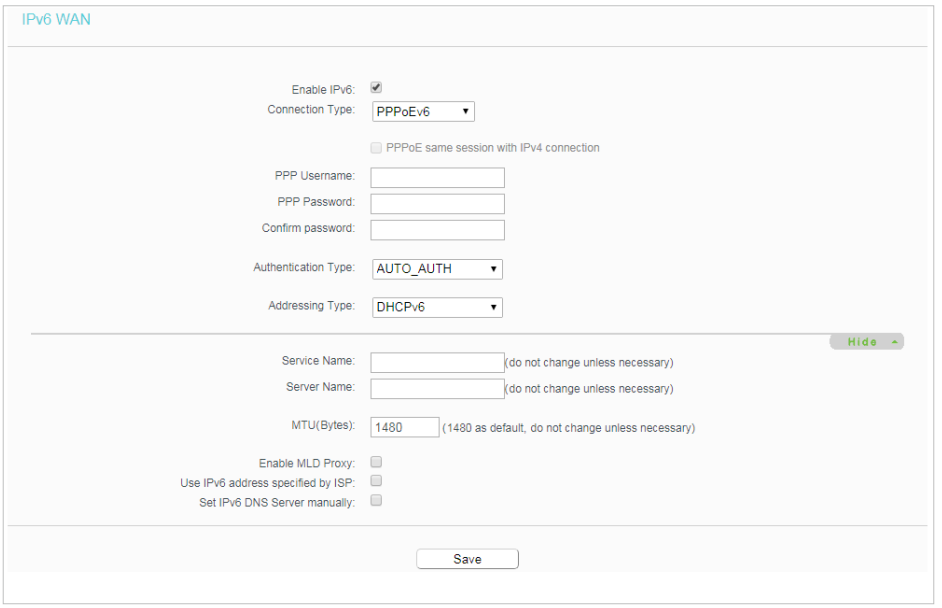
If you get "Address not found error" when you access a web site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

Static IPv6



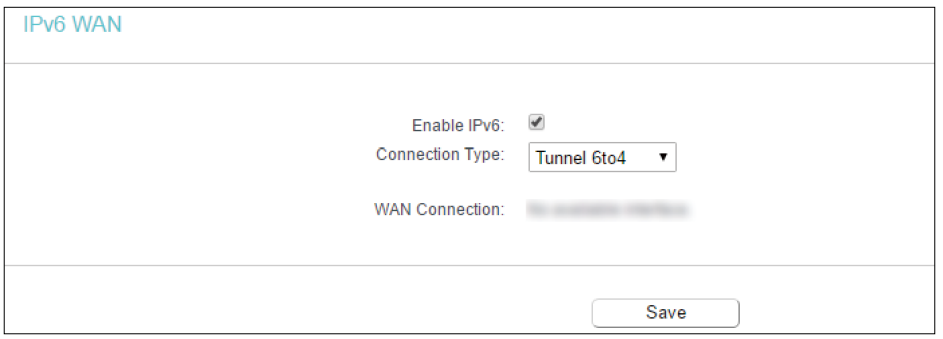
- IPv6 Address - Enter the IPv6 address provided by your ISP.
- Prefix Length - The length of IPv6 address prefix.
- IPv6 Gateway - Enter the default gateway provided by your ISP.
- IPv6 DNS Server - Enter the DNS IPv6 address provided by your ISP.
- Secondary IPv6 DNS Server - Enter another DNS IPv6 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) - 1480 as default, do not change unless necessary.
- 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

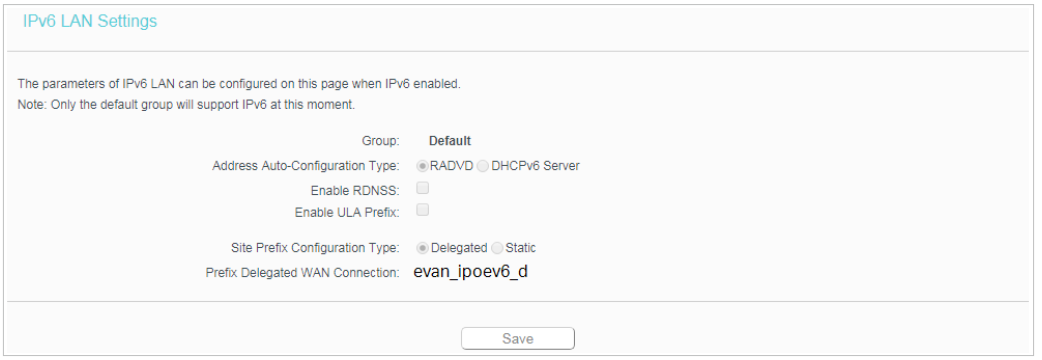


- WAN Connection - Display the available WAN connection.

5. Click Save.

4. 14. 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.



3. Select the Address Autoconfiguration Type which determines the way how the router assigns IPv6 address for PCs on the LAN:
   - Address Autoconfiguration Type - RADAD (Router Advertisement Daemon) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.
   - 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..

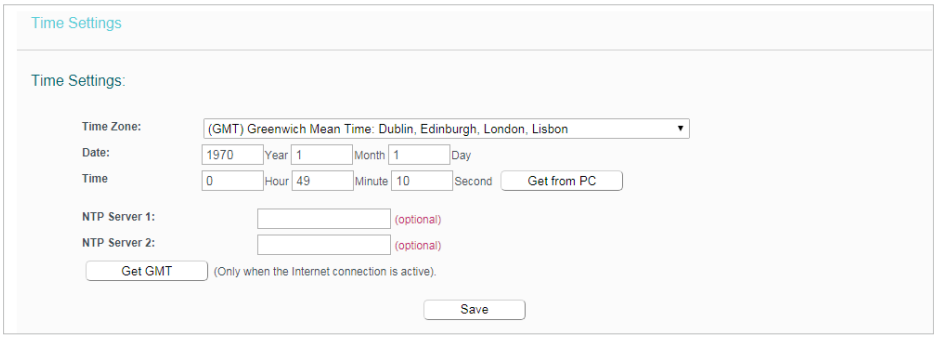
4. Click Save.

4. 15. System Tools

4. 15. 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 I or NTP Server II.
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 DaylightSaving.
2. Select the start time from the drop-down list in the Start field.
3. Select the end time from the drop-down list in the End field.
4. Click Save.

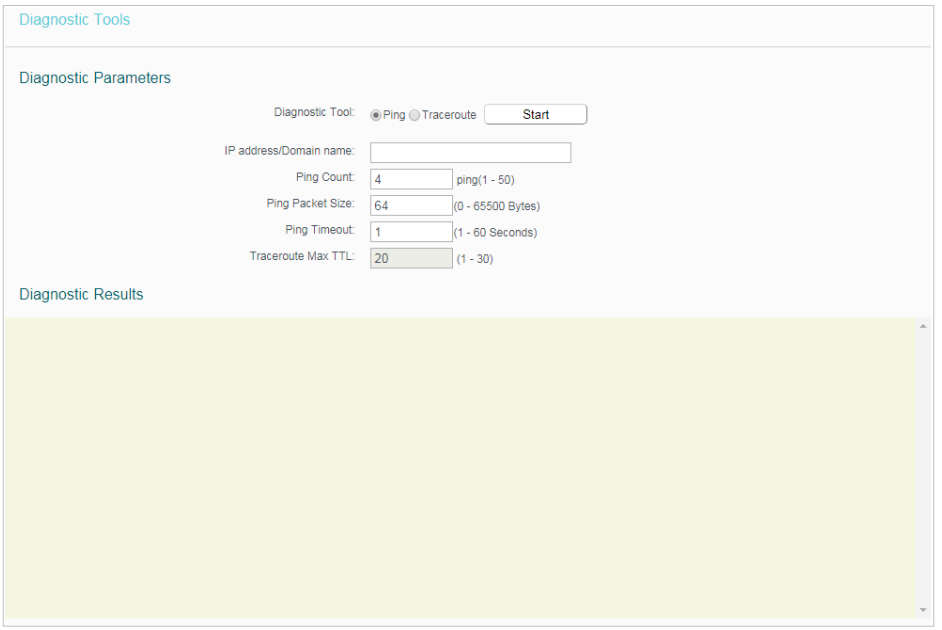
Note:

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. 15. 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.



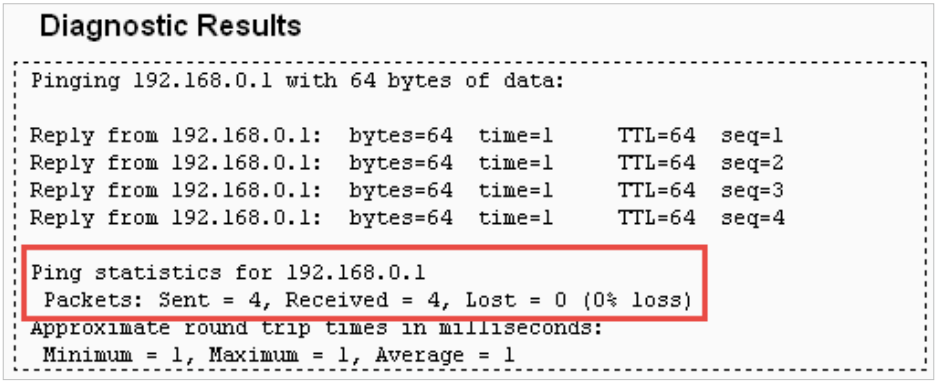
- Diagnostic Tool - Select one diagnostic tool.
  - Ping - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
  - Tracerouter - This diagnostic tool tests the performance of a connection.

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.



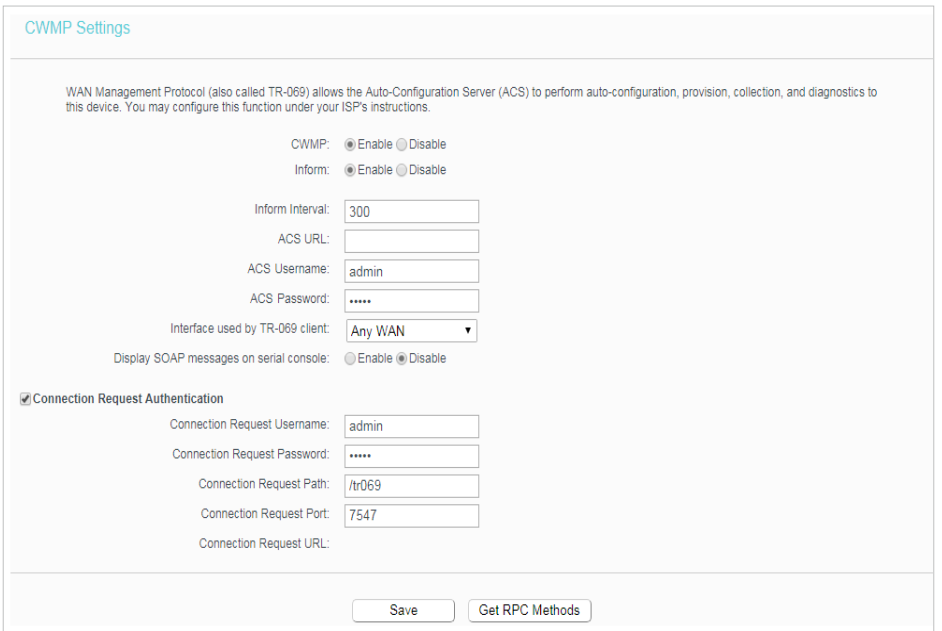
Note:

Only one user can use this tool at one time. Options "Ping Count", "Ping Packet Size" and "Ping Timeout" are used for the Ping function. Option "Traceroute Max TTL" is used for the Tracert function.

4. 15. 3. CWMP Settings

The router offers CWMP feature. The function supports TR-069 protocol which collects information, diagnoses the devices and configures the devices automatically via ACS (Auto-Configuration Server).

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



- CWMP:Enable the CWMP (CPE WAN Management Protocol) feature.
- Inform: Enable this feature to send an Inform message to the ACS (Auto Configuration Server) periodically.
-

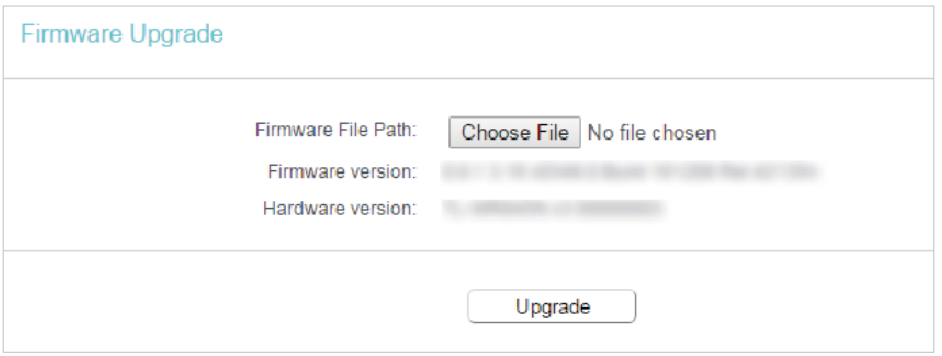
- Inform Interval: Enter the time interval in seconds when the Inform message will be sent to the ACS.
- ACS URL: Enter the web address of the ACS which is provided by your ISP.
- ACS Username/Password: Enter the username/password to log in to the ACS server.
- Interface used by TR-069 client: Select which interface to be used by the TR-069 client.
- Display SOAP messages on serial console: Toggle to enable or disable this feature.
- Connection Request Authentication: Select this checkbox to enable authentication for the connection request.
- Connection Request Username/Password: Enter the username/password for the ACS server to log in to the router.
- Connection Request Path: Connection request path, for an ACS to make a connection request notification to your router(CPE).
- Connection Request Port: Connection request server port, for an ACS to make a connection request notification to your router(CPE).
- Connection Request URL: Connection request url, for an ACS to make a connection request notification to your router(CPE).
- Get RPC methods: Click to get the methods to support CWMP.

3. Click Save.

4. 15. 4. Firmware Upgrade

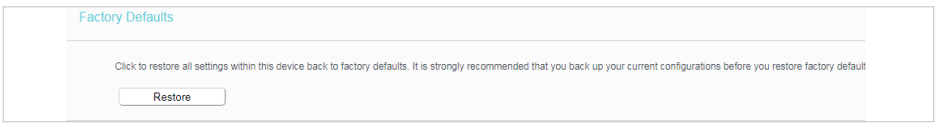
TP-Link is dedicated to improving and richening the product features, giving users a better network experience. We will release the latest firmware at TP-Link official website. You can download the latest firmware file from the Support page of our website www.tp-link.com and upgrade the firmware to the 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. 15. 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.

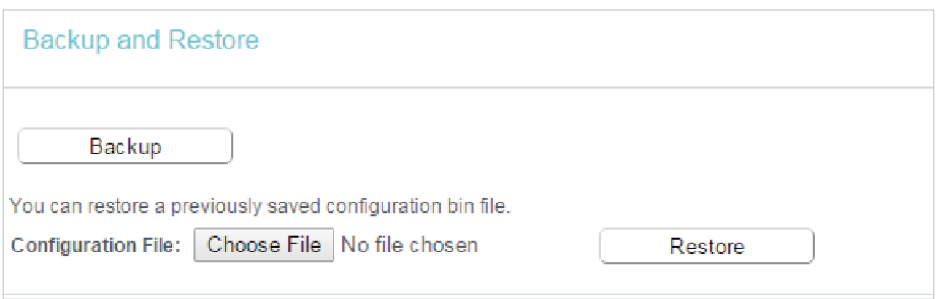


- The default Username: admin
- The default Password: admin
- The default IP Address: 192.168.0.1
- The default Subnet Mask: 255.255.255.0

4. 15. 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:**

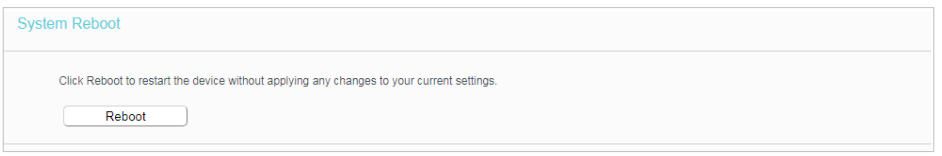
1. Click Choose File to locate the backup configuration file stored in your computer, and click Restore.
2. Wait a few minutes for the restoring and rebooting.

Note:

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

4. 15. 7. Reboot

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

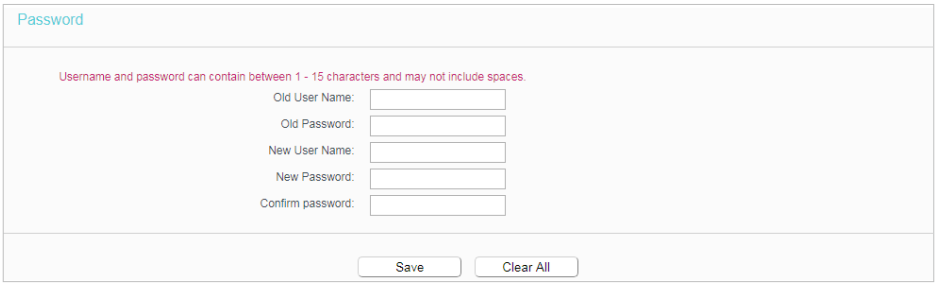


Some settings of the router will take effect only after rebooting, including:

- 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).

4. 15. 8. Password

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



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

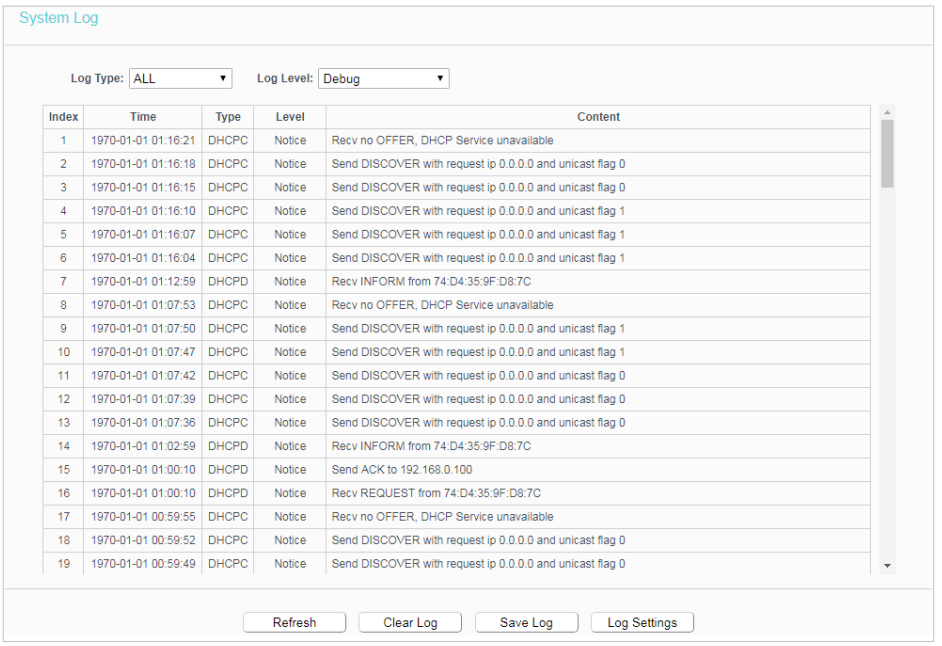
Note:

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

3. Click Save.

4. 15. 9. System Log

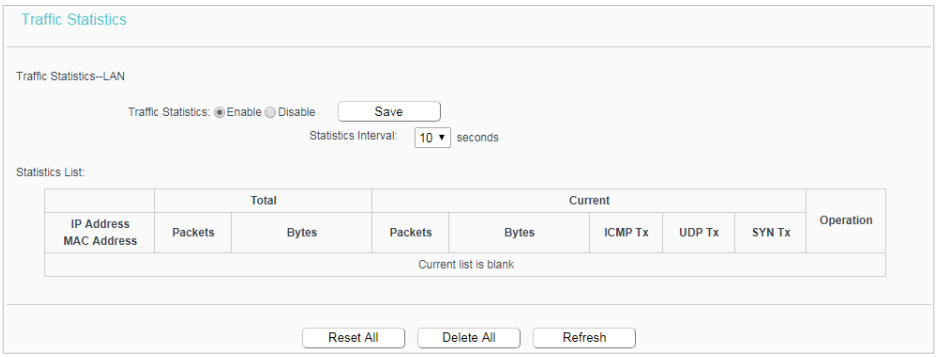
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to System Tools > System Log, and you can view the logs of the router.



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

4. 15. 10. Statistics

1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Go to System Tools > Statistics.
3. Enable Traffic Statistics and click Save to get the network traffic of each PC on the LAN.



IP/MAC Address		The IP and MAC address are displayed with related statistics.
Total	**Packets**	The total number of packets received and transmitted by the router.
	Bytes	The total number of bytes received and transmitted by the router.
Current	**Packets**	The total number of packets received and transmitted in the last Packets Statistic interval seconds.
	Bytes	The total number of bytes received and transmitted in the last Packets Statistic interval seconds.
	ICMP Tx	The number of the ICMP packets transmitted to WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
	UDP Tx	The number of UDP packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
	TCP SYN Tx	The number of TCP SYN packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
Operation	**Reset**	Reset the value of he entry to zero.
	Delete	Delete the existing entry in the table.

4. 16. Log Out

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

FAQ

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

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

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

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

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

If you have altered the username and password but Password Recovery is disabled:

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

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

Q3. What should I do if I cannot access the router's web management page?

1. Please try the methods below to log in again.

- Make sure your computer the has connected to the router correctly and the corresponding LED light up.
- Make sure the IP address of your computer is configured as Obtain an IP address automatically and Obtain DNS server address automatically.

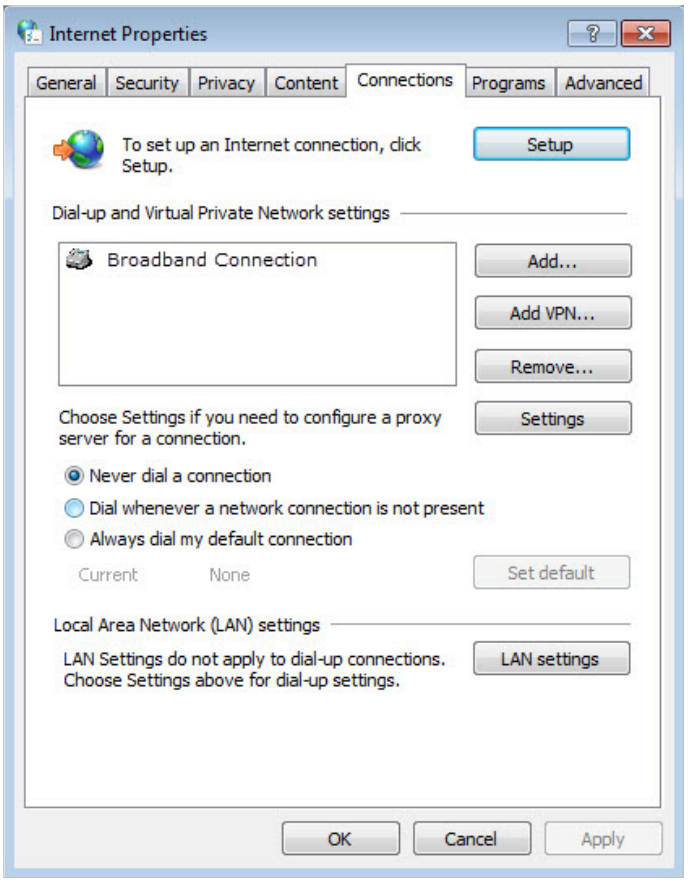
2. Make sure you enter the correct IP address to log in: http://tplinkwifi.net.

- Check your computer's settings:

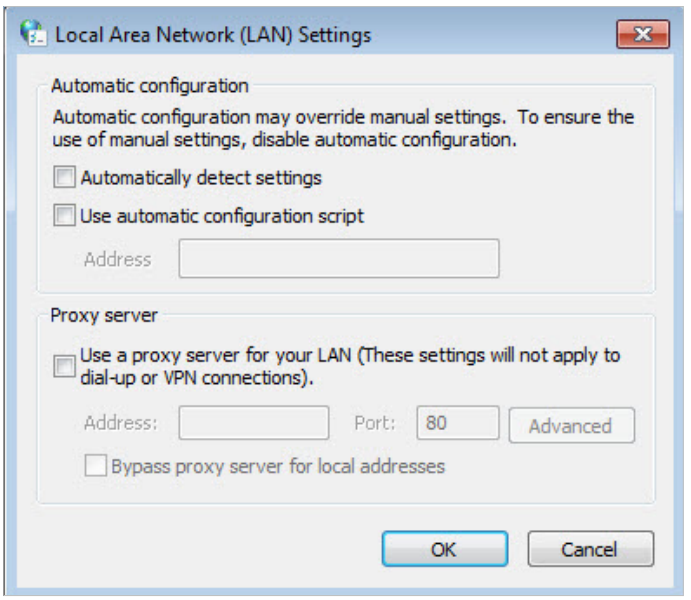
3. Go to Start > Control Panel > Network and Internet, and click View network status and tasks.

   1) Click Internet Options on the bottom left.

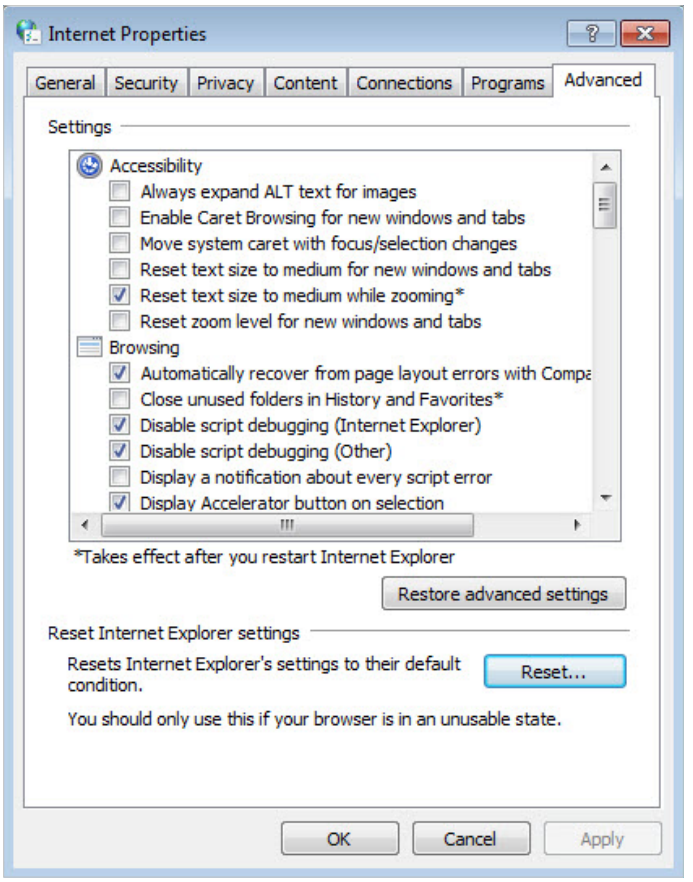
   2) Click Connections and select Never dial a connection.



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



4) Go to Advanced > Restore advanced settings, and click OK to save the settings.



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

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

Q4. How do I use the WDS Bridging function to extend my wireless network?

For example, my house covers a large area. The wireless coverage of the router I'm using (the root router) is limited. I want to use an extended router to extend the wireless network of the root router.

Note:

- WDS bridging only requires configuration on the extended router.

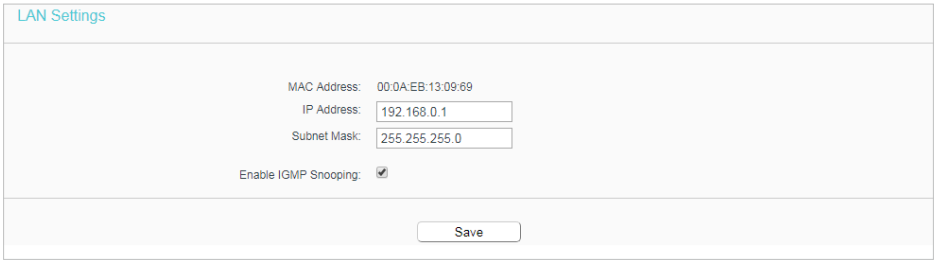
1. Visit http://tplinkwifi.net, and log in with the username and password you set for the router.
2. Configure the IP address of the router:

   1) Go to Network > LAN, configure the IP address of the extended router to be in the same subnet with the root router; (For example, the IP address of the root router is

192.168.0.1, the IP address of the extended router can be 192.168.0.2~192.168.0.254. We take 192.168.0.2 as example.)

2) Click Save.

Note: Log in to the web management page again if the IP address of the router is altered.



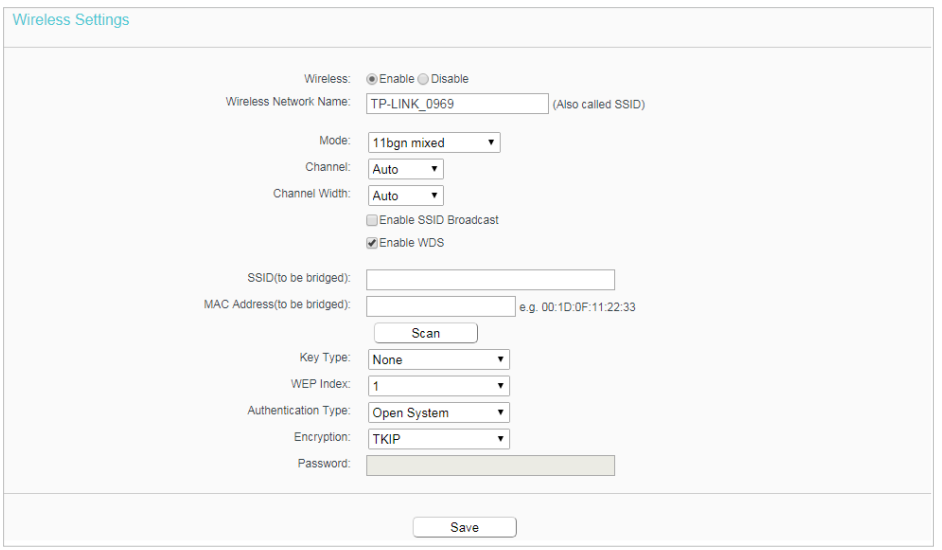
3. Survey the SSID to be bridged:

1) Go to Wireless > Basic Settings and click Enable WDS .

2) Click Scan, locate the root router's SSID and click Choose (Here we take TP-Link_2512 as example).

3) If the root router is set with a wireless password, you should enter the wireless password of the root router.

4) Click Save.



4. Disable DHCP:

1) Go to DHCP, select Disable, and click Save.

Now you can go to Status to check the WDS status. When the WDS status is Run, it means WDS bridging is successfully built.

Q5. What should I do if I cannot access the internet even though the configuration is finished?

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

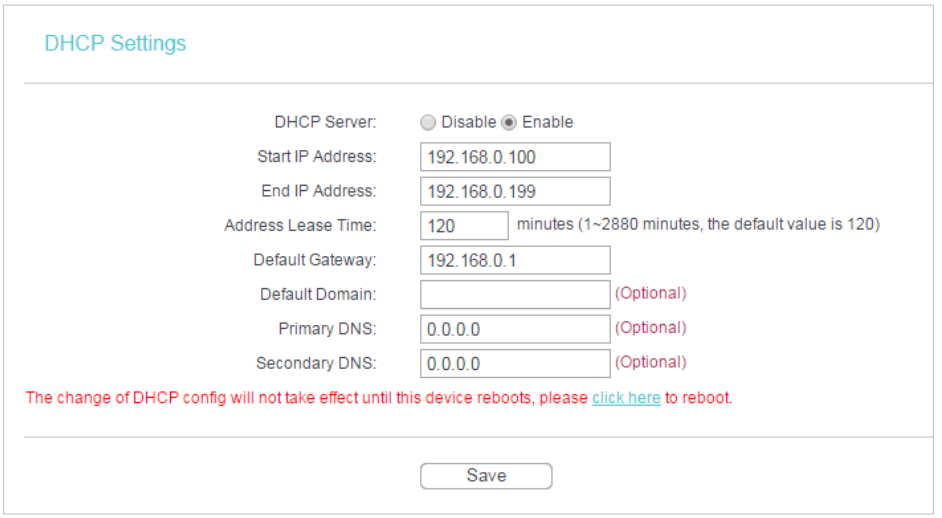
If IP Address is a valid one, please try the methods below and try again:

- Your computer might not recognize any DNS server addresses, please manually configure DNS server.

  1) Go to DHCP.

  2) Enter 8.8.8.8 as Primary DNS, and click Save.

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



- Restart the modem and the router.

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

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

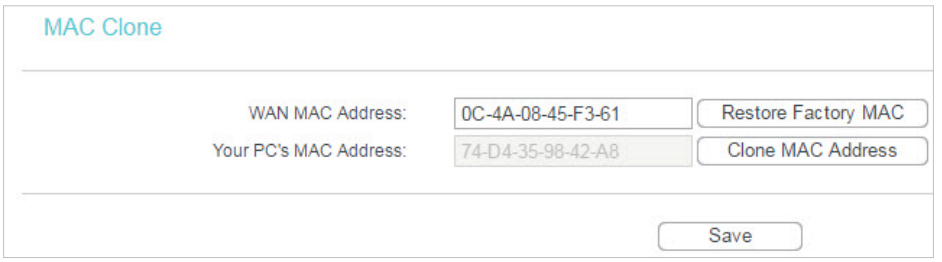
  3) Power on the router, and wait another 1 or 2 minutes and check the internet access.
- Reset the router to factory default settings and reconfigure the router.
- Upgrade the firmware of the router.
- Check the TCP/IP settings on the particular device if all other devices can get internet from the router.

If the IP Address is 0.0.0.0, please try the methods below and try again:

- Make sure the physical connection between the router and the modem is proper.
- Clone the MAC address of your computer.

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

2) Go to Network > MAC Clone, select Clone MAC Address and click Save.



Tips:

- Some ISPs will register the MAC address of your computer when you access the internet for the first time through their Cable modem, if you add a router into your network to share your internet connection, the ISP will not accept it as the MAC address is changed, so we need to clone your computer's MAC address to the router.
- The MAC addresses of a computer in wired connection and wireless connection are different.

- Modify the LAN IP address of the router.

Note:

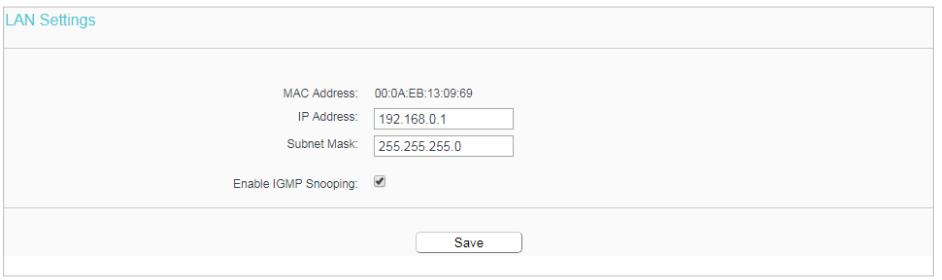
Most TP-Link routers use 192.168.0.1/192.168.1.1 as their default LAN IP address, it may conflict with the IP range of your existent ADSL modem/router. If so, the router is not able to communicate with your modem and cause you can't access the internet. To resolve this problem, we need to change the LAN IP address of the router to avoid such conflict, for example, 192.168.2.1.

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

2) Go to Network > LAN.

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

4) Click Save.



- Restart the modem and the router.

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

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

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

- Double check the internet Connection Type.

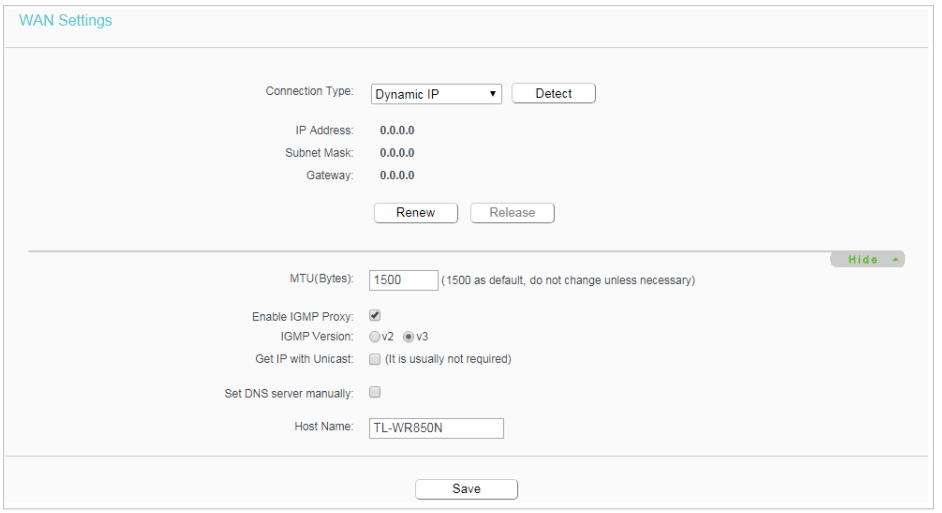
1) Confirm your internet Connection Type, which can be learned from the ISP.

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

3) Go to Network > WAN.

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

5) Click Save.



6) Restart the modem and the router.

- Please upgrade the firmware of the router.

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

Q6. What should I do if I cannot find my wireless network or I cannot connect the wireless network?

If you fail to find any wireless network, please follow the steps below:

- Make sure the wireless function of your device is enabled if you're using a laptop with a built-in wireless adapter. You can refer to the relevant document or contact the laptop manufacturer.
- Make sure the wireless adapter driver is installed successfully and the wireless adapter is enabled.
  - **On Windows 7**

  1) If you see the message No connections are available, it is usually because the wireless function is disabled or blocked somehow.

  2) Clicking Troubleshoot and windows might be able to fix the problem by itself.
  - **On Windows XP**

1) If you see the message Windows cannot configure this wireless connection, this is usually because windows configuration utility is disabled or you are running another wireless configuration tool to connect the wireless.

2) Exit the wireless configuration tool (the TP-Link Utility, for example).

3) Select and right click My Computer on Desktop, and select Manage to open Computer Management window.

4) Expand Services and Applications > Services, and find and locate Wireless Zero Configuration in the Services list on the right side.

5) Right click Wireless Zero Configuration, and then select Properties.

6) Change Startup type to Automatic, click Start and make sure the Service status is Started. And then click OK.

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

- Check the WLAN LED indicator on your wireless router/modem.
- Make sure your computer/device is still in the range of your router/modem. Move closer if it is currently too far away.

If you can find your wireless network but fail to connect, please follow the steps below:

- **Authenticating problem/password mismatch:**

1) Sometimes you will be asked to type in a PIN number when you connect to the wireless network for the first time. This PIN number is different from the Wireless Password/ Network Security Key. Usually you can only find it on the label of your router.

2) If you cannot find the PIN or PIN failed, you may choose Connecting using a security key instead, and then type in the Wireless Password/Network Security Key.

3) If it continues to show note of Network Security Key Mismatch, it is suggested to confirm the wireless password of your wireless router.

Note: Wireless Password/Network Security Key is case sensitive.

- **Windows unable to connect to XXXX / Can not join this network / Taking longer than usual to connect to this network:**

- Check the wireless signal strength of your network, if it is weak (1~3 bars), please move the router closer and try again.
- Change the wireless Channel of the router to 1, 6, or 11 to reduce interference from other networks.
- Re-install or update the driver for your wireless adapter of the computer.

COPYRIGHT & TRADEMARKS

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

FCC STATEMENT

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

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

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

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

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

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

FCC RF Radiation Exposure Statement

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

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

CE Mark Warning

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(the maximum transmitted power)

2412MHz—2472MHz(20dBm)

5180MHz—5240MHz(23dBm)

EU declaration of conformity

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

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

RF Exposure Information

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

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

Restricted to indoor use.

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

EAC

Safety Information

- Keep the device away from water, fire, humidity or hot environments.
- Do not attempt to disassemble, repair, or modify the device.
- Do not use damaged charger or USB cable to charge the device.
- Do not use any other chargers than those recommended
- Do not use the device where wireless devices are not allowed.
- Adapter shall be installed near the equipment and shall be easily accessible.
- Use only power supplies which are provided by manufacturer and in the original packing of this product. If you have any questions, please don't hesitate to contact us.

Please read and follow the above safety information when operating the device. We cannot guarantee that no accidents or damage will occur due to improper use of the device. Please use this product with care and operate at your own risk.

For EU/EFTA, this product can be used in the following countries:

AT	BE	BG	CH	CY	CZ	DE	DK
EE	EL	ES	FI	FR	HR	HU	IE
IS	IT	LI	LT	LU	LV	MT	NL
NO	PL	PT	RO	SE	SI	SK	UK

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.

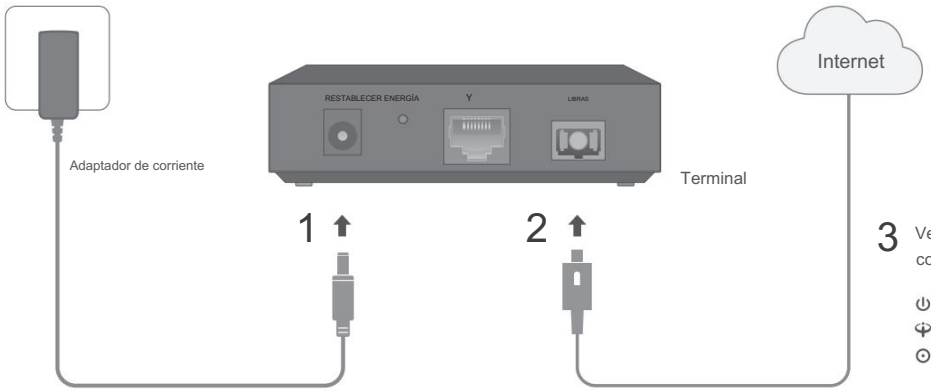
tp-link

Guía de Instalación Rápida

Terminal GPON Gigabit de 1 puerto

XZ000-G3

Conecte el hardware



3 Verifique que la conexión del hardware sea correcta verificando estos LED.

- Encendido
- PON: encendido o parpadeando
- LOS: Off

Registrar la Terminal

Si el LED PON está fijo, pase a Conectarse a Internet.

1 Conecte su computadora al Terminal mediante un cable Ethernet.

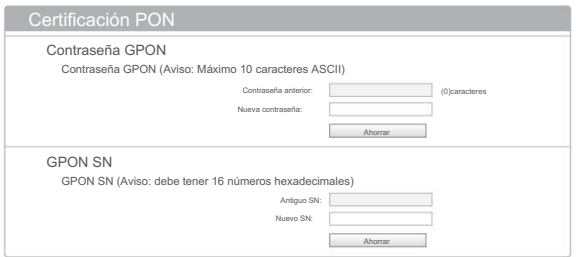
2 Configure las propiedades de TCP/IP manualmente en su computadora.

Si la dirección IP LAN de la terminal es 192.168.1.1, escriba la dirección IP 192.168.1.x (x es de 2 a 253), máscara de subred 255.255.255.0 y puerta de enlace predeterminada 192.168.1.1.

3 Registre el Terminal a través de un navegador web.

A Inicie un navegador web y escriba http://192.168.1.1 en la barra de direcciones. Utilice admin tanto para el nombre de usuario como para la contraseña para iniciar sesión en la Terminal.

B Vaya a Configuración de red > Certificación PON. Introducir el Contraseña GPON y/o SN GPON proporcionada por su ISP (Proveedor de Servicios de Internet) para registrar el Terminal y haga clic en Guardar.



Conectar a internet

Establezca su conexión a Internet de acuerdo con las instrucciones de su ISP.

Nota: Si necesita ayuda, comuníquese con su ISP.

¡Disfrutar!

Indicadores LED

CONDUJO	Estado	Indicación
(Fuerza)	En	La energía está encendida.
	Apagado	No hay energía.
(PON)	Verde encendido	La Terminal está registrada en la OLT y funciona en modo Puente, o la Terminal no tiene conexión a Internet.
	Azul encendido	Conexión a Internet establecida.
	Verde intermitente	La Terminal está intentando registrarse con la OLT.
	Apagado	La Terminal no está registrada en la OLT.
(LOS)	En	No se recibe ninguna señal óptica.
	Brillante	La señal recibida es demasiado débil.
	Apagado	El Terminal está recibiendo la señal óptica correctamente.
(Y)	En	Hay un dispositivo conectado al puerto LAN.
	Brillante	El puerto LAN está transmitiendo o recibiendo datos.
	Apagado	No hay ningún dispositivo conectado al puerto LAN.

¿Necesitas ayuda?

P1. ¿Qué debo hacer si no puedo acceder a la página de administración web?

A1. Asegúrese de que la computadora esté correctamente conectada al Terminal mediante el cable Ethernet.
A2. Asegúrese de que haya una dirección IP configurada para la computadora conectada al Terminal.
A3. Asegúrese de que http://192.168.1.1 esté ingresado correctamente o utilice otro navegador web e inténtelo nuevamente.
A4. Deshabilite y luego habilite el adaptador de red que se está utilizando.
A5. Restaure el Terminal a su configuración predeterminada de fábrica y reconfigure su Terminal siguiendo las instrucciones de esta Guía de instalación rápida.

P2. ¿Qué debo hacer si no puedo acceder a Internet?

A1. Asegúrese de que todos los cables estén conectados de forma adecuada y segura al Terminal.
A2. Verifique el LED PON y asegúrese de que esté encendido en azul y estable, lo que indica que Internet se establece la conexión. De lo contrario, asegúrese de que la contraseña GPON proporcionada y/o GPON SN se ingresan correctamente en la página Configuración de red > Certificación PON.
A3. Desenchufe y vuelva a conectar el cable de fibra al Terminal. Espere 2 minutos y vuelva a intentarlo.
A4. Asegúrese de seguir las instrucciones específicas de su ISP para conectarse a Internet.
A5. Asegúrese de que la computadora esté conectada a la Terminal.
A6. Comuníquese con su ISP si el problema persiste.

P3. ¿Cómo restauro mi Terminal a su configuración predeterminada de fábrica?

A. Con el Terminal encendido, presione y mantenga presionado el botón RESET en el panel posterior del Terminal. durante al menos 5 segundos y luego suelte el botón. La Terminal se restaurará y reiniciará automáticamente.

Declaración de conformidad de la UE

TP-Link declara por la presente que el dispositivo cumple con los requisitos esenciales y otras disposiciones relevantes de las directivas 2014/30/UE, 2014/35/UE, 2009/125/CE, 2011/65/UE y (UE)2015/ 863.
La Declaración de conformidad de la UE original se puede encontrar en https://www.tp-link.com/en/support/ce/

Declaración de conformidad del Reino Unido

TP-Link declara por la presente que el dispositivo cumple con los requisitos esenciales y otras disposiciones relevantes del Reglamento de Compatibilidad Electromagnética de 2016 y Equipos Eléctricos (Seguridad). Reglamento 2016.
La Declaración de conformidad original del Reino Unido se puede encontrar en https://www.tp-link.com/support/ukca

Información de seguridad

- Mantenga el dispositivo alejado del agua, fuego, humedad o ambientes calurosos.
- No intente desmontar, reparar ni modificar el dispositivo. Si necesita servicio, por favor contáctenos.
- No utilice un cargador o cable USB dañado para cargar el dispositivo.
- No utilice ningún otro cargador que los recomendados.
- El adaptador se instalará cerca del equipo y será de fácil acceso.

UBIQUITI®
NETWORKS

LiteBeam® AC GEN2

5 GHz airMAX® ac Radio with
InnerFeed® Technology

Model: LBE-5AC-Gen2

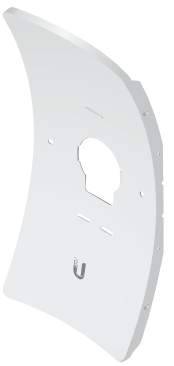
QUICK START GUIDE

Introduction

Thank you for purchasing the Ubiquiti Networks® LiteBeam® 5AC Gen 2 radio. This Quick Start Guide is designed to guide you through installation and also includes warranty terms.

Package Contents

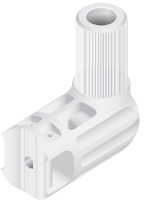
Antenna Feed



Center Reflector Panel

Side Reflector Panels (Qty. 2)

Feed Receiver



Azimuth Mount

Elevation Mount

Metal Strap

Wingnut Kit

Gigabit PoE* (24V, 0.3A) with Mounting Bracket

Power Cord*

Quick Start Guide

* Included only in the single-pack of the LBE-5AC-Gen2.

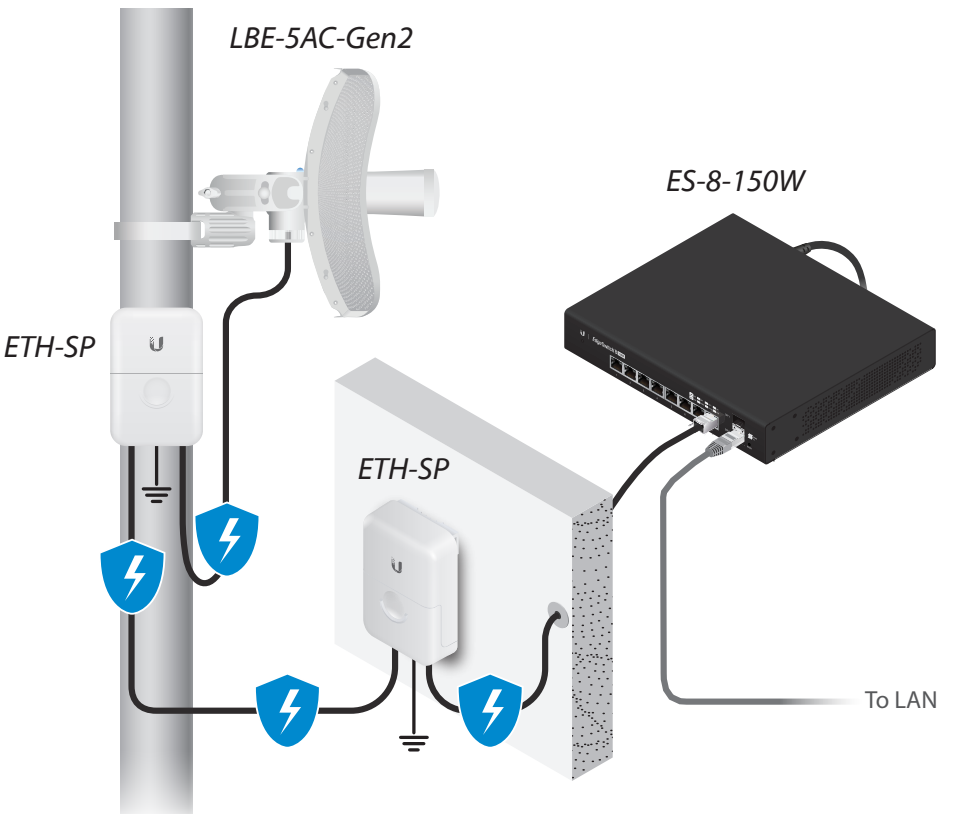
Products may be different from pictures and are subject to change without notice.

TERMS OF USE: Ubiquiti radio devices must be professionally installed. Shielded Ethernet cable and earth grounding must be used as conditions of product warranty. TOUGHCable™ is designed for outdoor installations. It is the professional installer's responsibility to follow local country regulations, including operation within legal frequency channels, output power, and Dynamic Frequency Selection (DFS) requirements.

Installation Requirements

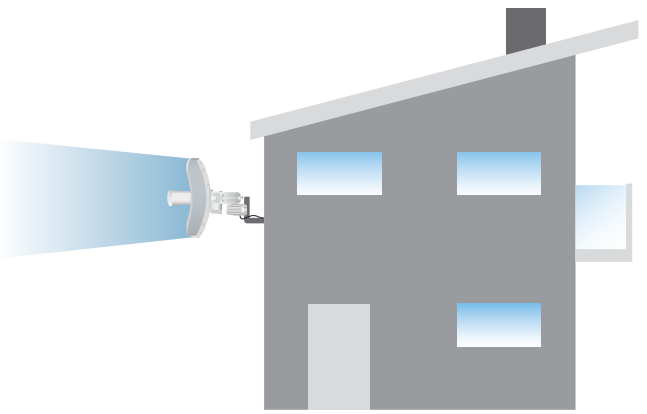
- 7 mm socket wrench or screwdriver
- Shielded Category 5 (or above) cabling with drain wire should be used for all wired Ethernet connections and should be grounded through the AC ground of the PoE.

  We recommend that you protect your networks from harmful outdoor environments and destructive ESD events with industrial-grade, shielded Ethernet cable from Ubiquiti Networks. For more details, visit **www.ubnt.com/toughcable**
- Surge protection should be used for all outdoor installations. We recommend that you use two Ethernet Surge Protectors, model ETH-SP, one near the LiteBeam and the other at the entry point to the building. The ETH-SP will absorb power surges and safely discharge them into the ground.

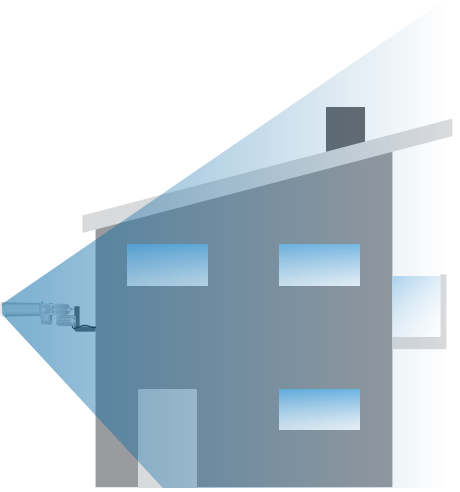


Application Examples

The LiteBeam AC mounted outdoors with the reflector installed provides directional outdoor coverage (gain reflector-dependent).



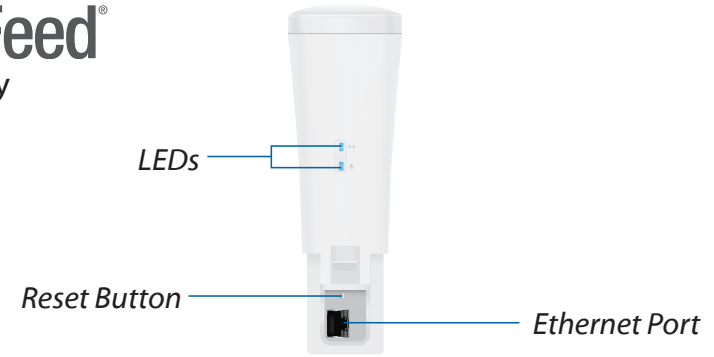
The LiteBeam AC mounted outdoors without the reflector installed provides outdoor-to-indoor coverage using the 3 dBi *Antenna Feed* only.



Hardware Overview

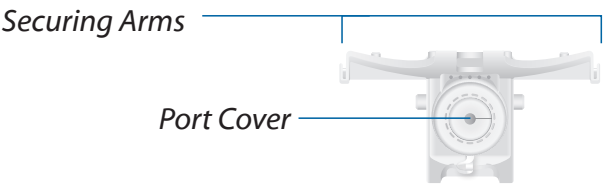
Bottom View

InnerFeed®
Technology

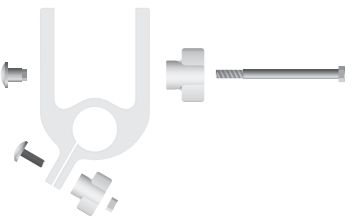


Antenna Feed

Reflector Assembly



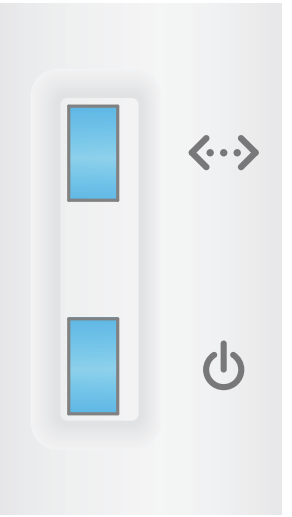
Feed Receiver



Elevation Mount

Azimuth Mount

LEDs



Ethernet The LED will light steady blue when an active Ethernet connection is made and flash when there is activity.

Power The LED will light blue when the device is connected to a power source.

Button

Reset To reset to factory defaults, press and hold the *Reset* button for more than 10 seconds while the LiteBeam AC is powered on. The LiteBeam AC may also be reset remotely using the auxiliary *Reset* button located on the bottom of the *Gigabit PoE* adapter.

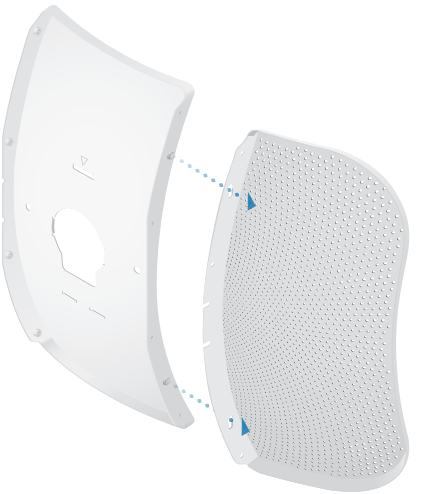
Port

Ethernet Supports 10/100/1000 connections and passive PoE. This port should be connected to the LAN and DHCP server.

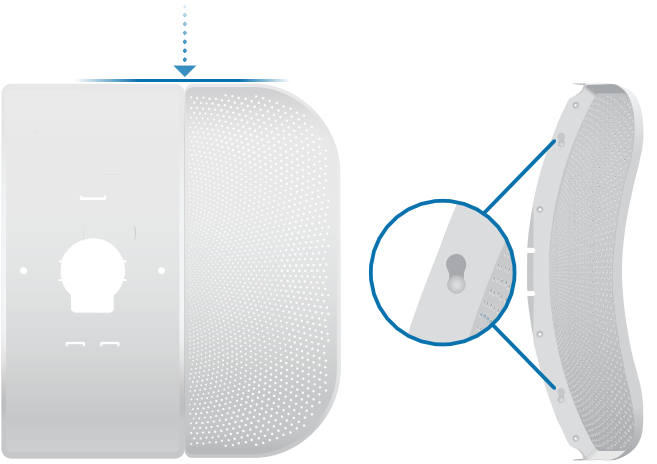
Hardware Installation

The LiteBeam AC was designed for outdoor use and quick mounting on a pole.

1. Assemble the antenna reflector by attaching the *Side Reflector Panels* to the *Center Reflector Panel*:
   a. Insert the heads of the two mounting studs on the *Center Reflector Panel* into the large opening of the slotted holes of the *Side Reflector Panel*.

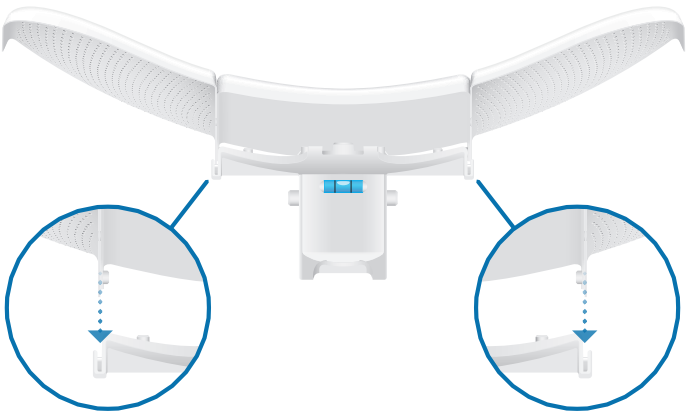


   b. Slide the *Side Reflector Panel* down until the top edges of the panels align. The *Side Reflector Panel* is captured when both heads of the mounting studs are positioned over the narrow opening of the slotted holes.



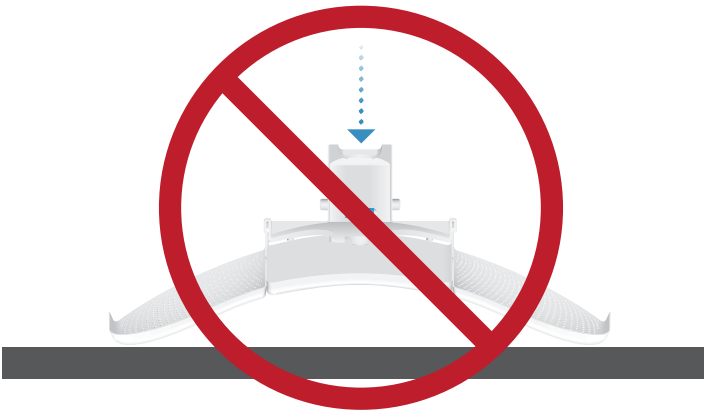
   c. Repeat the assembly for the other *Side Reflector Panel*.

2. Hold the reflector assembly by hand (do not use a tabletop or flat surface) and insert the *Feed Receiver* into the reflector assembly to secure the panels:
   a. Align the arrows on the *Center Reflector Panel* and the *Feed Receiver,* and insert both edges of the *Side Reflector Panels* and *Center Reflector Panels* into the *Securing Arms* of the *Feed Receiver.*

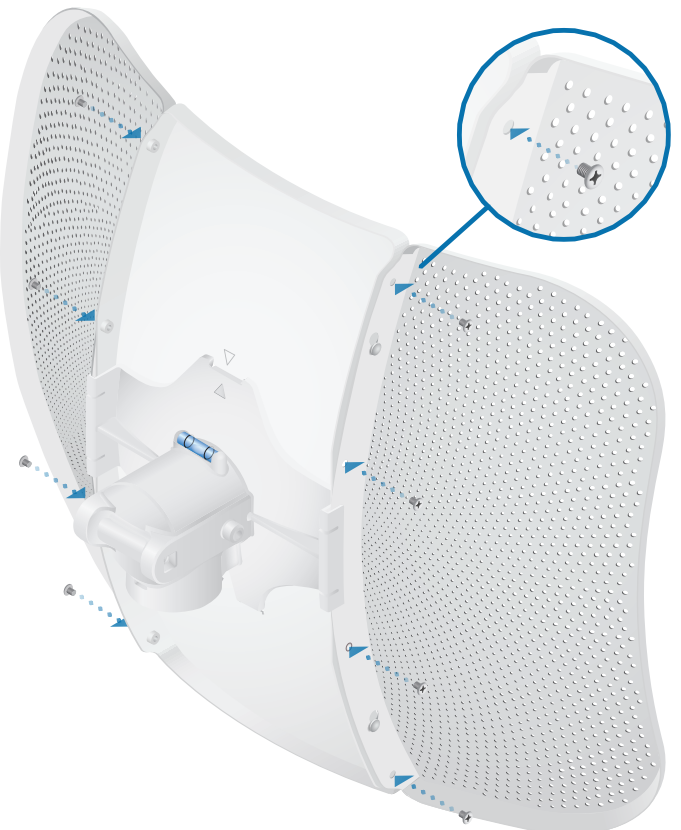


   b. Insert the *Feed Receiver* into the *Center Reflector Panel* by pressing the top and bottom snap hooks into the slots of the *Center Reflector Panel.*

WARNING: Do not install the *Feed Receiver* into the reflector assembly by pushing down onto a tabletop or other flat surface as this can deform the panels. Hold the reflector assembly by hand.

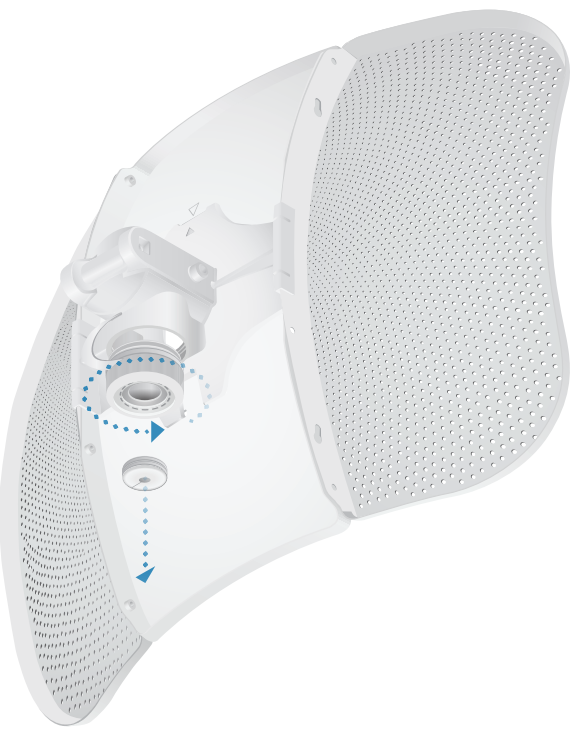


c. For additional support, there are eight machine screws that secure the *Side Reflector Panels* to the antenna assembly.



3. Insert the *Antenna Feed* into the *Feed Receiver* until the feed locks into place.

4. Turn the *Port Cover* counterclockwise to reveal the *Ethernet Port* on the *Antenna Feed*.



5. Take one end of an Ethernet cable and push it through the rubber housing on the *Port Cover* and connect it to the *Ethernet Port*.

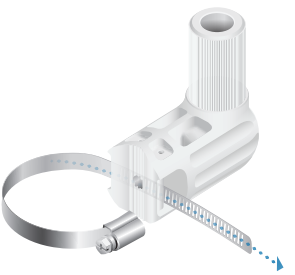
6. Reattach the *Port Cover* to the *Feed Receiver* by turning it clockwise until it is secure.

Pole Mounting

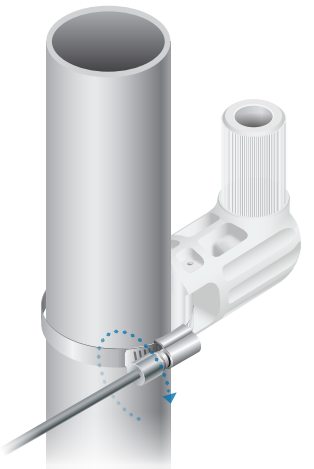
1. Attach the *Elevation Mount* to the *Feed Receiver* by lining up the notches with the pins on the *Feed Receiver* and pressing forward until the *Elevation Mount* snaps on.

2. Using the *Wingnut Kit*, install the carriage bolt and hex head cap through the *Elevation Mount* and loosely fasten the carriage nut and nylock nut.

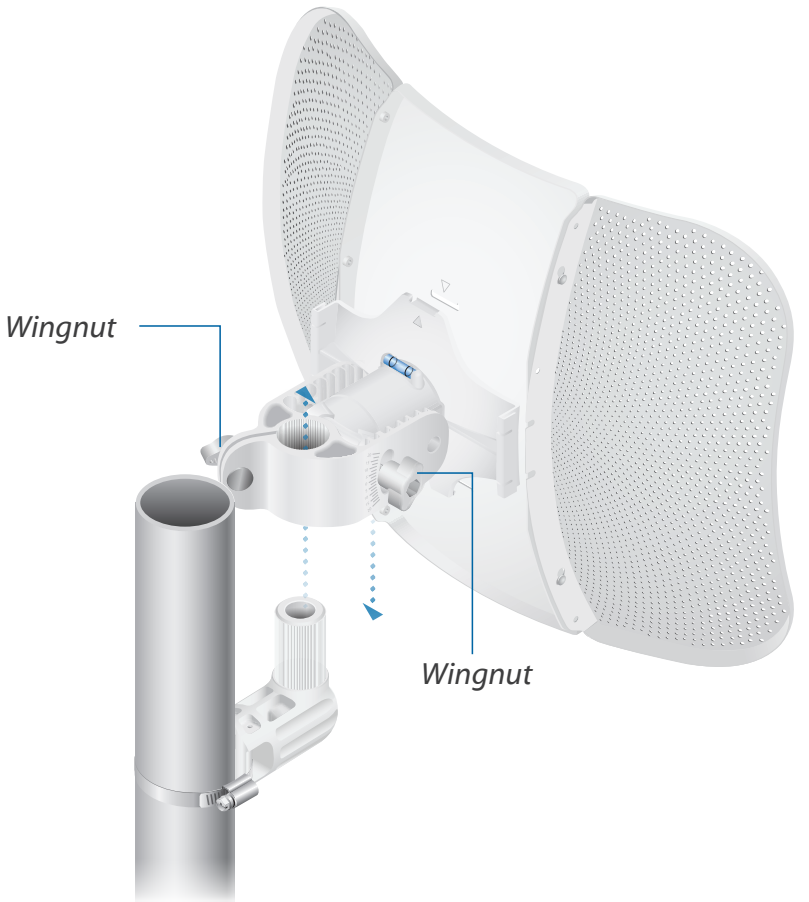
3. Open the *Metal Strap* and feed it through the slot of the *Azimuth Mount*.



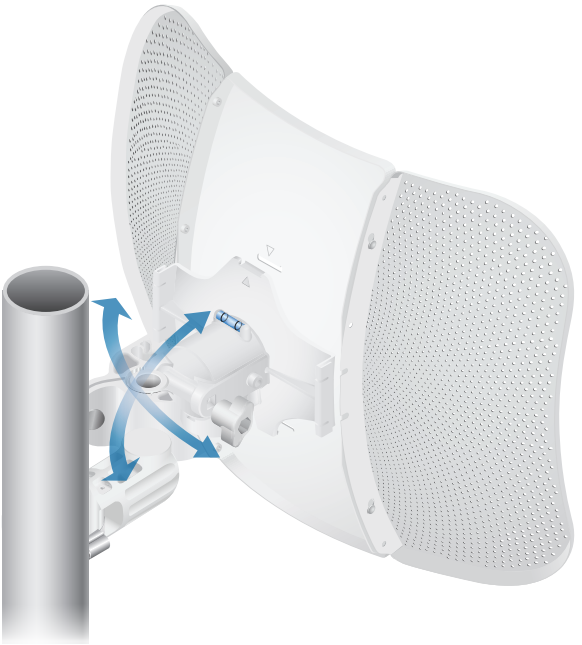
4. Wrap the *Metal Strap* around the pole. Use a 7 mm socket wrench or screwdriver to turn the screw clockwise and securely fasten the strap to the pole.



5. Attach the *Elevation Mount* to the *Azimuth Mount* as shown below. Do not tighten the *Wingnuts* completely until the LiteBeam assembly has been adjusted and aimed properly.



6. Aim the LiteBeam toward the other end of the wireless link. Use the bubble level on the back of the *Feed Receiver* to ensure proper level alignment.



7. Lock the aim by hand-tightening the *Wingnuts* clockwise on both the *Elevation Mount* and the *Azimuth Mount*.

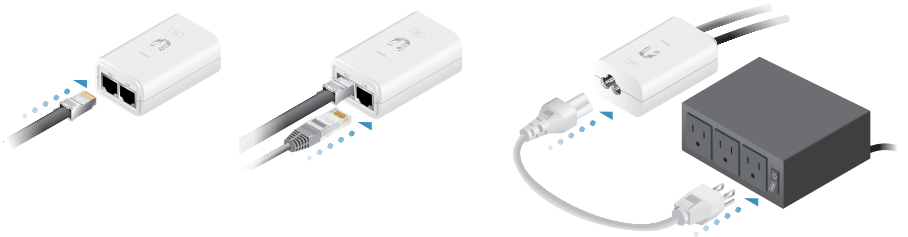
Connect the power using one of the following options:

- Using the included *Gigabit PoE Adapter*: Go to *Connecting to the PoE Adapter*.
- Using a separate PoE switch: Connect the Ethernet cable from the LiteBeam's *Ethernet* port to a PoE-enabled Ethernet port on the switch.

  WARNING: The switch port must comply with the power specifications listed in the *Specifications* section of this Quick Start Guide.

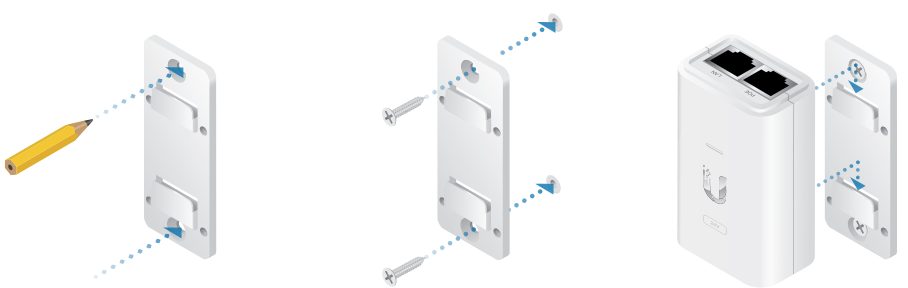
Connecting to the PoE Adapter

1. Connect the Ethernet cable from the LiteBeam AC to the **POE** port on the *Power Adapter.*
2. Connect an Ethernet cable from your LAN to the **LAN** port on the *Power Adapter.*
3. Connect the *Power Cord* to the *Power Adapter,* and then plug the *Power Cord* to a power outlet.



Mounting the PoE Adapter (Optional)

1. Remove the *PoE Mounting Bracket* from the adapter, place the bracket at the desired location, and mark the two holes.
2. Pre-drill the holes if necessary, and secure the bracket using two fasteners (not included).
3. Align the adapter's slots with the tabs of the *PoE Mounting Bracket*, and then slide the adapter down.



Accessing airOS via Wi-Fi

Verify connectivity in the airOS Configuration Interface. There are two methods, the UNMS™ App and Web Portal. Both are available for 15 minutes immediately after you power on the device. If necessary, you can power cycle the LiteBeam AC to re-enable its Wi-Fi.

Proceed to the appropriate instructions:

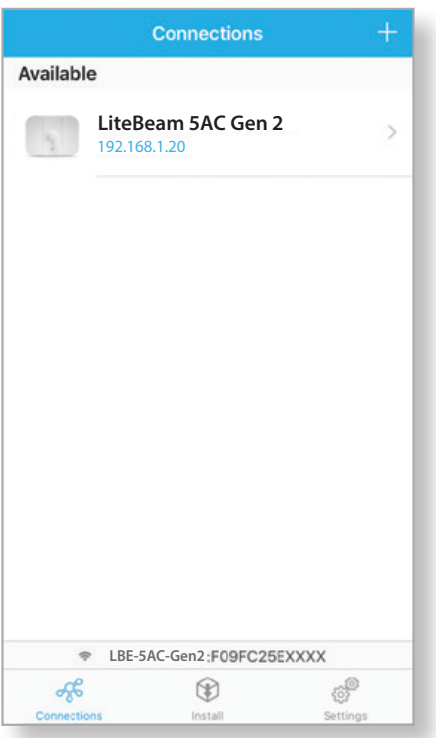
UNMS App

1. Download the UNMS app from the App Store (iOS) or Google Play™ (Android).

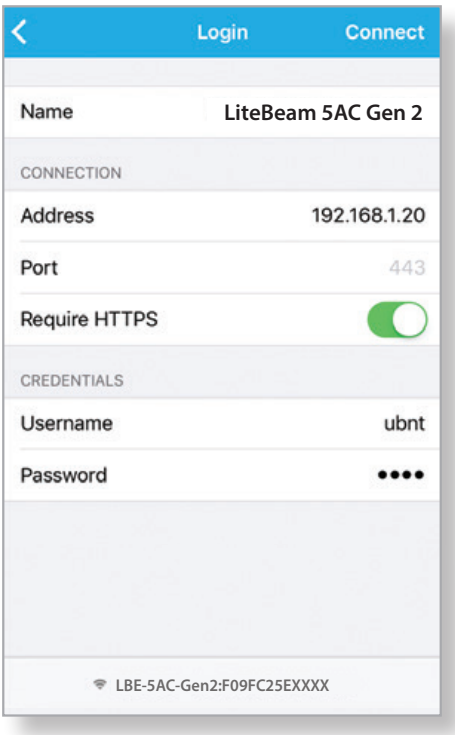
2. Connect your device's Wi-Fi to the LiteBeam AC SSID named: **LBE-5AC-Gen2:<MAC Address>**

   Note: Ensure that DHCP is enabled on your Wi-Fi adapter.

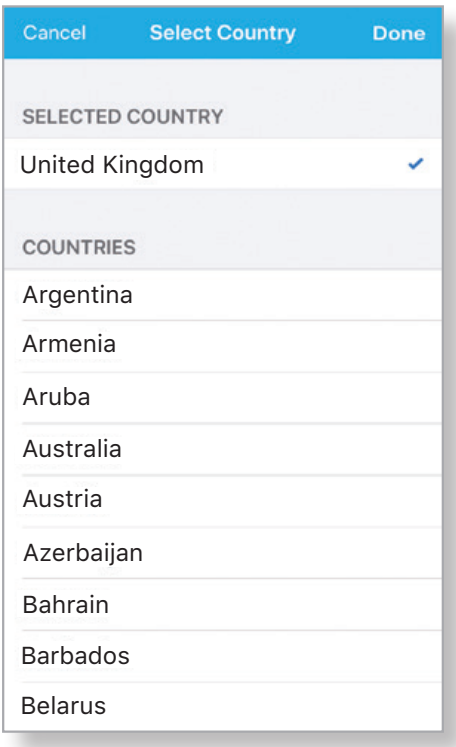
3. Launch the app.
4. Tap the LiteBeam 5AC on the *Connections* screen.



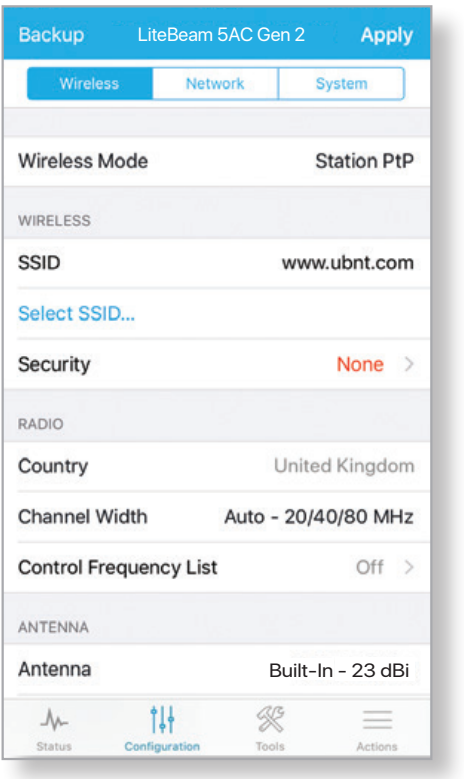
5. Tap **Connect** on the *Login* screen.



6. Select your *Country* and tap **Done**.



7. Under *Configuration*, customize your settings as needed.



Web Portal

1. Connect your device's Wi-Fi to the LiteBeam 5AC SSID named: **LBE-5AC-Gen2:<MAC Address>**

   Note: Ensure that your Wi-Fi connection has DHCP enabled.

2. Launch a web browser and go to: **http://setup.ubnt.com**

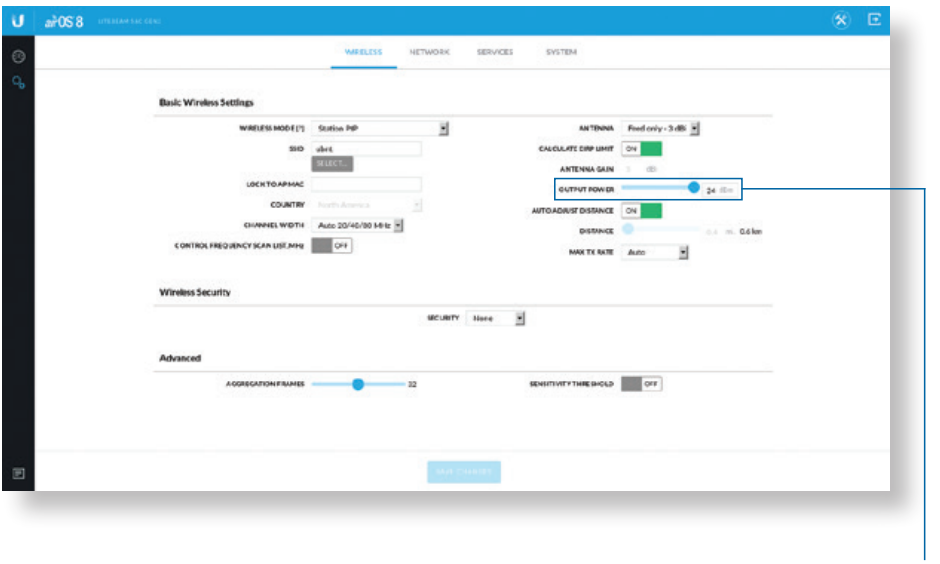
3. Enter **ubnt** in the *Username* and *Password* fields. Select your *Country* and *Language*. You must agree to the *Terms of Use* to use the product. Click **Login**.

Note: The *Country* setting for U.S. product versions is restricted to a choice of Canada, Puerto Rico, or the U.S. to ensure compliance with FCC/IC regulations.

The airOS Configuration Interface will appear, allowing you to customize your settings as needed. For additional details on the airOS Configuration Interface, refer to the User Guide available at **www.ubnt.com/download/airmax**

Installer Compliance Responsibility

Devices must be professionally installed and it is the professional installer's responsibility to make sure the device is operated within local country regulatory requirements.



The *Output Power* field is provided to the professional installer to assist in meeting regulatory requirements.

Specifications

LBE-5AC-Gen2	
Dimensions	358 x 271.95 x 272.50 mm (14.09 x 10.71 x 10.73")
Weight With Mount Without Mount	 980 g (2.16 lb) 800 g (1.76 lb)
Networking Interface	(1) 10/100/1000 Ethernet Port
Antenna Gain	23 dBi
Max. Power Output	25 dBm
Max. Power Consumption	7W
Power Supply	24V, 0.3A Gigabit PoE Adapter*
Power Method	Passive PoE (Pairs 4, 5+; 7, 8 Return)
Operating Temperature	-40 to 70° C (-40 to 158° F)
Operating Humidity	5 to 95% Noncondensing
ESD/EMP Protection	± 24 kV Contact / Air
Shock and Vibration	ETSI300-019-1.4
Wind Survivability	200 km/h (125 mph)
Wind Loading	275 N @ 200 km/h (61.8 lbf @ 125 mph)
Certifications	CE, FCC, IC

* Only the single-pack of the LBE-5AC-Gen2 includes a PoE adapter.

Operating Frequency (MHz)				
Worldwide	5150 - 5875			
USA	U-NII-1:	U-NII-2A:	U-NII-2C:	U-NII-3:
	5150 - 5250	5250 - 5350	5470 - 5725	5725 - 5850

Management Radio (MHz)	
Worldwide	2412 - 2472
USA	2412 - 2462

ZXHN F601
GPON ONT
User Manual

ZTE CORPORATION

ZXHN F601
GPON ONT
User Manual

Manual No: SJ-20141011144929-001
Edition Time: 2014-10-17 (R1.0)

LEGAL INFORMATION

1 Safety Precautions

Safety Precautions

Usage Cautions

- Read all the safety cautions carefully before using the device.
- Only use the accessories included in the package, such as power supply adapter.
- Do not extend the power cord, otherwise the device will not work.
- The power supply voltage must meet the requirements of the device input voltage (The voltage fluctuation range is less than 10%).
- Keep the power plug clean and dry to prevent any risk of electric shock or other dangers.
- Disconnect all the cables during a lightning storm to prevent the device from damage.
- Power off and unplug the power plug when the device is not in use for a long time.
- Do not attempt to open the covers of the device. It is dangerous to do so when the device is powered ON.
- Do not directly stare at the optical interface to prevent any eye injuries.
- Power off and stop using the device under the conditions such as, abnormal sound, smoke, and strange smell. Contact the service provider for maintenance if the device is faulty.

Note:

The users should read the usage cautions above carefully and will be responsible for any incident resulting from the violation of the above cautions.

Environment Requirements

- Ensure proper ventilation to the device. Place the device away from direct sunlight and never spill any liquid on the device.
- Do not place any object on the device to prevent any deformation or damage to the device.
- Do not place the device near any source of heat or water.
- Keep the device away from any household appliances with strong magnetic or electric fields, such as microwave oven and refrigerator.

Cleaning Requirements

- Before cleaning, power off the device, and unplug all the cables connected to the device, such as power cable, optical fiber, and Ethernet cable.
- Do not use any liquid or spray to clean the device. Use a soft dry cloth.

Environment Protection

- Do not dispose the device or battery improperly.
- Observe the local regulations about the equipment disposal or treatment.

2 Package Content

Please ensure the ZXHN F601 package contains the following items.

Item	Name	Quantity
	**ZXHN F601 unit**	**One**
	**AC-DC power supply adapter**	**One**
	**RJ-45 Ethernet cable**	**One**

One *ZXHN F601 GPON ONT User Manual*

Note:

The packing list is only for your reference. The actual package may be different from the packing list.

If any of the items included in the package is incorrect, lost or damaged, please contact your service provider. If you need to replace the product, please keep the package and all the items in good condition.

3 Indicator

Figure 3-1 shows the indicators on the front panel of the ZXHN F601 unit.

Figure 3-1 Indicators of the ZXHN F601 unit

Table 3-1 describes the indicators on the front panel of the ZXHN F601 unit.

Table 3-1 Indicators on the Front Panel

Indicator	Status	Description
Power	Off	No power
	Solid green	Power on
PON	Off	The ONT registration fails or the system is not powered on.
	Solid green	The ONT registration is successful.
	Flashing green	The ONT is being registered.
LOS	Off	The ONT received optical power is normal.
	Solid red	The optical transmitter of the PON interface is powered off.
	Flashing red	The ONT received optical power is lower than the optical sensitivity of the receiver .
Alarm	Off	The device is not powered on or works normally.
	Solid red	The device is not started or there are mechanical faults.
	Flashing red	The version is being updated or downloaded.

Indicator	Status	Description
LAN	Off	The device is not powered on or the network link is not established.
	Solid green	The network link has been established but no data is being transmitted or received.
	Flashing green	Data is being transmitted or received.

4 Interface

Figure 4-1 shows the ZXHN F601 interfaces and buttons on the ZXHN F601 unit.

Figure 4-1 Interfaces and Buttons

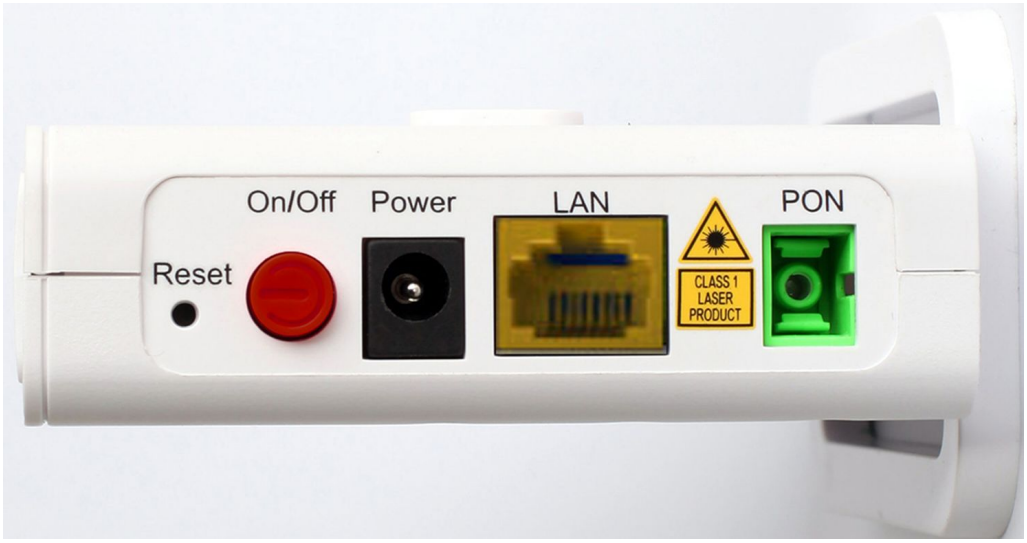


Table 4-1 describes the interfaces and buttons on the ZXHN F601 unit.

Table 4-1 Descriptions of the Interfaces and Buttons

Interface and Button	Description
Reset	When the device is powered on, use a needle to press the RESET button for more than five seconds to restore the factory default settings.
On/Off	Power switch.
Power	12 V DC power connector.
LAN	RJ-45 Ethernet interface, connected to the computer.
PON	PON interface, connected to the network provider through the fiber.

5 Product Features

Interfaces

- GPON interface: GPON standard, SC/APC.
- Ethernet interface: One RJ-45 (10/100/1000 Base-T) interface, complying with IEEE 802.3, IEEE 802.3u and IEEE 802.3ab to support 10/100/1000 Mbps auto-negotiation.

Technical Features

ZXHN F601 has the following features.

- Broadband service access: Connected to Internet through the GPON access method.
- Ethernet service access: Providing GE Ethernet interface, connected to the Ethernet devices, such as the PC. Providing Internet access and IPTV services.
- Security: Providing multi-level authentication based on the device, user and service, and Providing the data channel encryption for safety.

- QoS: Providing QoS assurance to meet the requirements of various services offered by ISP (Internet Service Provider).
- Network management: Providing multi-mode network management.

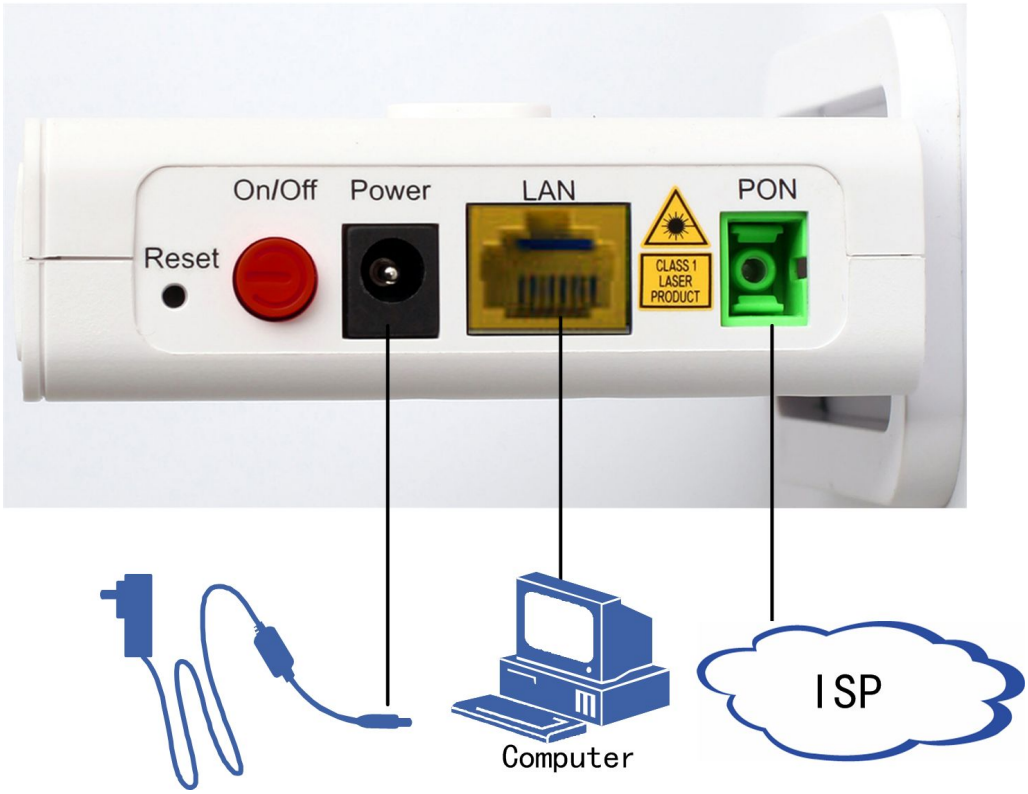
6 Technical Specification

Item	Specification
Dimension	110 mm × 96 mm × 53 mm (length × height × width)
Rated current	0.5 A
Rated voltage	12 V DC
Operation temperature	-0℃ – 40℃
Operation humidity	5% – 95%

7 Cable Connection

Figure 7-1 shows the devices that are connected to a ZXHN F601 device.

Figure 7-1 ZXHN F601 Cable Connection



After the cables are properly connected, press down the power switch on the side panel. When the power indicator on the front panel becomes solid on while the other indicators are normal, the services that the operator provides are available.

8 Troubleshooting

The Power indicator on the front panel is off after the power button is pressed.

The power adapter is not correctly connected to the device. Be sure to use the power adapter supplied with the device.

The LOS indicator is flashing red or solid red after the device is powered on.

- The PON fiber connection is abnormal.
- The optical fiber is not correctly connected to the ONT PON interface.
- The optical fiber is broken or damaged.
- If the indicator is solid red, please contact the service provider for maintenance.

The ALARM indicator is red after the device is powered on.

There are physical faults. Restart the device. If the alarm indicator is still red, please contact the service provider for maintenance.

The PON indicator on the front panel is off or flashing green after the device is powered on.

- The GPON link is not established.
- The ONT is not registered.
- Please contact the service provider for help.

The LAN indicator on the front panel is off after the device is powered on.

- The corresponding LAN link is not established.
- The Ethernet cable is not correctly connected to the LAN interface.
- The network device connected to the LAN interface is not powered on.

合格证
CERTIFICATION

检验员

CHECKER

日期

DATE

ZTE中兴

ZTE CORPORATION

NO. 55, Hi-tech Road South, ShenZhen, P.R.China

Postcode: 518057

Tel:+86-755-26771900

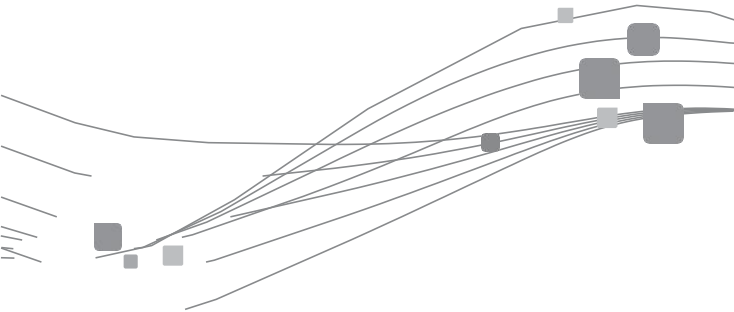
URL: http://support.zte.com.cn

E-mail: support@zte.com.cn

ZXHN F6600P

GPON ONT

User Manual



ZTE CORPORATION

ZXHN F6600P
GPON ONT
Manual de Usuario

CE

No: SJ-20211014111546-016
Fecha de edición: 2023- 06-09(R1.0)

INFORMACIÓN LEGAL

ZTE CORPORATION se reserva el derecho de actualizar o realizar cambios técnicos en este producto sin previo aviso.
Los usuarios pueden visitar el sitio web de soporte técnico de ZTE http://support.zte.com.cn para solicitar más información relacionada.
El derecho último de interpretación de este manual corresponde a ZTE CORPORATION.
.

1 Medidas de seguridad.

Nota

Los usuarios deben leer detenidamente las precauciones de uso siguientes y serán responsables de cualquier incidente derivado de la violación de las mismas.

Precauciones de uso

- Lea atentamente todas las medidas de seguridad antes de utilizar el aparato.
- Utilice únicamente los accesorios incluidos en el paquete, como el adaptador de corriente.
- No alargue el cable de alimentación, de lo contrario el dispositivo no funcionará.
- El voltaje de la fuente de alimentación debe cumplir con los requisitos del voltaje de entrada del dispositivo (el rango de fluctuación de voltaje debe ser inferior al 10%).
- Mantenga el enchufe limpio y seco para evitar cualquier riesgo de descarga eléctrica u otros peligros.
- Desconecte todos los cables durante una tormenta eléctrica para evitar que el aparato se dañe.
- Apague y desenchufe la fuente de alimentación cuando no se vaya a utilizar el aparato durante mucho tiempo.
- No intente abrir las carcasas del aparato. Es peligroso hacerlo cuando el aparato está encendido.
- Apague y deje de utilizar el aparato en caso de que se produzcan sonidos anormales, humo u olores extraños. Póngase en contacto con el proveedor de servicios para el mantenimiento si el dispositivo está defectuoso.
- No mire fijamente a la interfaz óptica del equipo para evitar posibles lesiones oculares.

Requisitos del entorno

- Asegure una ventilación adecuada del aparato. Coloque el aparato lejos de la luz solar directa.
- Mantenga el aparato ventilado y seco. No derrame nunca ningún líquido sobre el aparato.
- No coloque ningún objeto sobre el aparato para evitar que se deforme o se dañe.
- No coloque el aparato cerca de ninguna fuente de calor o agua.
- Mantenga el aparato alejado de cualquier aparato doméstico con fuertes campos magnéticos o eléctricos, como el microondas o el frigorífico.

Requisitos de limpieza

- Antes de la limpieza, apague el dispositivo y desenchufe todos los cables conectados al mismo, como el cable de alimentación, la fibra óptica y el cable Ethernet.
- No utilice ningún líquido o spray para limpiar el dispositivo. Utilice un paño suave y seco.

Protección del medio ambiente

- Deseche el dispositivo y la batería de forma adecuada.
- Respete la normativa local sobre la eliminación o el tratamiento de equipos electrónicos.

Restricciones en la banda de 5 GHz

De conformidad con el artículo 10(10) de la Directiva 2014/53/UE, el embalaje indica que este equipo de radio estará sujeto a determinadas restricciones cuando se comercialice en Bélgica(BE), Bulgaria(BG), la República Checa(CZ), Dinamarca(DK), Alemania(DE), Estonia(EE), Irlanda(IE), Grecia(EL), España(ES), Francia(FR), Croacia(HR), Italia(IT), Chipre(CY), Letonia(LV), Lituania(LT), Luxemburgo(LU), Hungría(HU), Malta(MT), Países Bajos(NL), Austria(AT), Polonia(PL), Portugal(PT), Rumanía(RO), Eslovenia(SI), Eslovaquia(SK), Finlandia(FI), Suecia(SE), Turquía(TR), Noruega(NO), Suiza(CH), Islandia(IS) y Liechtenstein(LI).

La función WLAN de este dispositivo está restringida a un uso exclusivo en interiores cuando opere en el rango de frecuencias de 5150 a 5350 MHz.

Información sobre la exposición a la RadioFrecuencia

El nivel de exposición máxima permitida (EMP) se calcula sobre la base de una distancia de 20 cm entre el dispositivo y el cuerpo humano. Para cumplir con el requisito de exposición a radiofrecuencias (RF), debe mantenerse una distancia mínima de separación de 20 cm entre el dispositivo y el cuerpo humano.

EU Declaration of Conformity

Por la presente, declara que el equipo con módulo radio modelo ZXHN F6600P cumple con la Directiva 2014/53/UE. El texto completo de la declaración de conformidad de la UE está disponible en la siguiente dirección de Internet: http://support.zte.com.cn/support/cer/EU.

Información medioambiental

El equipo adquirido ha requerido de la extracción y el uso de recursos naturales para su producción. Podría contener sustancias peligrosas para la salud de las personas y el medio ambiente. Con el fin de evitar la introducción de dichas sustancias en nuestro medio ambiente y de reducir la presión sobre nuestros recursos naturales, le pedimos que reutilice o recicle los equipos al final de su vida útil mediante un sistema acreditado de recogida de productos electrónicos.

Los símbolos que aparecen a continuación indican que este producto debe ser reutilizado o reciclado en lugar de ser simplemente desechado. Por favor, localice y utilice un sitio de reutilización y reciclaje apropiado.

Si necesita más información sobre los sistemas de recogida, reutilización y reciclaje, póngase en contacto con la autoridad local o regional competente en materia de residuos. También puede ponerse en contacto con su proveedor de equipos para obtener más información sobre el impacto medioambiental de estos productos.

2 Contenido del paquete

Asegúrese de que la caja de la ONT ZXHN F6600P contiene los elementos

referidos en la tabla a continuación.

Tabla 2-1 Elementos incluídos en la caja

Ítem	Cantidad
ZXHN F6600P	Uno
Fuente alimentación AC-DC	Uno
Manual de usuario	Uno

Nota

La lista es sólo de referencia. El contenido real puede variar.

Si alguno de los elementos incluidos en el paquete es incorrecto, se ha perdido o está dañado, póngase en contacto con su proveedor de servicios. Si necesita reemplazar el producto, mantenga el paquete y todos los elementos en buen estado.

3 Especificaciones del producto

Interfaces

- Interfaz GPON: estándar GPON, SC/APC, de acuerdo con estándares ITU-T G.984.1-G.984.5.
- Interfaces Ethernet: cuatro interfaces RJ45 con auto-negociación 100/1000 Mbps RJ-45 acordes con IEEE 802.3 y IEEE 802.3u.
- Interfaz de teléfono: un puerto POTS con conector RJ-11.
- Interfaces WLAN: acordes con IEEE 802.11b/g/n/ax@2.4GHz and IEEE 802.11a/ n/ac/ax@5GHz.
- Interfaz USB: una interfaz estándar USB 2.0.

Funcionalidades técnicas

- Servicio Acceso de banda ancha: conexión a Internet a través de acceso GPON.
- Acceso Ethernet: se proporcionan interfaces para la conexión de dispositivos Ethernet, tales como PC para el acceso de servicios de Internet o IPTV.
- Servicio de Voz: soporte de protocolo SIP.
- WLAN: los usuarios pueden conectar dispositivos finales a la ONT ZXHN F6600P utilizando interfaz inalámbrica WiFi.
- Backup, restauración y compartición de datos: el equipo proporciona una interfaz USB 2.0 habilitando la conexión de unidades de almacenamiento para la compartición de ficheros, realización de copias de

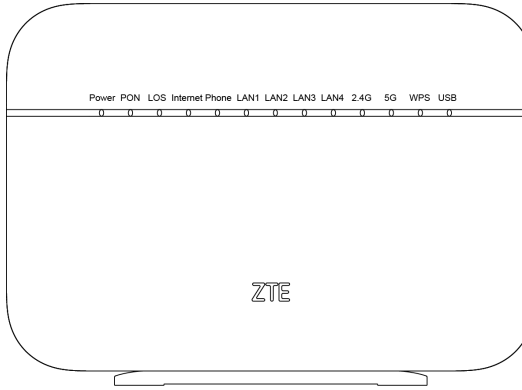
seguridad y restauración de configuración.

- Seguridad: proporciona multiples niveles de acceso por autenticación y encriptación del canal de comunicación.
- QoS: proporciona funcionalidades de calidad de servicio para asegurar/configurar las distintas necesidades de los distintos servicios gestionados por el equipo tanto a nivel local como hacia la red.
- Gestión: proporciona multiples modos de acceso y gestión tanto local como remotamente.

2 Indicadores LEDs

En la imagen 4-1 muestra los indicadores LED del panel frontal de la ZXHN F6600P.

Imagen 4-1 Indicadores LED de la ZXHN F6600P



La Tabla 4-1 explica la funcionalidad de los distintos indicadores LED del panel frontal de la ONT ZXHN F6600P unit.

Tabla 4-1 Indicadores del panel frontal

LED	Estado	Descripción
Power	Apagado	El equipo está apagado.
	Verde fijo	El equipo está encendido.

PON	Apagado	The device is powered off or the device has not started the registration process.
	Verde fijo	El equipo se ha registrado correctamente.
	Verde parpadeo lento	El equipo está en proceso de registro
	Verde parpadeo rápido	El equipo se está actualizando

LED	Estado	Descripción
LOS	Apagado	El equipo está apagado o la potencia óptica recibida es correcta.
	Rojo fijo	El transmisor óptico de la interfaz PON está apagado.
	Rojo parpadeante	La potencia óptica recibida es menor que la sensibilidad del receptor.
Internet	Apagado	El equipo está apagado, o no hay una interfaz WAN configurada,, o la sesión se ha desconectado por petición de unos de los dos extremos o no hay dirección IP asociada a la interfaz (no hay IP estática configurada o se ha producido DHCP release).
	Verde fijo	El equipo tiene conectividad y dirección IP asignada.
	Verde parpadeante	Se está cursando tráfico hacia Internet a través de la interfaz WAN (en cualquiera de las dos direcciones).
Phone	Apagado	El equipo está apagado o no ha sido capaz de registrar contra el servidor de Voz.
	Verde fijo	El equipo está registrado correctamente contra el servidor de Voz pero no hay

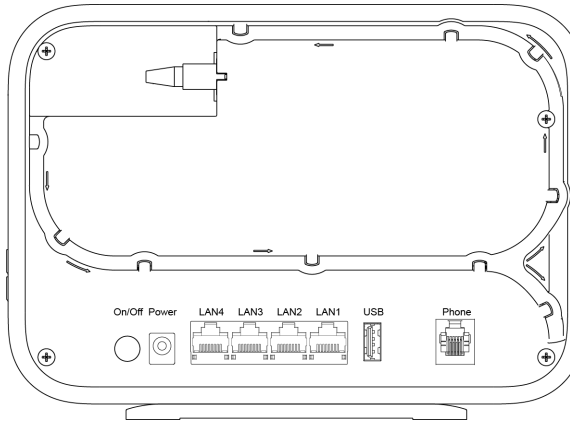
		llamada en curso.
	Verde parpadeante	El equipo está cursando una llamada.
LAN1–LAN4	Apagado	El equipo está apagado o no se ha establecido enlace en el puerto correspondiente.
	Verde fijo	Existe enlace establecido en el Puerto pero no es está cursando tráfico por el mismo.
	Verde parpadeante	Se está cursando tráfico por el Puerto correspondiente.
2.4G	Apagado	El equipo está apagado o la interfaz WiFi asociada está deshabilitada.
	Verde fijo	La interfaz WiFi está habilitada pero no está cursando tráfico.
	Verde parpadeante	La interfaz WiFi está cursando tráfico,
5G	Apagado	El equipo está apagado o la interfaz WiFi asociada está deshabilitada.
	Verde fijo	La interfaz WiFi está habilitada pero no está cursando tráfico.
	Verde parpadeante	La interfaz WiFi está cursando tráfico,
WPS	Apagado	El equipo está apagado o la funcionalidad WPS no está habilitada.

	Verde fijo	Algún dispositivo ha registrado correctamente usando WPS.
	Naranja parpadeante	Algún dispositivo está intentando registrar mediante WPS.
	Rojo parpadeante	Fallo en el registro WPS
USB	Apagado	El equipo está apagado o no hay USB conectado al equipo.
	Verde fijo	La interfaz USB está conectada y operative pero no hay transmisión de datos activa.
	Verde parpadeante	Transmisión de datos en curso.

3 Interfaces

Black Panel

La imagen 5-1 muestra las interfaces y botones disponibles en el panel trasero de la ONT ZXHN F6600P.



La tabla 5-1 a continuación describe las interfaces y botonoes del panel trasero de la ZXHN F6600P.

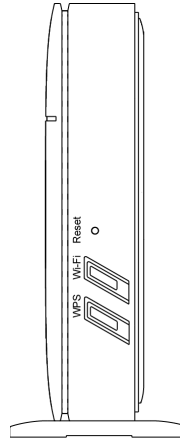
Tabla 5-1 Descripción de las interfaces y botones de la ZXHN F6600P

Interfaz/ Botón	Description
On/Off	Interruptor de alimentación.
Power	Conector de alimentación 12 V DC..
LAN1 – LAN4	Interfaces Ethernet 10 Mbps/100 Mbps/1000 Mbps Base-T con conector RJ-45.
USB	Interfaz estándar USB 2.0
Phone	Interfaz telefónica con conector para proporcionar servicio de voz.
PON	Interfaz óptica GPON con conector SC/APC.

Panel lateral

La imagen 5-2 a continuación muestra los botones del panel lateral de la ONT ZXHN F6600P.

Imagen 5-2 Botones del panel lateral de la ZXHN F6600P



La tabla 5-2 describe los botones del panel lateral.

Tabla 5-2 Descripción de los botones del panel lateral de la ZXHN F6600P

Botón	Descripción
Reset	El botón de reset se utiliza una vez el equipo está encendido y operativo. ● Usando una aguja, mantener presionado el botón de Reset durante un Segundo para reiniciar el equipo. La configuración actual del equipo no se perderá. ● Usando una aguja, mantener presionado el botón de Reset durante más de 5 segundos para realizer un reset de fábrica al dispositivo.
Wi-Fi	Botón WiFi. Tras pulsar el botón Wi-Fi la funcionalidad inalámbrica se habilitará/deshabilitará.
WPS	Botón mecanismo de asociación Wi-Fi. Tras pulsa el botón WPS, la funcionalidad asociada se habilitará.

4 Especificaciones del producto

Para la consulta de las especificaciones de la ONT ZXHN F6600P ,

consulte la tabla 6-1 a continuación.

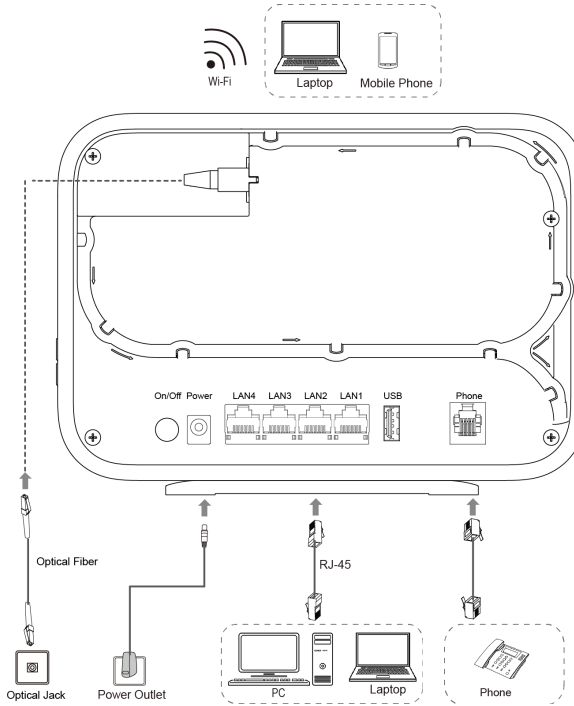
Tabla 6-1 Especificaciones de la F6600P

Especificaciones técnicas	
Dimensiones	203 mm (W) x 141 mm (D) x 33 mm (H) (sin considerar la base)

Certificaciones	Certificada CE y Wi-Fi (WFA)
Fuente alimentación	Entrada: AC 100 V to 240 V, 50 Hz/60 Hz
	Salida: DC 12 V, 1.5 A
Requisitos del entorno	
Temperatura de funcionamiento	0 °C hasta 40 °C (32 °F hasta 104 °F)
Humedad de funcionamiento	5% – 95% (sin condensación)
Especificaciones Wi-Fi	
Radiofrecuencias	Potencia máxima de salida
Banda Wi-Fi 2.4 GHz: 2400 MHz – 2483.5 MHz	EIRP: (19 ± 1) dBm
Banda baja Wi-Fi 5 GHz: 5150 MHz – 5350 MHz	EIRP: (22 ± 1) dBm
Banda alta Wi-Fi 5 GHz: 5470 MHz – 5725 MHz	EIRP: (29 ± 1) dBm

5 Conexiones del equipo

Imagen 7-1 Diagrama de conexión de la F6600P



Una vez que los dispositivos estén conectados al aparato ZXHN H3600P, pulse el botón de encendido. Cuando los indicadores correspondientes del panel frontal estén encendidos, podrá disfrutar de los diversos servicios proporcionados por el proveedor de servicios. Los factores que afectan al rango de cobertura de la red inalámbrica incluyen la ubicación del producto, la distancia entre el producto y el terminal inalámbrico, el número de obstáculos, el material y la densidad de los obstáculos y la fuente de interferencia.

Se recomienda colocar el producto de acuerdo con los siguientes principios para maximizar la intensidad de ls señal inalámbrica.

- El producto debe estar alejado de los objetos que afectan a la propagación de la señal inalámbrica; por ejemplo, elementos con alta reflectividad que puede ser, un objeto metálico o un espejo.
- El producto debe estar alejado de cualquier aparato eléctrico con un fuerte campo magnético o eléctrico; por ejemplo, un microondas, un frigorífico, un router inalámbrico, un teléfono inalámbrico o un dispositivo Bluetooth.
- El producto se debe instalar en el mismo suelo que la zona de operación.
- No coloque otros objetos sobre el producto. Intente reducir el número de obstáculos entre el producto y los terminales inalámbricos.
- Coloque el producto horizontalmente en el centro del área operativa, no lo ponga en una esquina.
- No coloque el producto en una posición alta mientras esté colocado horizontalmente. La altura recomendada es de 1,2 a 1,5 metros.

6 Resolución de problemas

El indicador LED Power del panel frontal permanece apagado después de pulsar el botón de alimentación.

- El interruptor de encendido no se enciende.
- El adaptador de corriente no está correctamente conectado al dispositivo.

Asegúrese de utilizar el adaptador de alimentación suministrado con el dispositivo.

El indicador LOS indicator parpadea en rojo o está rojo fijo tras el encendido del equipo.

- La fibra óptica no se ha conectado correctamente a la interfaz PON de la ONT.
- La fibra óptica está rota o dañada.
- Si tras la revision de los puntos anteriores, el indicador mantiene su estado, contacto con su proveedor de internet para su asistencia.

El indicador LED PON del panel frontal está apgado tras el encendido del equipo.

- No se ha establecido enlace GPON.
- La ONT no se ha registrado.
- Contacte a su proveedor de internet para su asistencia.

El indicador LAN del panel frontal permanece apagado después de encender el dispositivo.

- No se ha establecido el enlace LAN.
- El cable Ethernet no está correctamente conectado a la interfaz LAN.
- El dispositivo de red conectado a la interfaz LAN no está alimentado.

El indicador LED Phone del panel frontal permanece apagado tras el encendido del equipo.

El servicio de voz no funciona correctamente. Por favor llame a su proveedor de internet para su asistencia.


ZTE

Dirección: ZTE Plaza, Keji Road South, Hi-Tech Industrial Park, Nanshan District, Shenzhen,Guangdong, R.P. China
Cód poştal: 518057
Tel: +86-755-2677 1900
URL: http://support.zte.com.cn E-mail: support@zte.com.cn

CERTIFICATION
QC PASS