User Guide

SR20

Smart Home Router (SR20)

AC1900 Wi-Fi Router + Smart Home Hub + Touch Screen

REV1.0.1 1910012101

Contents

About This Guide

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

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 images, parameters and descriptions documented in this guide are used for demonstration only.

Conventions

In this guide, the following conventions are used:

Convention	Description
Underline	Hyperlinks are in teal and underlined. You can click to redirect to a website or a specific section.
Teal	Key information appears in teal, including management page text such as 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.
Symbols on the web page	• click to delete the corresponding entry. • click to view more information about items on the page.

More Info

- The latest firmware and management app are available from Download Center at http://www.tp-link.com/support.
- The Quick Start Guide (QIG) can be found where you find this guide or inside the product package.
- 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 http://www.tp-link.com/support.

Chapter 1

Introduction

This chapter introduces what the Smart Home Router can do and shows its main features and appearance.

1. 1. Product Overview

The AC1900 Wi-Fi Router plus Smart Home Hub plus Touch Screen (also referred to as Smart Home Router SR20), is an "all-in-one" Wi-Fi router with built-in smart home hub that eliminates the need for more standalone hubs in your home. It offers a centralized solution to unify all smart home technologies to seamlessly work together, such as TP-Link smart home products and other ZigBee and Z-Wave devices. From there, you can control them by way of the TP-Link Kasa mobile app together with the integrated 4.3-inch touch screen color display atop the router, revolutionizing a new way of visualizing and interacting with your connected home.

With AC1900-class and 3x3 MIMO technology, the Smart Home Router simultaneously delivers up to 1300Mbps over 5GHz and 600Mbps over 2.4GHz, offering the flexibility of two dedicated networks for basic tasks and bandwidth-intensive tasks such as streaming 4K Ultra HD media and online gaming.

The SR20 features four Gigabit Ethernet ports for lightning-fast data transfer, built-in NAT-router, Firewall, and Wireless Access Point (AP). The high-gain omni-directional antenna and powerful amplifiers boosts the Wi-Fi coverage throughout your home. Coupled with the advanced beamforming technology that allows the SR20 to concentrate the Wi-Fi signal directly at the connected devices, delivering a stronger and more reliable Wi-Fi connection.

The Smart Home Router is also a versatile dual-band solution that can function as a router, or access point to best serve your networking needs, making it an ideal choice for the Small Office/Home Office (SOHO) networks that demand higher speed and more reliable network performance. It complies with the next-generation 802.11ac Wi-Fi standard, and backward compatible with 802.11n, offering 3 times faster than wireless N speeds. With high power efficiency and robust network security, 802.11ac is the perfect way to accelerate a home multimedia network and solve traffic congestion caused by high-bandwidth devices.

Furthermore, the SR20 is equipped with two USB ports (3.0 and 2.0), giving you more flexibility to share printer(s), files (such as photos, music, and videos) across your home or office network, locally and remotely via the built-in FTP server.

The SR20 fully supports IPv6, which is the latest version of the Internet protocols that enables numerous services to interoperate seamlessly and improves user experience.

The product complies with the RSS-247 Section 6.4 (2) and (4).

1. 2. Features

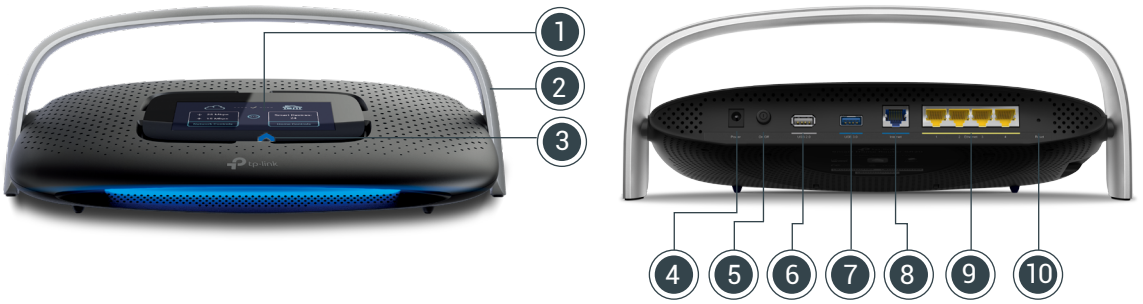
- Simple to set up and use
- Built-in touch screen display for easiest setup and home management

- Support Zigbee and Z-Wave devices
- Comply with IEEE 802.11ac
- Provide multiple encryption security types, including 64-bit, 128-bit, 152-bit WEP, and WPA-PSK/WPA2-PSK
- Support built-in DHCP server
- Support app-based and web-based managements
- Support for remote control of all Kasa devices (via app)
- Integrated third-party smart home devices
- Guest Network management
- Client Controls management

1. 3. System Requirements

- A smartphone or tablet running iOS 8 or higher; Android 4.1.x or higher
- Kasa account

1. 4. Physical Appearance



1 Touch Screen

A 4.3-inch capacitive color touch screen with intuitive user interface for basic network configuration and home automation controls.

2 MIMO Antenna

Position the antenna upright for optimal performance.

3 Home Button

Tap to wake the touch screen or go back to the main Home screen.

4 Power Connector

Connect the supplied power adapter.

5 On/Off Button

Press to turn the Smart Router ON or OFF.

6 USB 2.0 Port

Connect a USB 2.0 storage device or a USB 2.0 printer for file or printer sharing.

7 USB 3.0 Port

Connect a USB 3.0 storage device or a USB 3.0 printer for content sharing, printer sharing, or media streaming. This port is also compatible with USB 2.0 devices.

8 Internet Port

Connect your broadband DSL/Cable Modem to this port using an Ethernet cable.

9 Gigabit Ethernet 1-4 Ports

Connect Ethernet devices such as computers, game consoles, smart TVs or other devices that require a wired connection to the internet.

10 Reset Button

Press and hold for about 10 seconds or until the confirmation window appears on the touch screen, then release the button and click Yes to start resetting your router.

Chapter 2

Set up Your Router via Kasa App

2. 1. Position Your Router

The Smart Home Router is designed to be the "control center" of your home and with its modern appearance, it can be placed in a standing position or mounted on the wall. However, keep in mind that your router's location can affect wireless connections. For optimal end-user experience, we recommend that you choose a location that is near a power outlet, and where other devices (wired and wireless) will be able to connect to. Before installing the router, adhere to all safety precautions including the following:

- Place the router in a centralized area for a maximum wireless coverage
- Keep the router away from metal obstructions, Bluetooth® devices, cordless phones, transformers, heavy-duty motors, microwave ovens to prevent signal interference or loss
- Place the router in a well-ventilated location with at least 5 cm (approx. 2 inches) of clearance on all sides
- Avoid exposure to direct sunlight, liquids, excessive heat or cold
- Do not make repairs or modifications to the router
- Always update the router to the latest firmware

2. 2. Setting Up via Kasa App

2. 2. 1. Get Started

1. Download Kasa for Mobile from the App Store or Google Play.

2. Launch Kasa and create a Kasa account or log in using your email address.

3. On the Add Device screen, tap SMART ROUTER and follow the onscreen prompts to connect your Smart Router.

   a. Power off your modem by removing its power adapter and/or backup battery.

   b. Position the antenna upright.

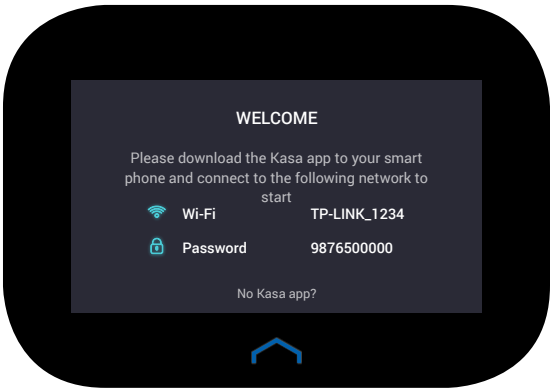
   c. Connect the provided blue Ethernet cable from the Internet port on the router to the modem.

   d. Re-insert the power adapter and/or battery into the modem.

e. Plug in and connect the router's power adapter.

f. Press the On/Off button on the back of the router and wait for the Welcome screen to appear with the default Wi-Fi network name and password.

4 Connect your mobile device to the default Wi-Fi network name using the password on the touch screen.



5 Tap Detect Internet to automatically configure your internet connection.

6 Set up your 2.4 Wi-Fi network with a Wi-Fi network name (SSID) and a password. Note that the 5GHz network will be automatically created with the same name appended by a suffix _5G.

7 Connect your mobile device to the new Wi-Fi network and return to Kasa. The Speed Test will begin immediately.

8 Once the Speed Test is done, tap Done to complete the setup.

2. 2. 2. Kasa Account

A Kasa account is required to set up the Smart Home Router. Signing up for an account is quick and easy! All you need to do is provide a valid email address and accept our terms and conditions. After creating your Kasa account, you will need to verify the email associated with your account by clicking a link in an email that Kasa sends you.

Signing up for a Kasa account provides added functionality such as:

- Unify various connected devices into a single, controllable network with Smart Home Router with Smart Home Hub (SR20) for a streamlined smart home experience
- Synchronization of settings and configurations to all your mobile devices
- Ability to control and configure the devices from outside your home
- A bility to customize your TP-Link Smart Home devices with "Scenes" for a truly automated experience

- Use of third-party services and products such as Amazon Echo

One Smart Home Router can only be associated with one Kasa account. Note that unbinding (deleting) the router from your Kasa account will factory reset the router, and you will have to repeat the configuration process using the Kasa app.

Chapter 3

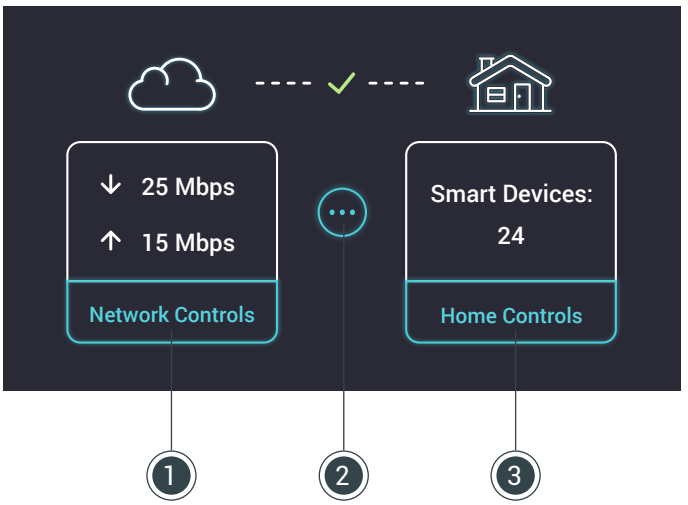
Touch Screen Settings

This chapter introduces what the touch screen of the Smart Home Router can do and shows its main features and appearance.

3. 1. Touch Screen Basics

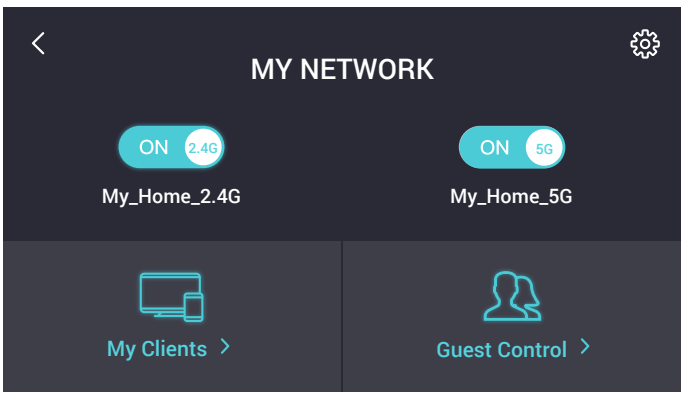
3. 1. 1. Home Screen

The main Home screen provides a visual overview of your network, along with ability to control your network and interact with your smart home devices.



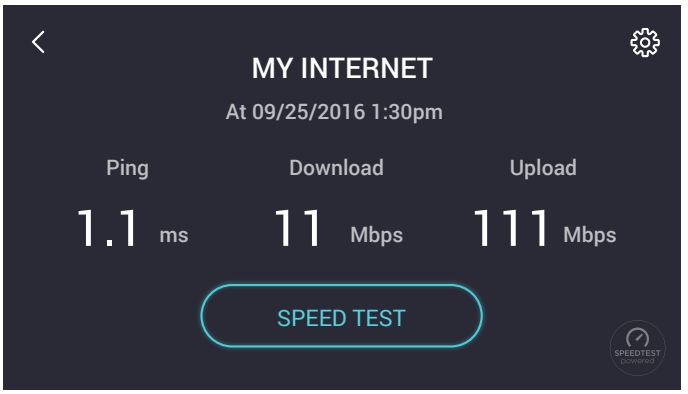
1 Network Controls

Tap on this interface to monitor and manage network access for the wireless clients or Guest network.



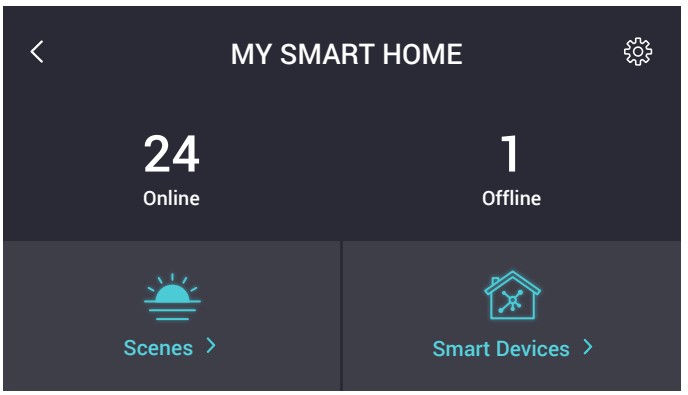
2 Speed Test

Tap on this icon to perform a speed test on your internet connection.



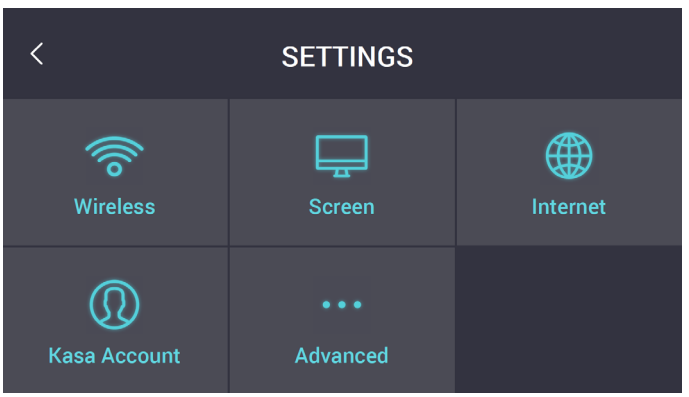
3 Home Controls

Tap on this interface to access your programmed scenes or interact with your connected devices on your network.



3. 1. 2. System Settings Screen

The system's Settings screen can be accessed from the main Home screen by tapping on Network Controls, Home Controls or the ··· icon and then tapping the (Settings) icon at the top-right corner.



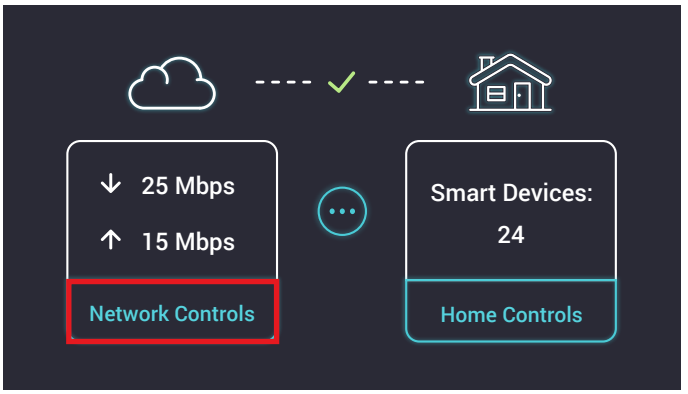
Wireless	Tap this icon to configure your Wi-Fi network settings such as Wi-Fi Network Name (SSID) and Wi-Fi password.
Screen	Tap this icon to adjust your router's screen brightness, set screen lockout with a PIN code to protect your configuration from being m odified and adjust the screen timeout. The touch screen automatically times out and enters sleep mode during periods of inactivity. To wake the touch screen, tap on it or the (Home) button on the router.
Internet	Tap this icon to configure your internet connection according to your Internet Service Provider (ISP).
Kasa Account	Tap this icon to check the Kasa account binded to your router.
Advanced	Tap this icon to view the IP address that you use to access the router's web management page for advanced settings such as LAN, DHCP, DDNS, and QoS configurations, or display the router information such as Hardware and Firmware version. You can also perform a full router factory reset.

3. 2. Basic Network Management

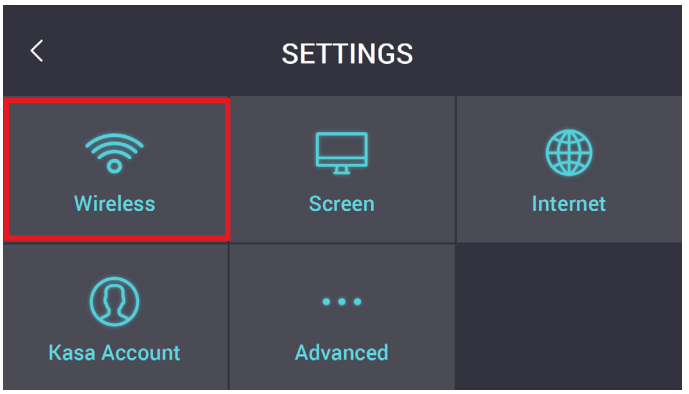
Initially setting up your Smart Home Router is a relatively straightforward process that is done on the Kasa app. You can change Wi-Fi settings, manage smart devices and configure other advanced functions in your Kasa App. Now, you can also manage your Wi-Fi settings, like changing the SSID and password, and enabling or disabling the guest network, and even block certain devices from connecting to your Wi-Fi network via the router's touch screen.

3. 2. 1. Changing Wi-Fi Settings

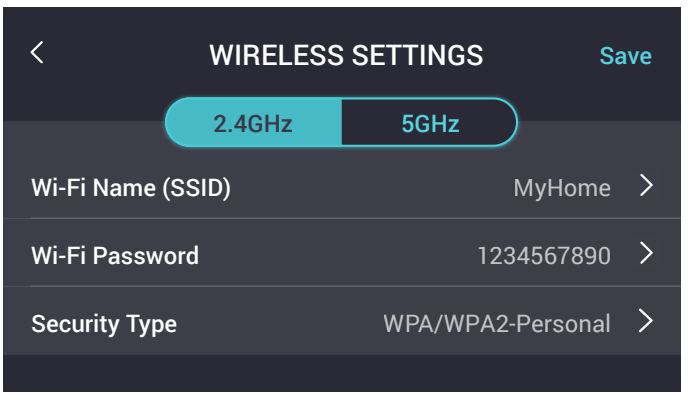
1. On the main Home screen, tap Network Controls.



2. Tap on the (Settings) icon at the top-right corner and then Wireless.



3. Change your 2.4GHz and/or 5GHz Wi-Fi settings and tap Save.

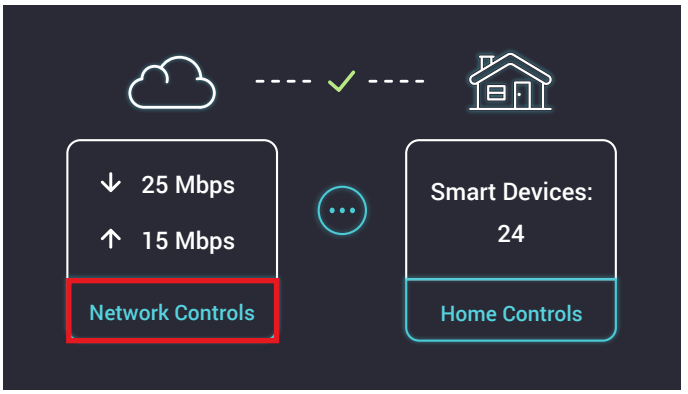


Note:
Changing your SSID or Wi-Fi password, Wi-Fi devices will need to be reconfigured to connect to the network with changes.

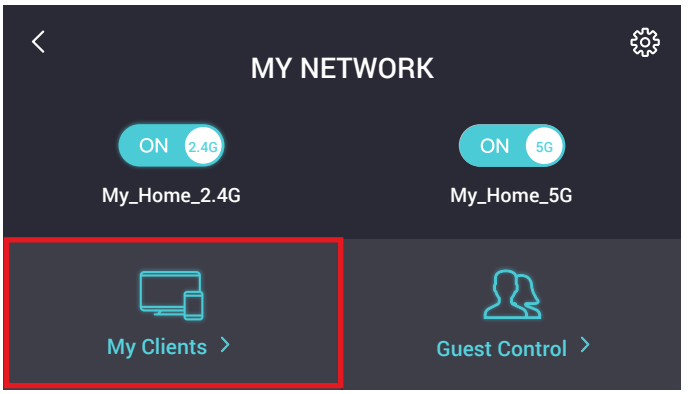
3. 2. 2. Client Controls

With Client Controls, you can monitor on a regular basis and trigger some network management such as blocking or temporarily disabling the internet connection of the currently connected devices on your Wi-Fi network.

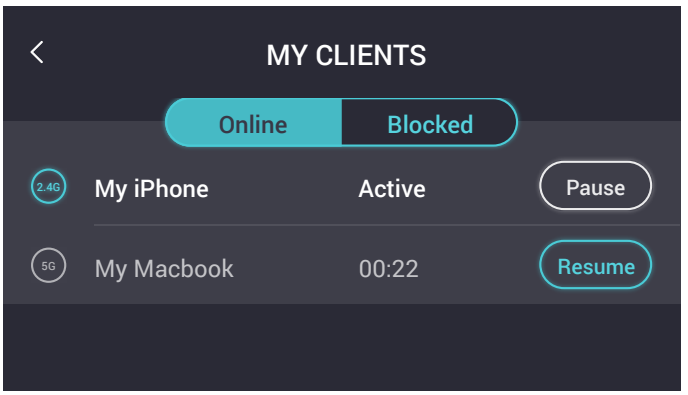
1. On the main Home screen, tap Network Controls.

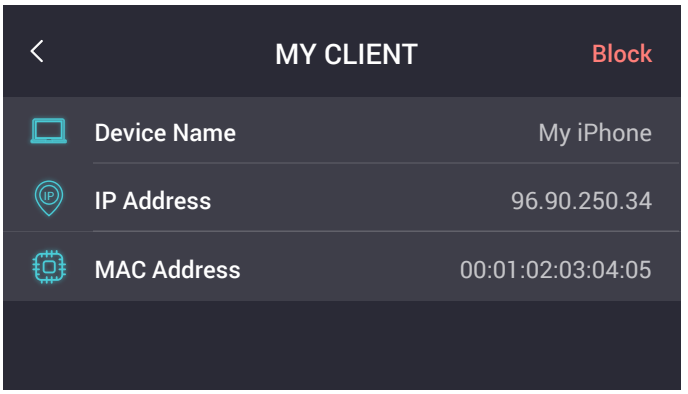


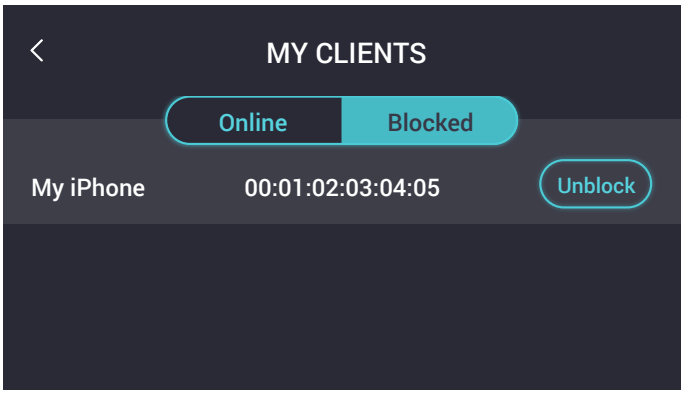
2. Tap My Clients to view the list of all active Wi-Fi clients on your network.



3. To suspend the client's internet connection for a period of time, tap Pause and select the duration. To block, tap on the client to go to its details screen, tap Block on the top-right corner of the screen, and confirm at the prompt. Note that the temporarily-paused client will resume its internet connection after the time expires. If the client is blocked, you'll have to unblock the device listed under the Blocked tab.



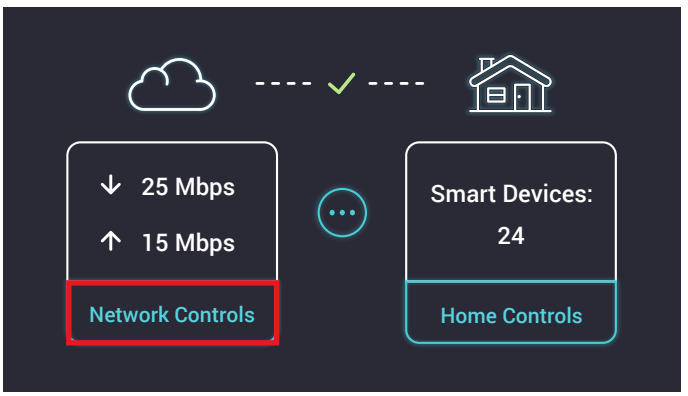




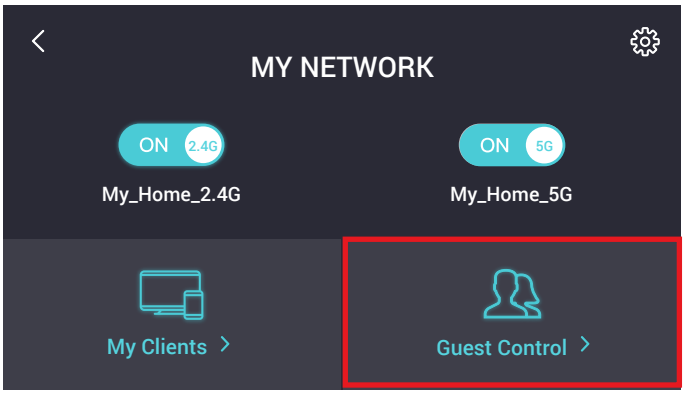
3. 2. 3. Guest Network Control

When you initially set up the router, a dedicated Wi-Fi network is automatically created for the guests to connect to, without interference with the devices connected to your private home network. The Guest Network SSID is the same as your wireless network name with a _Guest suffix, and also has its own Wi-Fi password. By default, the Guest Network password is set to auto-generate a new random password as specified (daily, weekly or monthly). However, you can set a one-time password by disabling the automatic password update feature.

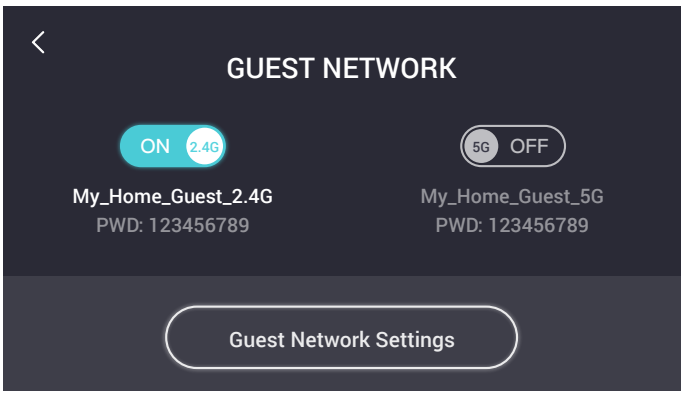
1. On the main Home screen, tap Network Controls.



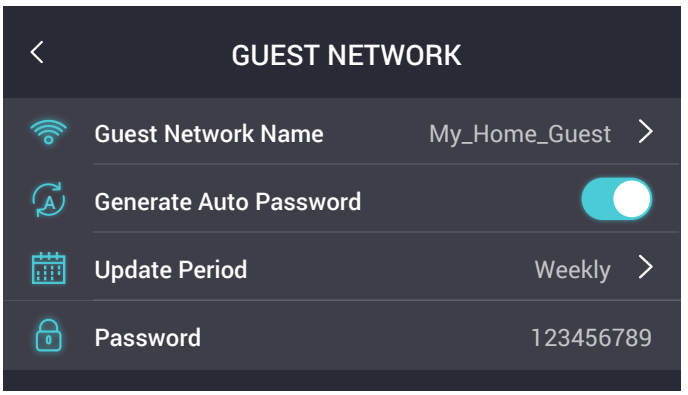
2. Tap Guest Control.



3. On the Guest Network screen, you can toggle the 2.4GHz and/or 5GHz Guest Network on or off.



4. To make changes to Guest Network, tap Guest Network Settings. You can change the Guest Network Name by tapping on it and set the frequency of the automatic password renewal to daily, weekly, or monthly. To create your own password, disable the Generate Auto Password and enter a new password.



Note:

Changing the Guest Network settings, guest devices will be disconnected from the Guest Network.

3. 3. Smart Home Configuration

3. 3. 1. Pairing ZigBee and Z-Wave Devices

Pairing various ZigBee and Z-Wave devices (such as Lights, Open/Closed Sensor, Motion Sensor, Door Locks, and Thermostats) can only be done via Kasa. Once paired, you can monitor and control your home automation devices locally and remotely through the app or control them on the router's touch screen.

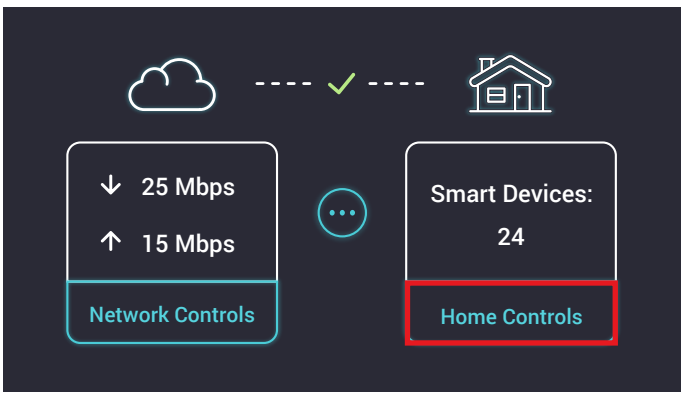
3. 3. 2. Scenes

Take full advantage of your smart home devices in your home with Scenes. A scene is a preset group of devices (such as Smart Wi-Fi Plugs Mini, Smart LED Bulbs and Smart Wi-Fi Switches) that can be programmed, customized and activated simultaneously at the touch of a button from your smartphone or tablet, allowing you to easily set your mood, activity or fit any special occasion. For example, set a customized Movie Time to turn on the home theater system plugged into a Smart Plug and dim down the lights controlled by the Smart Wi-Fi Switches in your entertainment room to 10% at the same time.

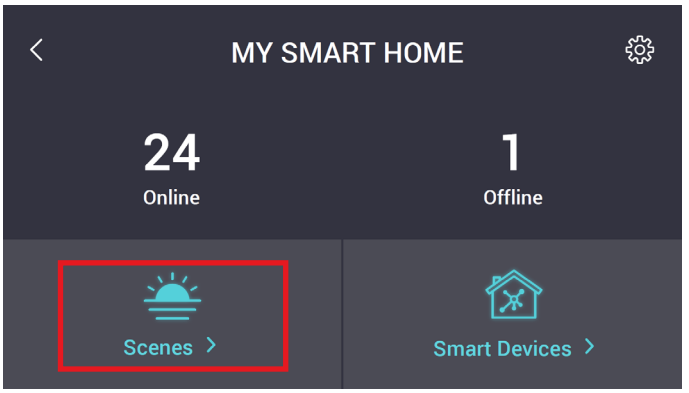
Note:

Scenes can only be created via Kasa, but will be synchronized and controllable right on the router's touch screen once you have bound your router to your Kasa account.

1. On the main Home screen, tap Home Controls.



2. Tap Scenes and select a screen you want to activate.



Note:

Scenes lets you control multiple devices simultaneously with one-button commands, while Smart Actions, which can only be done via Kasa, takes a step further in home automation to simplify your daily routine by allowing you to create smarter automatic controls based on simple logic. For instance, you can combine a Z-Wave or ZigBee Open/Closed Sensor to trigger other devices (such as lights) to turn on so that as soon as you open the door, the Smart Plug-controlled lights come on automatically.

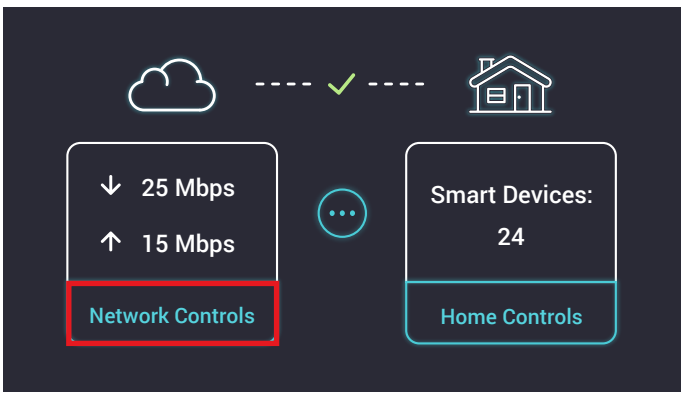
3. 4. Resetting Your Router via the Touch Screen

When you reset your router on your touch screen, all of your connected smart home devices will be disconnected, and all existing configuration settings will be deleted, including Wi-Fi settings, Kasa account association, IoT settings, any Dynamic DNS and firewall settings, and return them to factory defaults.

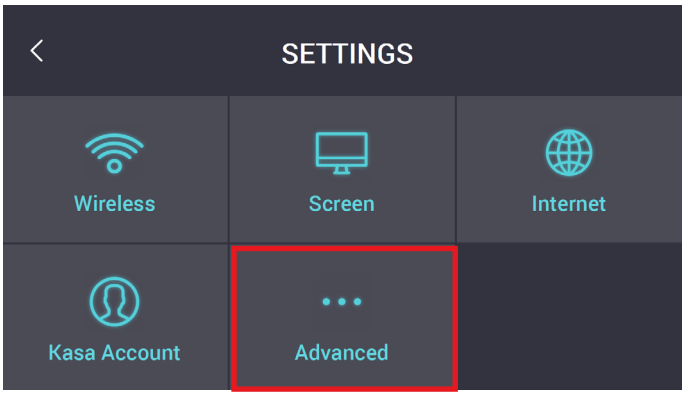
Note:

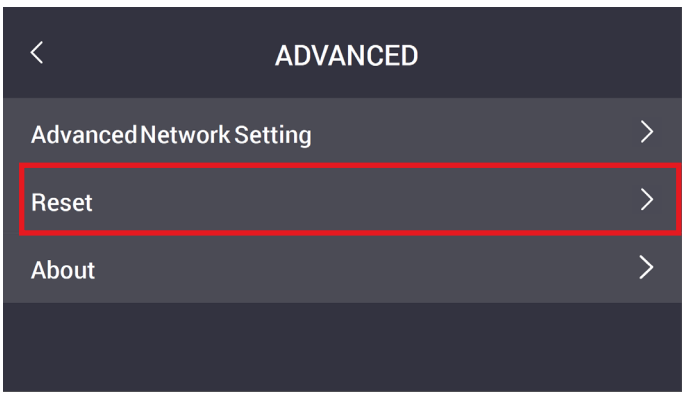
If you are simply having connection issues, you may not need to reset your router at all, but a reboot may solve the problem.

1. On the main Home screen, tap Network Controls.

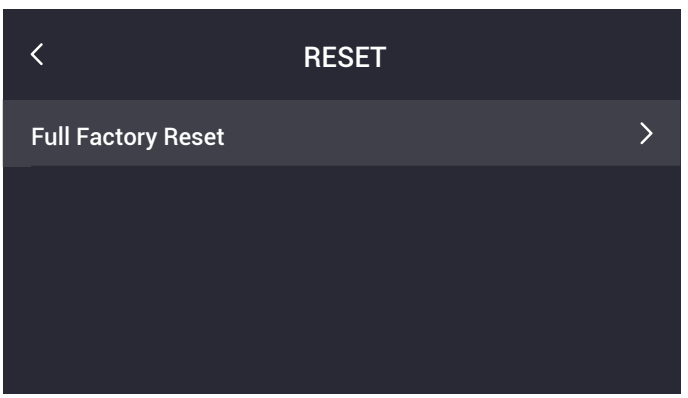


2. Tap on the (Settings) icon.
3. Tap • • • (Advanced) and then tap Reset.





4. On the Reset screen, you perform a full factory reset that will erase all configuration settings (such as network settings and wireless settings). Then confirm your selection when prompted.



Note:

The reset takes a few minutes to complete. DO NOT unplug the router or interrupt the reset process. The router will automatically reboot when the factory reset is finished.

Resetting your router can also be done via the Kasa App or using the Reset button on the rear panel of the router. Refer to Appendix: Troubleshooting for more information.

Chapter 4

Advanced Functions on Web Management Page

This chapter introduces how to configure and manage the Smart Home Router via the web management page, which supports a wide range of advanced system configurations such as QoS, VLANs, FTP connection, NAT forwarding, assigning static IP addresses for your network.

With a 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 Internet Explorer, Mozilla Firefox or Apple Safari.

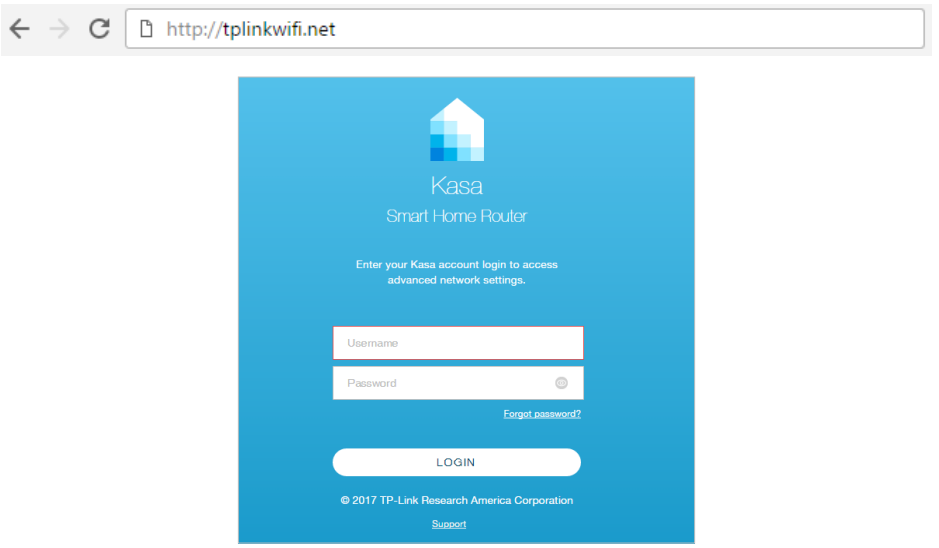
Changes made to any of the advanced functions on the web management page may negatively affect the performance of your router and local network. Therefore, such configurations should be performed with caution by experienced network users.

The (Help) icon on the upper-right corner provides help information about the settings you see on each particular screen.

4. 1. Accessing to Web Management Page

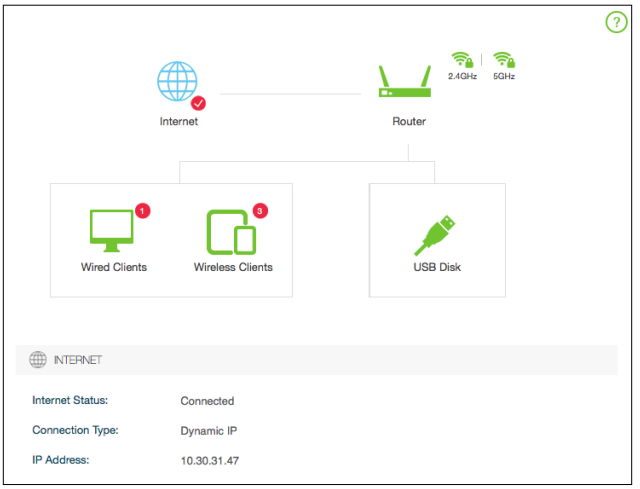
Follow the steps below to access to your router.

1. If the TCP/IP Protocol on your computer is set to the static (fixed) IP address, you need to change it to obtain an IP address automatically. Refer to Appendix: Troubleshooting to configure your computer.
2. Launch a web browser and go to http://tplinkwifi.net or http://192.168.0.1.
3. Enter your Kasa account that you used to set up your router, and click LOGIN.



4. 2. Network Status

Every time you log in to the web management page, you will be presented with a graphical Network Map that provides a static overview of your network status, including detailed information about the devices currently connected to the LAN.



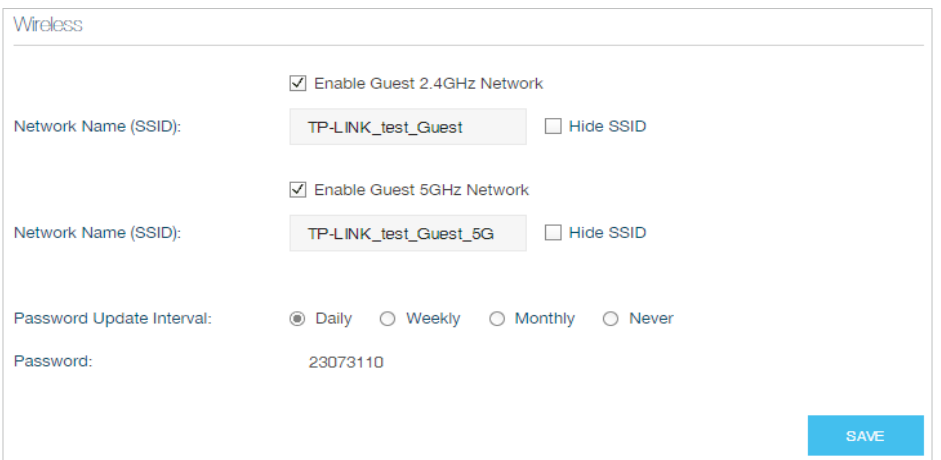
For a complete summary report of your router's health and its settings, go to Advanced > Status. The information on this page can be useful when you contact your Internet Service Provider (ISP) or TP-Link Technical Support for help.

4. 3. Guest Network

This function allows you to provide Wi-Fi access for guests without disclosing your main network. When you have guests in your house, apartment, or workplace, you can create a guest network for them. In addition, you can assign network authorities for guests to ensure network security and privacy.

4. 3. 1. Create a Network for Guests

1. Visit http://tplinkwifi.net, and log in with your Kasa account.
2. Go to Advanced > Guest Network. Locate the Wireless section.
3. Create 2.4GHz and 5GHz guest networks according to your needs.



1) Enable 2.4GHz network or 5GHz network or enable both according to your needs.

2) Set an easy-to-identify SSID. Don't select Hide SSID unless you want your guests and other people to manually input this SSID for Wi-Fi access.

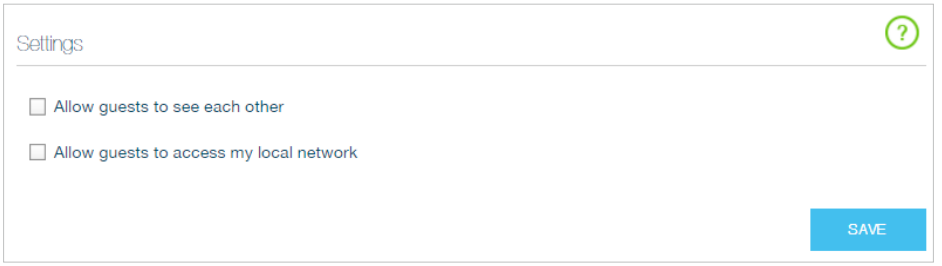
3) The 2.4GHz and 5GHz guest networks share one password. By default, the guest network password updates daily. You can change the update interval to weekly or monthly. Or you can also select Never to set a static password for your guest networks. If you select Never, please create a password between 8 and 63 ASCII characters or between 8 and 64 hexadecimal characters (0-9, a-f, A-F).

4. Click SAVE. Now your guests can access your guest network using the SSID and password you set!

Tips:
To view guest network information, go to Advanced > Status and find the Guest Network section.

4. 3. 2. Customize Guest Network Options

1. Visit http://tplinkwifi.net, and log in with your Kasa account.
2. Go to Advanced > Guest Network.



3. Assign network authorities according to your needs.
   - Allow guests to see each other

   Select this checkbox to allow the clients in your guest network to access each other.
   - Allow guests to access my local network

   Select this checkbox to allow the clients in your guest network to access your local network, not just internet access.
4. Click SAVE. Now users in your guest network can enjoy only the network authorities you assigned!

Tips:
To view guest network information, go to Advanced > Status and find the Guest Network section.

4. 4. NAT Forwarding

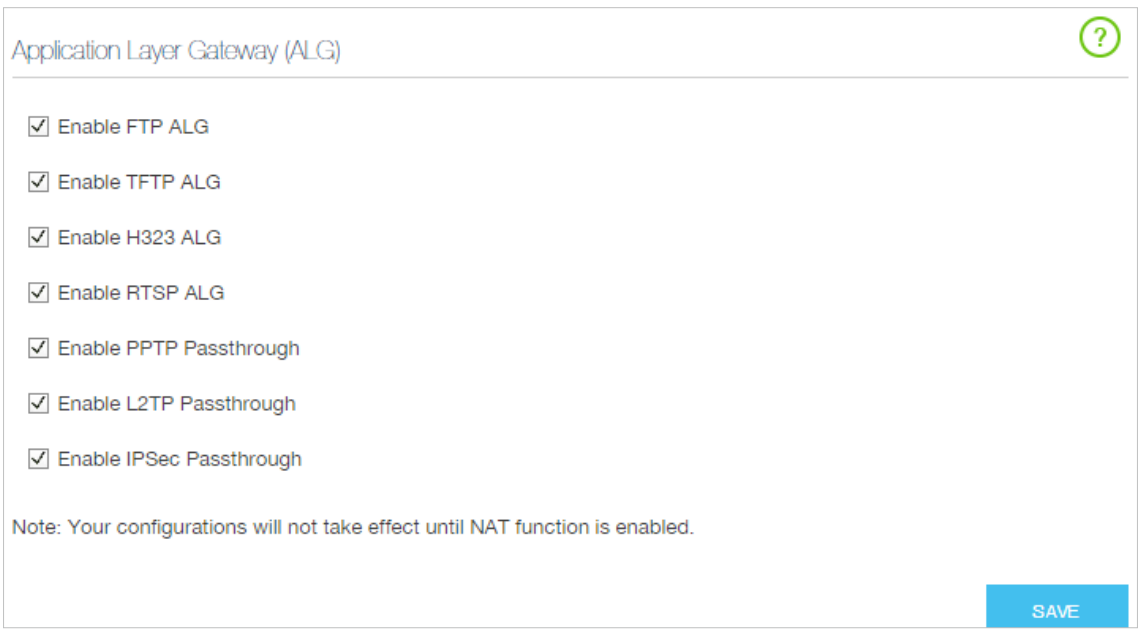
The router's NAT (Network Address Translation) feature makes the devices in the LAN use the same public IP address to communicate in the internet, which protects the local network by hiding IP addresses of the devices. However, it also brings about the problem that external host cannot initiatively communicate with the specified device in the local network. With forwarding feature the router can penetrate the isolation of NAT and allows the external hosts in the internet to initiatively communicate with the devices in the local network, thus to realize some special functions.

It 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. 4. 1. Translate Address and Port by ALG

ALG (Application Layer Gateway) allows customized NAT (Network Address Translation) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols: FTP, TFTP, H323 etc. Enabling ALG is recommended.

1. Visit http://tplinkwifi.net, and log in with your Kasa account.
2. Go to Advanced > NAT Forwarding > ALG.



- Enable FTP ALG: If enabled, it allows FTP (File Transfer Protocol) clients and servers to transfer data via NAT.
- Enable TFTP ALG: If enabled, it allows TFTP (Trivial File Transfer Protocol) clients and servers to transfer data via NAT.

- Enable H323 ALG: If enabled, it allows Microsoft NetMeeting clients to communicate via NAT.
- Enable RTSP ALG: If enabled, it allows RTSP (Real-Time Stream Protocol) clients and servers to transfer data via NAT.
- Enable PPTP Passthrough: If enabled, it allows Point-to-Point sessions to be tunneled through an IP network and passed through the router.
- Enable L2TP Passthrough: If enabled, it allows Layer 2 Point-to-Point sessions to be tunneled through an IP network and passed through the router.
- Enable IPSec Passthrough: If enabled, it allows IPSec (Internet Protocol Security) to be tunneled through an IP network and passed through the router. IPSec uses cryptographic security services to ensure private and secure communications over IP networks.

4. 4. 2. Share Local Resources in the Internet by Virtual Server

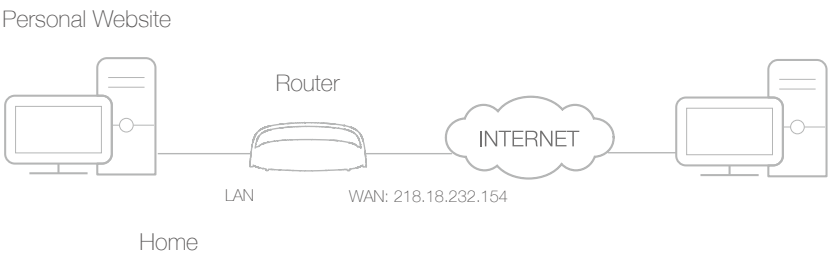
When you build up a server in the local network and want to share it on the internet, Virtual Server can realize the service and provide it to the internet users. At the same time virtual server can keep the local network safe as other services are still invisible from the internet.

Virtual server can be used for setting 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.

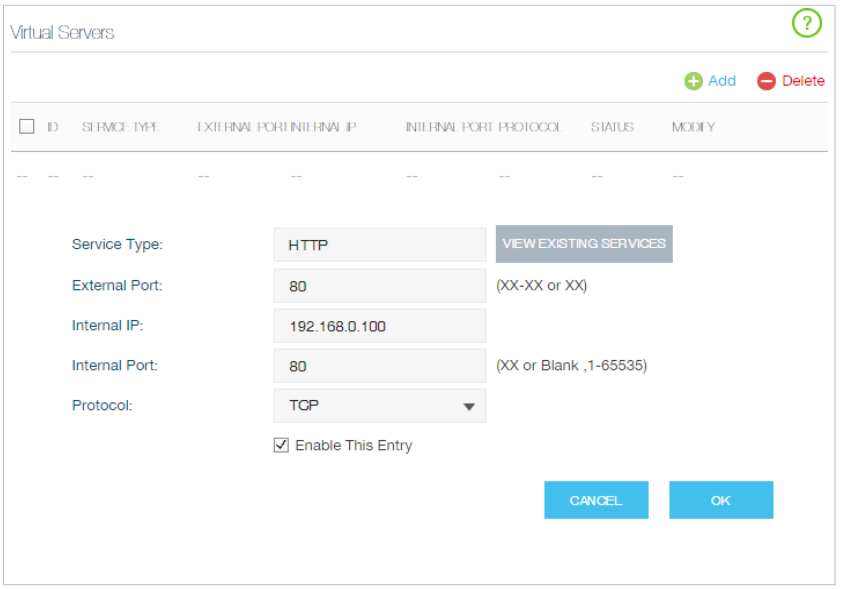
For example, the personal website has been built in my home PC (192.168.0.100). I hope that my friends in the internet can visit my website in some way. The PC is connected to the router with the WAN IP address 218.18.232.154.



How can I do that?

1. Assign a static IP address to your PC, for example 192.168.0.100.
2. Visit http://tplinkwifi.net, and log in with your Kasa account.

3. Go to Advanced > NAT Forwarding > Virtual Servers, click Add.



4. Click VIEW EXISTING SERVICES, and choose HTTP. The external port, internal port and protocol will be automatically filled with contents. Enter the PC's IP address 192.168.0.100 in the Internal IP field.

5. Click OK to save the settings.

Tips:

1. 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.
2. If the service you want to use is not in the Service Type, you can enter the corresponding parameters manually. You should verify the port number that the service needs.
3. You can add multiple virtual server rules if you want to provide several services in a router. Please note that the External Port cannot be overlapped.

Done!

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

Tips:

1. WAN IP should be a public IP address. For the WAN IP is assigned dynamically by ISP, it is recommended to apply and register a domain name for the WAN by DDNS, go to Set Up a Dynamic DNS Service Account for more information. Then you can use http://domain name to visit the website.
2. If you have changed the default External Port, you should use http://WAN IP: External Port or http://domain name: External Port to visit the website.

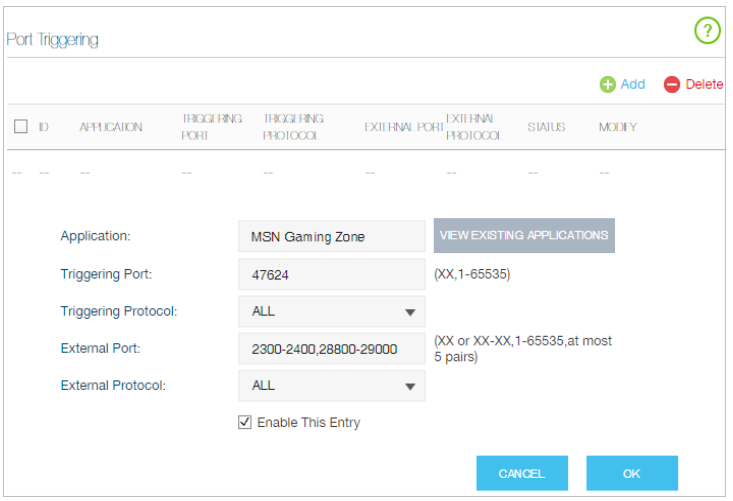
4. 4. 3. Open Ports Dynamically by Port Triggering

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 and video players. Common applications include MSN Gaming Zone, Dialpad and Quick Time 4 players, etc.

Follow the steps below to configure the port triggering rules:

1. Visit http://tplinkwifi.net, and log in with your Kasa account.
2. Go to Advanced > NAT Forwarding > Port Triggering and click Add.



3. Click VIEW EXISTING APPLICATIONS, and select the desired application. The triggering port and protocol, the external port and protocol will be automatically filled with contents. Here we take application MSN Gaming Zone as an example.
4. Click OK to save the settings.

Tips:

1. You can add multiple port triggering rules according to your network need.
2. If the application you need is not listed in the Existing Applications list, please enter the parameters manually. You should verify the external ports the application uses first and enter them into External Port field according to the format the page displays.

4. 4. 4. Make Applications Free from Port Restriction by 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, like 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.

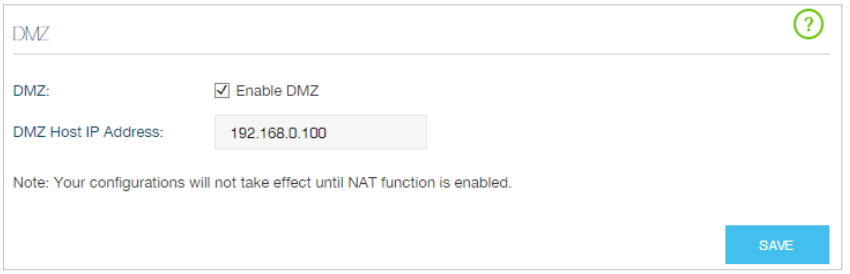
I want to:

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 login normally but cannot join a team with other players. To solve this problem, set your PC as a DMZ 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 your Kasa account.
3. Go to Advanced > NAT Forwarding > DMZ and select the checkbox to enable DMZ.



4. Enter the IP address 192.168.0.100 in the DMZ Host IP Address filed.
5. Click SAVE to save the settings.

Done!

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

4. 4. 5. Make Xbox Online Games Run Smoothly by UPnP

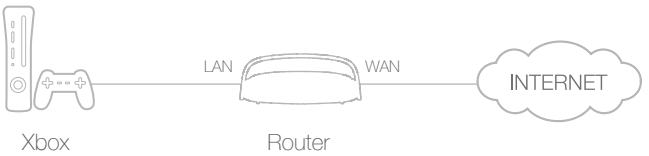
UPnP (Universal Plug and Play) protocol allows the applications or host devices to automatically find the front-end NAT device and send request to it to open the corresponding ports. With UPnP enabled, the applications or host devices in the both sides of NAT device can freely communicate with each other 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:

1. UPnP is enabled by default in this router.
2. Only the application supporting UPnP protocol can use this feature.
3. 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 has 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 your Kasa account.
2. Go to Advanced > NAT Forwarding > UPnP and toggle on or off according to your needs.

4. 5. USB Settings

This chapter describes how to share and access USB devices connected to the router among different clients. The router only supports USB external flash drives, hard drives and USB printers.

4. 5. 1. Local Storage Sharing

Share your USB storage devices with different users on the network.

4.5. 1.1. Access the USB disk

1. Connect Your USB Disk

   Insert your USB storage device into the router's USB port directly or using a USB cable.

   Tips:
   - If you use USB hubs, make sure no more than 4 devices are connected to the router.
   - If the USB storage device requires using bundled external power, make sure the external power has been connected.
   - If you use a USB hard drive, make sure its file system is FAT32, exFat, NTFS or HFS+.
   - Before you physically disconnect a USB device from the router, safely remove it to avoid data damage: Go to Advanced > USB Settings > Device Settings and click SAFELY REMOVE.

2. Access Your USB Disk

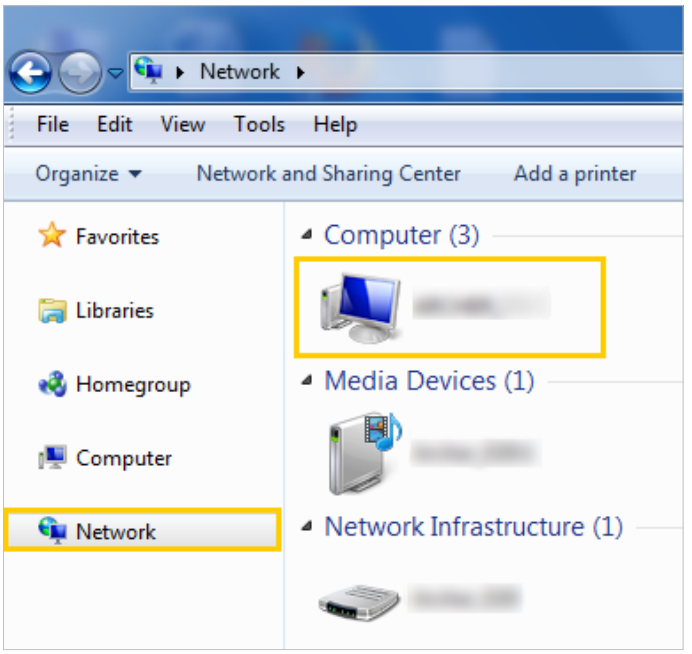
By default, all the network clients can access all folders on your USB disk. Refer to the following table for access instructions. You can also customize your sharing content and set a sharing account by referring to Customize Your Settings.

Windows computer

➢ **Method 1:**

Go to Computer > Network, then click the Network Server Name (SR20-share by default) in the Computer section.

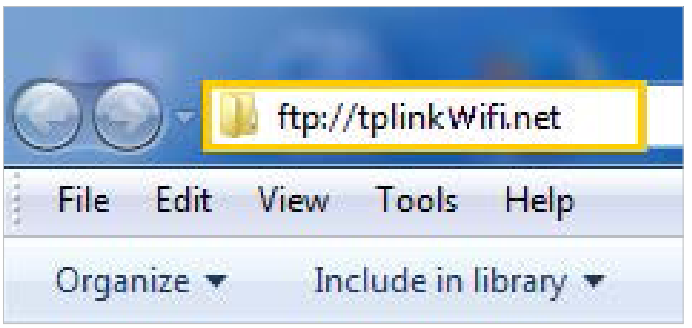
Note:
Operations in different systems are similar. Here we take Windows 7 as an example.

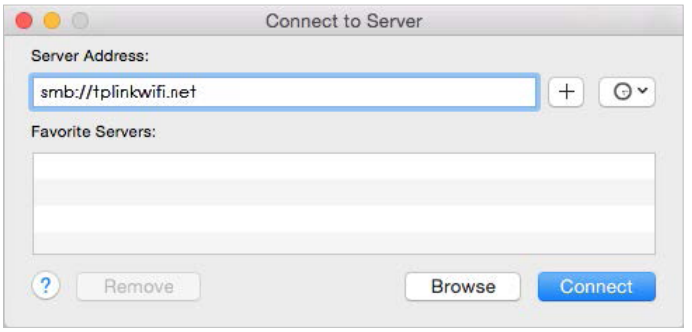


Windows computer

➢ **Method 2:**

Open the Windows Explorer (or go to Computer) and type the server address \\tplinkwifi.net or ftp://tplinkwifi.net in the address bar, then press Enter.



Mac	1) Select Go > Connect to Server 2) Type the server address smb://tplinkwifi.net 3) Click Connect  4) When prompted, select the Guest radio box. (If you have set up a username and a password to deny anonymous access to the USB disks, you should select the Registered User radio box. To learn how to set up an account for the access, refer toTo Set up Authentication for Data Security.
pad	Use a third-party app for network files management.

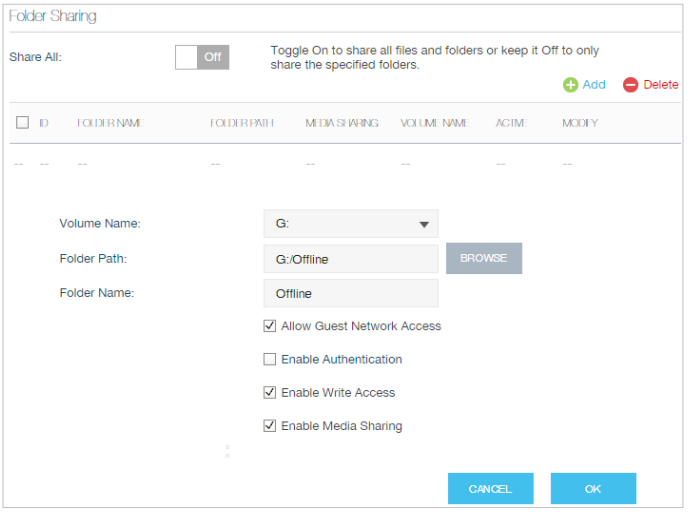
Tips:
You can also access your USB disk by using your Network/Media Server Name as the server address. Refer toTo Customize the Address of the USB Disk to learn more.

4.5. 1.2. Customize Your Settings

➢ **To Only Share Specific Content**

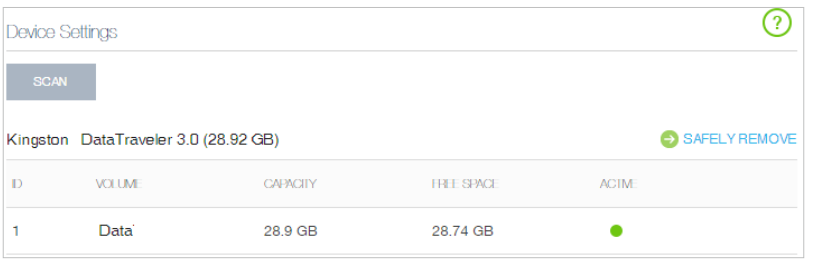
By default, Share All is enabled, so all content on the USB disk is shared. If you want to only share specific folders, follow the steps below:

1. Visit http://tplinkwifi.net, then log in with your Kasa account.
2. Select Basic > USB Settings. Focus on the Folder Sharing section. Click the button to disable Share All, then click Add to add a new sharing folder.



3. Select the Volume Name and Folder Path, then enter a Folder Name as you like.
4. Decide the way you share the folder:
   - Allow Guest Network Access: If you tick this check box, clients on Guest Network will be able to access the shared folders.
   - Enable Authentication: If you tick this check box, you will be required to use a username and password to access the folder. Refer to To Set up Authentication for Data Security to learn more.
   - Enable Write Access: If you tick this check box, network clients can modify the folder.
   - Enable Media Sharing: If you tick this check box, you can view photos, play music and watch movies in the folder directly from DLNA-supported devices. Click Media Sharing to learn more.
5. Click OK.

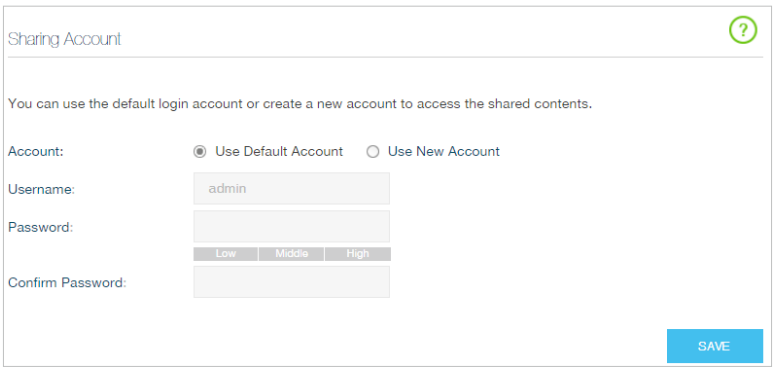
Tips:
The router can share 32 volumes at most. You can click ● on the page to detach the corresponding volume you do not need to share.



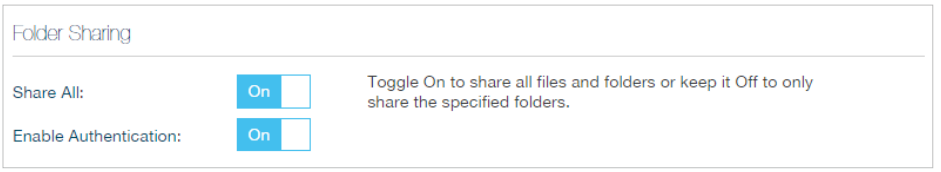
➢ To Set up Authentication for Data Security

If you enable Authentication, network clients will be required to enter the username and password you set when accessing the USB disk.

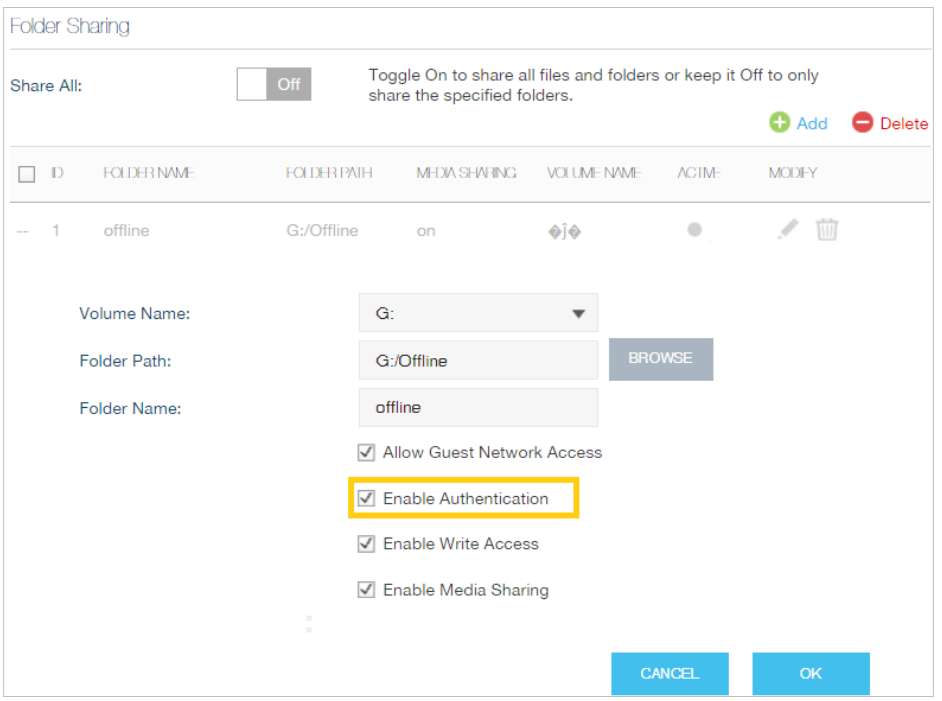
1. Visit http://tplinkwifi.net, then log in with your Kasa account.
2. Select Advanced > USB Settings > Sharing Access. Focus on the Sharing Account section.



3. Choose Use Default Account (admin) or Use New Account and click SAVE.
4. Enable Authentication to apply the account you just set.
   - If you leave Share All enabled, click the button to enable Authentication for all folders.



   - If Share All is disabled, enable Authentication for specific folders.

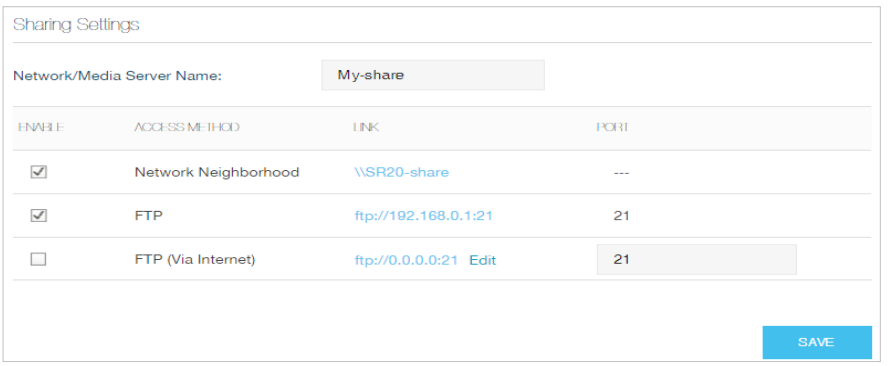


Note:
Due to Windows credential mechanism, you might be unable to access the USB disk after changing Authentication settings. Please log out from Windows and try to access again.

➢ **To Customize the Address of the USB Disk**

You can customize the server name and use the name to access your USB disk.

1. Visit http://tplinkwifi.net, then log in with the username and password you set for the router.
2. Select Advanced > USB Settings > Sharing Access. Focus on the Sharing Settings section.
3. Make sure Network Neighborhood is ticked, and enter a Network/Media Server Name as you like, such as My-share, then click SAVE.



4. Now you can access the USB disk by visiting \\My-share (for Windows) or smb://My-share (for Mac).

4. 5. 2. Remote Access via FTP Server

You can access your USB disk outside the local area network.

For example:

- Share photos and other large files with your friends without logging in to (and paying for) a photo-sharing site or email system.
- Get a safe backup for the materials for a presentation.
- Remove the files on your camera's memory card from time to time during the journey.

Note:
If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), you cannot use this feature because private addresses are not routed on the internet.

4.5. 2.1. Access the USB disk

1. **Connect Your USB Disk**

Insert your USB storage device into the router's USB port directly or using a USB cable.

Tips:

- If you use USB hubs, make sure no more than 4 devices are connected to the router.
- If the USB storage device requires using bundled external power, make sure the external power has been connected.
- If you use a USB hard drive, make sure its file system is FAT32, exFat, NTFS or HFS+.
- Before you physically disconnect a USB device from the router, safely remove it to avoid data damage: Select Advanced > USB Settings > Device Settings and click SAFELY REMOVE.

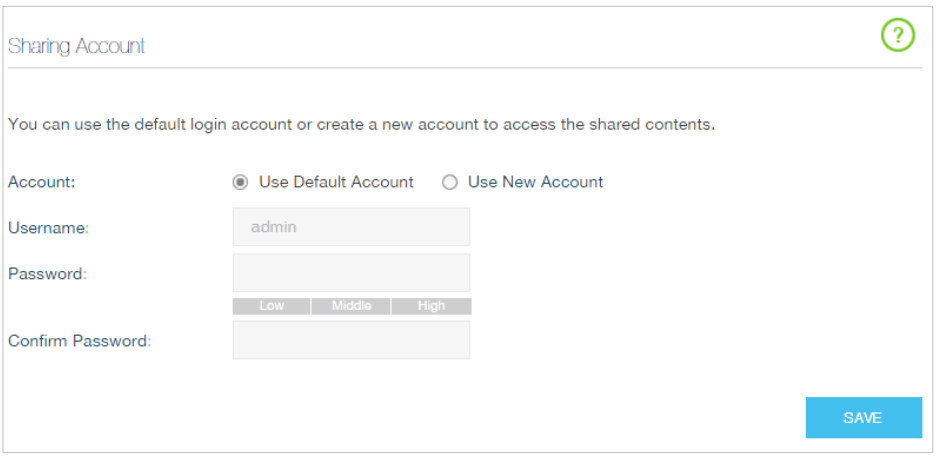
2. Enable Authentication for Data Security

It is strongly recommended that you set and apply a sharing account for data security.

1) Visit http://tplinkwifi.net, then log in with your Kasa account.

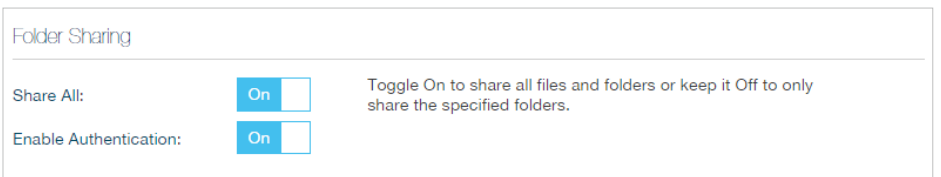
2) Select Advanced > USB Settings > Sharing Access.

3) Choose Use default Account (admin) or Use New Account and click SAVE.

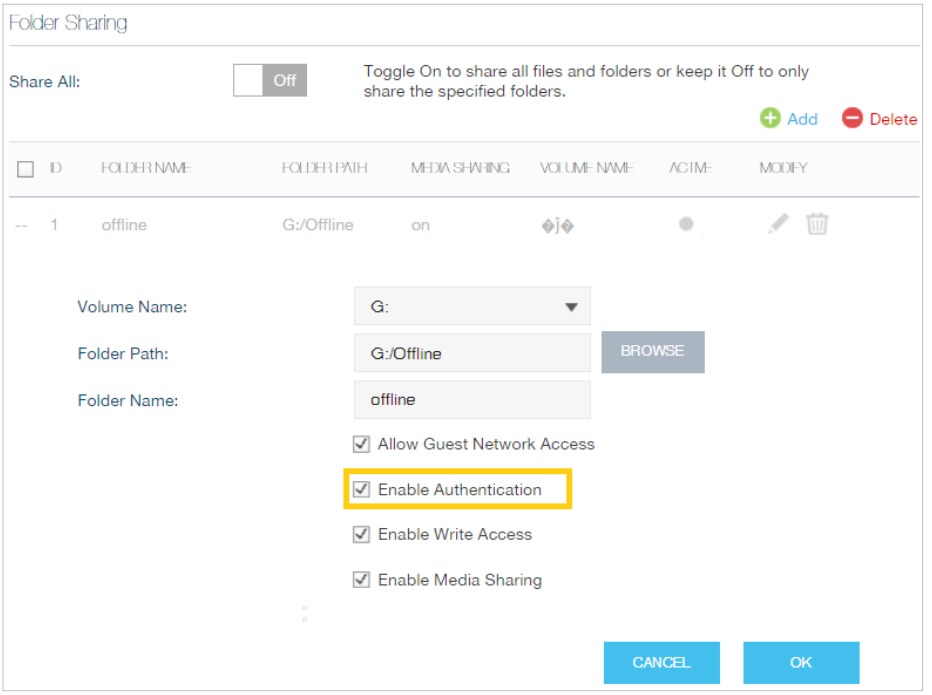


4) Enable Authentication to apply the sharing account.

- If you leave Share All enabled, click the button to enable Authentication for all folders.

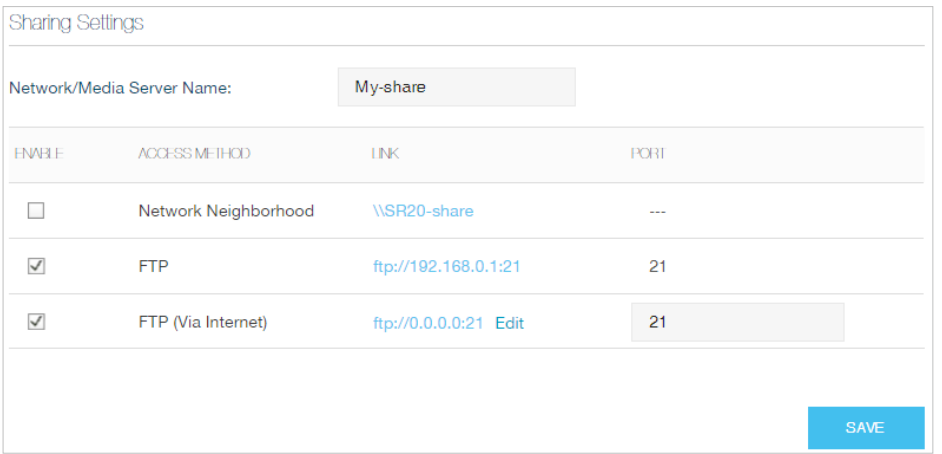


- If Share All is disabled, enable Authentication for specific folders.



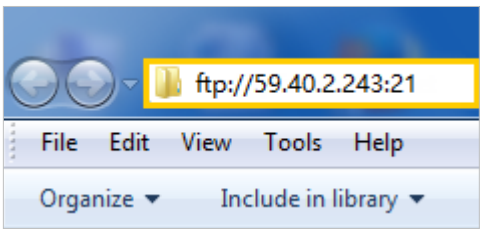
3. **Enable the FTP (via Internet)**

   Select the check box to enable FTP (via Internet), then click SAVE.



4. **Access Your USB Disk via Internet**

   Now different clients with internet connection can access the USB disk:

Computer	1) Open the Windows Explorer (or go to Computer, only for Windows users) or open a web browser. 2) Type the server address in the address bar: Type in ftp://<WAN IP address of the router>:<port number> (such as ftp://59.40.2.243:21). If you have specified the domain name of the router, you can also type in ftp://<domain name>:<port number> (such as ftp://MyDomainName:21)  The Address Bar of the Windows Explorer (Windows 7) 3) Press Enter on the keyboard. 4) Access with the username and password you set in Step 2. Tips: You can also access the USB disk via a third-party app for network files management, which can resume broken file transfers.
Pad	Use a third-party app for network files management.

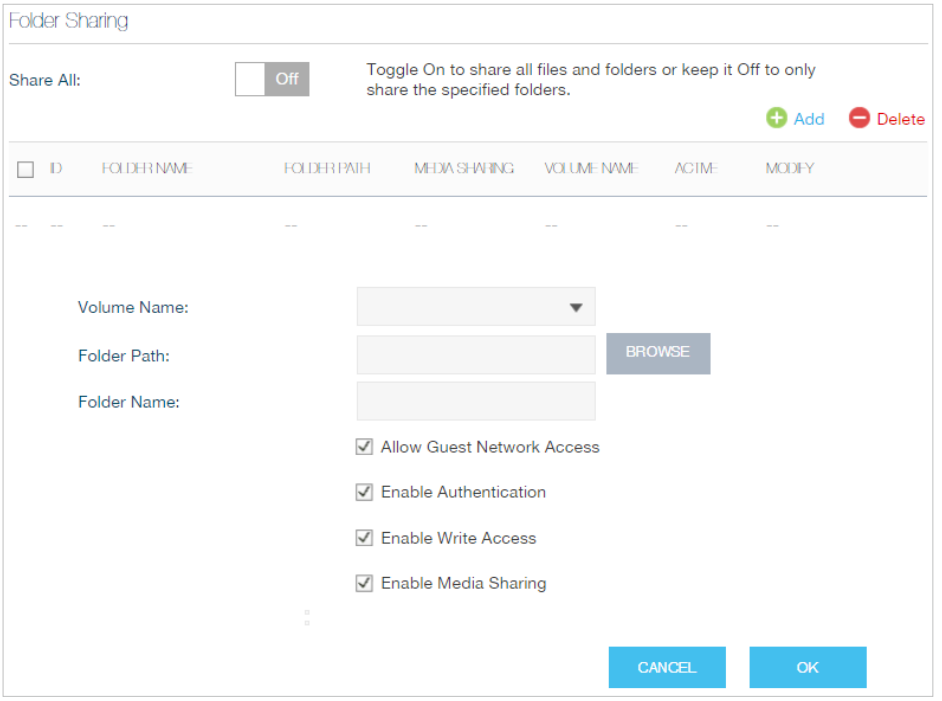
Tips:
Click Set Up a Dynamic DNS Service Account to learn how to set up a domain name for you router.

4.5. 2.2. Customize Your Settings

➢ **To Only Share Specific Content**

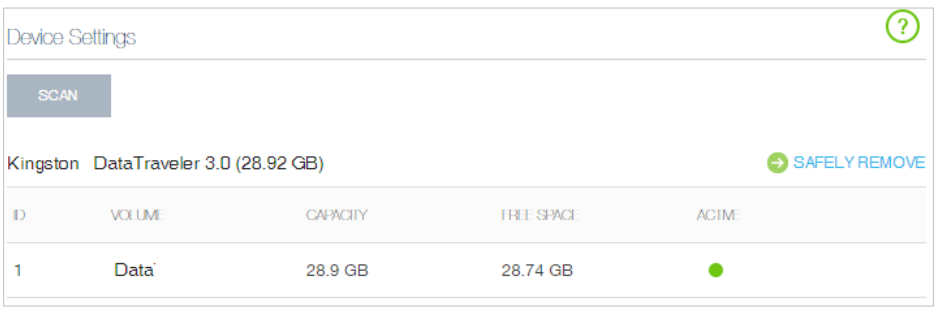
By default, Share All is enabled so all content on the USB disk is shared. If you want to only share specific folders, follow the steps below:

1. Visit http://tplinkwifi.net, then log in with your Kasa account.
2. Select Basic > USB Settings. Focus on the Folder Sharing section. Click the button to disable Share All, then click Add to add a new sharing folder.



3. Select the Volume Name and Folder Path, then specify the Folder Name as you like.
4. Tick Enable Authentication. If you allow network clients to modify this folder, tick Enable Write Access.
5. Click OK.

Tips:
The router can share 32 volumes at most. You can click ● on the page to detach the corresponding volume you do not need to share.



4. 5. 3. Media Sharing

The Media Sharing feature allows you to view photos, play music and watch movies stored on the USB disk directly from DLNA-supported devices, such as your computer, pad and PS2/3/4.

4.5. 3.1. Access the USB disk

1. Connect Your USB Disk

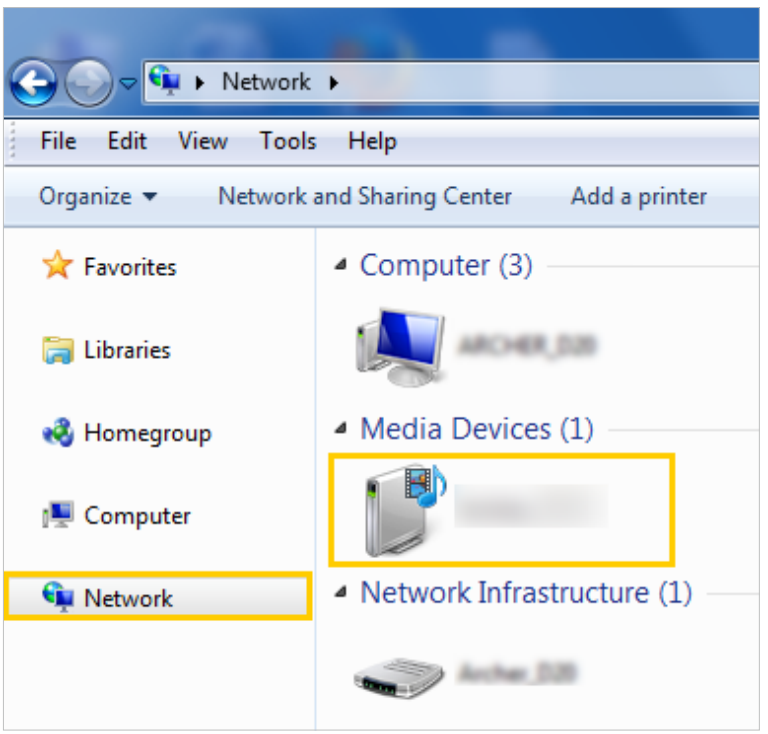
Insert your USB storage device into the router's USB port directly or using a USB cable.

Tips:

- If you use USB hubs, make sure no more than 4 devices are connected to the router.
- If the USB storage device requires using bundled external power, make sure the external power has been connected.
- If you use a USB hard drive, make sure its file system is FAT32, exFat, NTFS or HFS+.
- Before you physically disconnect a USB device from the router, safely remove it to avoid data damage: Go to Advanced > USB Settings > Device Settings and click SAFELY REMOVE.

2. Access the Media Files on Your USB Disk

Now the DLNA-supported devices (such as your computer and pad) connected to the router can detect and play the media files on the USB disks.

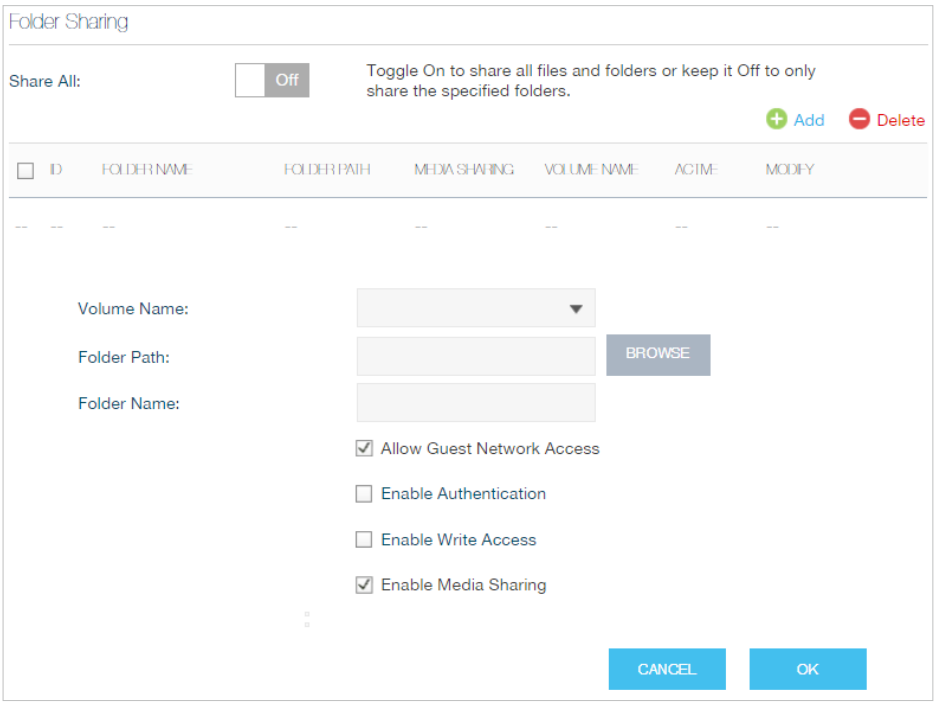
Windows computer	• Go to Computer > Network, then click the Media Server Name (SR20-share by default) in the Media Devices section. Note: Here we take Windows 7 as an example. 
Pad	• Use a third-party DLNA-supported player.

4.5. 3.2. Customize Your Settings

➢ **To Only Share Specific Content**

By default, Share All is enabled so all content on the USB disk is shared. If you want to only share specific folders, follow the steps below:

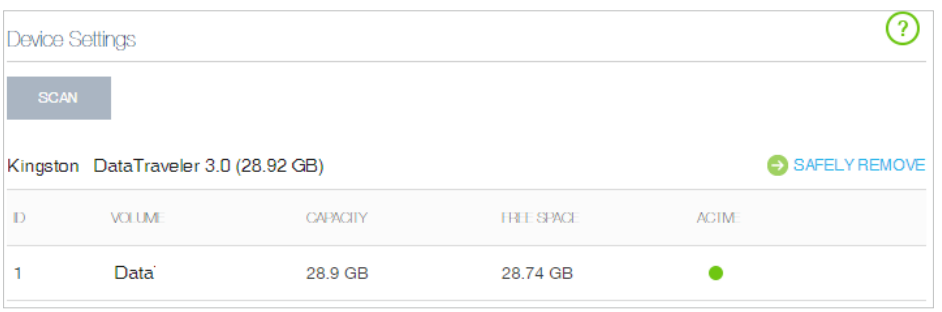
1. Visit http://tplinkwifi.net, then log in with your Kasa account.
2. Select Basic > USB Settings.
3. Focus on the section of Folder Sharing. Click the button to disable Share All, then click Add to add a new sharing folder.



4. Select the Volume Name and Folder Path, then enter a Folder Name as you like.
5. Tick Enable Media Sharing and click OK.

Tips:

The router can share 32 volumes at most. You can click ● on the page to detach the corresponding volume you do not need to share.



4. 5. 4. Printer Sharing

The Printer Sharing feature helps you share a printer with different computers connected to the router.

Note:
Printers unlisted on this page may be incompatible with the router:
http://www.tp-link.com/common/compatible/print-server/.

1. **Install the Driver of the Printer**

   Make sure you have installed the driver of the printer on each computer that needs printer service.

   If you do not have the driver, contact the printer manufacturer.

2. **Connect the Printer**

   Cable a printer to the USB port with the USB cable.

3. **Install the TP-LINK USB Printer Controller Utility**

   TP-LINK USB Printer Controller Utility helps you access the shared printer. Download and Install the utility on each computer that needs printer service.

   1) Visit http://www.tp-link.com/app/usb/.

   2) Click PC Utility (for Windows users) or Mac Utility to download the installation file and uncompress it.

   3) Open the uncompressed folder, then click TP-LINK USB Printer Controller Setup (for Windows users) or TP-Link UDS Printer Controller Installer (for Mac users) to install the utility.

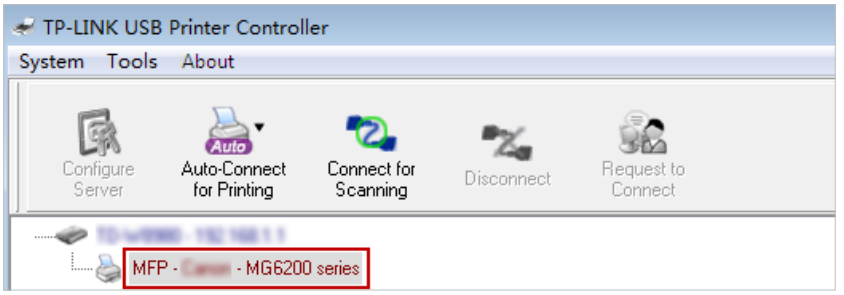
4. **Access the Printer**

   You should set the shared printer as Auto-Connect Printer on every computer that needs printer service.

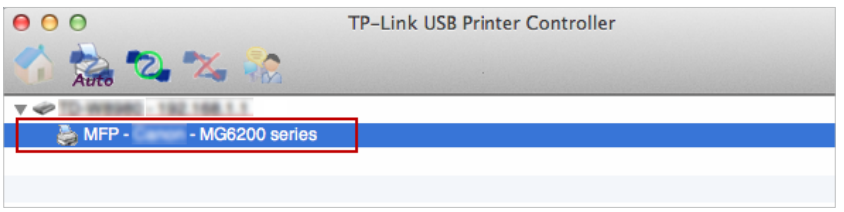
   1) Double-click the icon 

(USB Printer Controller) on your desktop to launch the USB Printer Controller.

   2) Highlight the printer you share.

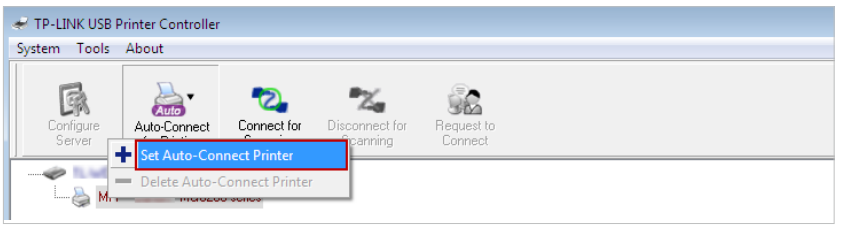


Windows

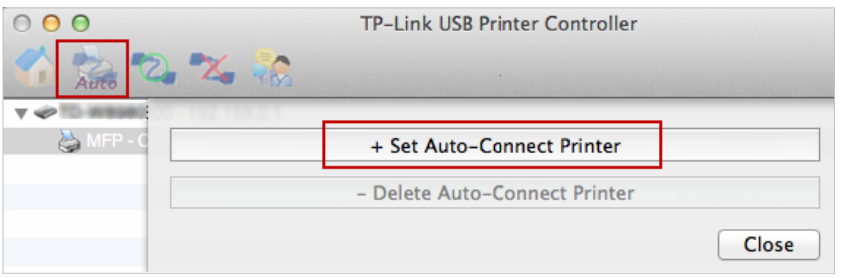


Mac

3) Click the Auto-Connect for printing tab to pull down a list, then select Set Auto-Connect Printer.

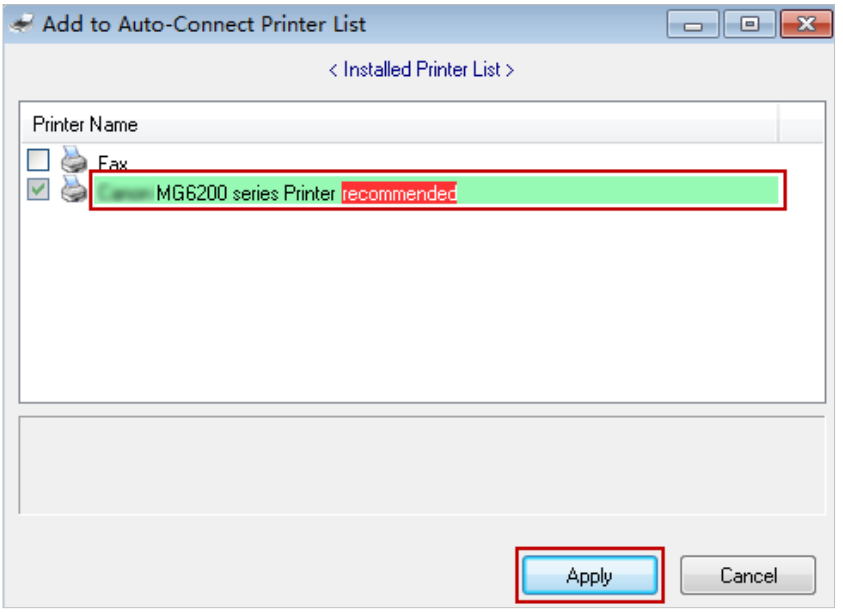


Windows

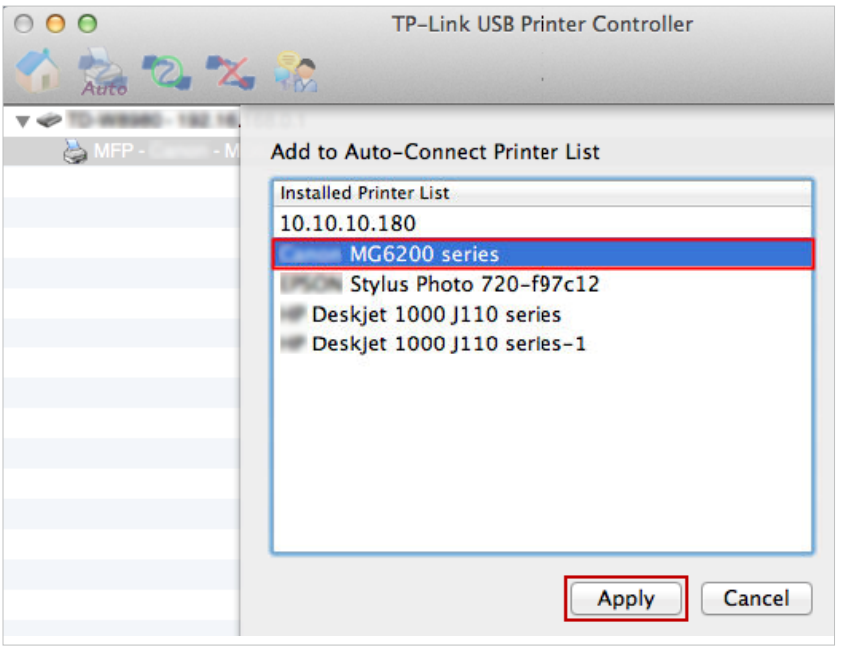


Mac

4) Select the printer you share, then click Apply.

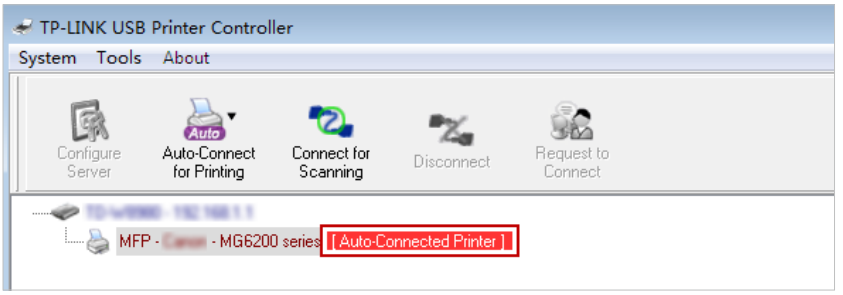


Windows



Mac

5) You will see the printer marked as Auto-Connect Printer. Now you can print with this printer.



Windows

Mac

Tips:
The Print Server also allows different clients to share the scan feature of MFPs (Multi-Function Printers). To scan with TP-LINK USB Printer Controller, right-click the printer and select Network Scanner. Then, a scanning window will pop up. Finish the scanning process by following on-screen instructions.

4. 6. Parental Controls

This function allows you to block inappropriate, explicit and malicious websites, and control access to specified websites at specified time.

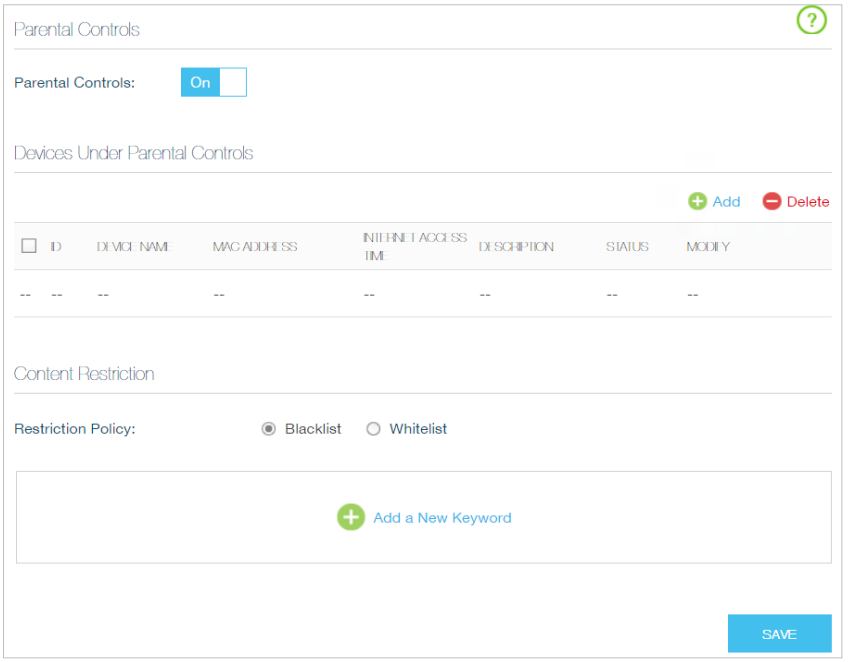
I want to:

Control what types of websites my children or other home network users can visit and even the time of day they are allowed to access the internet.

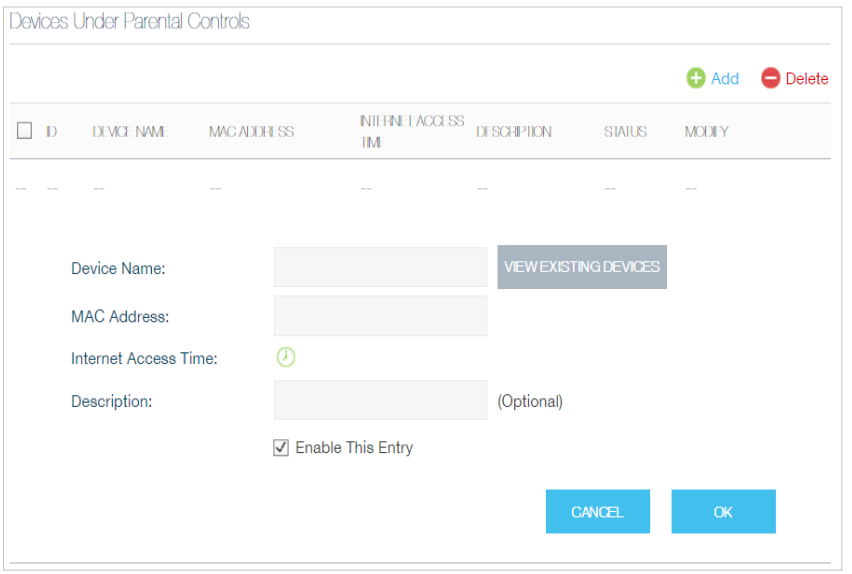
For example, I want to allow my children's devices (e.g. a computer or a tablet) to access only www.tp-link.com and wikipedia.org from 18:00 (6PM) to 22:00 (10PM) on weekdays and not other time.

How can I do that?

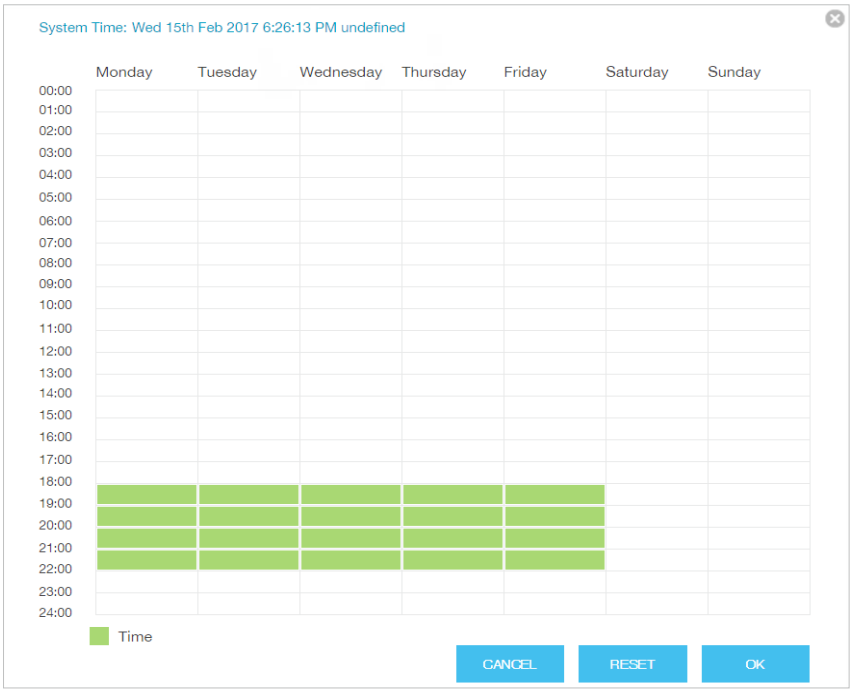
1. Visit http://tplinkwifi.net, and log in with your Kasa account.
2. Go to Advanced > Parental Controls and enable Parental Controls.



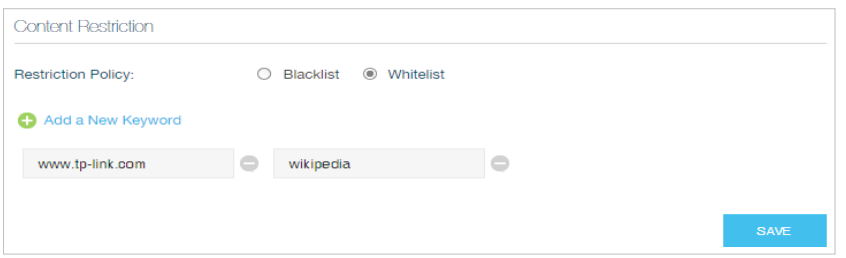
3. Click Add.



4. Click VIEW EXISTING DEVICES, and add the device to be controlled. Or, enter the Device Name and MAC Address manually.
5. Click the icon to set the Effective Time. Drag the cursor over the appropriate cell(s) and click OK.



6. Enter a Description for the entry.
7. Select the checkbox to enable this entry and click OK.
8. Locate Content Restriction and select the restriction mode.
   1) In Blacklist mode, the controlled devices cannot access any websites containing the specified keywords during the Effective Time period.
   2) In Whitelist mode, the controlled devices can only access websites containing the specified keywords during the Effective Time period.



9. Click Add a New Keyword. You can add many keywords for both Blacklist and Whitelist. Below are some sample entries to allow access.
   1) Enter a web address (e.g. www.tp-link.com) or a web address keyword (e.g. wikipedia) to only allow or block access to the websites containing that keyword.

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

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

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

4. 7. QoS

This part introduces how to create a QoS (Quality of Service) rule to prioritize traffic and minimize the impact caused when the connection is under heavy load.

4. 7. 1. Prioritize Internet Traffic with QoS

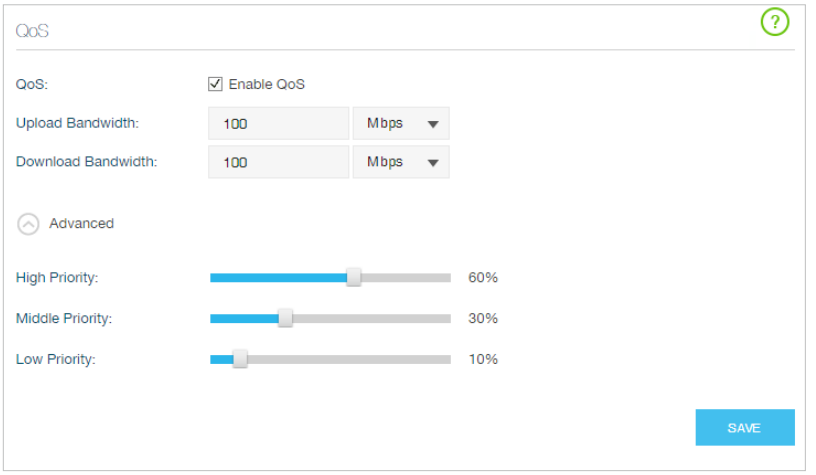
QoS (Quality of Service) is designed to ensure the efficient operation of the network when come across network overload or congestion.

I want to: Specify priority levels for some devices or applications.

For example, I have several devices that are connected to my wireless network. I would like to set an intermediate speed on the internet for my phone.

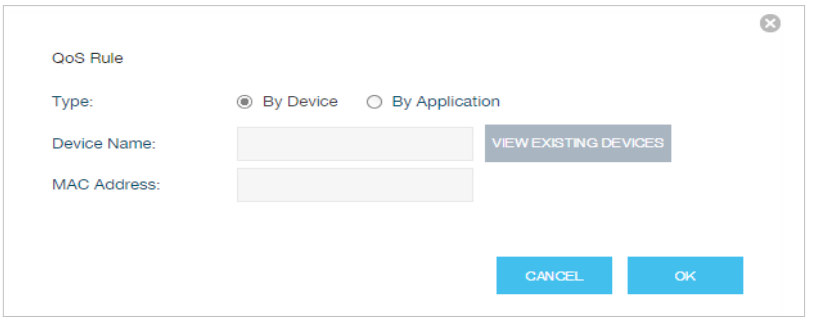
How can I do that?

1. Enable QoS and set bandwidth allocation.
   1) Visit http://tplinkwifi.net, and log in with your Kasa account.
   2) Go to Advanced > QoS > Settings.
   3) Select Enable QoS.
   4) Input the maximum upload and download bandwidth provided by your internet service provider. 1Mbps equals to 1024Kbps.
   5) Click Advanced and drag the scroll bar to set the bandwidth priority percentage.
   6) Click SAVE.

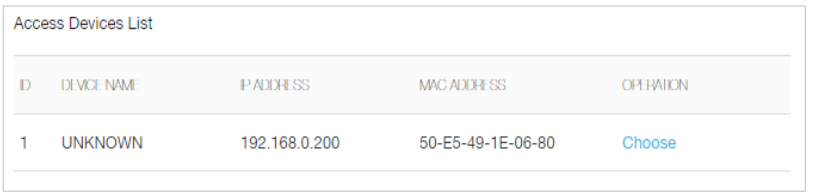


2. Add a middle priority QoS rule for the phone.

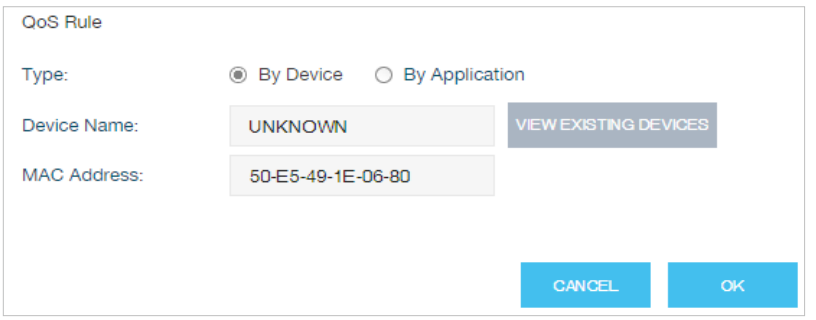
   1) Click Add in the Middle Priority area and then select By Device and click VIEW EXISTING DEVICES.



   2) Choose the respective device from the list.



   3) Click OK.



3. Refer to the steps above to apply other QoS rules if any.

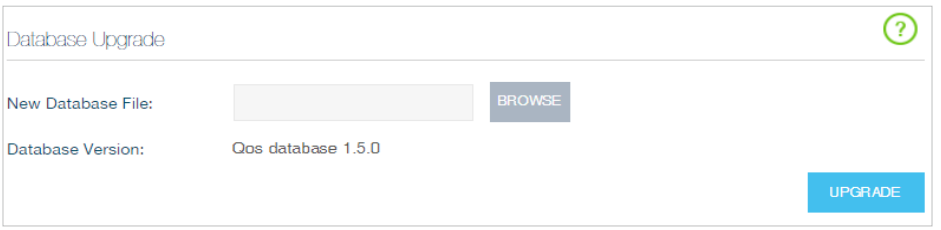
Note:
If you want to delete a QoS rule, click to remove the responding rule from the list.

Done! Now QoS is implemented to prioritize internet traffic.

4. 7. 2. Upgrade the Database

This function can help to add or update the applications the router supports. If the applications you need are not listed in the Application list, you can try to download the new version and upgrade the database. New database versions are posted at www.tp-link.com and can be downloaded for free.

1. Download the latest QoS database from our website (www.tp-link.com).
2. Visit http://tplinkwifi.net, and log in with your Kasa account.
3. Go to Advanced > QoS > Database. Click BROWSE to select the database upgrade file, and then click UPGRADE. Wait until the upgrade is completed and do not operate during the process.



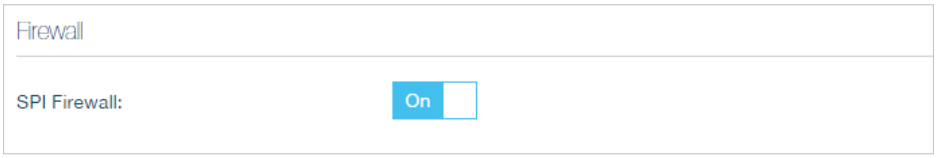
4. 8. Network Security

This part guides you on how to protect your home network from unauthorized users by implementing these three network security functions. You can block or allow specific client devices to access your wireless network using MAC Filtering, or using Access Control for wired and wireless networks, or you can prevent ARP spoofing and ARP attacks by using IP & MAC Binding.

4. 8. 1. Firewall & DoS Protection

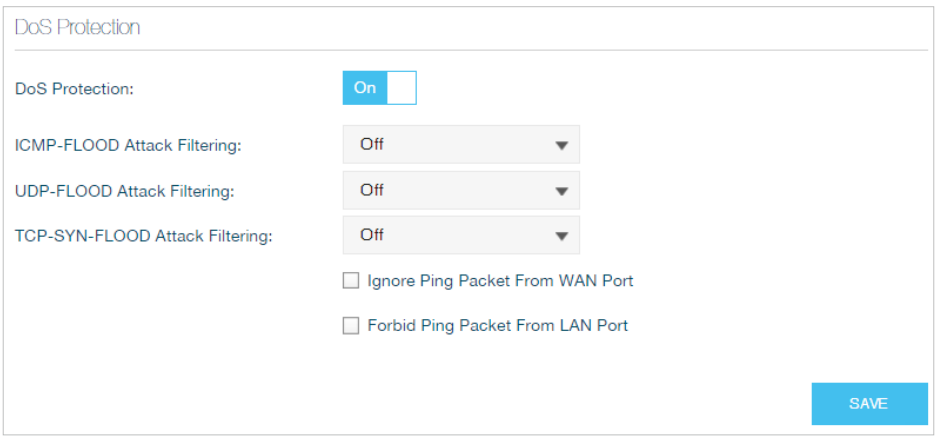
The SPI (Stateful Packet Inspection) Firewall and DoS (Denial of Service) Protection protect the router from cyber attacks.

The SPI Firewall can prevent cyber attacks and validate the traffic that is passing through the router based on the protocol. This function is enabled by default, and it's recommended to keep the default settings.



DoS Protection can protect your home network against DoS attacks from flooding your network with server requests. Follow the steps below to configure DoS Protection.

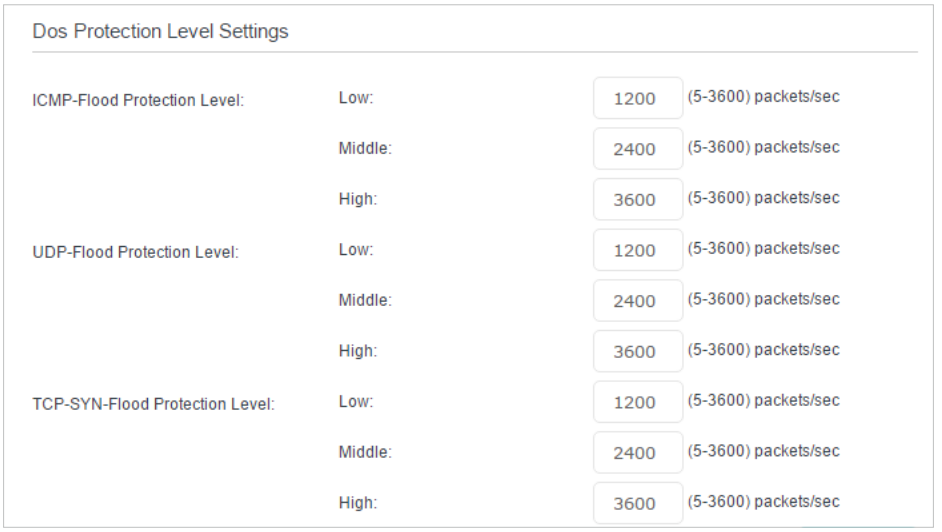
1. Visit http://tplinkwifi.net, and log in with your Kasa account.
2. Go to Advanced > Security > Settings > DoS Protection.



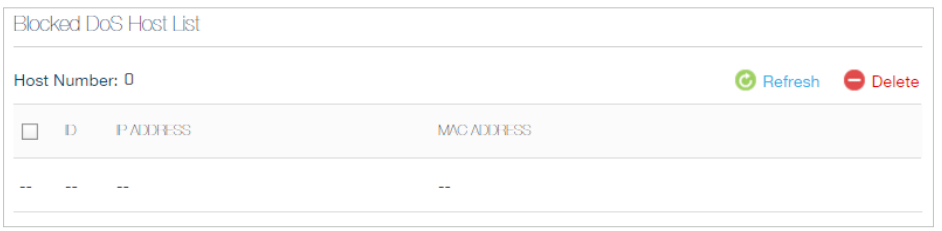
3. Enable DoS Protection.
4. Set the level (Off, Low, Middle or High) of protection for ICMP-Flood Attack Filtering, UDP-Flood Attack Filtering and TCP-SYN-Flood Attack Filtering.
   - ICMP-Flood Attack Filtering - Enable to prevent the ICMP (Internet Control Message Protocol) flood attack.
   - UDP-Flood Attack Filtering - Enable to prevent the UDP (User Datagram Protocol) flood attack.
   - TCP-SYN-Flood-Attack Filtering - Enable to prevent the TCP-SYN (Transmission Control Protocol-Synchronize) flood attack.
   - Enable Ingore Ping Packet From WAN/LAN Port or Forbid Ping Packet From LAN Port if necessary.
5. Click SAVE.

Tips:

1. The level of protection is based on the number of traffic packets. Specify the level at Advanced > System Tools > System Parameters.



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



4. 8. 2. Access Control

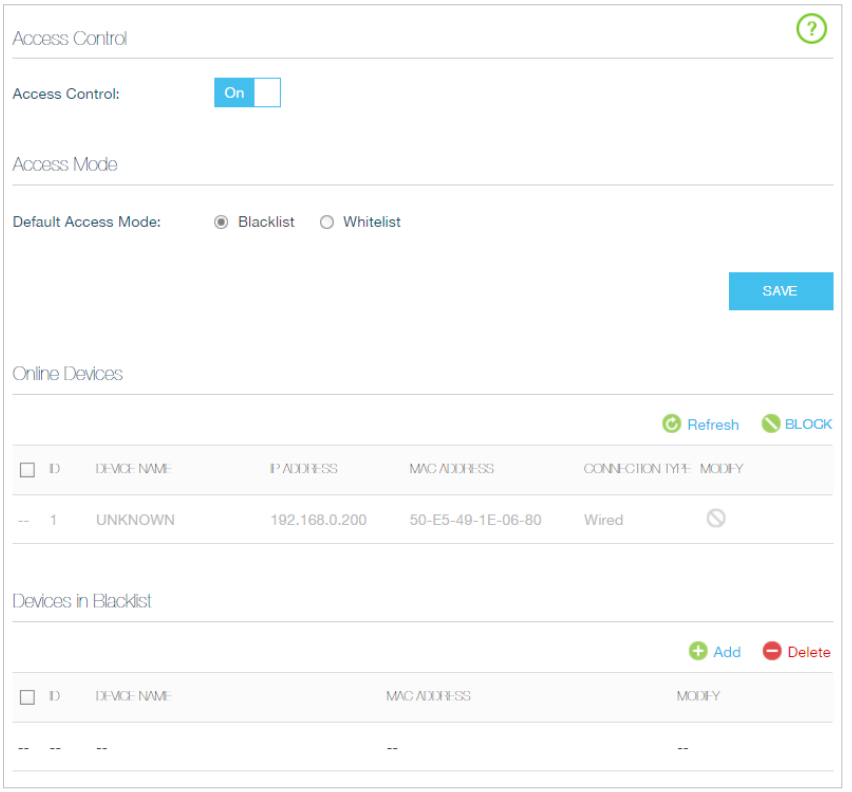
Access Control is used to block or allow specific client devices to access your network (via wired or wireless) based on a list of blocked devices (Blacklist) or a list of allowed devices (Whitelist).

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://tplinkwifi.net, and log in with your Kasa account.
2. Go to Advanced > Security > Access Control and enable 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.

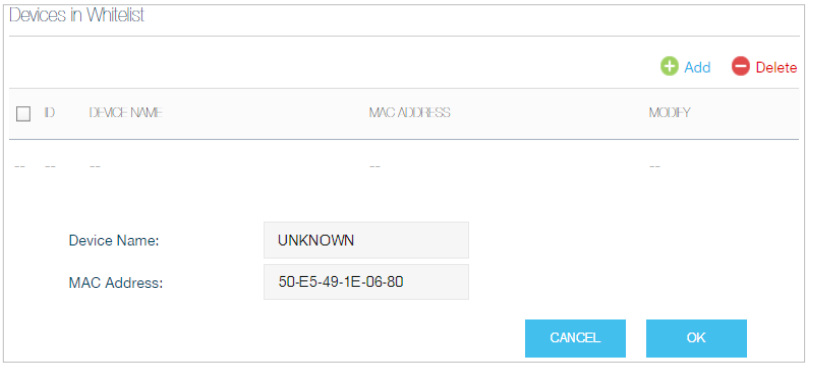
   2) Select the device(s) to be blocked in the Online Devices table.

   3) Click BLOCK above the Devices Online table. The selected devices will be added to Devices in Blacklist automatically.

   To allow specific device(s)

   1) Select Whitelist and click SAVE.

   2) Click Add.



3) Enter the Device Name and MAC Address (You can copy and paste the information from Online Devices table if the device is connected to your network).

4) Click OK.

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

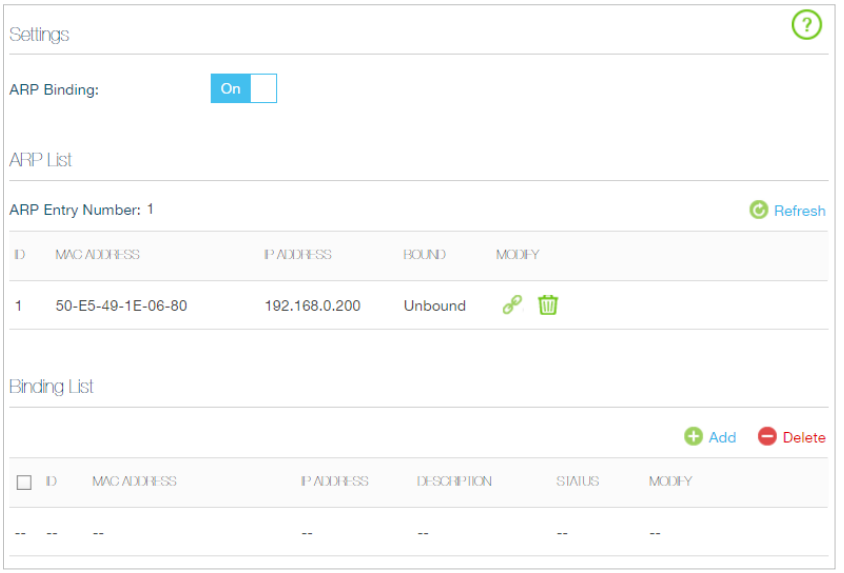
4. 8. 3. IP & MAC Binding

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://tplinkwifi.net, and log in with your Kasa account.
2. Go to Advanced > Security > IP & MAC Binding and enable IP & MAC Binding.



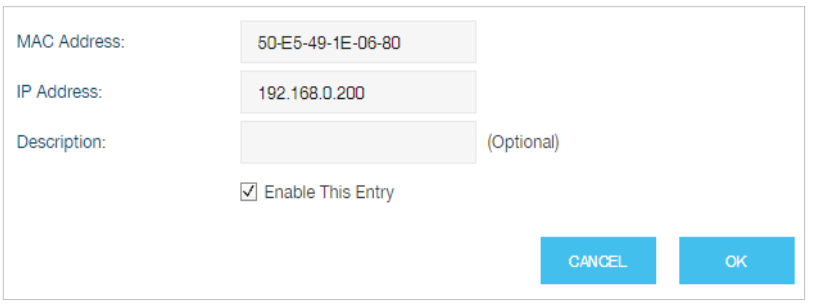
3. Bind your device(s) according to your needs.

   To bind the connected device(s)

   Click 🔗 to add the device(s) to be bound in the ARP List to the Binding List.

   To bind the unconnected device

   1) Click Add.



   2) Enter the MAC address and IP address that you want to bind. Enter the description of the entry if necessary.

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

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

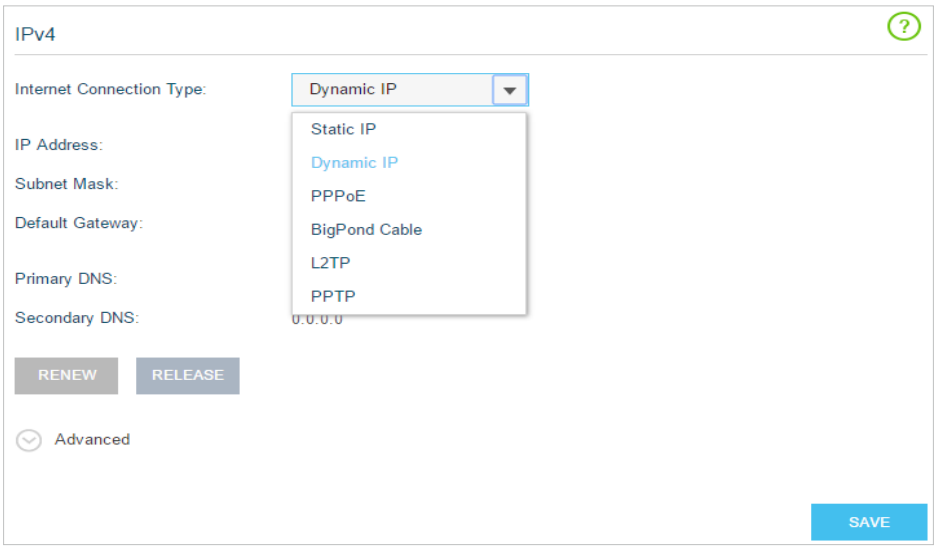
4. 9. IPv4 & IPv6

When you set up the router for the first time, the router will automatically detect your Internet (WAN) connection type. If the router cannot detect or you wish to manually

configure the internet connection type and its related settings, you should consult with your ISP before doing so.

4. 9. 1. IPv4

1. Visit http://tplinkwifi.net, and log in with your Kasa account.
2. Go to Netwrok > Internet.
3. Select the internet connection type provided by your ISP.



- Static IP: Select this option if your ISP has assigned a fixed (static) IP address. Enter the assigned IP address, subnet mask, default gateway IP address and the ISP's DNS server IP address(es).
- Dynamic IP: Select this option if you are provided with a DHCP server connection, typically cable modem. Click RENEW to renew the IP parameters from the ISP or click RELEASE to release the assigned IP parameters.
- PPPoE: Select this option if you have Digital Subscriber Line (DSL) service that requires an authorization to connect.
- BigPond Cable: Select this option if you have BigPond Cable service that requires an authorization.
- L2TP/PPTP: Select L2TP or PPTP if you connect to the ISP's VPN server.

4. Click SAVE to save all your settings.

Note:

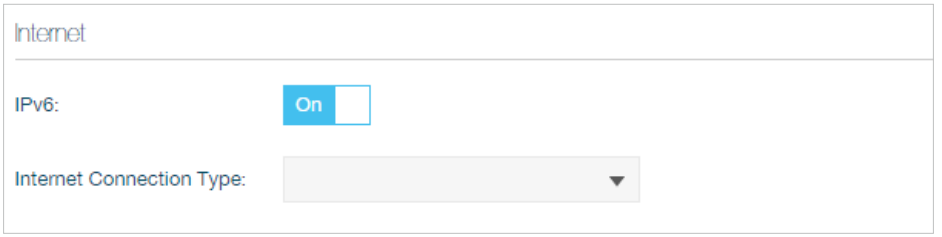
Click (Help) icon on the upper-right corner of the web management page to know more about items.

4. 9. 2. IPv6

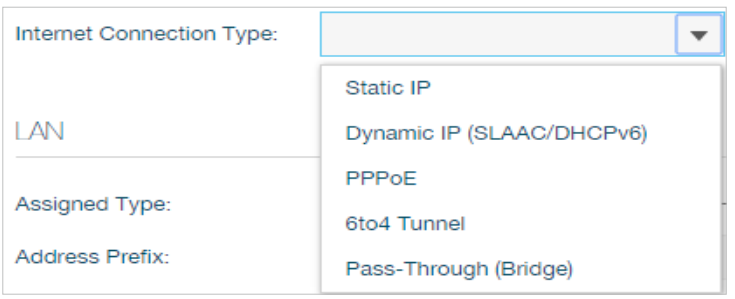
If your ISP provides IPv6 connection and has provided some detailed IPv6 parameters,

you can configure your router to permit IPv6 connection.

1. Visit http://tplinkwifi.net, and log in with your Kasa account.
2. Go to Advanced > IPV6 to enable IPV6 connection.



3. Select the internet connection type provided by ISP. Fill in the information as required.

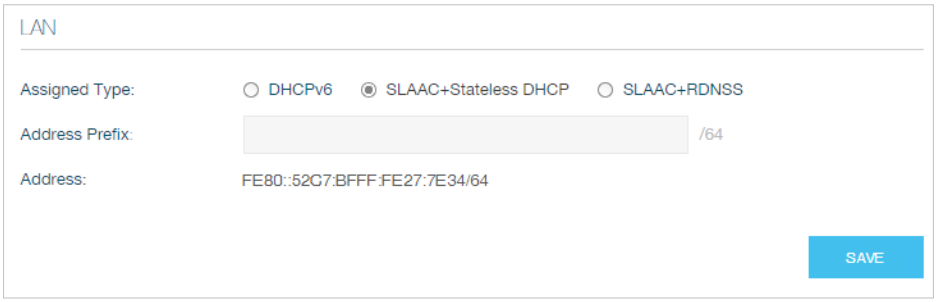


Note:

If you do not know what your internet connection type is, contact your ISP or judge according to the information provided by your ISP.

- Static IP: Select this type if your ISP uses Static IPv6 address assignment. Fill in the parameters as provided by the ISP.
- Dynamic IP: Select this type if your ISP uses Dynamic IPv6 address assignment. Click Advanced to have more configuration if ISP requires.
- PPPoE: Select this type if your ISP uses PPPoEv6 and provides a username and password. Fill in the Username and Password. Click Advanced to have more configuration if ISP requires.
- 6to4 Tunnel: Select this type if your ISP uses 6to4 deployment for assigning address. An IPv4 internet connection type is a prerequisite for this connection type. Click Advanced to have more configuration if ISP requires.
- Pass-Through (Bridge): Select this type if your ISP uses Pass-Through (Bridge) network deployment for assigning address. No configuration is required for this type of connection.

4. Configure LAN ports. Windows users are recommended to choose from the first two types. Fill in Address Prefix provided by ISP, and click SAVE.



Note:

Click (Help) icon on the upper-right corner of the web management page to know more about items.

5. Click Status on the left menu to check whether you succeed or not. The following figure is an example of a successful PPPoE configuration.

4. 9. 3. MAC Clone

Typically, you do not need to change the default MAC address of the router. However, some ISPs require MAC address authentication and only accept traffic from a specific MAC address. For example, your computer's MAC address that has been previously registered with the ISP when you first set up your internet service. If that is the case, you can clone your computer's MAC address to your router.

Also, you can manually change the MAC address of the router. It is helpful when your internet access account provided by your ISP is bound to one specific MAC address, in other words, your ISP just permits only one computer with the authenticated MAC address to access the internet. In this case, you can use MAC Clone to allow more computers to access the internet via the same account.

1. Select one of the following options:
   - Use Default MAC Address: Select this option touse the default MAC address of the computer.
   - Use Current Computer MAC Address: Select this option to copy the registered MAC address of the computer if you are using the computer with the authenticated MAC address to access the router.
   - Use Custom MAC Address: Select this option to enter a specific MAC address that your ISP requires for internet connection if you know the authenticated MAC address.
2. Click SAVE to save your settings.
3. Restart your broadband modem.

4. 10. Specify Your Network Settings

This part introduces how to change the default settings or adjust the basic configuration of the router using the web management page.

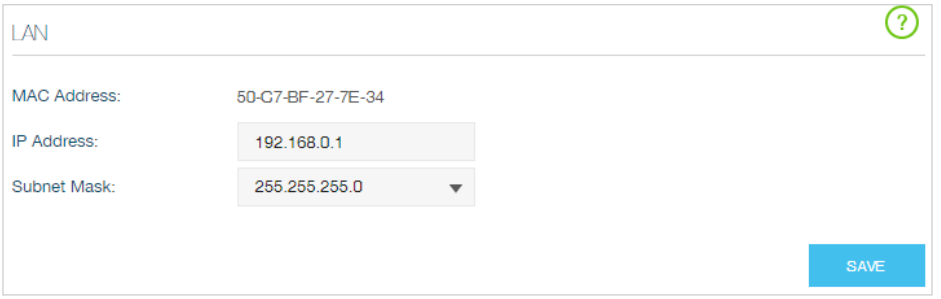
4. 10. 1. LAN Settings

4.10. 1.1. Change the LAN IP Address

The router is preset with a default LAN IP 192.168.0.1, which you can use to log in to its web management page. The LAN IP address together with the Subnet Mask also defines the subnet that the connected devices are on. If the IP address conflicts with another device in your local network or your network requires a specific IP subnet, you can change it.

Follow the steps below to change your IP address.

1. Visit http://tplinkwifi.net, and log in with your Kasa account.
2. Go to Advanced > Network > LAN page.



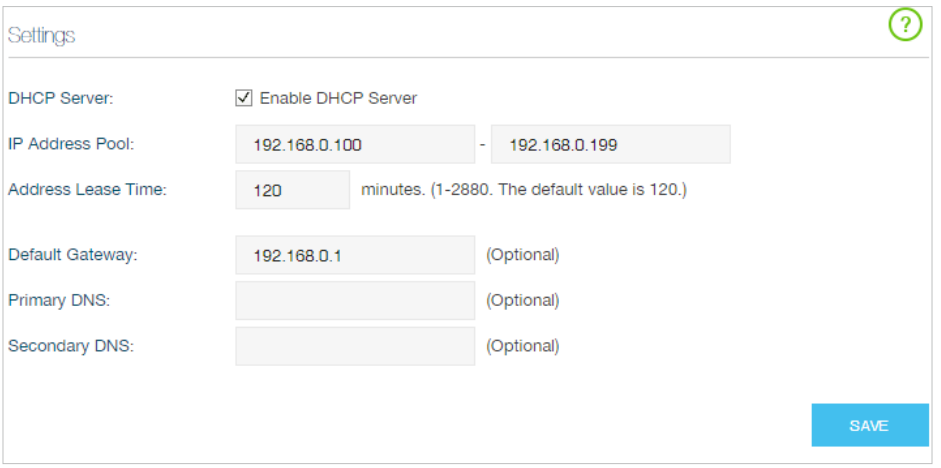
3. Type in a new IP Address appropriate to your needs, and you can use this address to access to the web management page next time.
4. Select the Subnet Mask from the drop-down list. The subnet mask together with the IP address identifies the local IP subnet.
5. Click SAVE to make the settings effective.

4.10. 1.2. Use the Router as a DHCP Server

You can configure the router to act as a DHCP server to assign IP addresses to its clients. To use the DHCP server function of the router, you must configure all computers on the LAN to obtain an IP Address automatically.

Follow the steps below to configure DHCP server.

1. Visit http://tplinkwifi.net, and log in with your Kasa account.
2. Go to Advanced > Network > DHCP Server page and enable DHCP Server.



3. Specify the IP Address Pool, the start address and end address must be on the same subnet with LAN IP. The router will assign addresses within this specified range to its clients. It is from 192.168.0.100 to 192.168.0.199 by default.
4. Enter a value for the Address Lease Time. The Address Lease Time is the amount of time in which a DHCP client can lease its current dynamic IP address assigned

by the router. After the dynamic IP address expires, the user will be automatically assigned a new dynamic IP address. The default is 120 minutes.

5. Keep the rest of the settings as default and click SAVE.

Note:

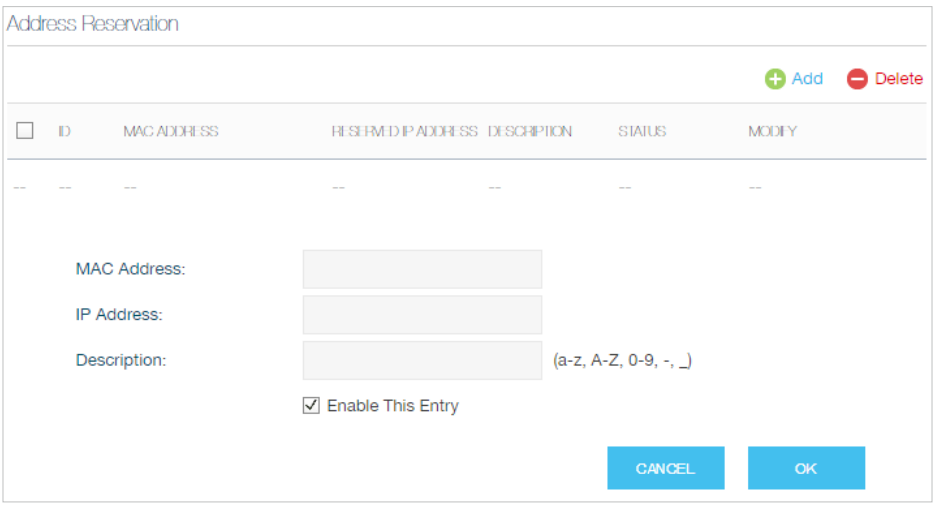
1. The router can be configured to work as a DHCP Relay. A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. If it is enabled, the DHCP requests from local PCs will be forwarded to the DHCP server that runs on WAN side.
2. You can also appoint IP addresses within a specified range to devices of the same type by using Condition Pool feature. For example, you can assign IP addresses within the range (192.168.0.50 to192.168.0.80) to Camera devices, thus facilitating the network management. Enable DHCP feature and configure the parameters according to your actual situation on Advanced > Network > DHCP Server page.

4.10. 1.3. Reserve LAN IP Addresses

You can view and add a reserved address for a client. When you specify an IP address for a device on the LAN, that device will always receive the same IP address each time when it accesses the DHCP server. If there are some devices in the LAN that require permanent IP addresses, please configure Address Reservation on the router for the purpose.

Follow the steps below to reserve an IP address for your device.

1. Visit http://tplinkwifi.net, and log in with your Kasa account.
2. Go to Advanced > Network > DHCP Server page.
3. Scroll down to locate the Address Reservation table and click Add to add an address reservation entry for your device.



4. Enter the MAC address of the device for which you want to reserve IP address.
5. Specify the IP address which will be reserved by the router.
6. Enter the desciption for this enrty.

7. Check to Enable this entry and click OK to make the settings effective.

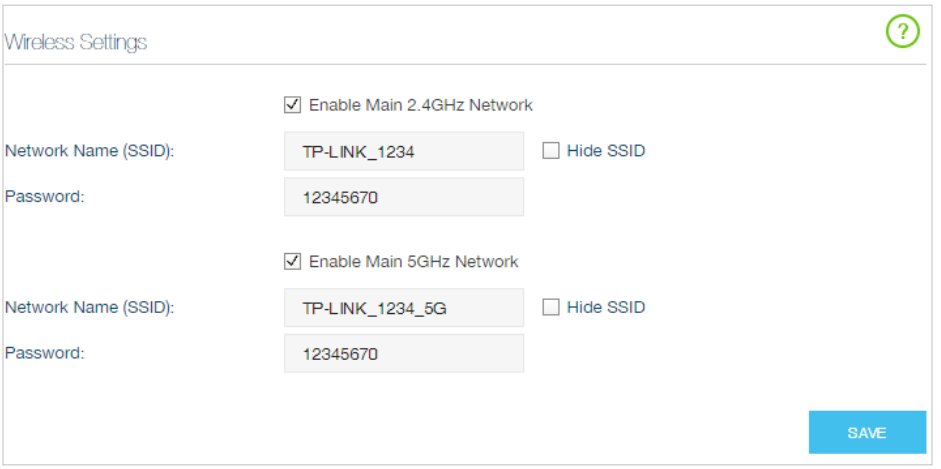
4. 10. 2. Wireless Settings

4.10. 2.1. Specify Basic Wireless Settings

The router's wireless network name (SSID) and password, and security option are preset in the factory. The preset SSID and password can be found on the product label. You can customize the wireless settings according to your needs.

1. Visit http://tplinkwifi.net, and log in with your Kasa account .

1. Go to Basic > Wireless page.



➢ **To enable or disable the wireless function:**

Enable the 2.4 GHz or 5GHz Wireless Network. If you don't want to use the wireless function, just deselect the box. If you disable the wireless function, all the wireless settings won't be effective.

➢ **To change the wireless network name (SSID) and wireless password:**

Enter a new SSID using up to 32 characters. The value is case-sensitive.

Note:

If you use a wireless device to change the wireless settings, you will be disconnected after the new settings are effective. Please write down the new SSID and password for future use.

➢ **To hide SSID:**

Select Hide SSID, and your SSID will not broadcast. Your SSID won't display on your wireless device when you scan for local wireless network list and you need to manually join the network.

➢ **To change the mode or channel:**

Go to Advanced > Wireless > Wireless Settings page and select the wireless network 2.4GHz or 5GHz.

- Mode: Select the desired mode.
  - 802.11n only: Select only if all of your wireless clients are 802.11n devices.
  - 802.11gn mixed: Select if you are using both 802.11g and 802.11n wireless clients.
  - 802.11bgn mixed: Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.

    Note: When 802.11n only mode is selected, only 802.11n wireless stations can connect to the router. It is strongly recommended that you select 802.11bgn mixed, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the router.
- Channel: Select the channel you want to use from the drop-down list. 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.
- Channel Width: Select the channel width from the drop-down list. The default setting is Auto, which can adjust the channel width for your clients automatically.
- Transmit Power: Select Low, Middle, or High to specify the data transmit power. The default and recommended setting is High.

➢ **To change the security option:**

1. Go to Advanced > Wireless > Wireless Settings page.
2. Select the wireless network 2.4GHz or 5GHz.
3. Select an option from the Security drop-down list. The router provides four options, None, WPA/WPA2 Personal (Recommended), WPA/WPA2 Enterprise, WEP. WPA2 uses the newest standard and the security level is the highest. We recommend you don't change the default settings unless necessary.

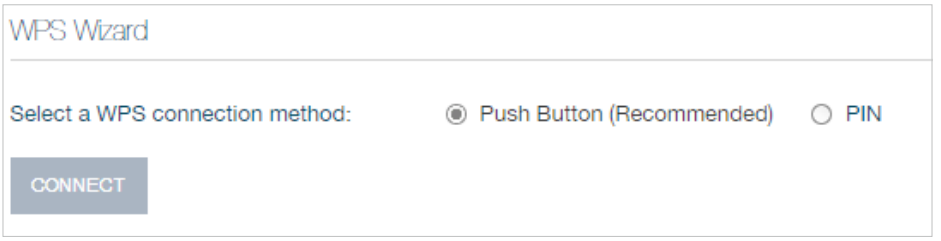
4.10. 2.2. Use WPS for Wireless Connection

You can use WPS (Wi-Fi Protected Setup) feature to add a new wireless device to your existing network quickly.

Method 1 Use the WPS Button on the Web Management Page

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

1. Visit http://tplinkwifi.net, and log in with your Kasa account.
2. Go to Advanced > Wireless > WPS page and locate WPS Wizard.

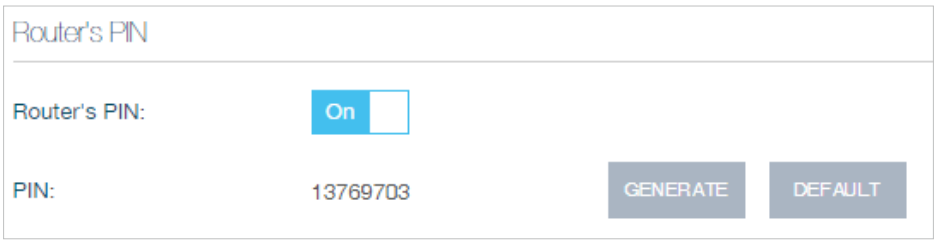


3. Select Push Button on the page.
4. Press the WPS button of the client device directly.
5. When Success appears on the above page, the client device has successfully connected to the router.

Method 2 Enter the router's PIN on your client device

Use this method if your client device asks for the router's PIN.

1. Visit http://tplinkwifi.net, and log in with your Kasa account.
2. Go to Advanced > Wireless > WPS page. Enable Router's PIN.



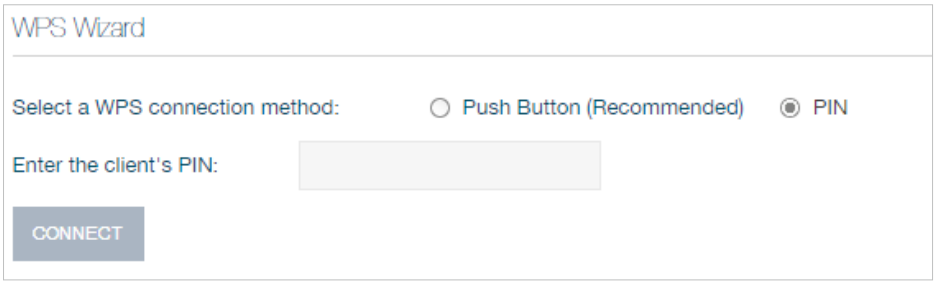
3. Take a note of the Current PIN of the router. You can also click the GENERATE button to get a new PIN.
4. On the client device, enter the router's PIN. (The default PIN is also printed on the label of the router.)
5. When Success appears on the above page, the client device has successfully connected to the router.

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 configuring the WPS.

Method 3 Enter the client device's PIN on the router

1. Visit http://tplinkwifi.net, and log in with your Kasa account.
2. Go to Advanced > Wireless > WPS page and locate WPS Wizard.

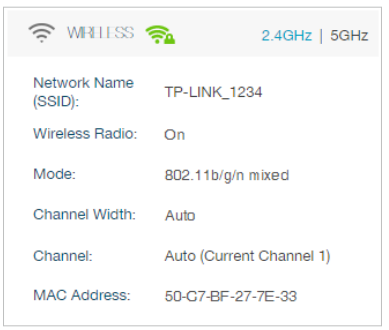


3. Select PIN.
4. Enter the client device's PIN in the field, and click CONNECT.
5. When Success appears on the above page, the client device has successfully connected to the router.

4.10. 2.3. View Wireless Information

➢ **To view the detailed wireless network settings:**

1. Visit http://tplinkwifi.net, and log in with your Kasa account.
2. Go to Advanced > Status page. You can see the Wireless box.
3. Select 2.4GHz or 5GHz to view the wireless details.



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

➢ **To view the detailed information of the connected wireless clients:**

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

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

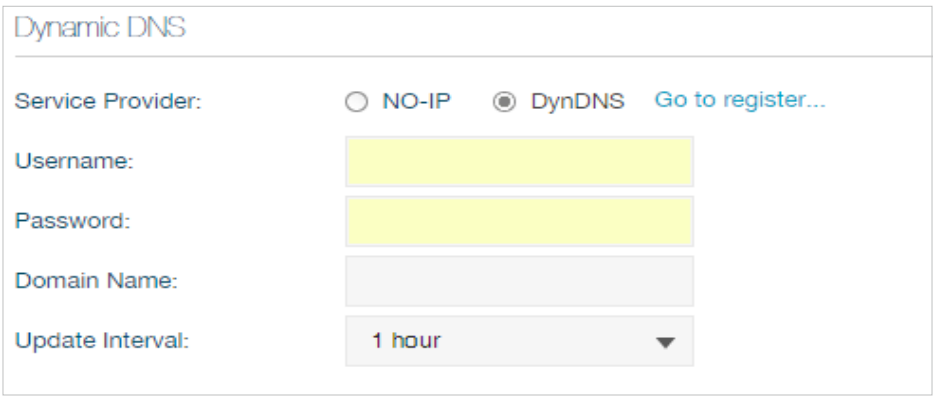
4. 10. 3. Set Up a Dynamic DNS Service Account

Most ISPs (Internet service providers) assign a dynamic IP address to the router and you can use this IP address to access your router remotely. However, the IP address can change any time and you don't know when it changes. In this case, you might need the DDNS (Dynamic Domain Name Server) feature on the router to allow you and your friends to access your router and local servers (FTP, HTTP, etc.) using domain name, in no need of checking and remembering the IP address.

Note: DDNS does not work if the ISP assigns a private WAN IP address (such as 192.168.0.x) to the router.

To set up DDNS, please follow the instructions below:

1. Visit http://tplinkwifi.net, and log in with your Kasa account.
2. Go to Advanced > Network > Dynamic DNS.
3. Select the Service Provider (NO-IP, Dyndns and many other DNS services).
4. If you choose the DDNS service, you should log in with your DDNS account, select a service provider and click Go to register. Enter the username, password and domain name of the account (such as lisa.ddns.net).



5. Click LOGIN AND SAVE.

Tips: If you want to use a new DDNS account, please logout first, then log in with the new account.

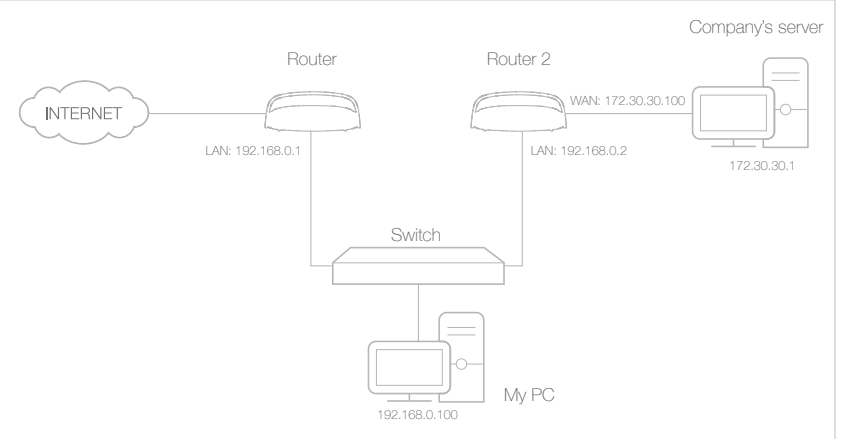
4. 10. 4. Create Static Routes

A static route is a pre-determined path that network information must travel to reach a specific host or network. Data from one point to another will always follow the same path regardless of other considerations. Normal internet usage does not require this setting to be configured.

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

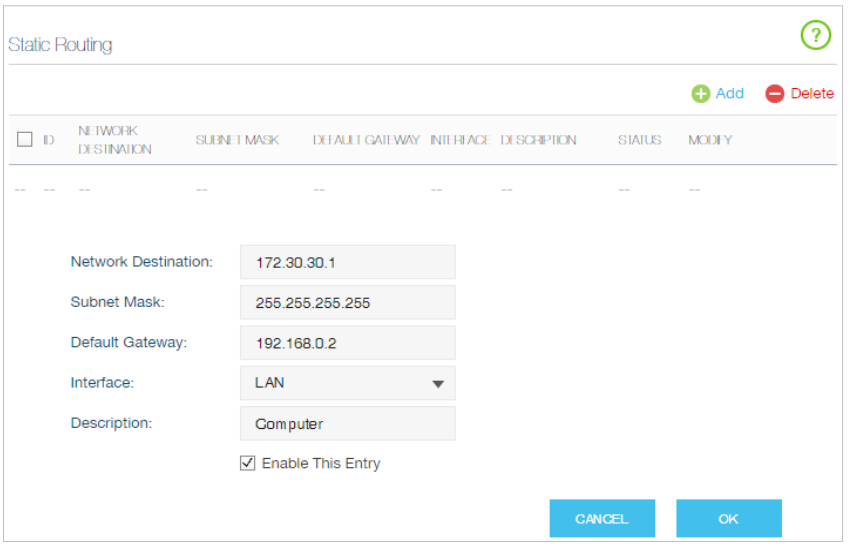
For example, in a small office, my PC can surf the internet, but I also want to visit my company's server. Now I have a switch and

another router. I connect the devices as shown in the following figure so that the physical connection between my PC and my company's server is achieved. To surf the internet and visit my company's network at the same time, I need to configure the static routing.



How can I do that?

1. Make sure the routers use different LAN IP addresses on the same subnet. Disable Router 2's DHCP function.
2. Visit http://tplinkwifi.net, and log in with your Kasa account.
3. Go to Advanced > Network > Advanced Routing.
4. Click Add to add a new static routing entry. 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 the router. In

the example, the IP address of the company network is the destination IP address, so here enters 172.30.30.1.

- Subnet Mask: Determines the destination network with the destination IP address. If the destination is a single IP address, enter 255.255.255.255; otherwise, enter the subnet mask of the corresponding network IP. In the example, the destination network is a single IP, so here enters 255.255.255.255.
- 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 the data. In the example, the data packets will be sent to the LAN port of Router 2 and then to the Server, so the default gateway should be 192.168.0.2.
- Interface: Determined by the port (WAN/LAN) that sends out the data packets. In the example, the data is sent to the gateway through the LAN port, so LAN should be selected.

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

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

4. 11. Administrate Your Network

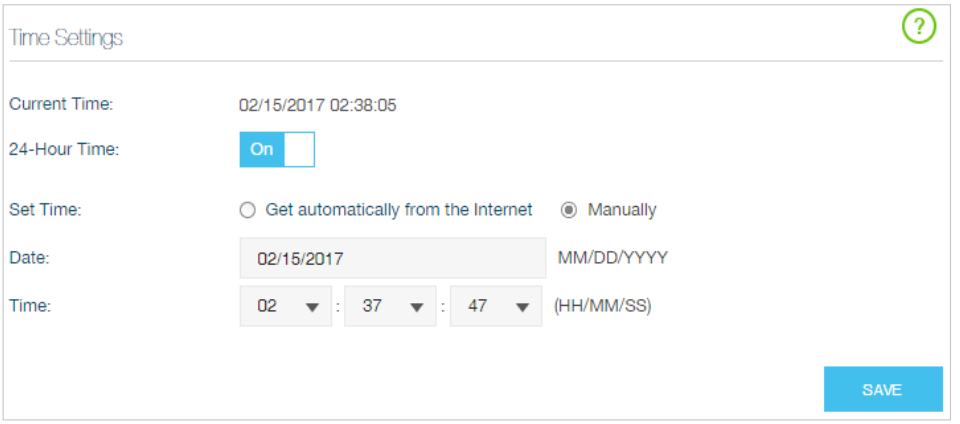
This part introduces how to change the system settings and administrate your router's network.

4. 11. 1. Set System Time

System time is the time displayed while the router is running. The system time you configure here will be used for other time-based functions like Parental Controls. You can manually set how to get the system time.

Follow the steps below to set your system time.

1. Visit http://tplinkwifi.net, and log in with your Kasa account.
2. Go to Advanced > System Tools > Time Settings page.



3. Configure the system time using the following methods:

   Get automatically from the Internet: Click this button if you want to get time from the internet. Make sure your router can access the internet before you select this way to get system time.

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

4. Click SAVE.

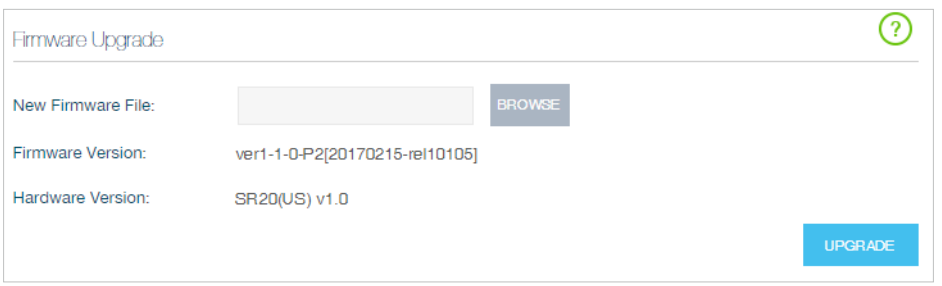
4. 11. 2. Update the Firmware

TP-Link is dedicated to improving and richening the product features, giving you a better network experience. We will inform you through the Kasa App if there's any update firmware available for your router. Also, the latest firmware will be released at TP-Link official website, you can download it from the Support page on our website www.tp-link.com for free.

Note:

1. Make sure that you have a stable connection between the router and your computer. It is NOT recommended to upgrade the firmware wirelessly.
2. Make sure you remove any USB storage device connected to the router before the firmware upgrade to prevent data loss.
3. Do NOT turn off the router during the firmware upgrade.

1. Visit http://tplinkwifi.net, and log in with your Kasa account.
2. Go to Advanced > System Tools > Firmware Upgrade.
3. Click BROWSE to locate the downloaded new firmware file, and click UPGRADE.

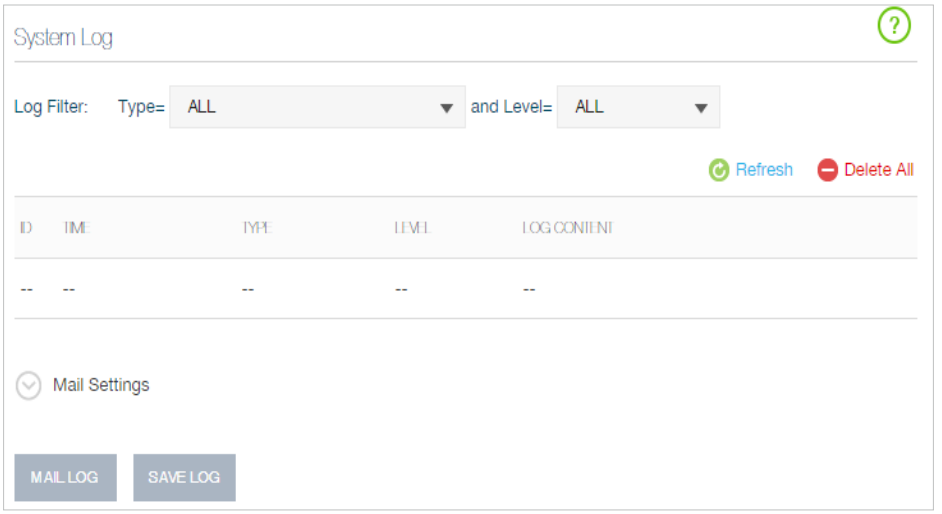


4. Wait a few moments for the upgrading and rebooting.

4. 11. 3. System Log

System Log can help you know what happened to your router, facilitating you to locate the malfunctions. For example when your router does not work properly, you will need to save the system log and send it to the technical support for troubleshooting.

1. Visit http://tplinkwifi.net, and log in with your Kasa account.
2. Click Advanced > System Tools > System Log page.



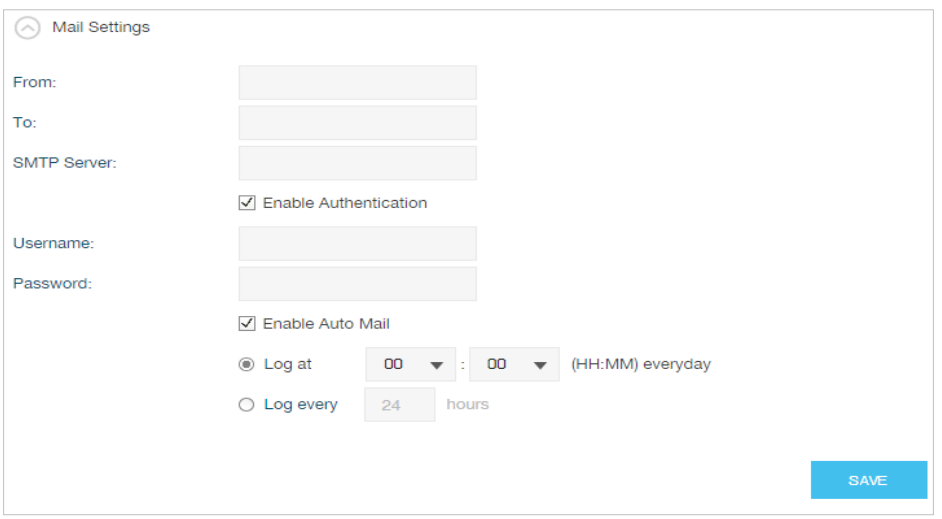
➢ **To view the system logs:**

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

Click Refresh to refresh the log list.

Click SAVE LOG to save the logs in a txt file to your computer.

➢ **To configure email settings for system logs:**



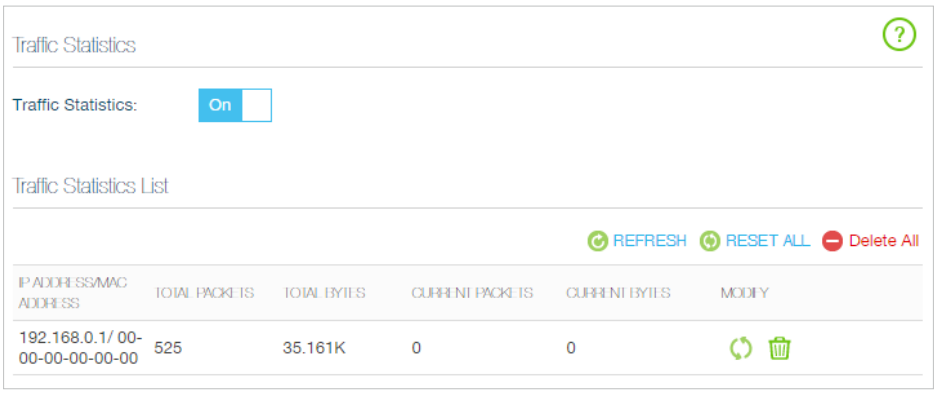
1. Click Mail Settings.
2. Enter the valid emial address to be used for outgoing email (From).
3. Enter the valid emial address to be used for incoming email (To).
4. Enter the SMTP server that the router uses to send the system logs via email.
5. Select Enable Authentication if the SMTP server requires authentication for sending email. Username and password are case-sensitive.
6. Select Enable Auto Mail to specify what time of day the system log should be sent automatically.
   - Log at: To send the email at a specific time. Enter the Hours and Minutes in 24-hour clock format, e.g. 16:00 is 4PM.
   - Log every: To send the email at a specific hour or time interval. Enter the number of hours.

Click MAIL LOG to mail the logs.

4. 11. 4. Monitor the Internet Traffic Statistics

The Traffic Statistics page displays the network traffic of the interfaces, including the received and sent packets.

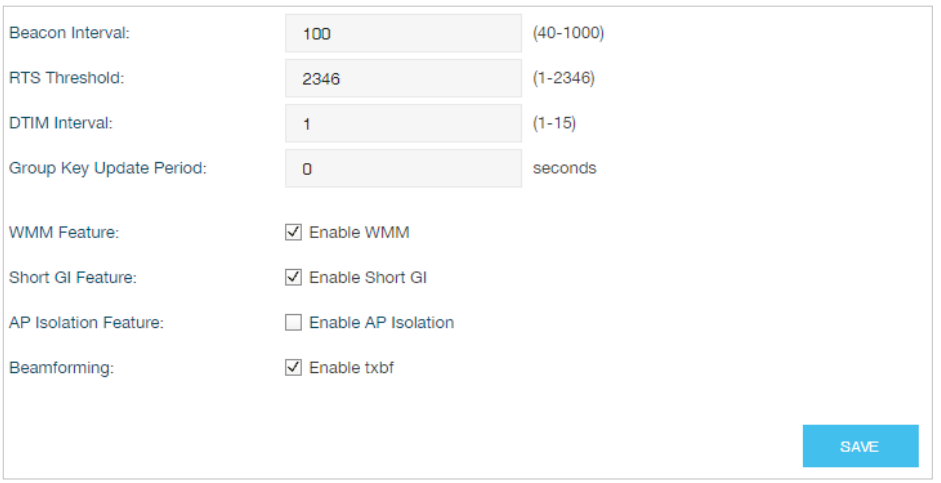
1. Visit http://tplinkwifi.net, and log in with your Kasa account.
2. Go to Advanced > System Tools > Traffic Statistics.
3. Toggle on Traffic Statistic, and then you can see the packets received and sent via this interface in the past ten minutes. This function is disabled by default.



4. 11. 5. System Parameters

Advanced wireless settings are for those who have a network concept. If you are not familiar with the settings on this page, it's strongly recommended that you keep the provided default values; otherwise it may result in lower wireless network performance.

1. Visit http://tplinkwifi.net, and log in with your Kasa account.
2. Go to Advanced > System Tools > System Parameters page to configure the wireless network 2.4GHz or 5GHz



- Beacon Interval: Enter a value between 40 and 1000 in milliseconds to determine the duration between which beacon packets are broadcasted by the router to synchronize the wireless network. The default is 100 milliseconds.
- RTS Threshold: Enter a value between 1 and 2346 to determine the packet size of data transmission through the router. By default, the RTS (Request to Send) Threshold size is 2346. If the packet size is greater than the preset threshold, the router sends Request to Send frames to a particular receiving station and negotiates the sending of a data frame, or else the packet will be sent immediately.
- DTIM Interval: Enter a value between 1 and 255 to determine the interval of the Delivery Traffic Indication Message (DTIM). The default vanlue is 1, indicating the DTIM Interval is the same as Beacon Interval.
- Group Key Update Period: Enter the number of seconds (miimum 30) to control the time interval for the encryption key automatic renewal. The default is 0, indicating no key renewal.
- WMM Feature: This feature guarantees the packets with high-priority messages being transmitted preferentially. WMM is enabled compulsively under 802.11n or 802.11ac mode. It is strongly recommended to enable WMM.
- Short GI: This feature is enabled by default and recommended to increase the data capacity by reducing the Guard Interval (GI) time.
- AP Isolation: Select this check box to enable the AP Isolation feature that allows you to confine and restrict all wireless devices on your network from interacting with each other, but still able to access the internet. AP isolation is disabled by default.

- Beamforming: Select this check box to enable txbf feature that focuses the Wi-Fi transmission in the direction of your connected devices, concentrating the signal where you need it the most. Beamforming technology allows you to enjoy fast, stable Wi-Fi in every part of your home.

Appendix: Troubleshooting

T1. How do I factory reset my router?

Resetting your router can be done via the Kasa App, its touch screen or the Reset button on the rear panel of the router. Keep in mind that factory resetting the router will erase all of your configuration settings (such as network settings and wireless settings), unbind the router from your Kasa account account, and return them to an out-of-box configuration.

- Via the Kasa App

  Slide to the left to remove the router on the Devices page of the Kasa App.

- Via the Reset button

  While the router is powered on, press and hold the Reset button for about 10 seconds or until the confirmation window appears on the touch screen, then release the button and click Yes to start resetting your router.

- Via the router's touch screen

  On the main Home screen, tap Network Controls, and then go to Settings > Advanced > Reset. Refer to Reset the Router for more detailed information.

T2. What can I do if I cannot access the internet?

- Check your network connectivity.
- Reboot the Smart Home Router.
- Factory reset the Smart Home Router and try to add it again.

T3. What should I do when I cannot access the router's web management page using a computer?

- Make sure your computer is set to obtain an IP address automatically (DHCP).
- Check your network connectivity.
- Make sure you enter http://tplinkwifi.net or http://192.168.0.1 into the address bar.
- Check your web browser and make sure the Proxy server is not enabled.

T4. How can I change my computer's settings to obtain an IP address automatically?

To change the computer's network settings, follow the steps below.

- For MAC OS X:

1) Click the Apple icon, and select System Preferences from the drop-down list.

2) Click the Network icon.

3) Select Ethernet (for wired connection) or Wi-Fi (for wireless connection) in the left panel, then click Advanced.

4) Click TCP/IP.

5) From the Configure IPv4 drop-down list, select Using DHCP.

6) Click OK.

- For Windows 7/8/8.1/10:

1) Right-click the Network icon on the system tray and select Open Network and Sharing Center > Change adapter settings.

2) Right-click your network connection (wired or wireless) and select Properties.

3) Double-click Internet Protocol Version 4 (TCP/IPv4).

4) Select both Obtain an IP address automatically and Obtain DNS server address automatically, then click OK.

5) Click OK again to save your configuration.

- For Windows XP:

1) Right-click the Network icon on the system tray and select Open Network Connections.

2) Right-click your network connection (wired or wireless) and select Properties.

3) Double-click Internet Protocol (TCP/IP).

4) Select both Obtain an IP address automatically and Obtain DNS server address automatically, then click OK.

5) Click OK again to save your configuration.

Visit www.tp-link.com/support for technical support and troubleshooting information.

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

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.

RF Exposure Information

This device meets the EU requirements (1999/5/EC 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.

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

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;

Avertissement

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;

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 and 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)

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

EAC

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。

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。

Safety Information

- When product has power button, the power button is one of the way to shut off the product; when there is no power button, the only way to completely shut off power is to disconnect the product or the power adapter from the power source.
- Don't disassemble the product, or make repairs yourself. You run the risk of electric shock and voiding the limited warranty. If you need service, please contact us.

- Avoid water and wet locations.
-  Use only power supplies which are provided by manufacturer and in the original packing of this product.

For EU/EFTA, this product can be used in the following countries:

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

Explanation of the symbols on the product label

Symbol	Explanation
	DC voltage
	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.
	Indoor use only