User Guide

AC1200 Wireless Dual Band Gigabit Router
Archer C5

1910012297 REV4.0.0

Contents

About This Guide

This guide is a complement of Quick Installation Guide. The Quick Installation Guide instructs you on quick Internet setup, and this guide provides details of each function and shows you the way to configure these functions appropriate to your needs.

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

Conventions

In this guide the following conventions are used:

Convention	Description
Underlined	Underlined words or phrases are hyperlinks. You can click to redirect to a website or a specific section.
Teal	Contents to be emphasized and texts on the web page are in teal, including the menus, items, buttons, etc.
>	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 edit the corresponding entry. • 🗑 click to delete the corresponding entry. • 💡 click to enable or disable the corresponding entry. • ? click to view more information about items on the page.

Chapter 1

Get to Know About Your Router

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

It contains the following sections:

- Product Overview
- Panel Layout

1. 1. Product Overview

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

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

1. 2. Panel Layout

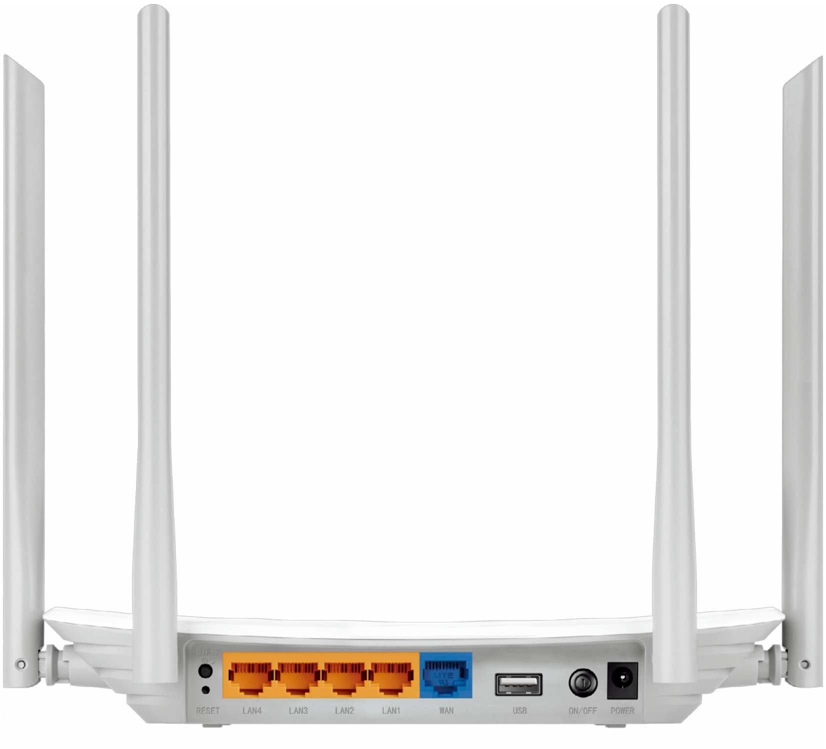
1. 2. 1. The Front Panel

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

LED Explanation

Name	Status	Indication
Power	On	The system has started up successfully.
	Flashing	The system is starting up or the firmware is being upgraded. Do not disconnect or power off your router.
	Off	Power is off.
2.4GHz	On	The 2.4GHz wireless band is enabled.
	Off	The 2.4GHz wireless band is disabled.
5GHz	On	The 5GHz wireless band is enabled.
	Off	The 5GHz wireless band is disabled.
Internet	Green On	Internet service is available.
	Orange On	The router's Internet port is connected, but the internet service is not available.
	Off	The router's Internet port is unplugged.
Ethernet	On	At least a powered-on device is connected to the router's LAN port.
	Off	No powered-on device is connected to the router's LAN port.
USB	On	The inserted USB device is ready to use.
	Flashing	A USB device is being identified.
	Off	No device is plugged into the USB port.
WPS	On/Off	This light remains on for 5 minutes when a WPS connection is established, then turns off.
	Flashing	WPS connection is in progress. This may take up to 2 minutes.

1. 2. 2. The Back Panel



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

Item	Description
WPS/Wi-Fi On/Off Button	Press and hold this button for less than 5 seconds to enable the WPS function.
	Press and hold this button for about 2 seconds to turn on or off the wireless function of your router.
Reset Button	Press and hold this button for more than 5 seconds to reset the router to its factory default settings.
Ethernet Ports (1/2/3/4)	For connecting your wired devices to the router.
WAN Port	For connecting to a DSL/Cable modem, or an Ethernet jack.
USB Port	For connecting to a USB device.
Power On/Off Button	Press this button to power on or off the router.
Power Port	For connecting the router to a power socket via the provided power adapter.
Antennas	Used for wireless operation and data transmit. Upright them for the best Wi-Fi performance.

Chapter 2

Connect the Hardware

This chapter contains the following sections:

- Position Your Router
- Connect Your Router

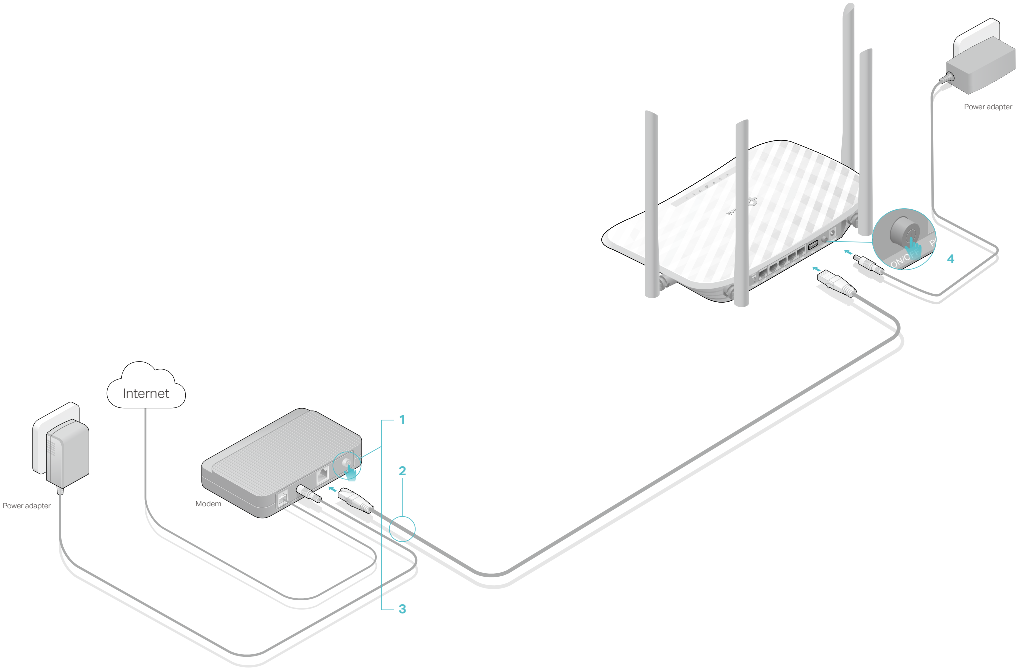
2. 1. Position Your Router

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

2. 2. Connect Your Router

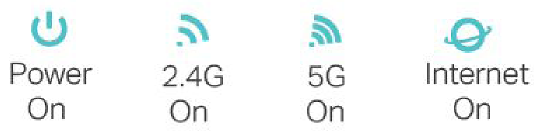
Follow the steps below to connect your router.

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



1. Turn off the modem, and remove the backup battery if it has one.
2. Connect the modem to your router's WAN port with an Ethernet cable.
3. Turn on the modem, and then wait about **2 minutes** for it to restart.
4. Connect the power adapter to the router and turn on the router.

5. Verify that the following LEDs are on and solid before continuing with the configuration.



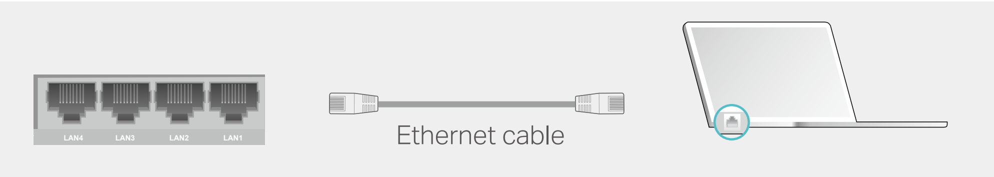
Note:

If the 2.4G LED and 5G LED are off, please press the WPS/Wi-Fi On/Off button for 2 seconds and check the LEDs again a few seconds later.

6. Connect your computer to the router.

- **Method 1: Wired**

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

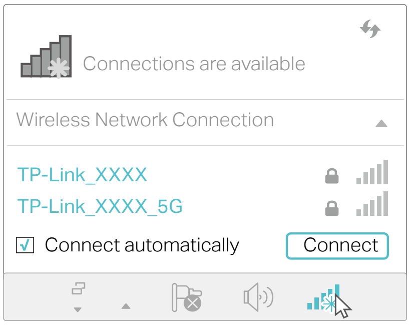


- **Method 2: Wirelessly**

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

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

Computer



Connections are available

Wireless Network Connection

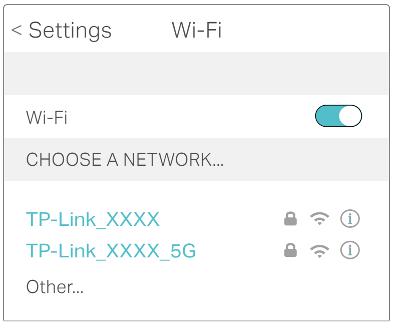
TP-Link_XXXX

TP-Link_XXXX_5G

☑ Connect automatically [Connect]

OR

Smart Device



< Settings Wi-Fi

Wi-Fi ●

CHOOSE A NETWORK...

TP-Link_XXXX

TP-Link_XXXX_5G

Other...

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

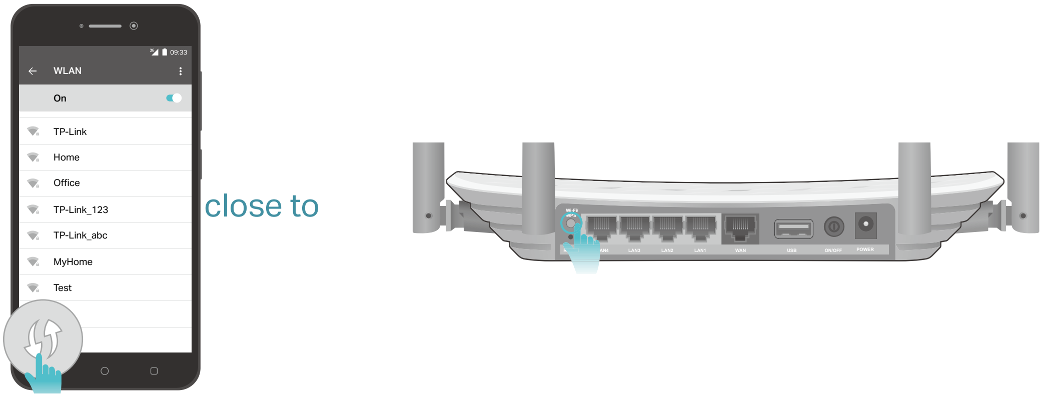
Wireless devices that support WPS, including Android phones, tablets, and most USB network adapters, can be connected to your router through this method.

Note:

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

1) Tab the WPS icon on the device’s screen. Here we take an Android phone for instance.

2) Within two minutes, press the WPS/Wi-Fi On/Off button on your router.



close to

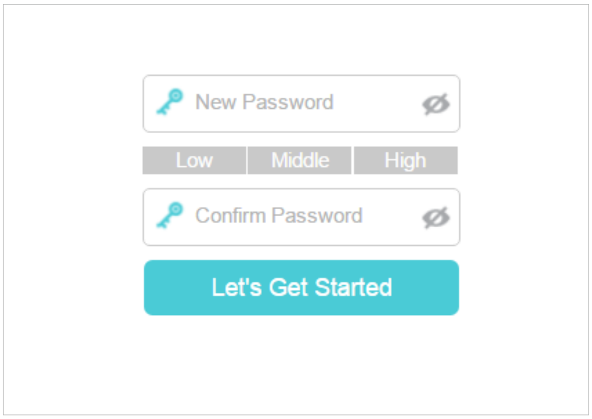
Chapter 3

Log In to Your Router

With a web management page, it is easy to configure and manage the modem 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.

Follow the steps below to log into 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 Troubleshooting to configure your computer.
2. Launch a web browser and go to http://tplinkwifi.net or http://192.168.0.1. Create a strong password and click Let's Get Started to log in.



Chapter 4

Set Up Internet Connection

This chapter introduces how to connect your router to the internet. The router is equipped with a web-based Quick Setup wizard. It has necessary ISP information built in, automates many of the steps and verifies that those steps have been successfully completed. Furthermore, you can also set up an IPv6 connection if your ISP provides IPv6 service.

It contains the following sections:

- Use Quick Setup Wizard
- Manually Set Up Your Internet Connection
- Test Internet Connectivity
- Set Up an IPv6 Internet Connection

4. 1. Use Quick Setup Wizard

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

Follow the steps below to set up your router.

1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with the password you set for the router.
2. Click Quick Setup on the top of the page. Then follow the step-by-step instructions to connect your router to the internet.

Note:

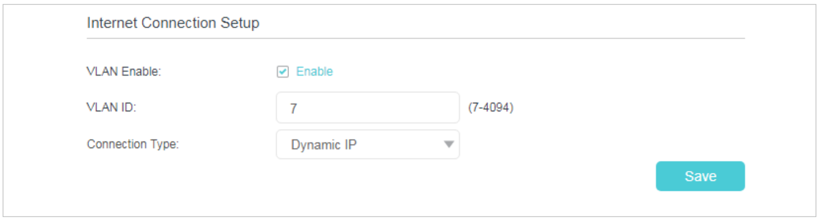
- If you have changed the preset wireless network name (SSID) and wireless password during the Quick Setup process, all your wireless devices must use the new SSID and password to connect to the router.

4. 2. Manually Set Up Your Internet Connection

In this part, you can check your current internet connection settings. You can also modify the settings according to the service information provided by your ISP.

Follow the steps below to check or modify your internet connection settings.

1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with your the password you set for the router.
2. Go to Basic > Internet.
3. Select your internet connection type from the drop-down list.



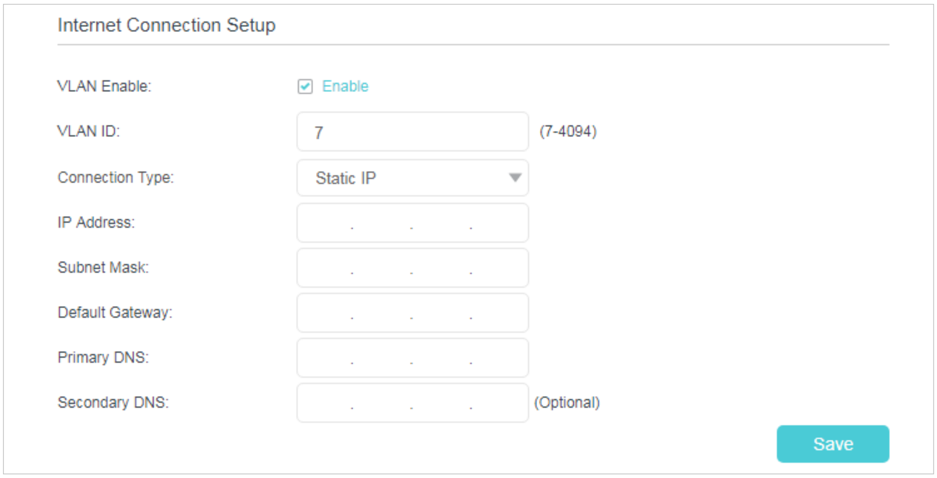
Internet Connection Setup

VLAN Enable: ☑ Enable

VLAN ID: 7 (7-4094)

Connection Type: Dynamic IP

4. Follow the instructions on the page to continue the configuration. Parameters on the figures are just used for demonstration.
   1) If you choose Dynamic IP, you don't need to set any parameters. Dynamic IP users are usually equipped with a cable TV or fiber cable.
   2) If you choose Static IP, enter the information provided by your ISP in the corresponding fields.



Internet Connection Setup

VLAN Enable: ☑ Enable

VLAN ID: 7 (7-4094)

Connection Type: Static IP

IP Address: . . .

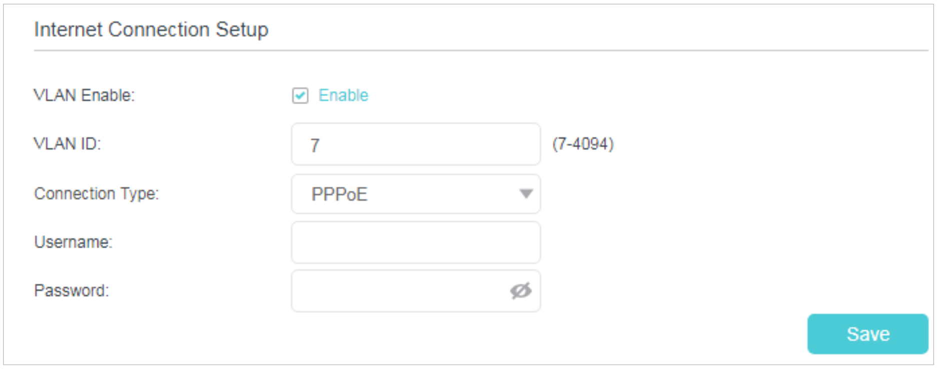
Subnet Mask: . . .

Default Gateway: . . .

Primary DNS: . . .

Secondary DNS: . . . (Optional)

3) If you choose PPPoE, enter the Username and Password provided by your ISP. PPPoE users usually have DSL cable modems.



Internet Connection Setup

VLAN Enable: ☑ Enable

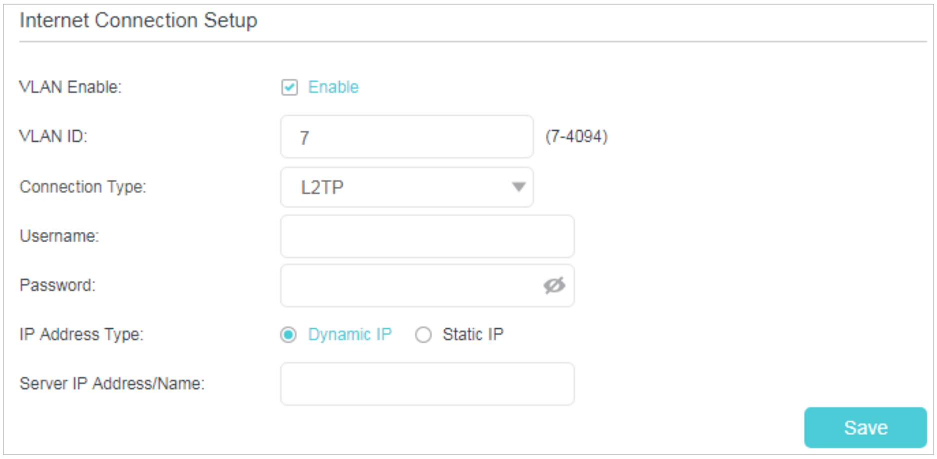
VLAN ID: 7 (7-4094)

Connection Type: PPPoE

Username:

Password:

4) If you choose L2TP, enter the Username and Password and choose the IP Address Type provided by your ISP. Different parameters are needed according to the IP Address Type you have chosen.



Internet Connection Setup

VLAN Enable: ☑ Enable

VLAN ID: 7 (7-4094)

Connection Type: L2TP

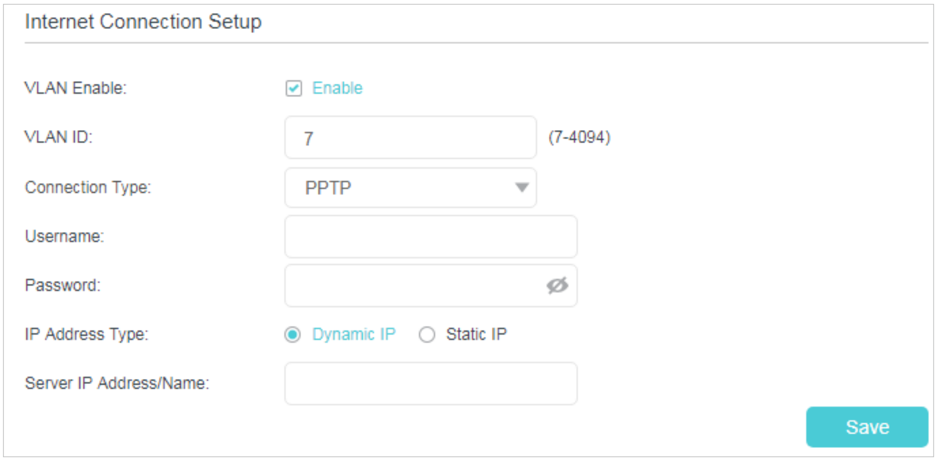
Username:

Password:

IP Address Type: ● Dynamic IP ○ Static IP

Server IP Address/Name:

5) If you choose PPTP, enter the Username and Password, and choose the IP Address Type provided by your ISP. Different parameters are needed according to the IP Address Type you have chosen.



Internet Connection Setup

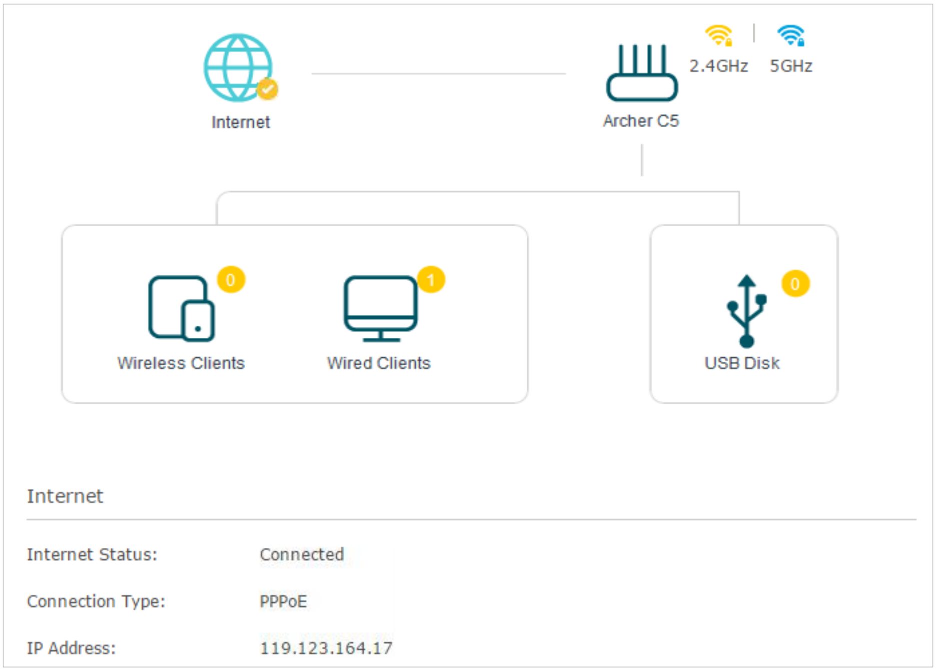
VLAN Enable:	☑ Enable
VLAN ID:	7 (7-4094)
Connection Type:	PPTP
Username:	
Password:	
IP Address Type:	● Dynamic IP ○ Static IP
Server IP Address/Name:	

5. Click Save.

6. To check your internet connection, click Network Map on the left of the page. After the connection succeeds, the screen will display as follows. Here we take PPPoE as an example.

Note:

It may take 1-2 minutes to make the settings valid.



Internet

Internet Status:	Connected
Connection Type:	PPPoE
IP Address:	119.123.164.17

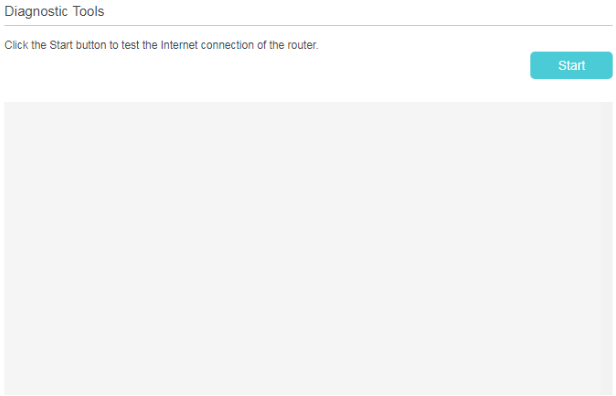
Tips:

- If your internet connection type is BigPond Cable, please go to Advanced > Network > Internet to set your router.
- If you use Dynamic IP and PPPoE and you are provided with any other parameters that are not required on the page, please go to Advanced > Network > Internet to complete the configuration.
- If you still cannot access the internet, refer to the Troubleshooting section for further instructions.

4. 3. Test Internet Connectivity

After manually setting up the Internet connection, you need to test the Internet connectivity. The router provides a diagnostic tool to help you locate the malfunction.

1. Visit http://tplinkwifi.net orhttp://192.168.0.1, and log in with the account you set for the router.
2. Go to Advanced > System Tools > Diagnostics Page.



Diagnostic Tools

Click the Start button to test the Internet connection of the router.

3. Click Start to test the Internet connectivity and you will see the test result in the gray box.

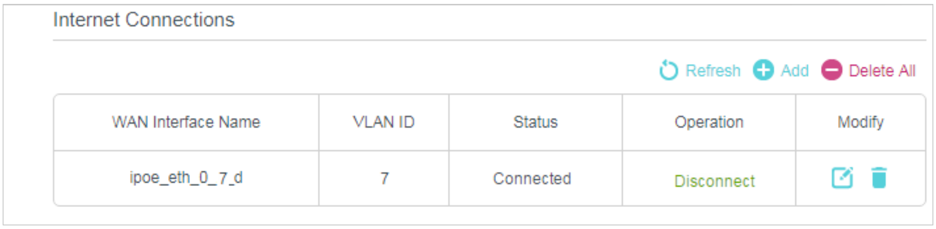
4. 4. Set Up an IPv6 Internet Connection

If your ISP provides IPv6 connection and some detailed IPv6 parameters, you can manually set up an IPv6 connection.

If your ISP provides an IPv4-only connection or IPv6 tunnel service, permit IPv6 connection by referring to Set Up the IPv6 Tunnel.

Follow the steps below to set up an IPv6 connection:

1. Visit http://tplinkwifi.net or http://192.168.0.1, and log in with the password you set for the router.
2. Go to Advanced > Network > Internet page.

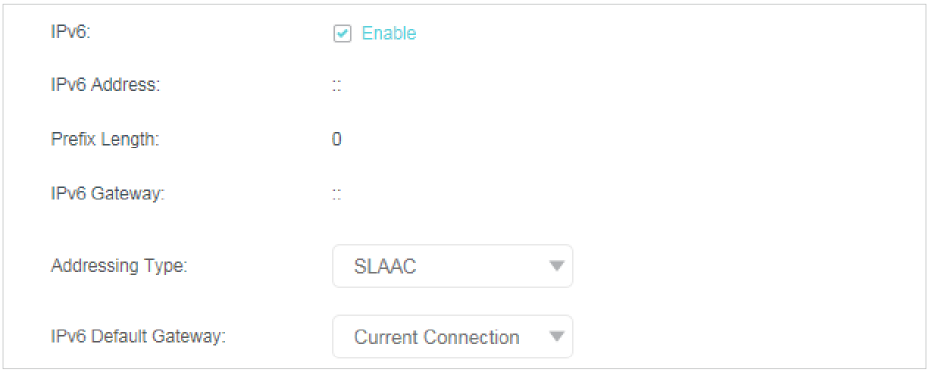


Internet Connections

WAN Interface Name	VLAN ID	Status	Operation	Modify
ipoe_eth_0_7_d	7	Connected	Disconnect	✎ 🗑

3. Select your WAN Interface Name (Status should be Connected) and click the ✎ (Edit) icon.

4. Scroll down the page, enable IPv6, and configure the IPv6 parameters.



IPv6: ☑ Enable

IPv6 Address: ::

Prefix Length: 0

IPv6 Gateway: ::

Addressing Type: SLAAC

IPv6 Default Gateway: Current Connection

- Addressing Type: Consult your ISP for the addressing type, DHCPv6 or SLAAC. SLAAC is the most commonly used addressing type.

Note: If your ISP has provided the IPv6 address, click Advanced to reveal more settings. Check to use IPv6 specified by ISP and enter the parameters provided by your ISP.

5. Click Save to make the settings effective. Now IPv6 service is available for your network.

Chapter 5

USB Settings

This chapter describes how to use the USB ports to share files, media and a printer from the USB storage devices over your home network locally, or remotely through the internet.

The router supports USB external flash drives, hard drives and USB printers.

It contains the following sections:

5. 1. Access the USB Storage Device

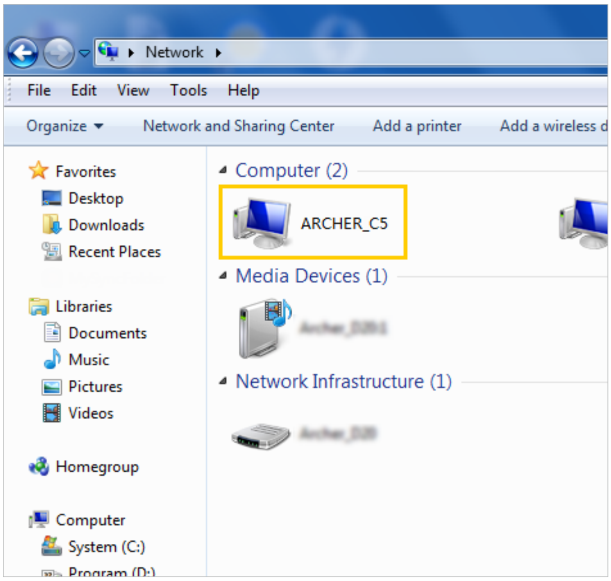
Insert your USB storage device into the router's USB port and then access files stored there locally or remotely.

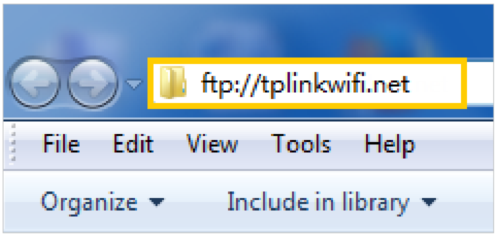
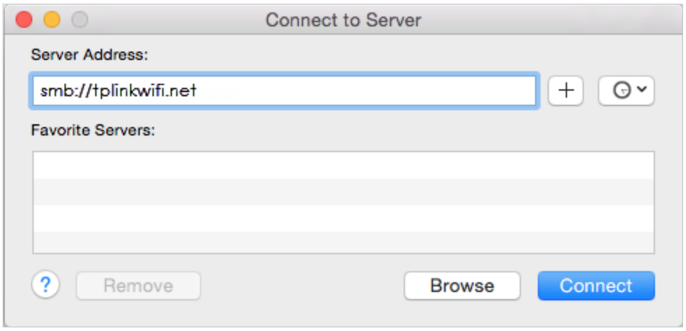
Tips:

- 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 Sharings > USB Storage Devices and click Remove .

5. 1. 1. Access the USB Device Locally

Insert your USB storage device into the router's USB port and then refer to the following table to access files stored on your USB storage device.

Windows computer	➢ **Method 1:** Go to Computer > Network, then click the Network Server Name (ARCHER_model number by default) in the Computer section. **Note:** Operations in different systems are similar. Here we take Windows 7 as an example.  Network File Edit View Tools Help Organize Network and Sharing Center Add a printer Add a wireless d Favorites Desktop Downloads Recent Places Libraries Documents Music Pictures Videos Homegroup Computer System (C:) Program (D:) Computer (2) ARCHER_C5 Media Devices (1) Network Infrastructure (1)

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. ftp://tplinkwifi.net
Mac	1) Select Go > Connect to Server. 2) Type the server address smb://tplinkwifi.net. 3) Click Connect. Connect to Server Server Address: smb://tplinkwifi.net Favorite Servers: 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 to To set up authentication for data security:.)
Smart device	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 to To customize the address of the USB disk: to learn more.

5. 1. 2. Access the USB Device Remotely

You can access your USB disk outside the local area network. For example, you can:

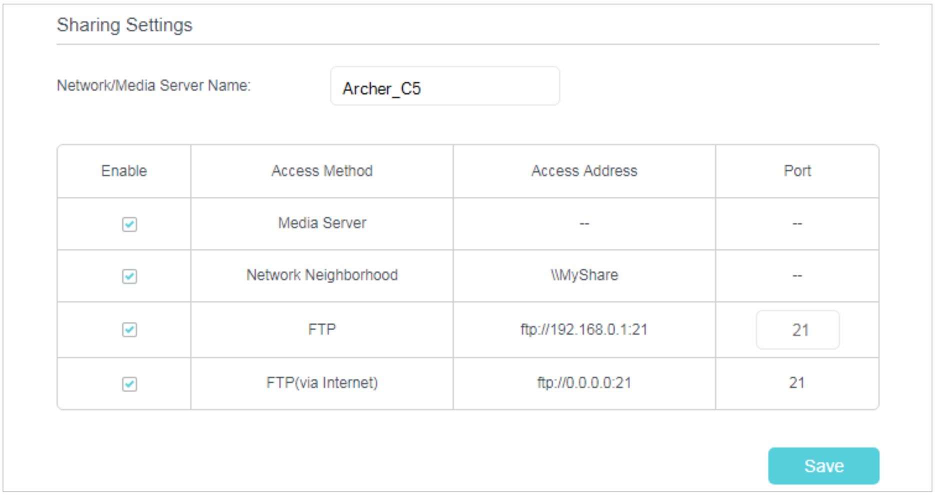
- Share photos and other large files with your friends without logging in to (and paying for) a photo-sharing site or email system.
- Get a safe backup for the materials for a presentation.
- Remove the files on your camera's memory card from time to time during the journey.

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.

Follow the steps below to configure remote access settings.

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > USB Sharing > USB Storage Device page.
3. Tick the FTP (via Internet) checkbox, and then click Save.

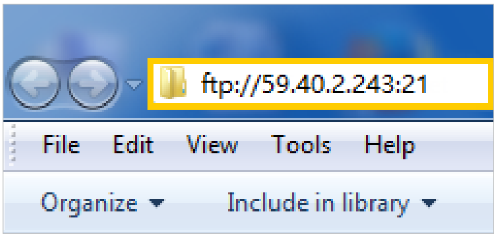


Sharing Settings

Network/Media Server Name: Archer_C5

Enable	Access Method	Access Address	Port
☑	Media Server	--	--
☑	Network Neighborhood	\\MyShare	--
☑	FTP	ftp://192.168.0.1:21	21
☑	FTP(via Internet)	ftp://0.0.0.0:21	21

4. Refer to the following table to access your USB disk remotely.

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: 3) 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)  ftp://59.40.2.243:21 4) Press Enter on the keyboard. 5) Access with the username and password you set in To set up authentication for data security:. Tips: You can also access the USB disk via a third-party app for network files management, which can resume broken file transfers.
Smart device	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.

5. 1. 3. Customize the Access Settings

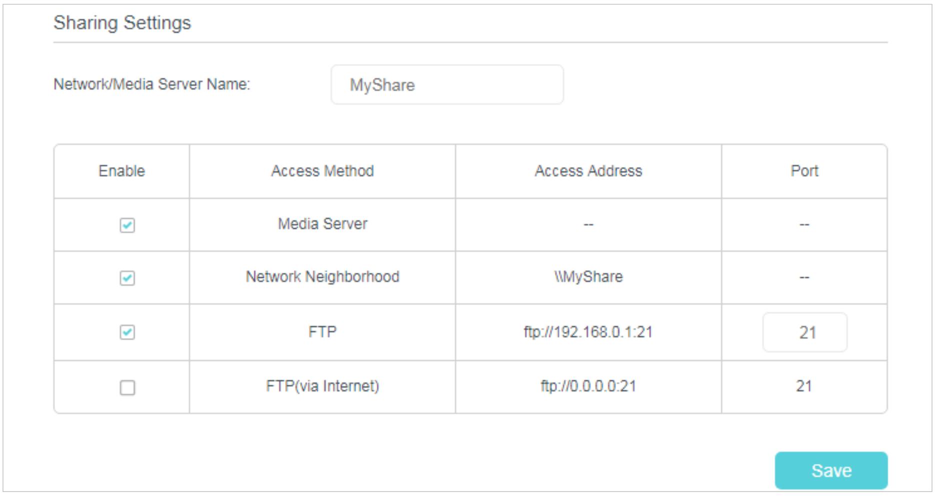
By default, all the network clients can access all folders on your USB disk. You can customize your sharing settings by setting a sharing account, sharing specific contents and setting a new sharing address on the router's web management page.

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > USB Sharing > USB Storage Device page.

➢ **To customize the address of the USB disk:**

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

1. On the Sharing Settings part, make sure Network Neighborhood is ticked, and enter a Network/Media Server Name as you like, such as MyShare, then click Save.



Sharing Settings

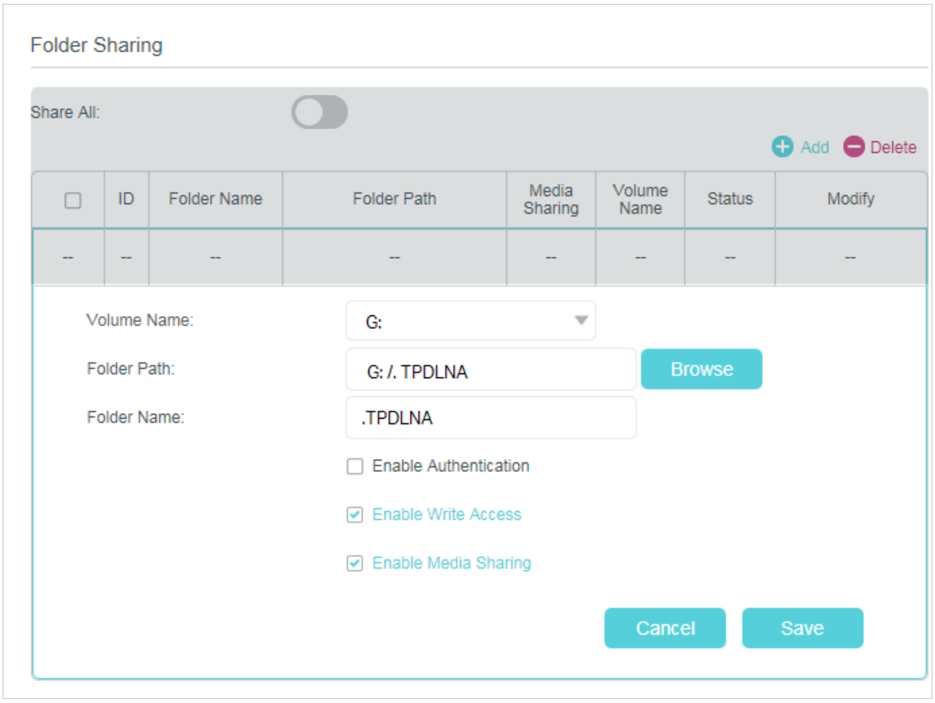
Network/Media Server Name: MyShare

Enable	Access Method	Access Address	Port
☑	Media Server	--	--
☑	Network Neighborhood	\\MyShare	--
☑	FTP	ftp://192.168.0.1:21	21
□	FTP(via Internet)	ftp://0.0.0.0:21	21

2. Now you can access the USB disk by visiting \\MyShare (for Windows) or smb://MyShare(for Mac).

➢ **To only share specific content:**

1. Focus on the Folder Sharing section. Click the button to disable Share All, then click Add to add a new sharing folder.



Folder Sharing

Share All: ○

□	ID	Folder Name	Folder Path	Media Sharing	Volume Name	Status	Modify
--	--	--	--	--	--	--	--

Volume Name: G:

Folder Path: G: /. TPDLNA

Folder Name: .TPDLNA

□ Enable Authentication

☑ Enable Write Access

☑ Enable Media Sharing

2. Select the Volume Name and Folder Path, then enter a Folder Name as you like.

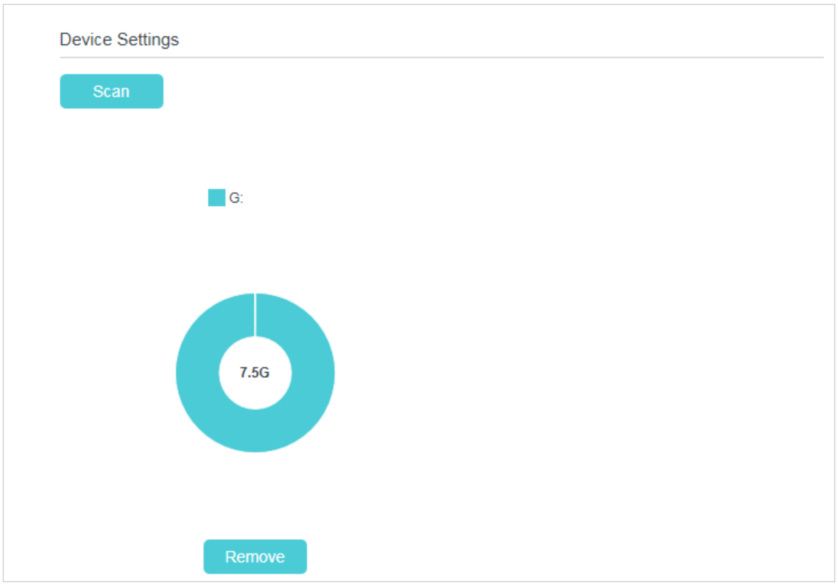
3. Decide the way you share the folder:

- Enable Authentication: Tick to enable authentication for this folder sharing, and you will be required to log in to the Sharing Account to access the USB disk. Refer to To set up authentication for data security: to learn more.

- Enable Write Access: If you tick this checkbox, network clients can modify this folder.
- Enable Media Sharing: Tick to enable media sharing for this folder, and you can view photos, play music and watch movies stored on the USB disk directly from DLNA-supported devices. Click Media Sharing to learn more.

4. Click Save.

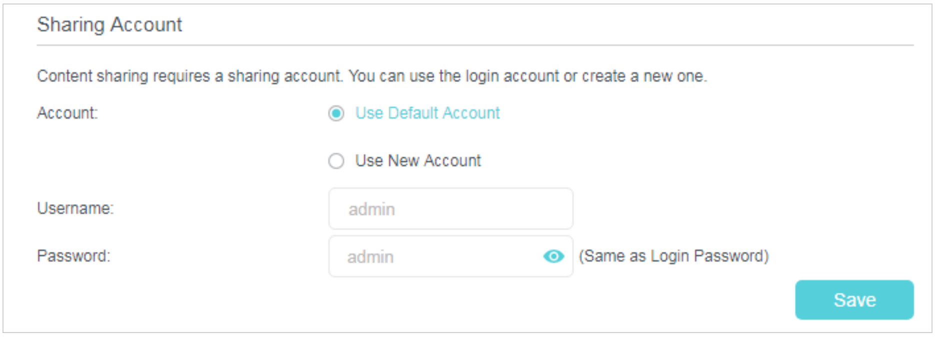
Tips:
The router can share 32 volumes at most.



➢ **To set up authentication for data security:**

You can set up authentication for your USB device so that network clients will be required to enter username and password when accessing the USB disk.

1. On the Sharing Accout part, Choose Use Default Account or Use New Account. The username is admin and the password is admin for Default Account. If your choose Use New Account, you have to customize the username and a password.



Sharing Account

Content sharing requires a sharing account. You can use the login account or create a new one.

Account: ● Use Default Account
○ Use New Account

Username: admin

Password: admin (Same as Login Password)

Save

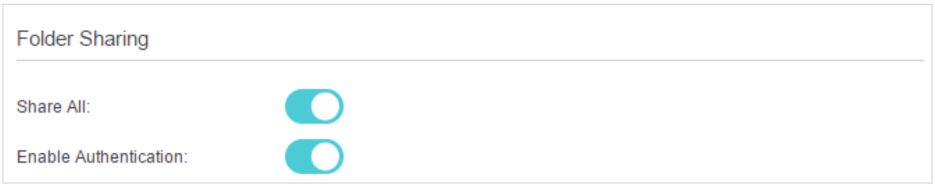
Note:

For Windows users, do not set the sharing username the same as the Windows username. Otherwise, Windows credential mechanism may cause the following problems:

- If the sharing password is also the same as the Windows password, authentication will not work since the Windows will automatically use its account information for USB access.
- If the sharing password is different from the Windows password, the Windows will be unable to remember your credentials and you will always be required to enter the sharing password for USB access.

2. Enable Authentication to apply the account you just set.

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

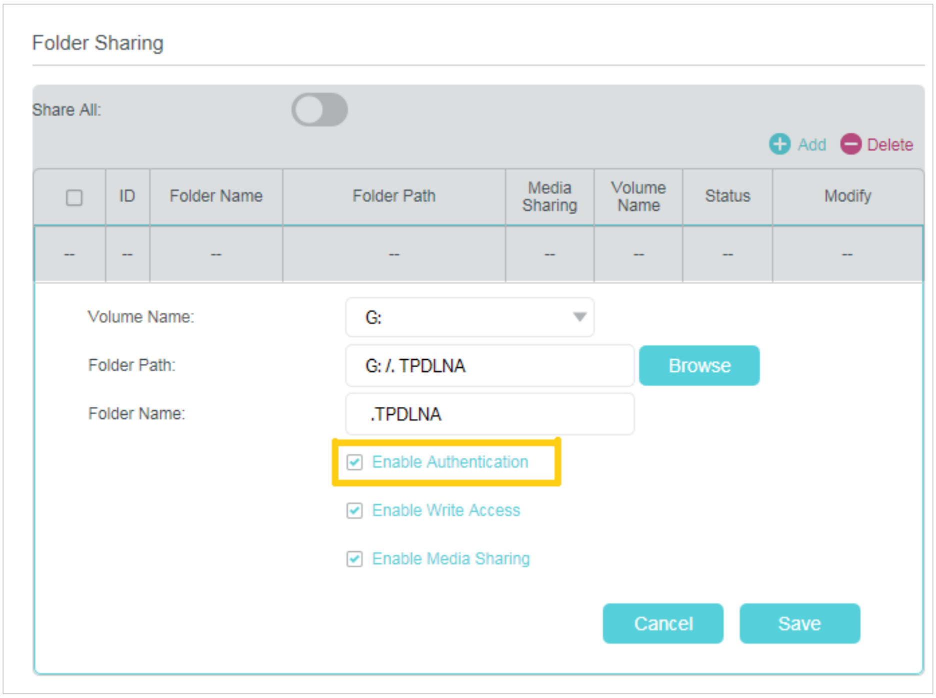


Folder Sharing

Share All: ●

Enable Authentication: ●

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



Folder Sharing

Share All: ○

□	ID	Folder Name	Folder Path	Media Sharing	Volume Name	Status	Modify
--	--	--	--	--	--	--	--

Volume Name: G:

Folder Path: G: /. TPDLNA

Folder Name: .TPDLNA

☑ Enable Authentication

☑ Enable Write Access

☑ Enable Media Sharing

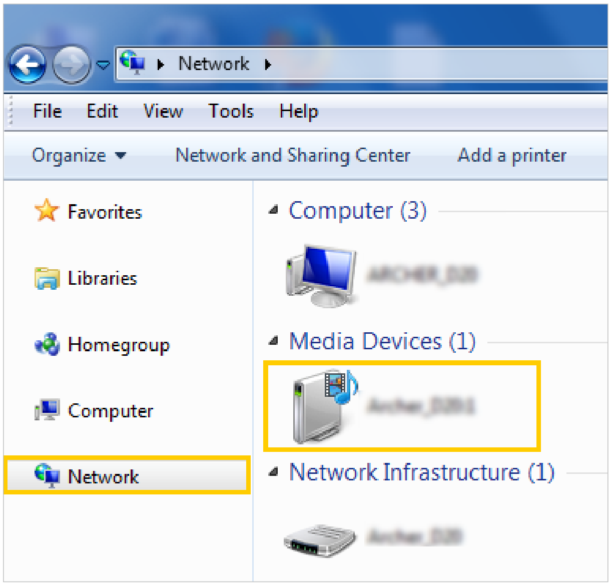
Note:

Due to Windows credential mechanism, you might be unable to access the USB disk after changing Authentication settings. Please log out from the Windows and try to access again. Or you can change the address of the USB disk by referring to To customize the address of the USB disk:.

5. 2. Media Sharing

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

1. When your USB disk is inseted into the router, your DLNA-supoorted devices (such as your computer and pad) connected to the router can detect and play the media files on the USB disks.
2. Refer to the following table for detailed instructions.

Windows Computer	• Go to Computer > Network, then click the Media Server Name (Model number-share by default) in the Media Devices section. **Note:** Here we take Windows 7 as an example.  Network File Edit View Tools Help Organize Network and Sharing Center Add a printer Favorites Libraries Homegroup Computer Network Computer (3) Media Devices (1) Network Infrastructure (1)
Smart device	• Use a third-party DLNA-supported player.

5. 3. 3G/4G Settings

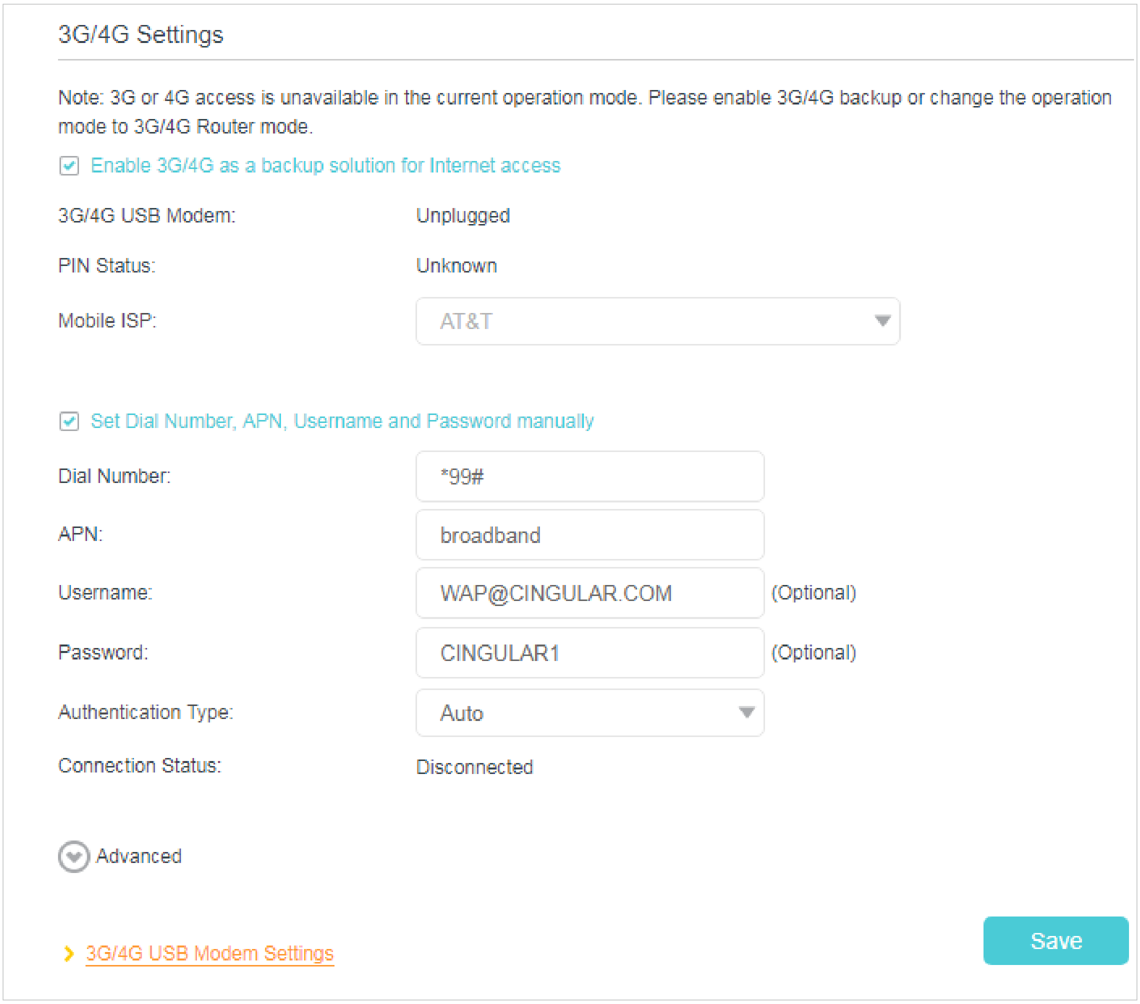
The router can be used as a 3G/4G wireless router if you have a 3G/4G USB modem. You can use your 3G/4G network as a backup solution for Internet access:

5. 3. 1. As a Backup Solution for Internet Access

Using 3G/4G network as a backup solution for Internet access, your router will be directly connected to the 3G/4G network when the original network service fails. When the WAN port is not connected, 3G/4G network is the only way to access the Internet.

Follow the steps below to set your 3G/4G network as a backup for Internet access:

1. Plug your USB modem into the USB port of your router.
2. Visit http://tplinkwifi.net, then log in with the password you set for the router.
3. Go to Advanced > USB Sharing > 3G/4G Settings, and select the box of Enable 3G/4G as a backup solution for Internet access.



3G/4G Settings

Note: 3G or 4G access is unavailable in the current operation mode. Please enable 3G/4G backup or change the operation mode to 3G/4G Router mode.

☑ Enable 3G/4G as a backup solution for Internet access

3G/4G USB Modem:	Unplugged
PIN Status:	Unknown
Mobile ISP:	AT&T

☑ Set Dial Number, APN, Username and Password manually

Dial Number:	*99#	
APN:	broadband	
Username:	WAP@CINGULAR.COM	(Optional)
Password:	CINGULAR1	(Optional)
Authentication Type:	Auto	
Connection Status:	Disconnected	

4. Verify that your 3G/4G USB Modem is successfully identified.

Note:
The 3G/4G USB modem will not be identified if it is incompatible with the router. Find the 3G/4G Compatibility List on the web page: http://www.tp-link.com/en/comp-list.html. If your USB modem is incompatible, contact our technical support.

5. Verify that the router has correctly recognized your Mobile ISP. When your Mobile ISP is correct, you have successfully set 3G/4G network as a backup solution for Internet access. Otherwise, select the box of Set the Dial Number, APN, Username and Password manually and enter the information provided by your 3G/4G network service provider.
6. Click Advanced to have more configurations if needed.
7. Click Save to make the settings effective.

Chapter 6

Parental Controls

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

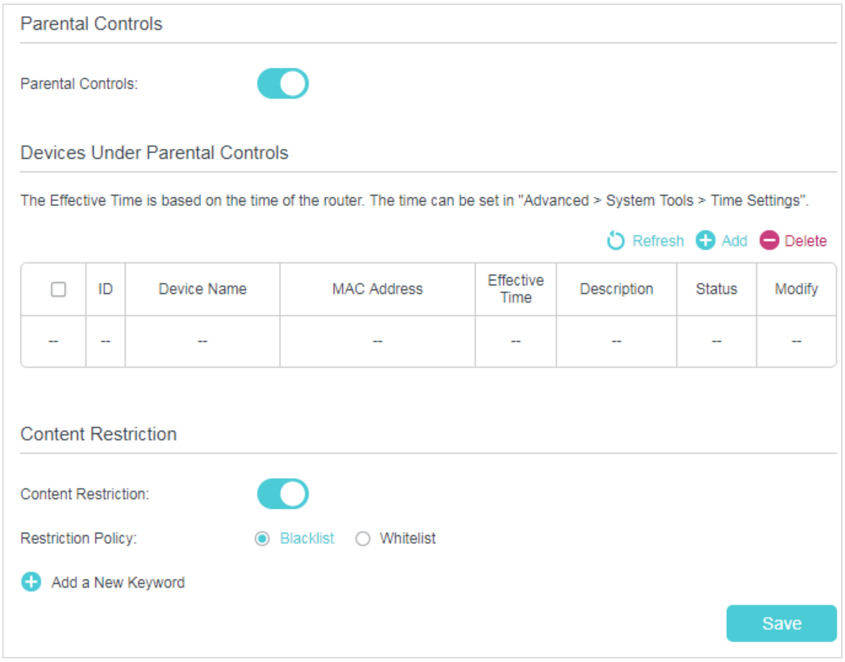
I want to:

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 the account you set for the router.
2. Go to Basic or Advanced > Parental Controls and enable Parental Controls.



Parental Controls

Parental Controls:

Devices Under Parental Controls

The Effective Time is based on the time of the router. The time can be set in "Advanced > System Tools > Time Settings".

Refresh Add Delete

□	ID	Device Name	MAC Address	Effective Time	Description	Status	Modify
--	--	--	--	--	--	--	--

Content Restriction

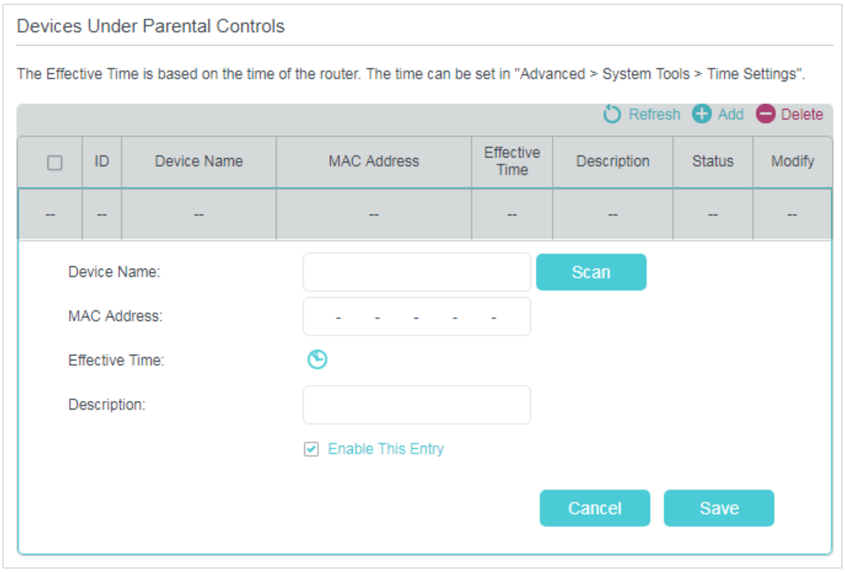
Content Restriction:

Restriction Policy: ● Blacklist ○ Whitelist

Add a New Keyword

Save

3. Click Add.



Devices Under Parental Controls

The Effective Time is based on the time of the router. The time can be set in "Advanced > System Tools > Time Settings".

Refresh ⊕ Add ⊖ Delete

□	ID	Device Name	MAC Address	Effective Time	Description	Status	Modify
--	--	--	--	--	--	--	--

Device Name: Scan

MAC Address: - - - - -

Effective Time: 🕓

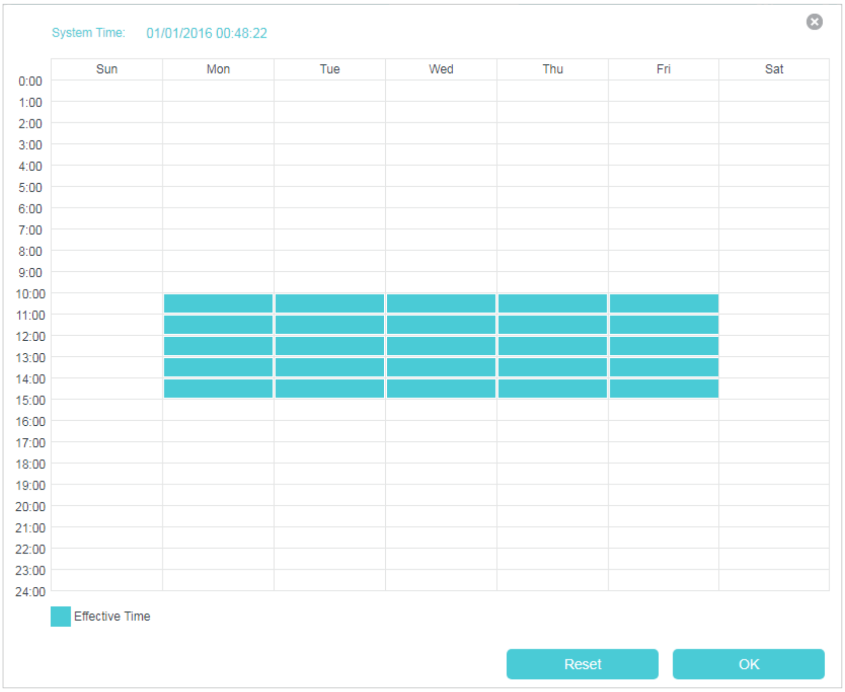
Description:

☑ Enable This Entry

Cancel Save

4. Click Scan, and add ⊕ the device to be controlled. Or, enter the Device Name and MAC Address manually.

5. Click the 🕓 icon to set the Effctive Time. Drag the cursor over the appropriate cell(s) and click Save.



System Time: 01/01/2016 00:48:22

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
0:00							
1:00							
2:00							
3:00							
4:00							
5:00							
6:00							
7:00							
8:00							
9:00							
10:00		🟦	🟦	🟦	🟦	🟦	
11:00		🟦	🟦	🟦	🟦	🟦	
12:00		🟦	🟦	🟦	🟦	🟦	
13:00		🟦	🟦	🟦	🟦	🟦	
14:00		🟦	🟦	🟦	🟦	🟦	
15:00							
16:00							
17:00							
18:00							
19:00							
20:00							
21:00							
22:00							
23:00							
24:00							

🟦 Effective Time

Reset OK

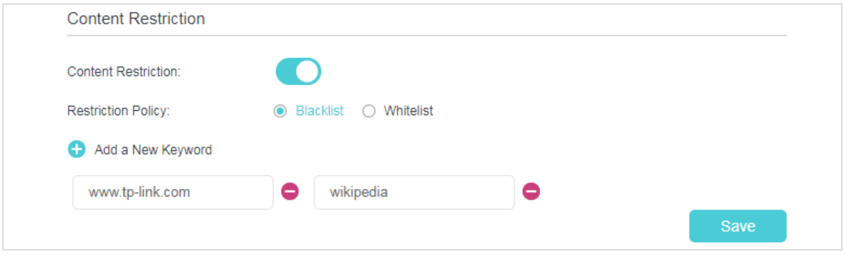
6. Enter a Description for the entry.

7. Select the checkbox to enable this entry and click Save.

8. Enable Content Restriction and select the restriction mode.

1) In Blacklist mode, the controlled devices cannot access any websites containing the specified keywords during the Internet Access Time period.

2) In Whitelist mode, the controlled devices can only access websites containing the specified keywords during the Effective Time period.



Content Restriction

Content Restriction: On

Restriction Policy: ● Blacklist ○ Whitelist

www.tp-link.com

wikipedia

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.

Chapter 7

Bandwidth Control

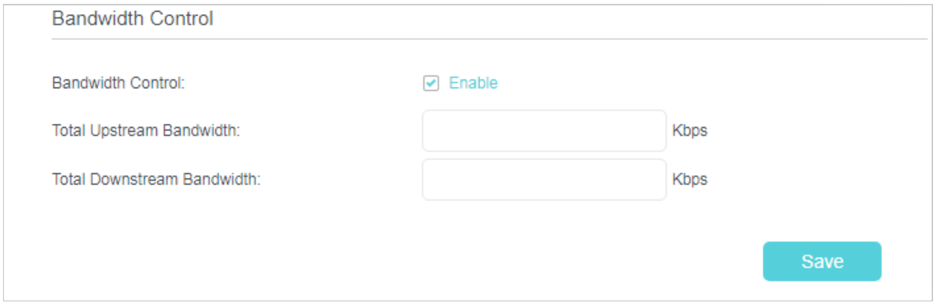
This chapter describes how to use the Bandwidth Control function to control the bandwidth by configuring rules for limiting various data flows. In this way, the network bandwidth can be reasonably distributed and utilized.

It contains the following sections:

7. 1. Configure the Bandwidth Control

Bandwidth Control allows you to configure the Upstream Bandwidth and Downstream Bandwidth of the network, follow the steps below to configure the Bandwidth Control.

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > Bandwidth Control page and enable Bandwidth Control.
3. Input the total upload and download speed through the WAN port in the Total Upstream Bandwidth and Total Downstream Bandwidth field. For optimal bandwidth control, please consult your ISP for the total allowed bandwidth for upstream and downstream.



Bandwidth Control

Bandwidth Control: ☑ Enable

Total Upstream Bandwidth: Kbps

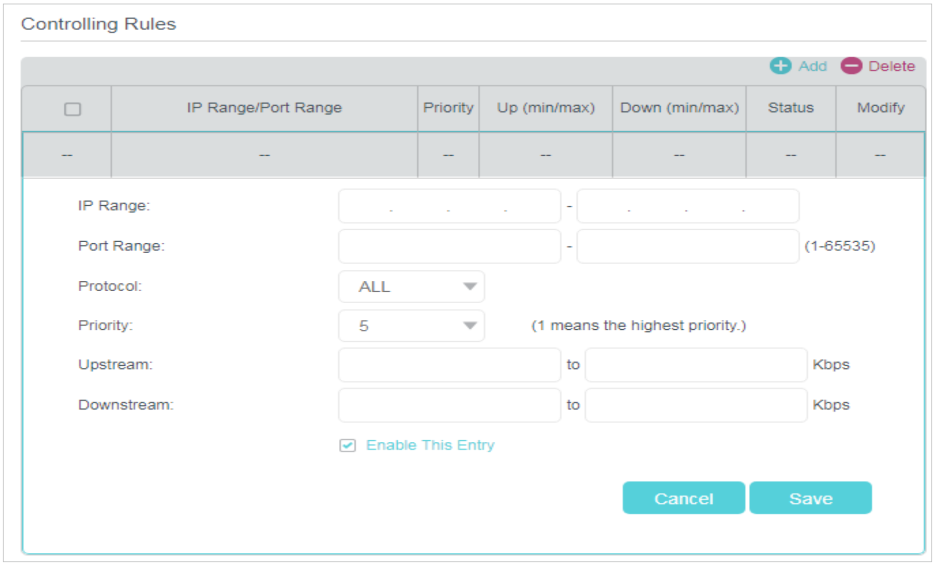
Total Downstream Bandwidth: Kbps

4. Click Save.

7. 2. Controlling rules

To add a new rule for the Bandwidth Control.

1. Click Add.



Controlling Rules

□	IP Range/Port Range	Priority	Up (min/max)	Down (min/max)	Status	Modify
--	--	--	--	--	--	--

IP Range: . . . - . . .

Port Range: - (1-65535)

Protocol: ALL

Priority: 5 (1 means the highest priority.)

Upstream: to Kbps

Downstream: to Kbps

☑ Enable This Entry

2. Enter a range of IP addresses and port numbers to be controlled.

3. Select the protocol type for this rule.
4. Select a priority level for this rule. 1 is the highest priority level and 8 is the lowest priority level. The total upload and download bandwidth will be allocated to guarantee the minimal rate of all bandwidth control rules.
5. Enter the minimum and maximum upload bandwidth and download bandwidth through the WAN port.
6. Select Enable This Entry.
7. Click Save.

Chapter 8

Network Security

This chapter guides you on how to protect your home network from unauthorized users by implementing these two network security functions. you can use Access Control for wired and wierless networks, or you can prevent ARP spoofing and ARP attacks using IP & MAC Binding.

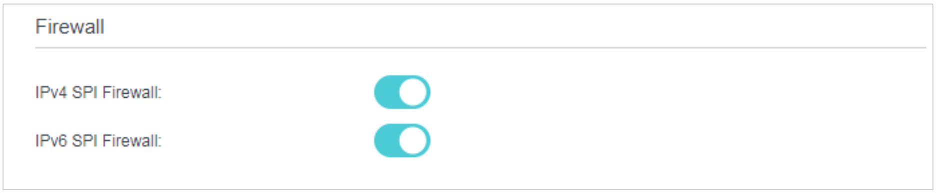
It contains the following sections:

- Firewall & DoS Protection
- Service Filtering
- Access Control
- IP & MAC Binding

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.



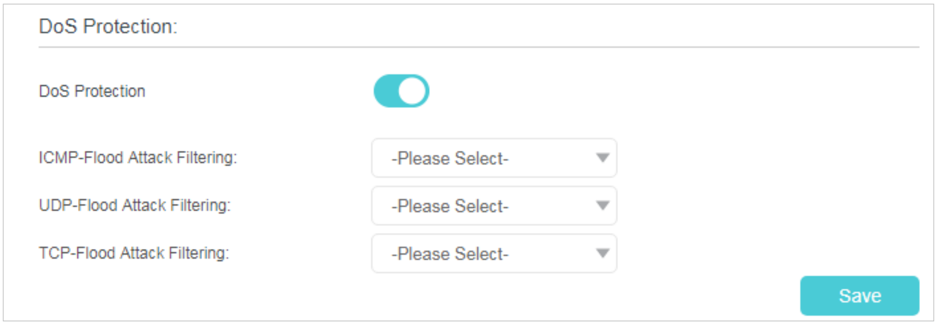
Firewall

IPv4 SPI Firewall:

IPv6 SPI Firewall:

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 the account you set for the router.
2. Go to Advanced > Security > Firewall & DoS Protection.



DoS Protection:

DoS Protection

ICMP-Flood Attack Filtering: -Please Select-

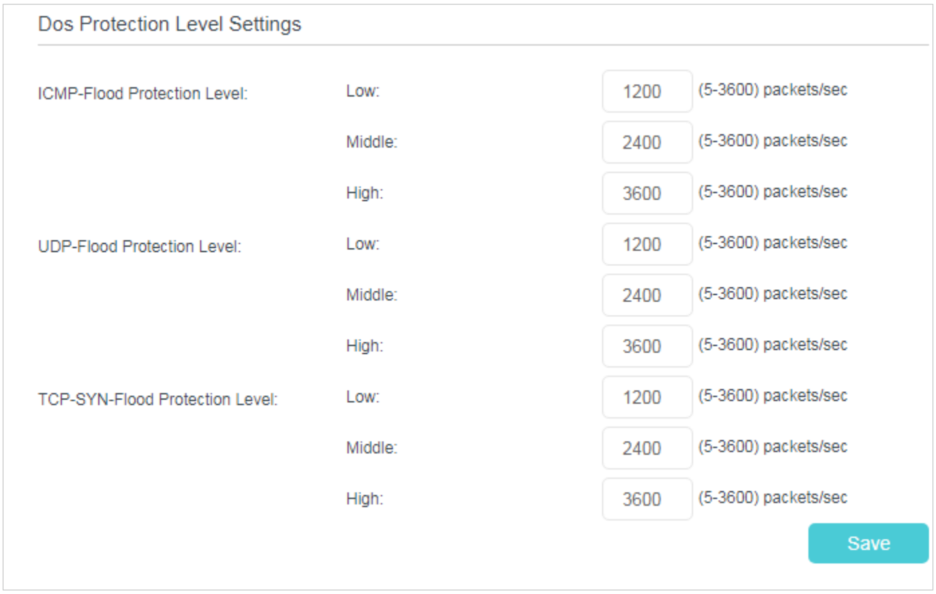
UDP-Flood Attack Filtering: -Please Select-

TCP-Flood Attack Filtering: -Please Select-

3. Enable DoS Protection.
4. Set the level (Low, Middle or High) of protection for ICMP-FLOOD Attack Filtering, UDP-FIOOD Attack Filtering and TCP-FLOOD Attack Filtering.
   - ICMP-FLOOD Attack Filtering - Enable to prevent the ICMP (Internet Control Message Protocol) flood attack.
   - UDP-FIOOD Attack Filtering - Enable to prevent the UDP (User Datagram Protocol) flood attack.
   - TCP-FLOOD Attack Filtering - Enable to prevent the TCP (Transmission Control Protocol) flood attack.
5. Click Save.

Tips:

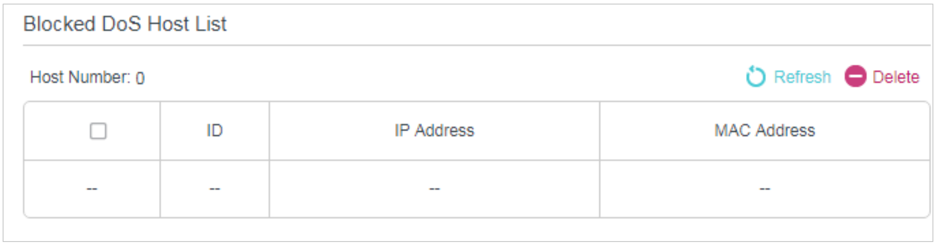
1. The level of protection is based on the number of traffic packets. Specify the level at DoS Protection Level Settings.



Dos Protection Level Settings

ICMP-Flood Protection Level:	Low:	1200	(5-3600) packets/sec
	Middle:	2400	(5-3600) packets/sec
	High:	3600	(5-3600) packets/sec
UDP-Flood Protection Level:	Low:	1200	(5-3600) packets/sec
	Middle:	2400	(5-3600) packets/sec
	High:	3600	(5-3600) packets/sec
TCP-SYN-Flood Protection Level:	Low:	1200	(5-3600) packets/sec
	Middle:	2400	(5-3600) packets/sec
	High:	3600	(5-3600) packets/sec

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.



Blocked DoS Host List

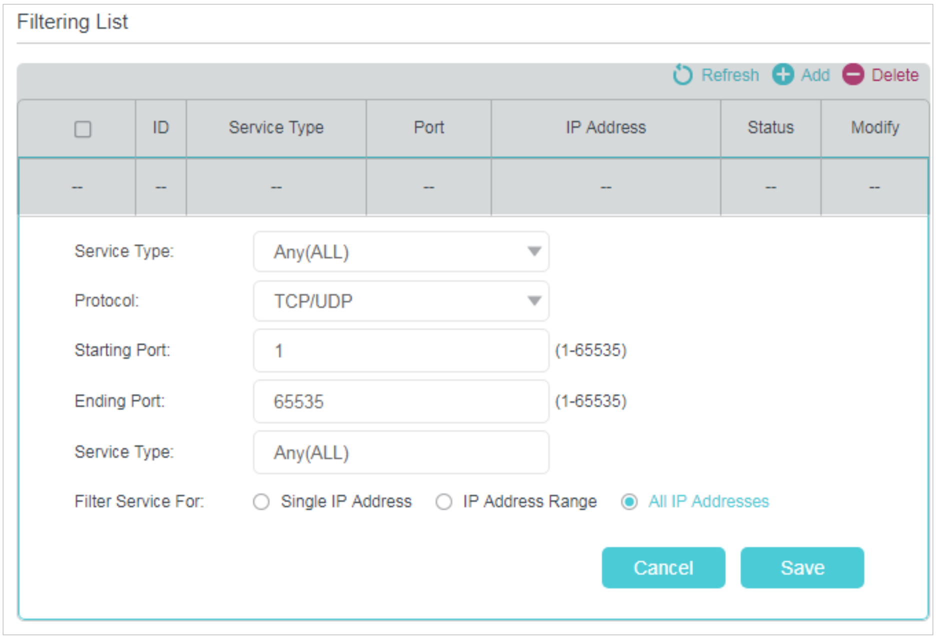
Host Number: 0

□	ID	IP Address	MAC Address
--	--	--	--

8. 2. Service Filtering

With Service Filtering, you can prevent certain users from accessing the specified service, even block internet access completely.

1. Visit http://tplinkwifi.net, and log in with the account you set for the router.
2. Go to Advanced > Security > Service Filtering.
3. Toggle On Service Filtering.
4. Click Add.



Filtering List

□	ID	Service Type	Port	IP Address	Status	Modify
--	--	--	--	--	--	--

Service Type: Any(ALL)

Protocol: TCP/UDP

Starting Port: 1 (1-65535)

Ending Port: 65535 (1-65535)

Service Type: Any(ALL)

Filter Service For: ○ Single IP Address ○ IP Address Range ● All IP Addresses

5. Select a Service Type from the drop-down list and the following four fields will be auto-populated. Select Custom when your desired service type is not listed, and enter the information manually.
6. Specify the IP address(es) that this filtering rule will apply to.
7. Click Save.

Note: If you want to disable this entry, click the Bulb icon .

8. 3. Access Control

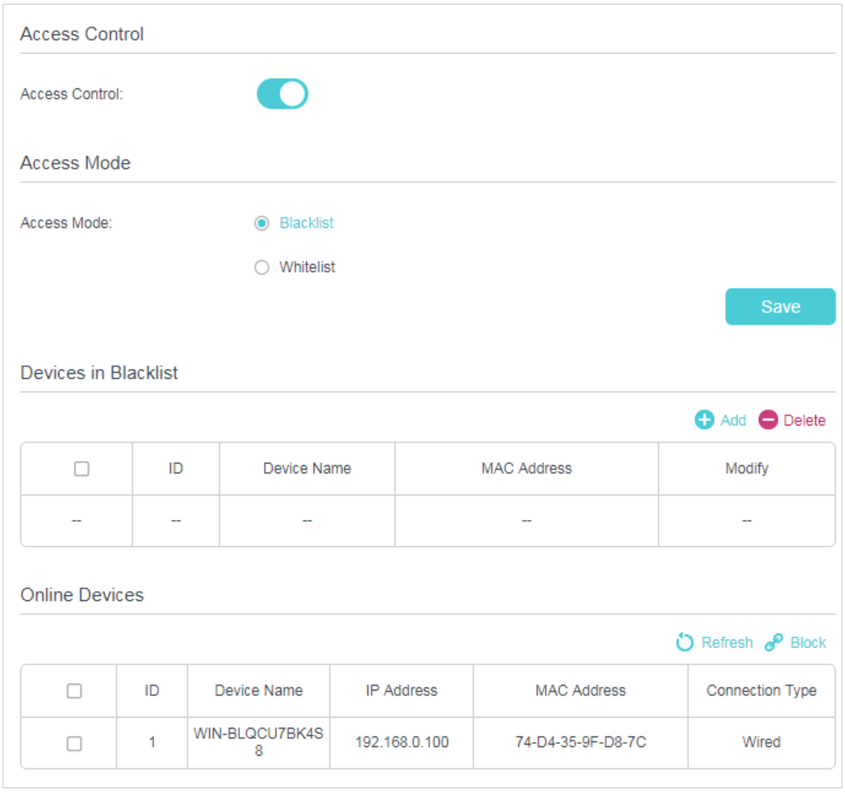
Access Control is used to block or allow specific client devices to access your network (via wired or wireless) based on a list of blocked devices (Blacklist) or a list of allowed devices (Whitelist).

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 the account you set for the router.
2. Go to Advanced > Security > Access Control and enable Access Control.



Access Control

Access Control: ●

Access Mode

Access Mode: ● Blacklist

○ Whitelist

Devices in Blacklist

□	ID	Device Name	MAC Address	Modify
--	--	--	--	--

Online Devices

□	ID	Device Name	IP Address	MAC Address	Connection Type
□	1	WIN-BLQCU7BK4S8	192.168.0.100	74-D4-35-9F-D8-7C	Wired

1. 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.

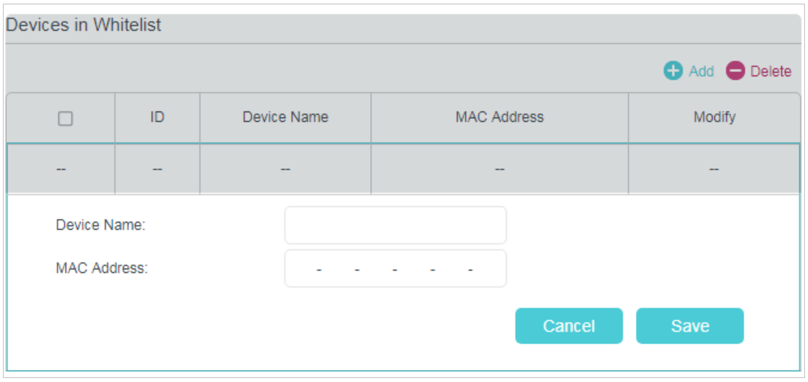
   2) Select the device(s) to be blocked in the Online Devices table.

   3) Click Block above the Online Devices 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.



Devices in Whitelist

□	ID	Device Name	MAC Address	Modify
--	--	--	--	--

Device Name:

MAC Address: - - - - -

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

4) Click Save.

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

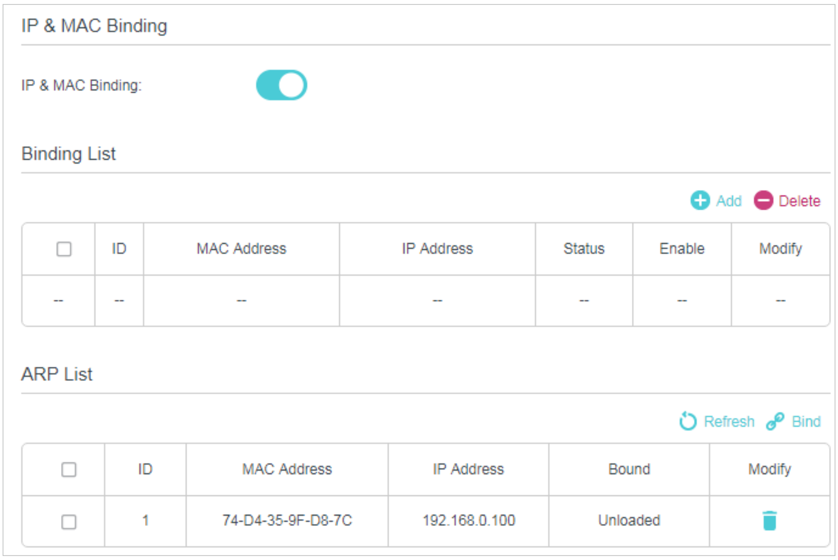
8. 4. IP & MAC Binding

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 the account you set for the router.
2. Go to Advanced > Security > IP & MAC Binding and enable IP & MAC Binding.



Binding List

□	ID	MAC Address	IP Address	Status	Enable	Modify
--	--	--	--	--	--	--

ARP List

□	ID	MAC Address	IP Address	Bound	Modify
□	1	74-D4-35-9F-D8-7C	192.168.0.100	Unloaded	🗑

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

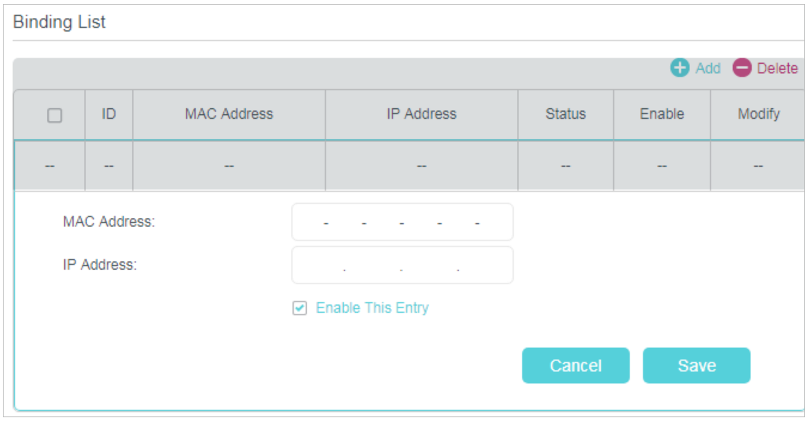
To bind the connected device(s)

1) Select the device(s) to be bound in the ARP List.

2) Click Bind to add to the Binding List.

To bind the unconnected device

1) Click Add.



Binding List

□	ID	MAC Address	IP Address	Status	Enable	Modify
--	--	--	--	--	--	--

MAC Address: - - - - -

IP Address: . . .

☑ Enable This Entry

2) Enter the MAC address and IP address that you want to bind.

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

Done!

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

Chapter 9

NAT Forwarding

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

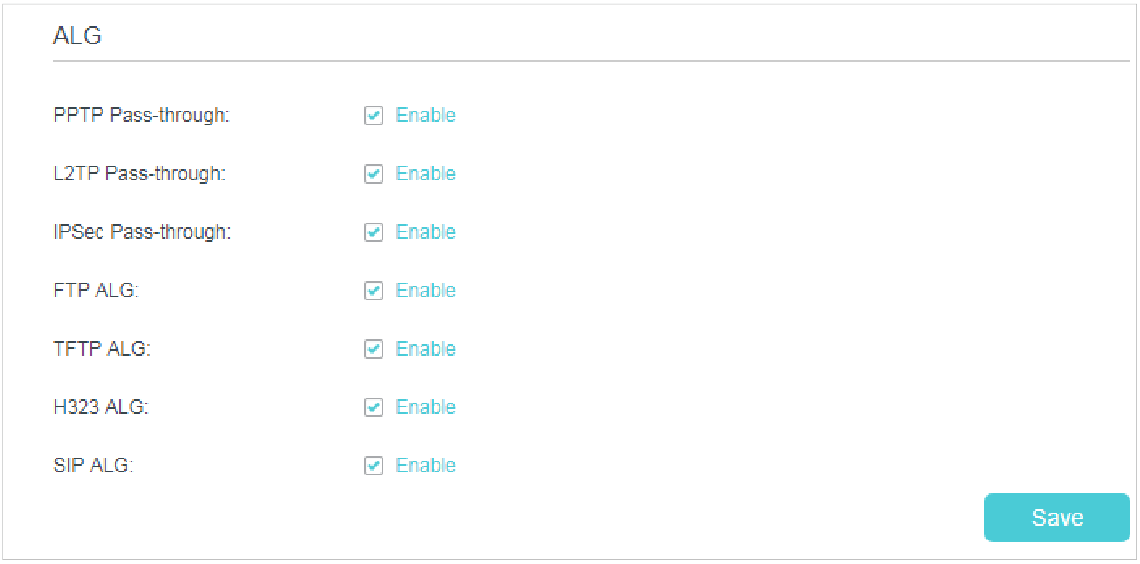
With the forwarding feature the router can penetrate the isolation of NAT and allows devices on the internet to initiatively communicate with devices on the local network, thus realizing some special functions.

The TP-Link router supports 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.

It contains the following sections:

9. 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.



ALG

PPTP Pass-through: ☑ Enable

L2TP Pass-through: ☑ Enable

IPSec Pass-through: ☑ Enable

FTP ALG: ☑ Enable

TFTP ALG: ☑ Enable

H323 ALG: ☑ Enable

SIP ALG: ☑ Enable

- PPTP Pass-through: If enabled, it allows Point-to-Point sessions to be tunneled through an IP network and passed through the router.
- L2TP Pass-through: If enabled, it allows Layer 2 Point-to-Point sessions to be tunneled through an IP network and passed through the router.
- IPSec Pass-through: 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.
- FTP ALG: If enabled, it allows FTP (File Transfer Protocol) clients and servers to transfer data via NAT.
- TFTP ALG: If enabled, it allows TFTP (Trivial File Transfer Protocol) clients and servers to transfer data via NAT.
- H323 ALG: If enabled, it allows Microsoft NetMeeting clients to communicate via NAT.
- SIP ALG: If enabled, it allows clients communicate with SIP (Session Initiation Protocol) servers via NAT.

9. 2. Share Local Resources on the Internet by Virtual Servers

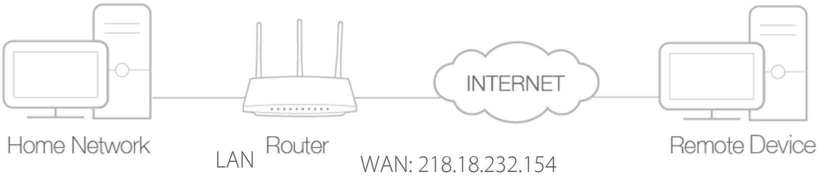
When you build up a server on the local network and want to share it on the internet, Virtual Servers can realize the service and provide it to internet users. At the same time Virtual Servers can keep the local network safe as other services are still invisible from the internet.

Virtual Servers can be used for setting up public services on your local network, such as HTTP, FTP, DNS, POP3/SMTP and Telnet. Different services use different service ports. 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:

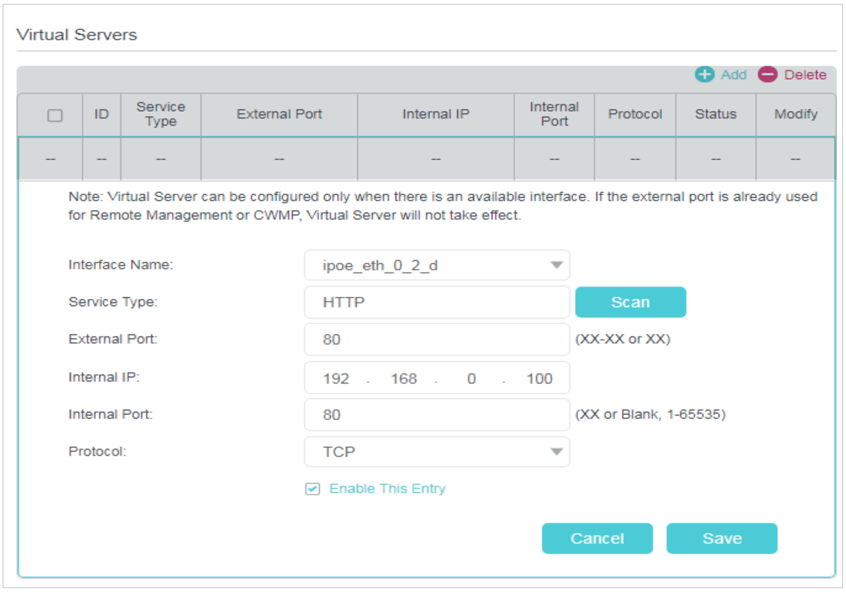
Share my personal website I've built in local network with my friends through the internet.

For example, the personal website has been built on my home PC (192.168.0.100). I hope that my friends on 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 the password you set for the router.
3. Go to Advanced > NAT Forwarding > Virtual Servers.
4. Click Add. Click Scan and choose HTTP. The External Port, Internal Port and Protocol will be automatically filled in. Enter the PC's IP address 192.168.0.100 in the Internal IP field.
5. Click Save.



Virtual Servers

☐	ID	Service Type	External Port	Internal IP	Internal Port	Protocol	Status	Modify
--	--	--	--	--	--	--	--	--

Note: Virtual Server can be configured only when there is an available interface. If the external port is already used for Remote Management or CWMP, Virtual Server will not take effect.

Interface Name:	ipoe_eth_0_2_d	
Service Type:	HTTP	Scan
External Port:	80	(XX-XX or XX)
Internal IP:	192 . 168 . 0 . 100	
Internal Port:	80	(XX or Blank, 1-65535)
Protocol:	TCP	

☑ Enable This Entry

Tips:

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

Done!

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

Tips:

- The WAN IP should be a public IP address. For the WAN IP is assigned dynamically by the ISP, it is recommended to apply and register a domain name for the WAN referring to Set Up a Dynamic DNS Service Account . Then users on the internet can use http:// domain name to visit the website.
- 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.

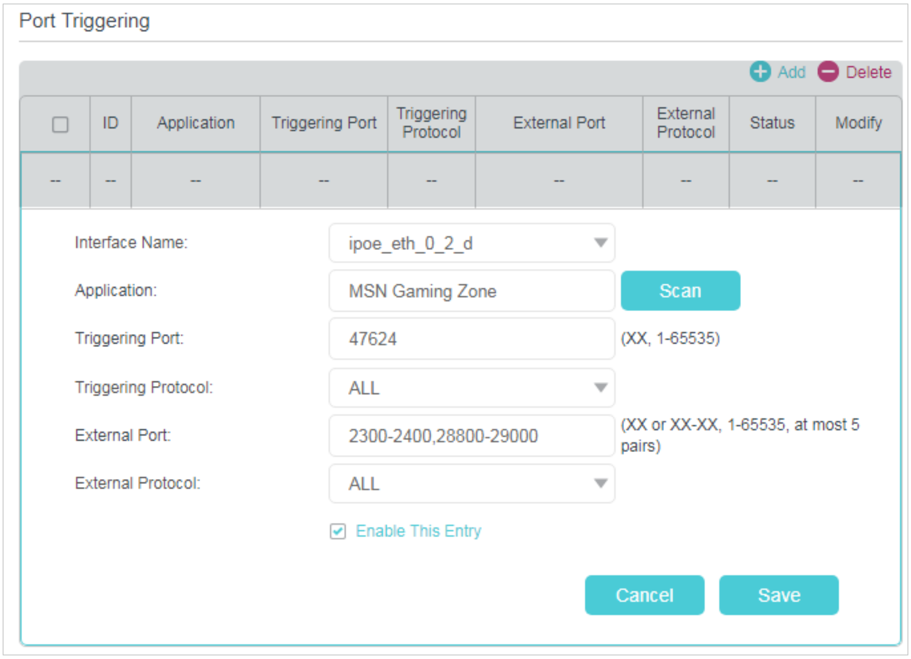
9. 3. Open Ports Dynamically by Port Triggering

Port Triggering can specify a triggering port and its corresponding external ports. When a host on the local network initiates a connection to the triggering port, all the external ports will be opened for subsequent connections. The router can record the IP address of the host. When the data from the internet return to the external ports, the router can forward them to the corresponding host. Port Triggering is mainly applied to online games, VoIPs, video players and common applications including MSN Gaming Zone, Dialpad 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 TP-Link ID or the password you set for the router.
2. Go to Advanced > NAT Forwarding > Port Triggering and click Add.

3. Click Scan, and select the desired application. The triggering port and protocol, the external port and protocol will be automatically filled with contents . The following picture takes application MSN Gaming Zone as an example.
4. Click Save.


Port Triggering

□	ID	Application	Triggering Port	Triggering Protocol	External Port	External Protocol	Status	Modify
--	--	--	--	--	--	--	--	--

Interface Name:	ipoe_eth_0_2_d	
Application:	MSN Gaming Zone	Scan
Triggering Port:	47624	(XX, 1-65535)
Triggering Protocol:	ALL	
External Port:	2300-2400,28800-29000	(XX or XX-XX, 1-65535, at most 5 pairs)
External Protocol:	ALL	

☑ Enable This Entry

Tips:

- You can add multiple port triggering rules according to your network need.
- The triggering ports can not be overlapped.
- 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.

9. 4. Make Applications Free from Port Restriction by DMZ

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

Note:

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

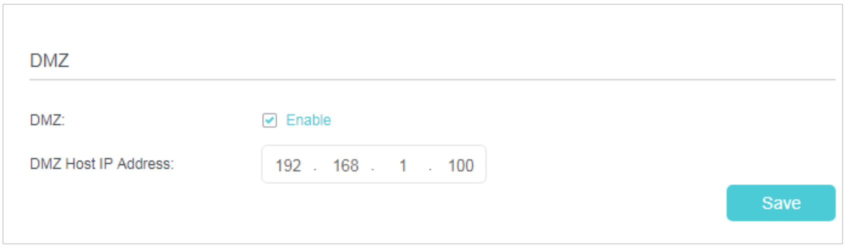
I want to:

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 host with all ports open.

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 TP-Link ID or the password you set for the router.
3. Go to Advanced > NAT Forwarding > DMZ and select Enable DMZ.
4. Enter the IP address 192.168.0.100 in the DMZ Host IP Address filed.



DMZ

DMZ: ☑ Enable

DMZ Host IP Address: 192 . 168 . 1 . 100

5. Click Save.

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.

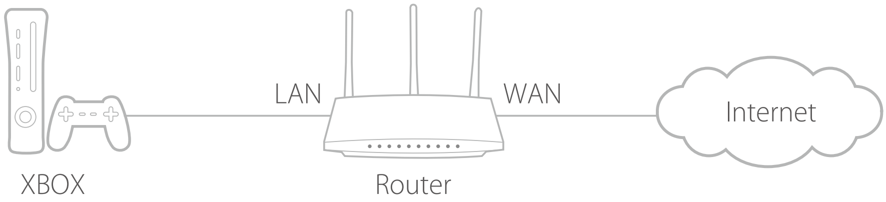
9. 5. Make Xbox Online Games Run Smoothly by UPnP

The UPnP (Universal Plug and Play) protocol allows applications or host devices to automatically find the front-end NAT device and send request to it to open the corresponding ports. With UPnP enabled, the applications or host devices on the local network and the internet can freely communicate with each other thus realizing the seamless connection of the network. You may need to enable the UPnP if you want to use applications for multiplayer gaming, peer-to-peer connections, real-time communication (such as VoIP or telephone conference) or remote assistance, etc.

Tips:

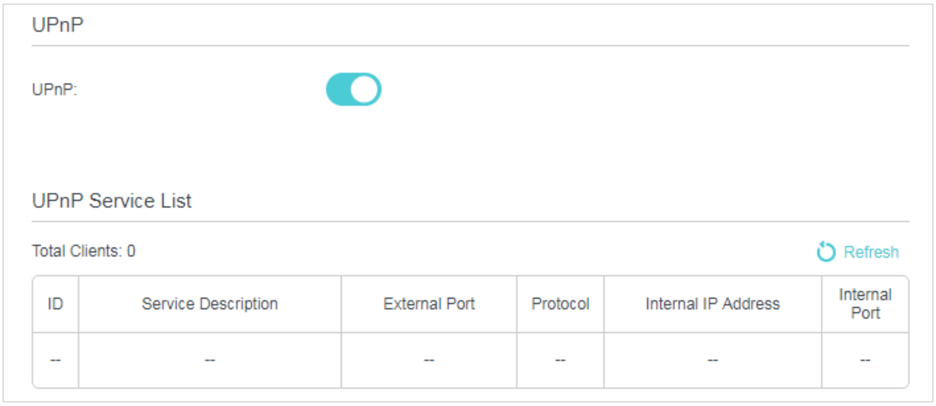
- UPnP is enabled by default in this router.
- Only the application supporting UPnP protocol can use this feature.
- UPnP feature needs the support of operating system (e.g. Windows Vista/ Windows 7/ Windows 8, etc. Some of operating system need to install the UPnP components).

For example, when you connect your Xbox to the router which 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 TP-Link ID or the password you set for the router.
2. Go to Advanced > NAT Forwarding > UPnP and toggle on or off according to your needs.



UPnP

UPnP: ●

UPnP Service List

Total Clients: 0

ID	Service Description	External Port	Protocol	Internal IP Address	Internal Port
--	--	--	--	--	--

Chapter 10

VPN Server

The VPN (Virtual Private Networking) Server allows you to access your home network in a secured way through internet when you are out of home. The router offers two ways to set up VPN connection: OpenVPN and PPTP (Point to Point Tunneling Protocol) VPN.

OpenVPN is somewhat complex but with greater security and more stable. It is suitable for restricted environment, such as campus network and company intranet.

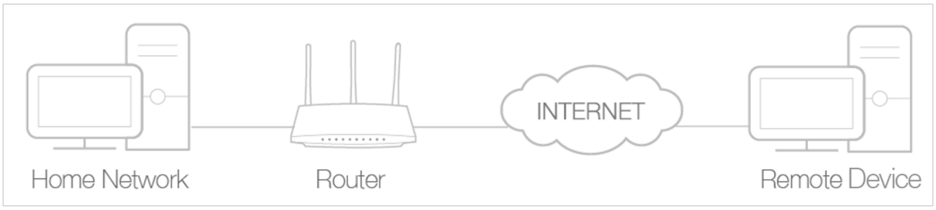
PPTP VPN is more easily used and its speed is faster, it's compatible with most operating systems and also supports mobile devices. Its security is poor and your packets may be cracked easily, and PPTP VPN connection may be prevented by some ISP.

It contains the following sections, please choose the appropriate VPN server connection type as needed.

- Use Open VPN to Access Your Home Network
- Use PPTP VPN to Access Your Home Network

10. 1. Use Open VPN to Access Your Home Network

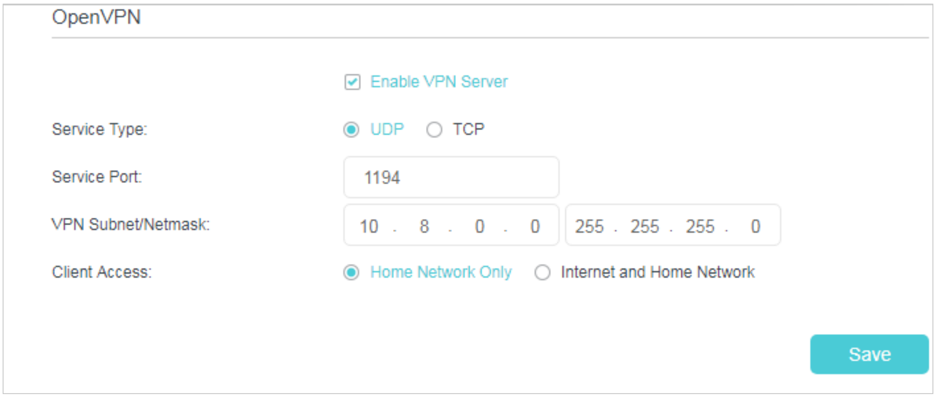
In the OpenVPN connection, the home network can act as a server, and the remote device can access the server through the router which acts as an OpenVPN Server gateway. To use the VPN feature, you should enable OpenVPN Server on your router, and install and run VPN client software on the remote device. Please follow the steps below to set up an OpenVPN connection.



10. 1. 1. Step1. Set up OpenVPN Server on Your Router

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

2. Go to Advanced > VPN Server > OpenVPN, and select Enable VPN Server.



OpenVPN

☑ Enable VPN Server

Service Type: ● UDP ○ TCP

Service Port: 1194

VPN Subnet/Netmask: 10 . 8 . 0 . 0 255 . 255 . 255 . 0

Client Access: ● Home Network Only ○ Internet and Home Network

Note:

- Before you enable VPN Server, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router's WAN port and synchronize your System Time with internet.
- The first time you configure the OpenVPN Server, you may need to Generate a certificate before you enable the VPN Server.

3. Select the Service Type (communication protocol) for OpenVPN Server: UDP, TCP.

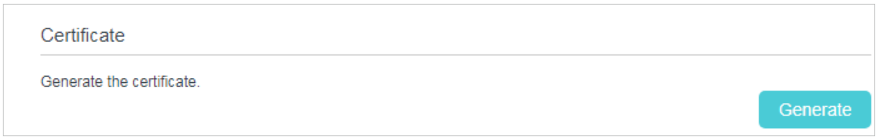
4. Enter a VPN Service Port to which a VPN device connects, and the port number should be between 1024 and 65535.

5. In the VPN Subnet/Netmask fields, enter the range of IP addresses that can be leased to the device by the OpenVPN server.

6. Select your Client Access type. Select Home Network Only if you only want the remote device to access your home network; select Internet and Home Network if you also want the remote device to access internet through the VPN Server.

7. Click Save.

8. Click Generate to get a new certificate.

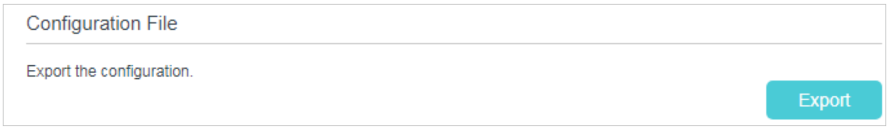

Certificate

Generate the certificate.

Note:

If you have already generated one, please skip this step, or click Generate to update the certificate.

9. Click Export to save the OpenVPN configuration file which will be used by the remote device to access your router.


Configuration File

Export the configuration.

10. 1. 2. Step 2. Configure OpenVPN Connection on Your Remote Device

1. Visit http://openvpn.net/index.php/download/community-downloads.html to download the OpenVPN software, and install it on your device where you want to run the OpenVPN client utility.

Note:

You need to install the OpenVPN client utility on each device that you plan to apply the VPN funxtion to access your router. Mobile devices should download a third-party app from Google Play or Apple App Store.

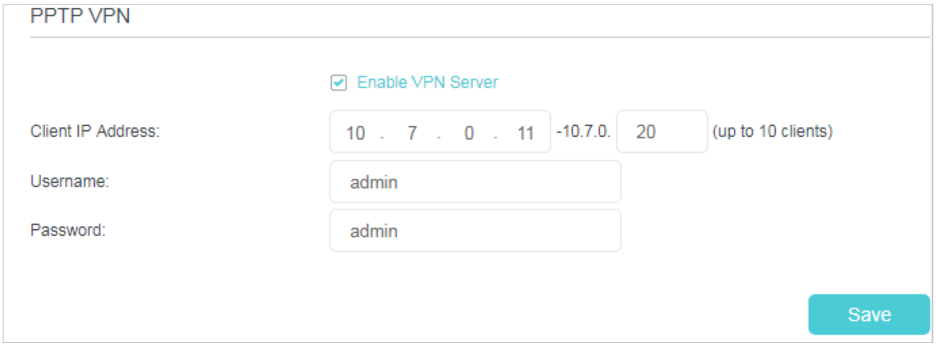
2. After the installation, copy the file exported from your router to the OpenVPN client utility’s “config” folder (for example, C:\Program Files\OpenVPN\config on Windows). The path depends on where the OpenVPN client utility is installed.
3. Run the OpenVPN client utility and connect it to OpenVPN Server.

10. 2. Use PPTP VPN to Access Your Home Network

PPTP VPN Server is used to create a VPN connection for remote device. To use the VPN feature, you should enable PPTP VPN Server on your router, and configure the PPTP connection on the remote device. Please follow the steps below to set up a PPTP VPN connection.

10. 2. 1. Step 1. Set up PPTP VPN Server on Your Router

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > VPN Server > PPTP VPN, and select Enable VPN Server.



PPTP VPN

☑ Enable VPN Server

Client IP Address: 10 . 7 . 0 . 11 -10.7.0. 20 (up to 10 clients)

Username: admin

Password: admin

Note:

Before you enable VPN Server, we recommend you configure Dynamic DNS Service (recommended) or assign a static IP address for router's WAN port and synchronize your System Time with internet.

3. In the Client IP Address filed, enter the range of IP addresses (up to 10) that can be leased to the devices by the PPTP VPN server.

4. Enter Username and Password to authenticate clients to the PPTP VPN server.

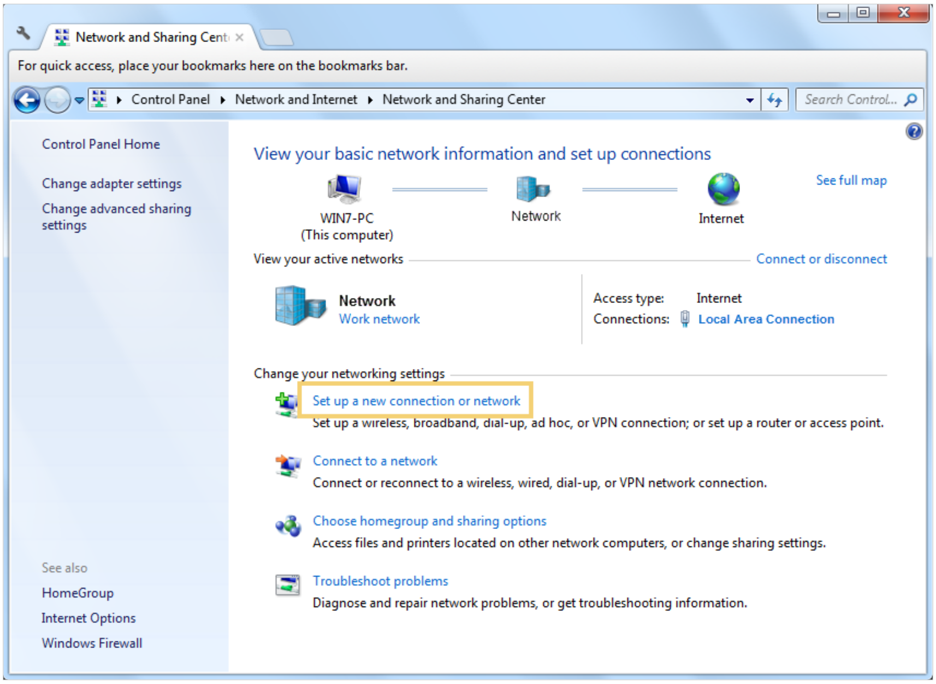
5. Click Save.

10. 2. 2. Step 2. Configure PPTP VPN Connection on Your Remote Device

The remote device can use the Windows built-in PPTP software or a third-party PPTP software to connect to PPTP Server. Here we use the Windows built-in PPTP software as an example.

1. Go to Start > Control Panel > Network and Internet > Network and Sharing Center.

2. Select Set up a new connection or network.



Network and Sharing Cent

For quick access, place your bookmarks here on the bookmarks bar.

Control Panel ▸ Network and Internet ▸ Network and Sharing Center

Search Control...

Control Panel Home

Change adapter settings

Change advanced sharing settings

See also

HomeGroup

Internet Options

Windows Firewall

View your basic network information and set up connections

See full map

WIN7-PC
(This computer)

Network

Internet

View your active networks — Connect or disconnect

Network
Work network

Access type: Internet
Connections: Local Area Connection

Change your networking settings

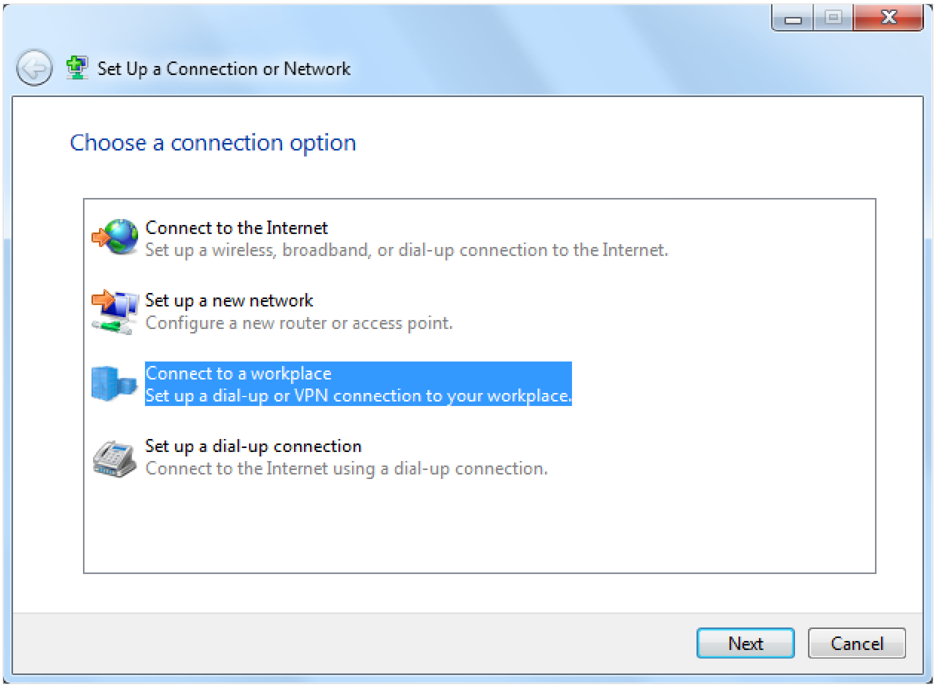
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

3. Select Connect to a workplace and click Next.



Set Up a Connection or Network

Choose a connection option

Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.

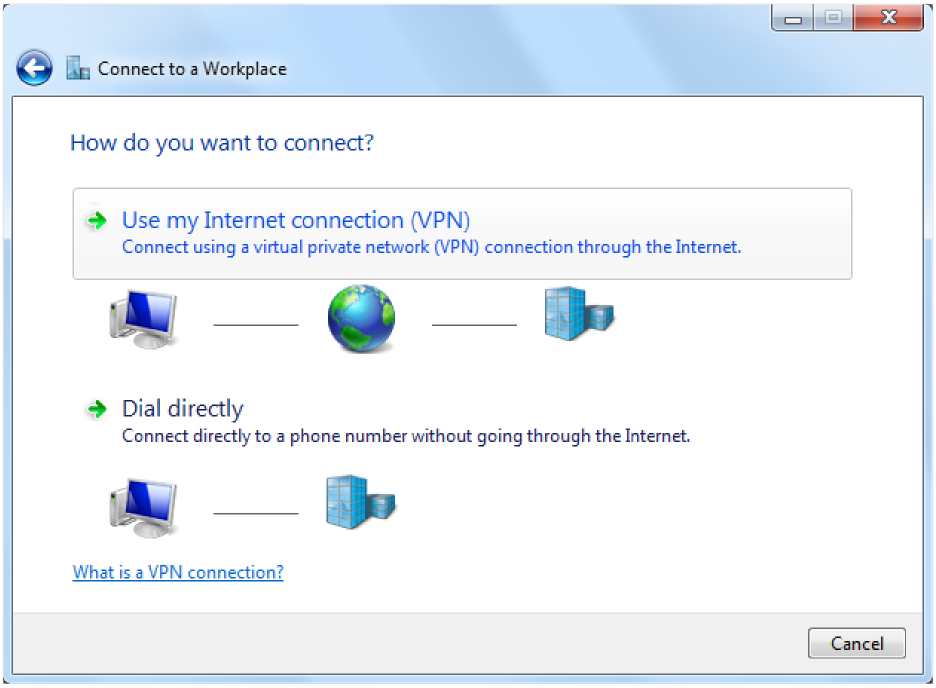
Set up a new network
Configure a new router or access point.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Set up a dial-up connection
Connect to the Internet using a dial-up connection.

Next Cancel

4. Select Use my Internet connection (VPN).



Connect to a Workplace

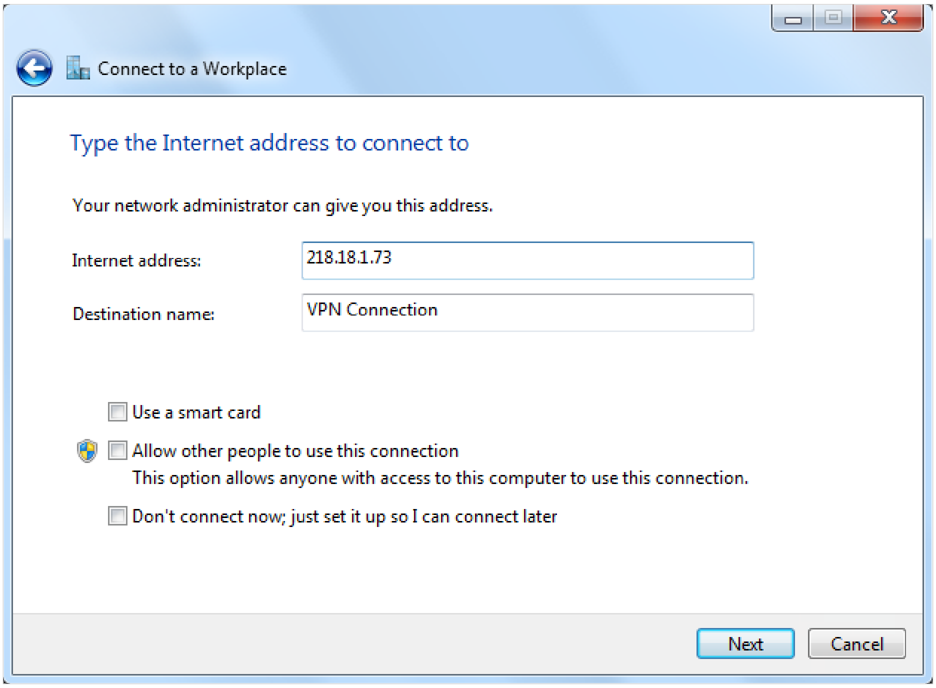
How do you want to connect?

→ Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

→ Dial directly
Connect directly to a phone number without going through the Internet.

What is a VPN connection?

5. Enter the internet IP address of the router (for example: 218.18.1.73) in the Internet address field. Click Next.



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 218.18.1.73

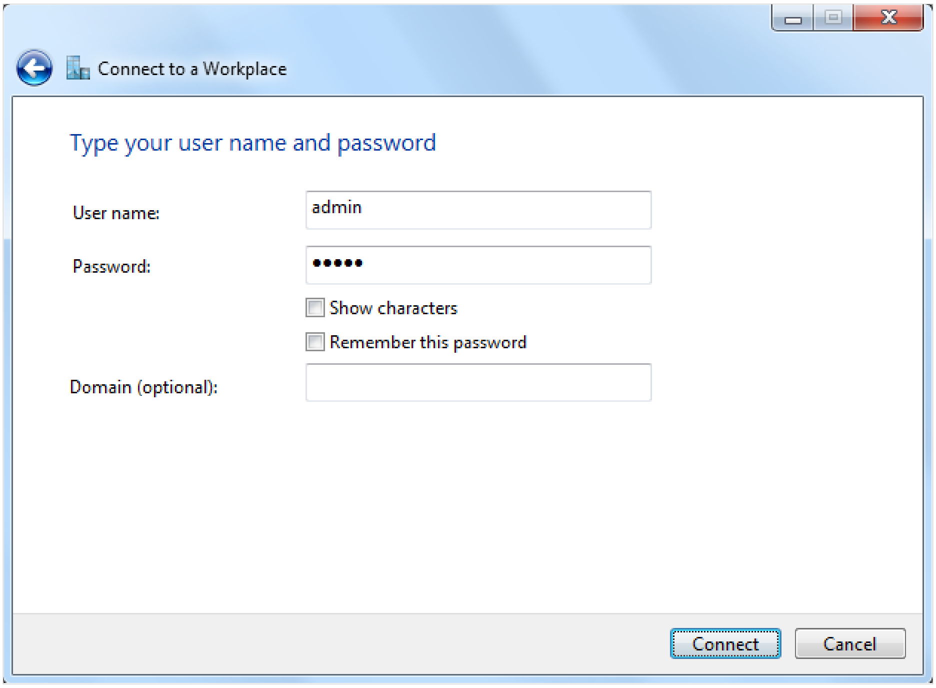
Destination name: VPN Connection

□ Use a smart card

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

□ Don't connect now; just set it up so I can connect later

6. Enter the User name and Password you have set for the PPTP VPN server on your router, and click Connect.


Connect to a Workplace

Type your user name and password

User name: admin

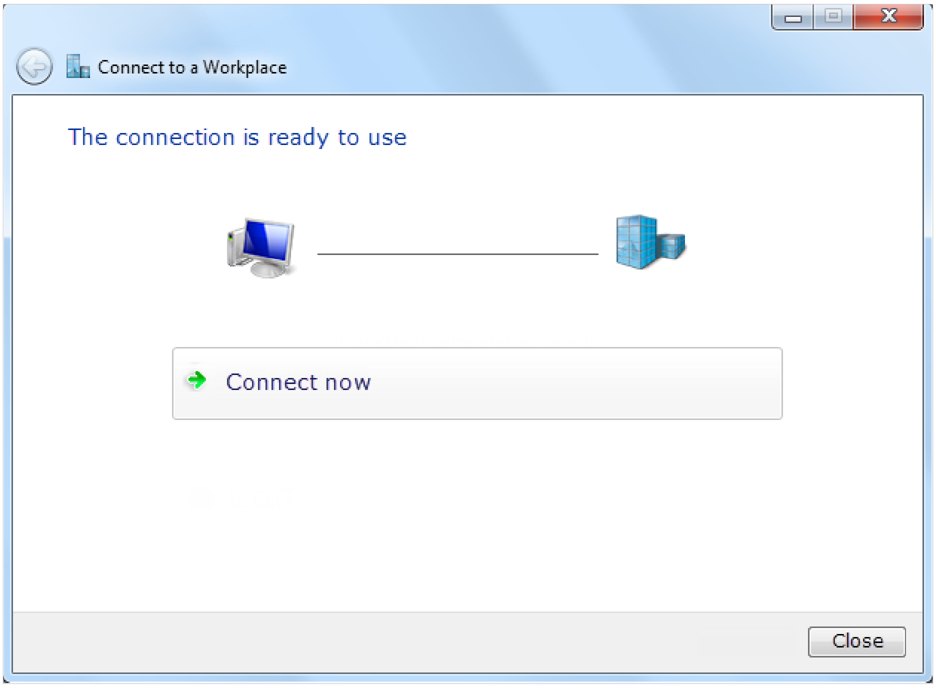
Password: •••••

□ Show characters

□ Remember this password

Domain (optional):

7. The PPTP VPN connection is created and ready to use.


Connect to a Workplace

The connection is ready to use

Chapter 11

Specify Your Network Settings

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

It contains the following sections:

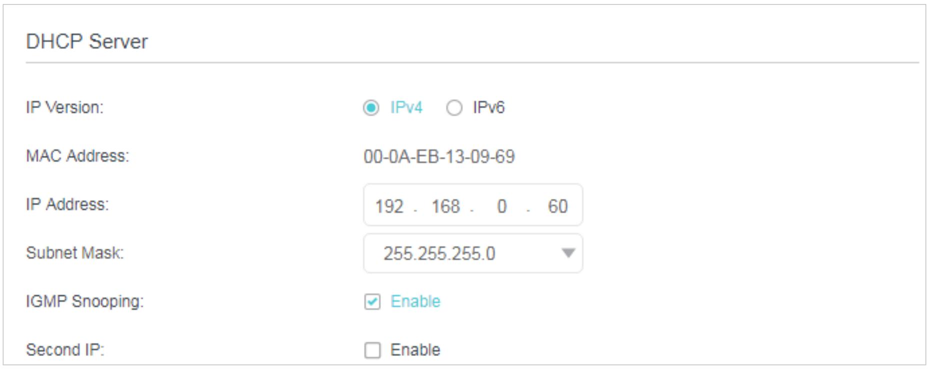
11. 1. LAN Settings

11. 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 the account you set for the router.
2. Go to Advanced > Network > LAN Settings page and select IPv4.



DHCP Server

IP Version: ● IPv4 ○ IPv6

MAC Address: 00-0A-EB-13-09-69

IP Address: 192 . 168 . 0 . 60

Subnet Mask: 255.255.255.0

IGMP Snooping: ☑ Enable

Second IP: □ Enable

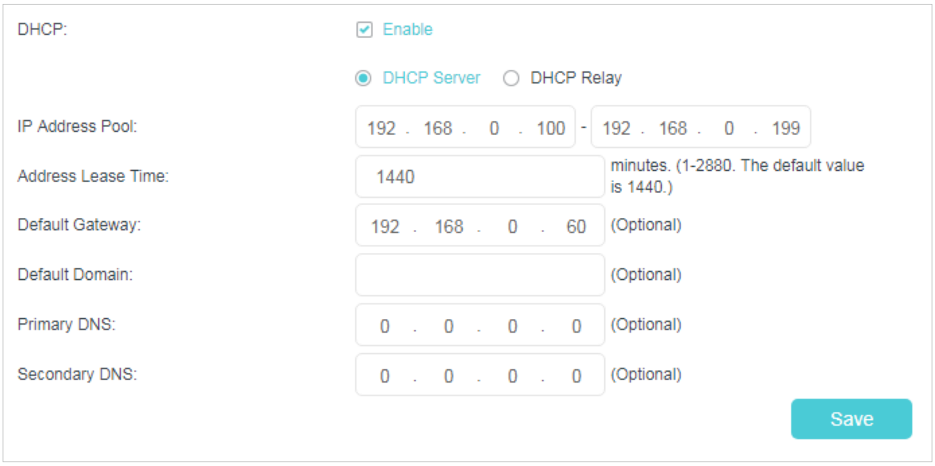
3. Type in a new IP Address appropriate to your needs.
4. Select the Subnet Mask from the drop-down list. The subnet mask together with the IP address identifies the local IP subnet.
5. Keep IGMP Snooping as enabled by default. IGMP snooping is the process of listening to IGMP (Internet Group Management Protocol) network traffic. The function prevents hosts on a local network from receiving traffic for a multicast group they have not explicitly joined.
6. You can configure the modem router's Second IP and Subnet Mask for LAN interface through which you can also access the web management page.
7. Leave the rest of the default settings as they are.
8. Click Save to make the settings effective.

11. 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 the account you set for the router.
2. Go to Advanced > Network > LAN Settings page and select IPv4.



DHCP:	☑ Enable	
	● DHCP Server ○ DHCP Relay	
IP Address Pool:	192 . 168 . 0 . 100 - 192 . 168 . 0 . 199	
Address Lease Time:	1440	minutes. (1-2880. The default value is 1440.)
Default Gateway:	192 . 168 . 0 . 60	(Optional)
Default Domain:		(Optional)
Primary DNS:	0 . 0 . 0 . 0	(Optional)
Secondary DNS:	0 . 0 . 0 . 0	(Optional)

3. Select DHCP to enable the DHCP function and select DHCP Server.
4. 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.
5. 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 modem router. After the dynamic IP address expires, the user will be automatically assigned a new dynamic IP address. The default is 1440 minutes.
6. Keep the rest of the settings as default and click Save.

Note:

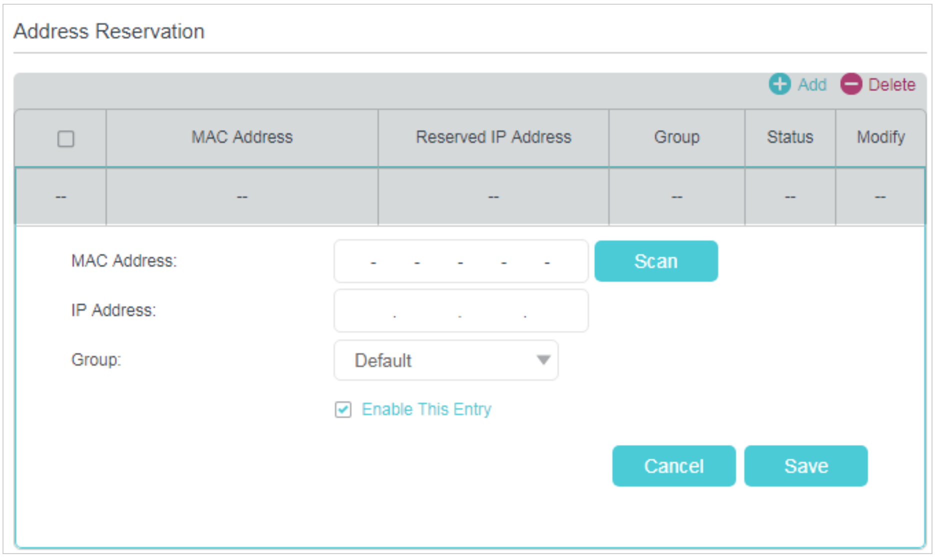
1. The router can be configured to work as a DHCP Relay. A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. If it is enabled, the DHCP requests 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 > LAN Settings page.

11. 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 the account you set for the router.
2. Go to Advanced > Network > LAN Settings page and select IPv4.
3. Scroll down to locate the Address Reservation table and click Add to add an address reservation entry for your device.



Address Reservation

□	MAC Address	Reserved IP Address	Group	Status	Modify
--	--	--	--	--	--

MAC Address:	- - - - -
IP Address:	. . .
Group:	Default

☑ Enable This Entry

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

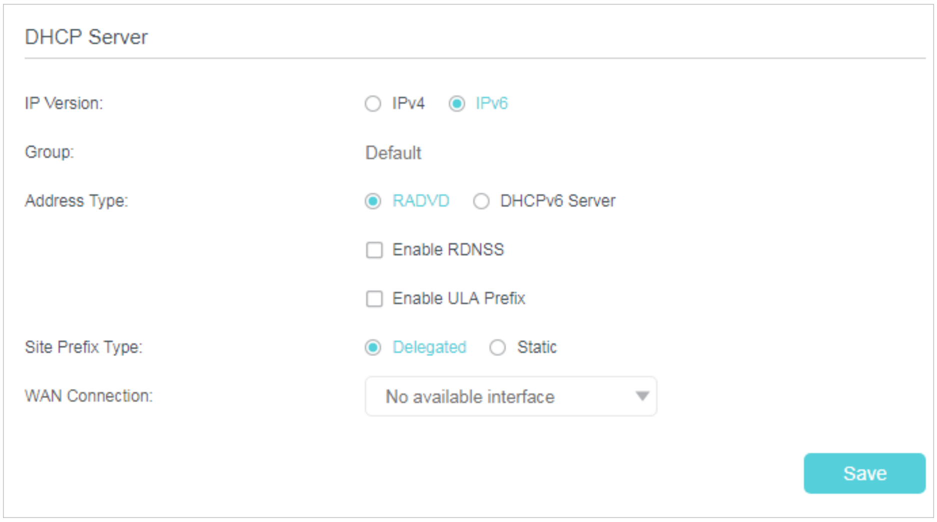
11. 2. IPv6 LAN Settings

Based on the IPv6 protocol, the router provides two ways to assign IPv6 LAN addresses:

- Configure the RADVD (Router Advertisement Daemon) address type
- Configure the DHCPv6 Server address type

11. 2. 1. Configure the RADVD Address Type

1. Visit http://tplinkwifi.net, and log in with the account you set for the router.
2. Go to Advanced > Network > LAN Settings.
3. Select IPv6 to configure IPv6 LAN parameters.



DHCP Server

IP Version: ○ IPv4 ● IPv6

Group: Default

Address Type: ● RADVD ○ DHCPv6 Server

□ Enable RDNSS

□ Enable ULA Prefix

Site Prefix Type: ● Delegated ○ Static

WAN Connection: No available interface

1) Select the RADVD address type to make the router assign IPv6 address prefixes to hosts.

Note:

Do not select the Enable RDNSS and Enable ULA Prefix check boxes unless required by your ISP. Otherwise you may not be able to access the IPv6 network. For more information about RDNSS and ULA Prefix, contact our technical support.

2) Keep Site Prefix Type as the default value Delegated. If your ISP has provided a specific IPv6 site prefix, select Static and enter the prefix.

3) Keep WAN Connection as the default value.

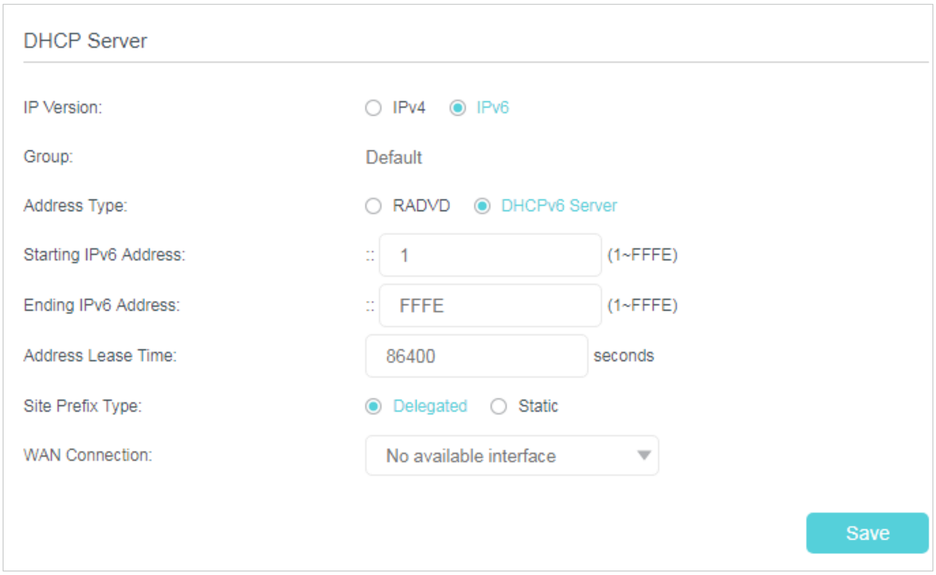
4. Click Save to make the settings effective.

11. 2. 2. Configure the DHCPv6 Server Address Type

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

2. Go to Advanced > Network > LAN Settings.

3. Select IPv6 to configure IPv6 LAN parameters.



DHCP Server

IP Version: ○ IPv4 ● IPv6

Group: Default

Address Type: ○ RADVD ● DHCPv6 Server

Starting IPv6 Address: :: 1 (1~FFFE)

Ending IPv6 Address: :: FFFE (1~FFFE)

Address Lease Time: 86400 seconds

Site Prefix Type: ● Delegated ○ Static

WAN Connection: No available interface

1) Select the DHCPv6 Server address type to make the router assign IPv6 addresses to hosts.

2) Specify the Start/End IPv6 Address for the IPv6 suffixes. The router will generate IPv6 addresses within the specified range.

3) Keep Leased Time as the default value.

4) Keep Site Prefix Type as the default value Delegated. If your ISP has provided a specific IPv6 site prefix, select Static and enter the prefix.

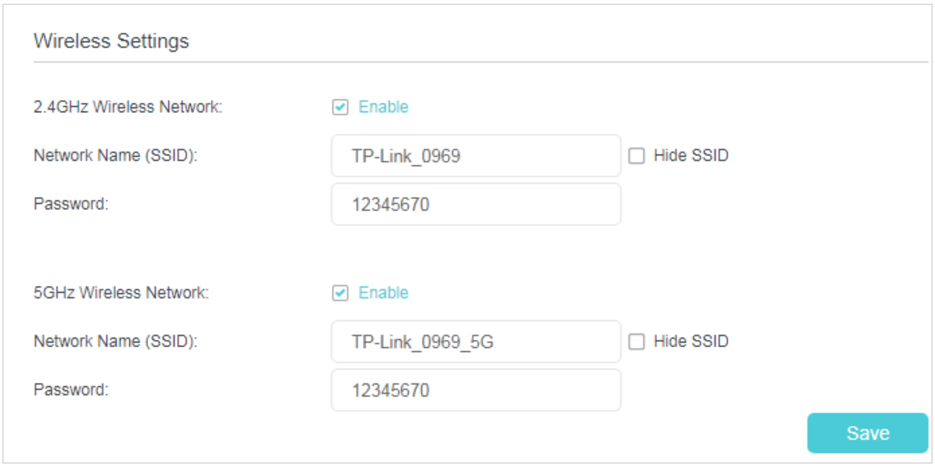
5) Keep WAN Connection as the default value.

4. Click Save to make the settings effective.

11. 3. 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.

Visit http://tplinkwifi.net, and log in with the account you set for the router. Go to Basic > Wireless page.



Wireless Settings

2.4GHz Wireless Network: ☑ Enable

Network Name (SSID): TP-Link_0969 □ Hide SSID

Password: 12345670

5GHz Wireless Network: ☑ Enable

Network Name (SSID): TP-Link_0969_5G □ Hide SSID

Password: 12345670

➢ **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 modem 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 modem router.
- 802.11ac/n mixed (5GHz): Select if you are using both 802.11ac and 802.11n wireless clients.

- 802.11a/n/ac mixed (5GHz): Select if you are using a mix of 802.11a, 802.11n and 802.11ac wireless clients. It is strongly recommended that you select 11a/n/ac mixed.

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.

➢ **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, No Security, 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.

11. 3. 1. 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

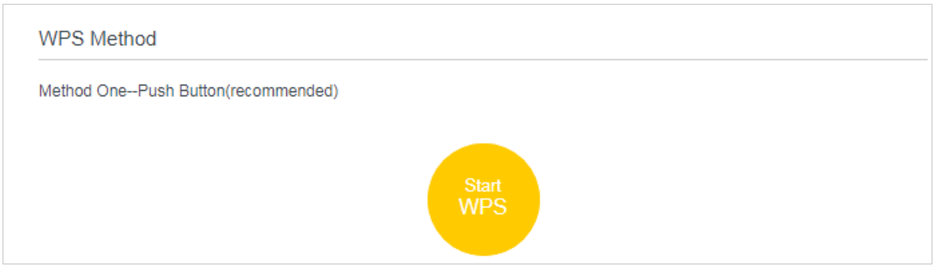
Use this method if your client device has a WPS button.

1. Press the WPS button of the modem router for 1 second.
2. Press the WPS button of the client device directly.
3. The WPS LED flashes for about 2 minutes during the WPS process.
4. When the WPS LED is on, the client device has successfully connected to the modem router.

Method 2 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 the account you set for the router.
2. Go to Advanced > Wireless > WPS page.



WPS Method

Method One--Push Button(recommended)

3. Click Start WPS on the page.

4. Press the WPS button of the client device directly.

5. The WPS LED of the router flashes for about 2 minutes during the WPS process.

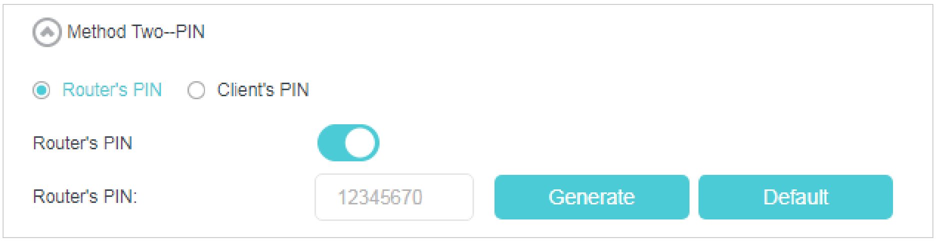
6. When the WPS LED is on, the client device has successfully connected to the router.

Method 3 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 the account you set for the router.

2. Go to Advanced > Wireless > WPS page. Click Method Two--PIN.



Method Two--PIN

● Router's PIN ○ Client's PIN

Router's PIN: on

Router's PIN: 12345670

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. The WPS LED flashes for about two minutes during the WPS process.

6. When the WPS LED is on, the client device has successfully connected to the router.

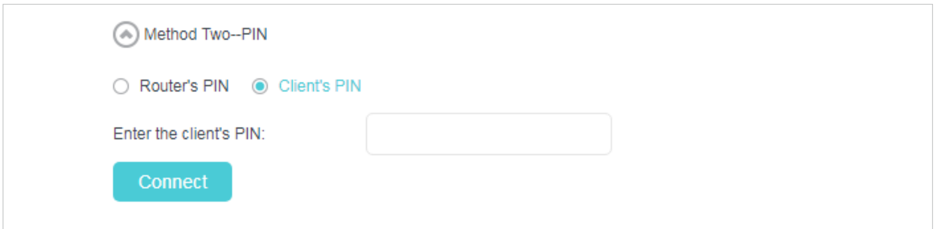
Note:

1. The WPS LED on the router will light on for five minutes if the device has been successfully added to the network.
2. The WPS function cannot be configured if the wireless function of the modem router is disabled. Please make sure the wireless function is enabled before configuring the WPS.

Method 4 Enter the client device’s PIN on the router

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

2. Go to Advanced > Wireless > WPS page. Click Method Two--PIN.



Method Two--PIN

○ Router's PIN ● Client's PIN

Enter the client's PIN:

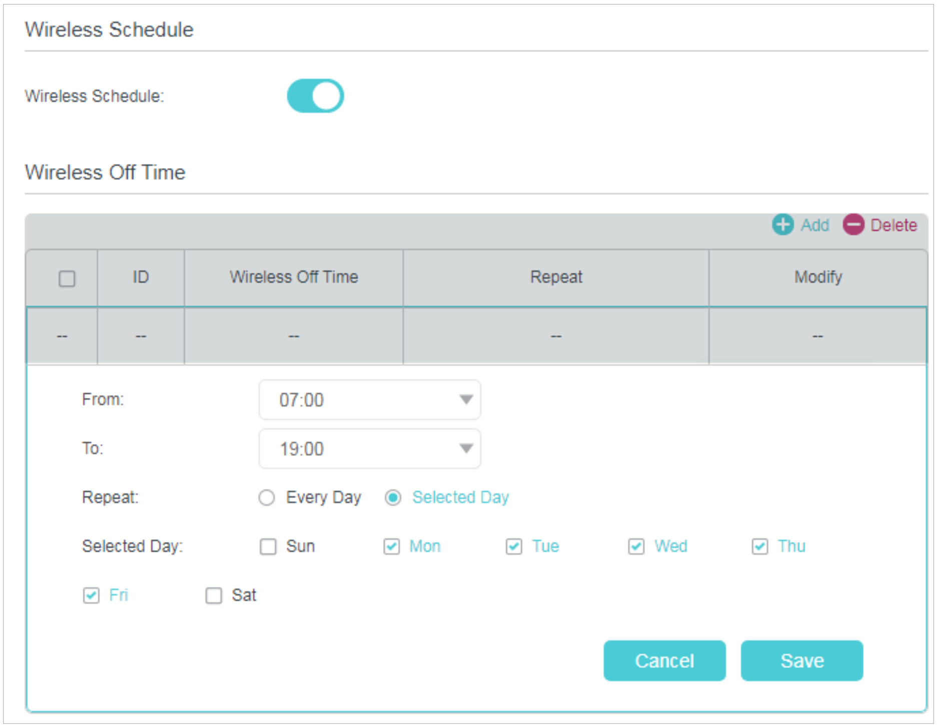
Connect

3. Select Client's PIN.
4. Enter the client device's PIN in the field. Then click the Connect button.
5. Connect successfully will appear on the above screen, which means the client device has successfully connected to the router.

11. 3. 2. Schedule Your Wireless Function

You can automatically turn off your wireless network (both 2.4GHz and 5GHz) when you do not need the wireless connection.

1. Visit http://tplinkwifi.net, and log in with the account you set for the router.
2. Go to Advanced > Wireless > Wireless Schedule page.
3. Toggle on the button to enable the Wireless Schedule feature.



Wireless Schedule

Wireless Schedule: (on)

Wireless Off Time

Add Delete

□	ID	Wireless Off Time	Repeat	Modify
--	--	--	--	--

From: 07:00

To: 19:00

Repeat: ○ Every Day ● Selected Day

Selected Day: □ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat

Cancel Save

4. Click Add to set the Wireless Off Time, and click Save to save the settings.
5. Repeat steps 3 and 4 to set another entry.

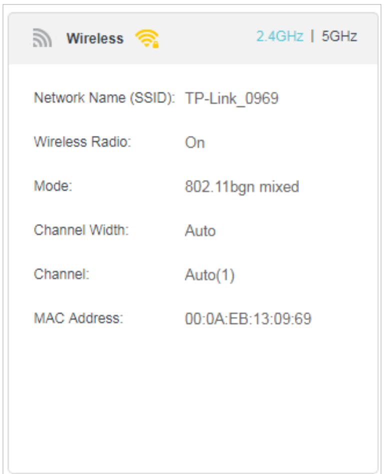
Note:

1. Make sure that the time of the router is correct before using this function. For details, refer to Set System Time.
2. If you just set time for one wireless band, the other wireless band is still always on, so set time for both of the two bands to schedule your whole wireless network.
3. The wireless LED (2.4GHz , 5GHz) will turn off if the corresponding wireless network is disabled.
4. The wireless network will be automatically turned on after the time period you set.

11. 3. 3. View Wireless Information

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

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



Network Name (SSID): TP-Link_0969
Wireless Radio: On
Mode: 802.11bgn mixed
Channel Width: Auto
Channel: Auto(1)
MAC Address: 00:0A:EB:13:09:69

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 the account you set for the router.
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.

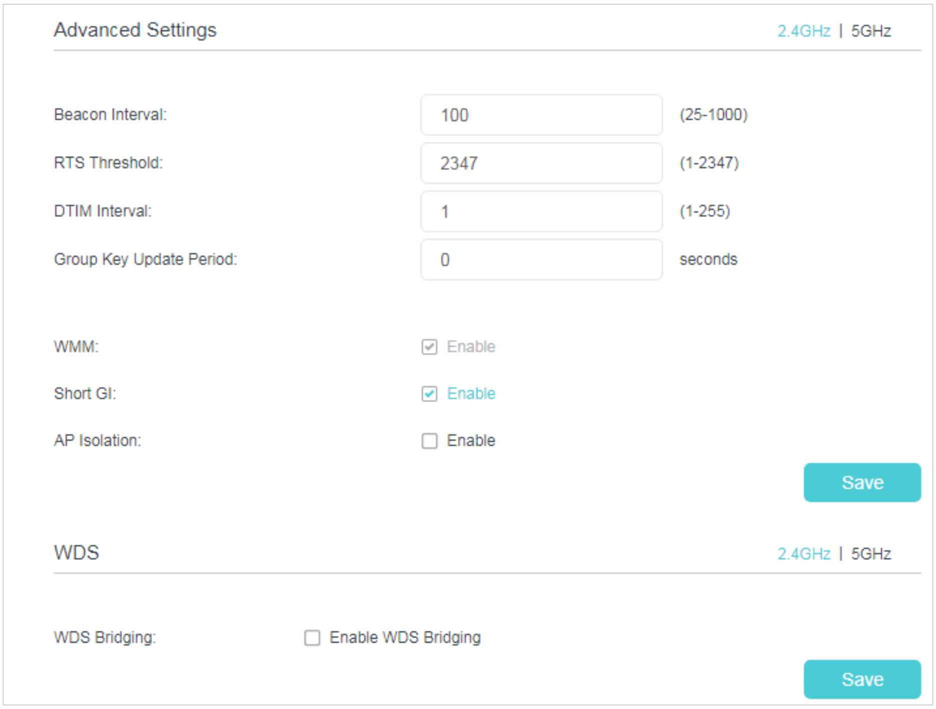
Tips: You can also see the wireless details by clicking the wireless clients icon on Basic> Network Map.

11. 3. 4. Advanced Wireless Settings

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 the account you set for the router.

2. Go to Advanced > Wireless > Advanced Settings page.



Advanced Settings 2.4GHz | 5GHz

Beacon Interval: 100 (25-1000)

RTS Threshold: 2347 (1-2347)

DTIM Interval: 1 (1-255)

Group Key Update Period: 0 seconds

WMM: ☑ Enable

Short GI: ☑ Enable

AP Isolation: □ Enable

WDS 2.4GHz | 5GHz

WDS Bridging: □ Enable WDS Bridging

- Beacon Interval: Enter a value between 25 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 2347 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). 1 indicates the DTIM Interval is the same as Beacon Interval.
- Group Key Update Period: Enter the number of seconds to control the time interval for the encryption key automatic renewal. The default is 0, indicating no key renewal.
- WMM: 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.

- WDS Bridging: Select this check box to enable the WDS (Wireless Distribution System) Bridging feature to allow the router to bridge with another access point (AP) in a wireless local area network (WLAN). Refer to Troubleshooting for detailed instructions.

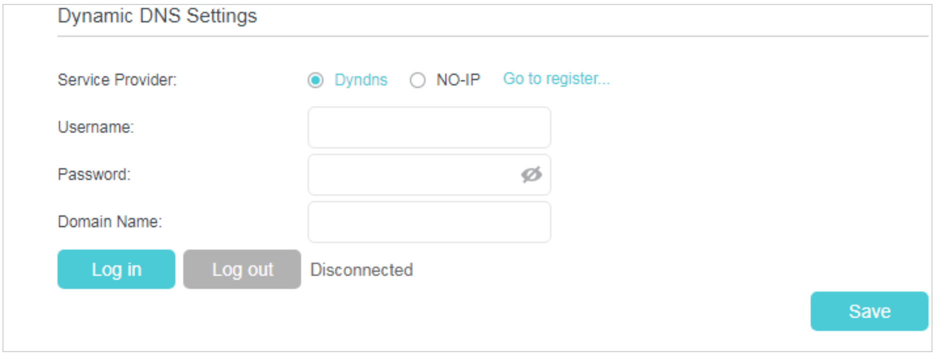
11. 4. Set Up a Dynamic DNS Service Account

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 the account you set for the router.
2. Go to Advanced > Network> Dynamic DNS.
3. Select the DDNS service provider (Dyndns, NO-IP and many other DNS services).
4. 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).



Dynamic DNS Settings

Service Provider: ● Dyndns ○ NO-IP Go to register...

Username:

Password:

Domain Name:

Disconnected

5. Click Log in and Save.

Tips: If you want to use a new DDNS account, please Logout first, then login with the new account.

11. 5. Interface Grouping

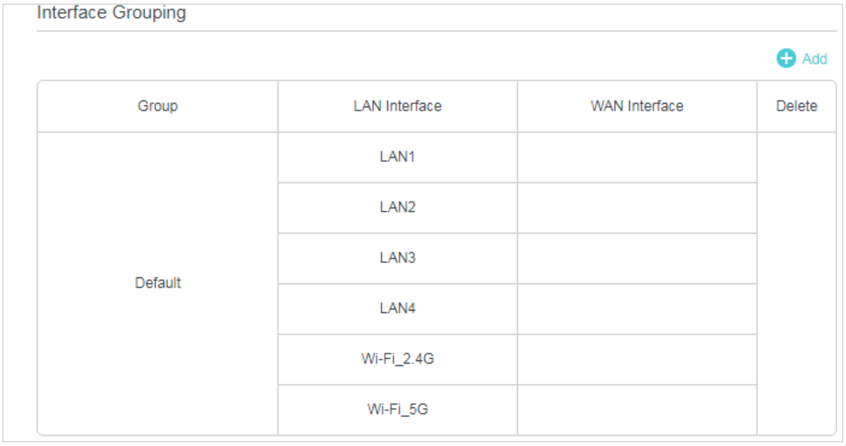
I want to: Divide my devices connected to the modem router into different groups and disallow devices' cross-group communication.

For example, in my house, devices connected to LAN1 and LAN3 are for work, while others for entertainment. I want to isolate working devices from others while keep all devices' access to the internet.

How can I do that?

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

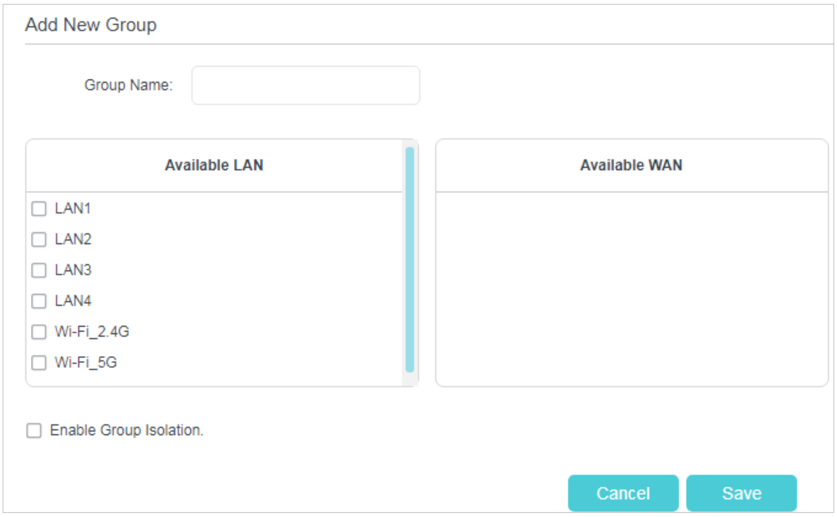
2. Go to Advanced > Network > Interface Grouping to open the configuration page where some interfaces can be grouped together.



Interface Grouping

Group	LAN Interface	WAN Interface	Delete
Default	LAN1		
	LAN2		
	LAN3		
	LAN4		
	Wi-Fi_2.4G		
	Wi-Fi_5G		

3. Click to Add a new group.



Add New Group

Group Name:

Available LAN	Available WAN
□ LAN1 □ LAN2 □ LAN3 □ LAN4 □ Wi-Fi_2.4G □ Wi-Fi_5G	

□ Enable Group Isolation.

4. Name the group.

5. Check the boxes of LAN1 and LAN3 in Available LAN. Here Wi-Fi 2.4G network and Wi-Fi 5G network are viewed as a LAN interface respectively.

6. Click Enable Group Isolation to isolate working devices and disallow other devices from communicating with them.

7. Click Save to save the settings.

Done!

Now your working devices connected to LAN1 and LAN3 are in an isolated group!

Note: VLAN function is enabled by default. You cannot disable it when IPTV is enabled.

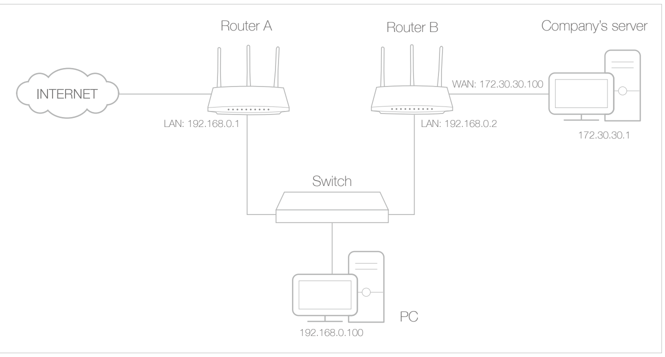
11. 6. Create Static Routes

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:

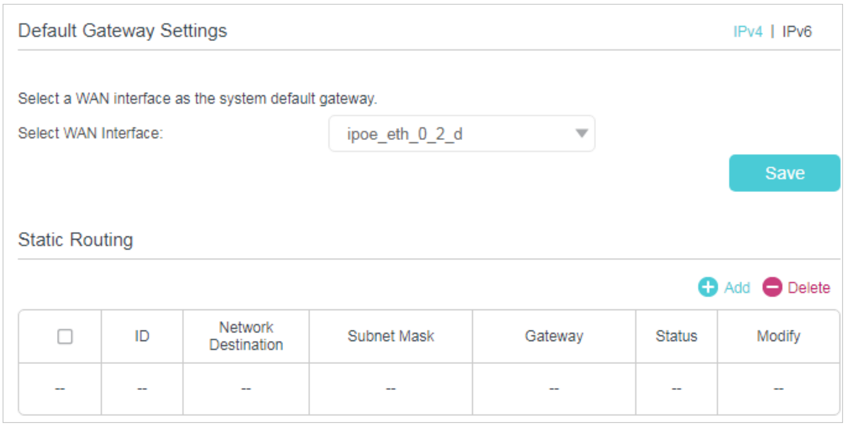
Visit multiple networks and multiple servers at the same time.

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



How can I do that?

1. Make sure the routers use different LAN IP addresses on the same subnet. Disable Router B's DHCP function.
2. Visit http://tplinkwifi.net, and log in with the account you set for the router.
3. Go to Advanced > Network > Static Routing. Select your current WAN Interface and click Save.



Default Gateway Settings

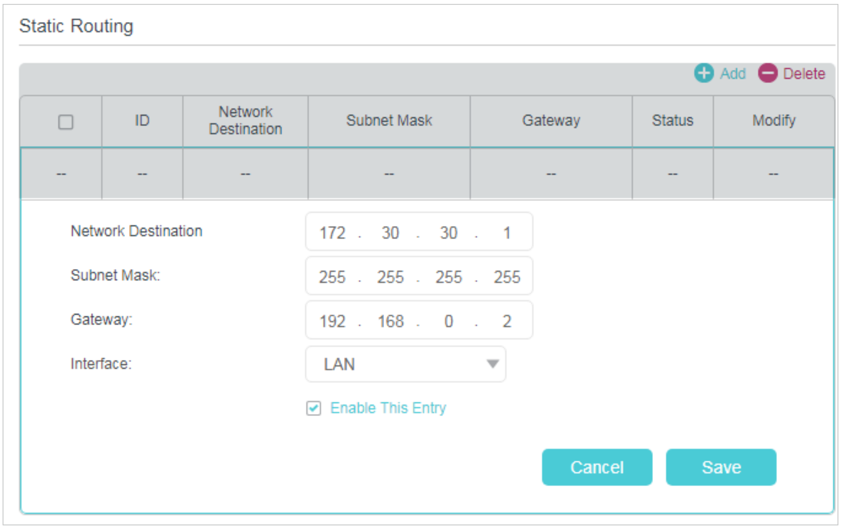
Select a WAN interface as the system default gateway.

Select WAN Interface: ipoe_eth_0_2_d

Static Routing

□	ID	Network Destination	Subnet Mask	Gateway	Status	Modify
--	--	--	--	--	--	--

4. Click Add to add a new static routing entry. Finish the settings according to the following explanations:



Static Routing

□	ID	Network Destination	Subnet Mask	Gateway	Status	Modify
--	--	--	--	--	--	--

Network Destination: 172 . 30 . 30 . 1

Subnet Mask: 255 . 255 . 255 . 255

Gateway: 192 . 168 . 0 . 2

Interface: LAN

☑ Enable This Entry

- Network Destination: The destination IP address that you want to assign to a static route. This IP address cannot be on the same subnet with the WAN IP or LAN IP of Router A. In the example, the IP address of the company network is the destination IP address, so here enter 172.30.30.1.
- Subnet Mask: 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 enter 255.255.255.255.
- 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 Save to save the settings.

Done!

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

11. 7. Set Up the IPv6 Tunnel

The IPv6 Tunnel feature helps you obtain IPv6 resources based on an IPv4 WAN connection or vice versa.

IPv6 Tunnel is a transition mechanism that enables IPv6-only hosts to reach IPv4 services or vice versa and allows isolated IPv6 hosts and networks to reach each other over IPv4-only infrastructure before IPv6 completely supplants IPv4. It is a temporary solution for networks that do not support native dual-stack, where both IPv6 and IPv4 run independently.

The router provides three tunneling mechanisms: 6to4, 6rd and DS-Lite. The way to set up 6rd and DS-Lite tunnel are similar.

11. 7. 1. Use the Public IPv6 Tunnel Service-6to4

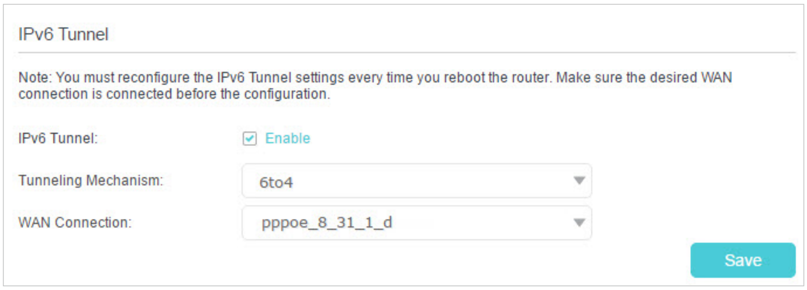
The 6to4 tunnel is a kind of public service. If there is any 6to4 server in your network, you can use this mechanism to access IPv6 service. If your ISP provides you with an IPv4-only connection but you want to visit IPv6 websites, you can try to set up a 6to4 tunnel.

I want to:

Set up the IPv6 tunnel though my ISP doesn't provide me with the tunnel service.

How can I do that?

1. Visit http://tplinkwifi.net, and log in with the account you set for the router.
2. Go to Advanced > Network > IPv6 Tunnel.
3. Tick the check box, select 6to4 as the tunneling mechanism and select a WAN connection from the drop-down list, then click Save.



IPv6 Tunnel

Note: You must reconfigure the IPv6 Tunnel settings every time you reboot the router. Make sure the desired WAN connection is connected before the configuration.

IPv6 Tunnel: ☑ Enable

Tunneling Mechanism: 6to4

WAN Connection: pppoe_8_31_1_d

Note:

If there is no available WAN connection to choose, make sure you have connected to the Internet and the connection type is not Bridge.

Done! Now you can visit the IPv6 websites with the 6to4 tunnel.

Note:

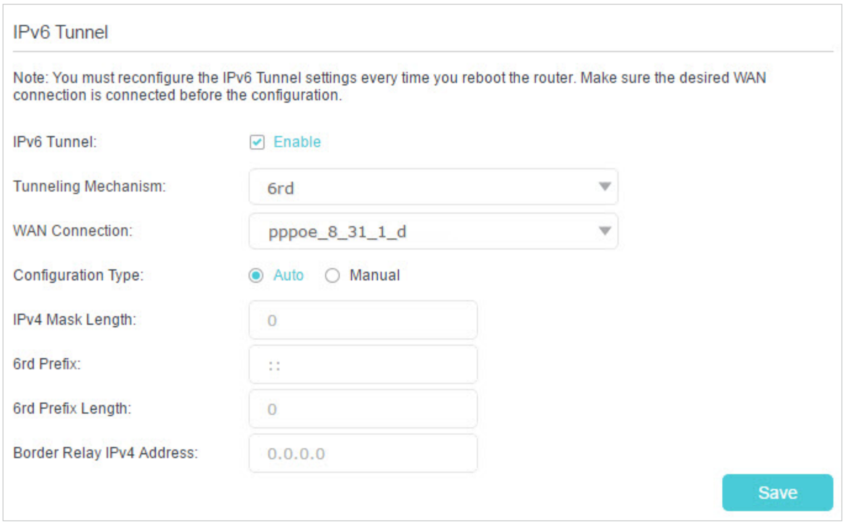
Still not being able to access IPv6 resources means that not any 6to4 public server was found in your network. You can contact your ISP to sign up for IPv6 connection service.

11. 7. 2. Specify the 6rd Tunnel with Parameters Provided by Your ISP

I want to: Specify the 6rd tunnel with the parameters provided by my 6rd tunnel service provider.

How can I do that?

1. Visit http://tplinkwifi.net, and log in with the account you set for the router.
2. Go to Advanced > Network > IPv6 Tunnel.
3. Tick the check box, select 6rd as the tunneling mechanism and select a WAN connection from the drop-down list.
4. According to the parameters provided by your ISP, choose Auto or Manual. More parameters are needed if you choose Manual.
5. Click Save.



IPv6 Tunnel

Note: You must reconfigure the IPv6 Tunnel settings every time you reboot the router. Make sure the desired WAN connection is connected before the configuration.

IPv6 Tunnel: ☑ Enable

Tunneling Mechanism: 6rd

WAN Connection: pppoe_8_31_1_d

Configuration Type: ● Auto ○ Manual

IPv4 Mask Length: 0

6rd Prefix: ::

6rd Prefix Length: 0

Border Relay IPv4 Address: 0.0.0.0

Note:

If there is no available WAN connection to choose, make sure you have connected to the Internet and the connection type is not Bridge.

Done!

Now you can visit the IPv6 websites with the 6rd tunnel.

Tips:

The way to set up DS-Lite tunnel is similar to that of 6rd tunnel. If you are provided with an IPv6-only WAN connection and have signed up for DS-Lite tunnel service, specify the DS-Lite tunnel by referring to the steps above.

Chapter 12

Manage the Router

This chapter will show you the configuration for managing and maintaining your router.

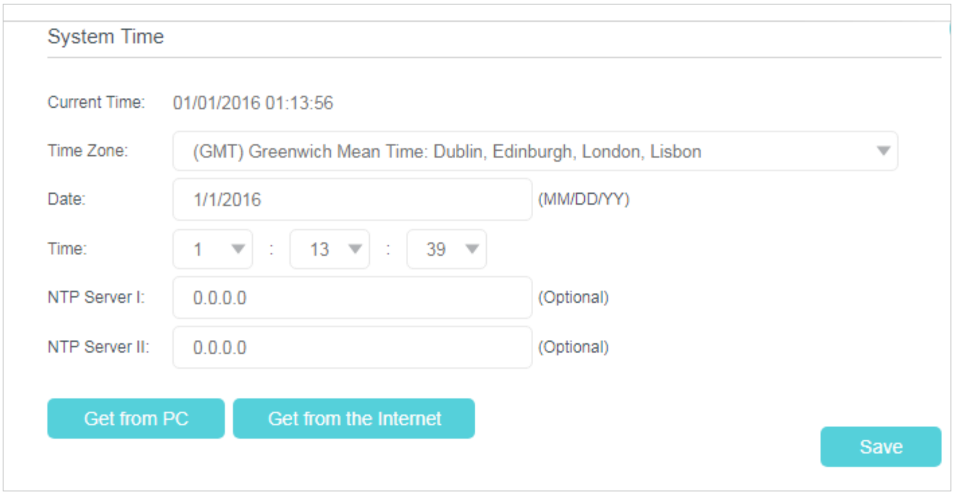
It contains the following sections:

- Use OpenVPN to Access Your Home Network
- Update the Firmware
- Back up and Restore Configuration Settings
- Change the Administrator Account
- Local Management
- Remote Management
- System Log
- CWMP Settings
- SNMP Settings
- Monitor the Internet Traffic Statistics

12. 1. Use OpenVPN to Access Your Home Network

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 choose the way to obtain the system time as needed.

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



System Time

Current Time:	01/01/2016 01:13:56	
Time Zone:	(GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon	
Date:	1/1/2016	(MM/DD/YY)
Time:	1 : 13 : 39	
NTP Server I:	0.0.0.0	(Optional)
NTP Server II:	0.0.0.0	(Optional)

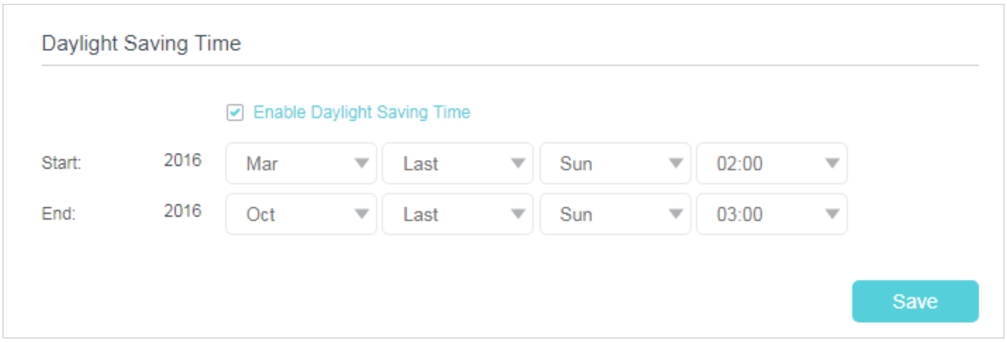
3. Configure the system time using the following methods:

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

   Get from PC: Click this button if you want to use the current managing PC's time.

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

4. Click Save.
5. After setting the system time, you can set Daylight Saving Time according to your needs. Tick the checkbox to enable Daylight Saving Time, set the start and end time and then click Save to make the settings effective.



Daylight Saving Time

☑ Enable Daylight Saving Time

Start:	2016	Mar	Last	Sun	02:00
End:	2016	Oct	Last	Sun	03:00

12. 2. Update the Firmware

TP-Link is dedicated to improving and richening the product features, giving you a better network experience.

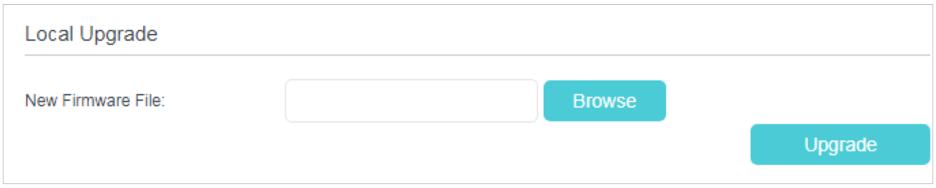
We will inform you through the web management page if there's any update firmware available for your router. Also, the latest firmware will be released at TP-Link official website, you can download it from the Support page of our website www.tp-link.com for free.

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. Back up your router configuration before upgrading the firmware.
4. Do NOT turn off the router during the firmware upgrade.

12. 2. 1. Local Upgrade

1. Download the latest firmware file for the router from our website www.tp-link.com.
2. Visit http://tplinkwifi.net, and log in with the account you set for the router.
3. Go to Advanced > System Tools > Firmware Upgrade.
4. Focus on the Device Information section. Make sure the downloaded firmware file matches with the Hardware Version.
5. Focus on the Local Upgrade section. Click Browse to locate the downloaded new firmware file, and click Upgrade.



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

12. 3. Back up and Restore Configuration Settings

The configuration settings are stored as a configuration file in the router. You can back up the configuration file to your computer for future use and restore the router to a previous settings from the backup file when needed. Moreover, if needed you can erase the current settings and reset the modem router to the default factory settings.

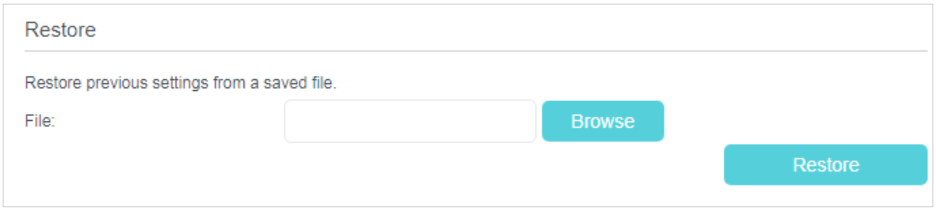
➢ **To back up configuration settings**

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

2. Click Advanced > System Tools > Backup & Restore page.
3. Click Backup to save a copy of the current settings to your local computer. A conf.bin file will be stored to your computer.

➢ **To restore configuration settings**

1. Visit http://tplinkwifi.net, and log in with the account you set for the router.
2. Click Advanced > System Tools > Backup & Restore page.



Restore

Restore previous settings from a saved file.

File:

3. Click Browse to locate the previous backup configuration file, and click Restore.
4. Wait for the restoring and then the router will automatically reboot.

➢ **To reset the router to factory default settings**

1. Visit http://tplinkwifi.net, and log in with the account you set for the router.
2. Click Advanced > System Tools > Backup & Restore page.
3. Click Restore to restore all configuration settings to default values, except your login. Click Factory Restore to reset the router.
4. Wait for the resetting and then the router will automatically reboot.

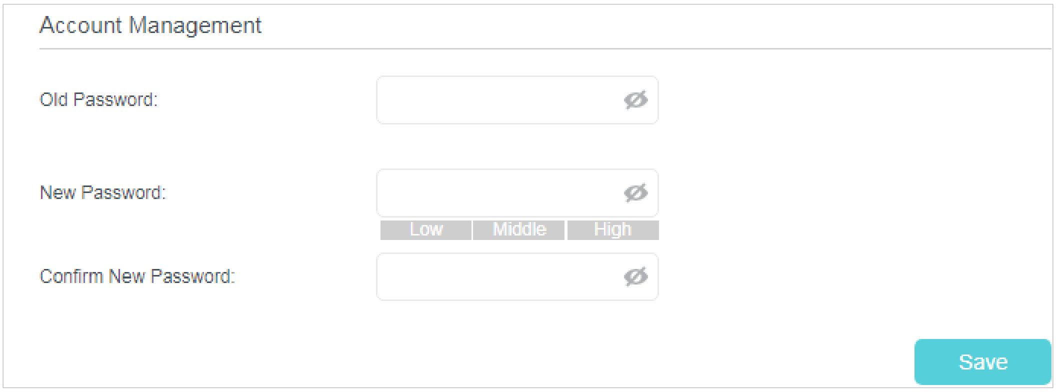
Note:

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

12. 4. Change the Administrator Account

Admin account is used to log in to the router's web management page. You are required to set the admin account at first login. You can also change it on the web page.

1. Visit http://tplinkwifi.net, and log in with the account you set for the router.
2. Go to Advanced > System Tools> Administration page. Locate the Account Management section.



Account Management

Old Password:

New Password:

Confirm New Password:

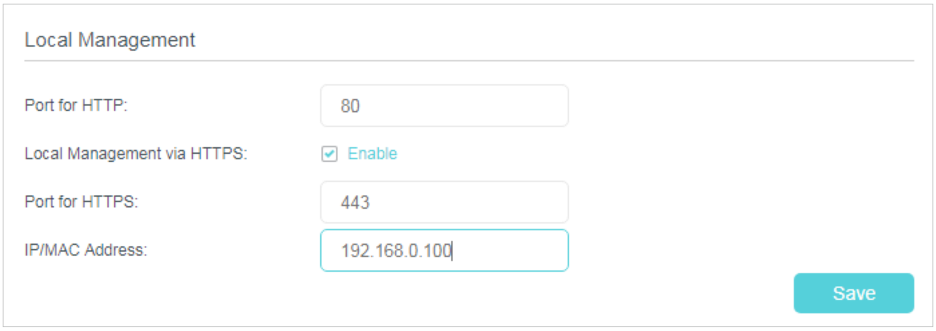
3. Enter the old password. Enter the new password and enter again to confirm.
4. Click Save to make the settings effective.

12. 5. Local Management

You can control the local devices' authority to manage the router via Local Management feature. By default all local connected devices are allowed to manage therouter. You can also allow only one device to manage the router and enable local management over a more secure way, HTTPS.

➢ **To allow only the specific device to manage the router via the local management over HTTPS**

1. Visit http://tplinkwifi.net, and log in with the account you set for the router.
2. Go to Advanced > System Tools > Administration page. Locate the Local Management section.
3. Keep the Port as the default setting. Enable Management over HTTPS and keep the Port for HTTPS as the default setting. Enter the IP address or MAC address of the local device to manage the router.



Local Management

Port for HTTP: 80

Local Management via HTTPS: ☑ Enable

Port for HTTPS: 443

IP/MAC Address: 192.168.0.100

4. Click Save.

Now, you can manage the router over both HTTP (http://tplinkwifi.net) and HTTPS (https://tplinkwifi.net).

Note:

If you want that all local devices can manage the router, just leave the IP/MAC Address field blank.

12. 6. Remote Management

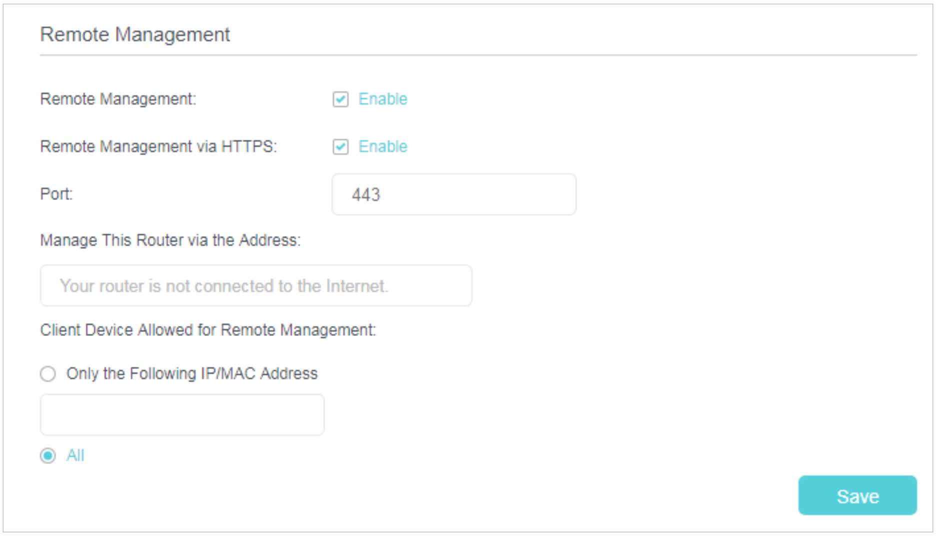
By default, the remote devices are not allowed to manage the router from the internet. You can enable remote management over HTTP and/or HTTPS if needed. HTTPS is a more secure way to access the router.

Note:

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

Follow the steps below to allow remote devices to mange the router over HTTPS.

1. Visit http://tplinkwifi.net, and log in with the account you set for the router.
2. Go to Advanced > System Tools > Administration page. Locate the Remote Management section.



Remote Management

Remote Management: ☑ Enable

Remote Management via HTTPS: ☑ Enable

Port: 443

Manage This Router via the Address:

Your router is not connected to the Internet.

Client Device Allowed for Remote Management:

○ Only the Following IP/MAC Address

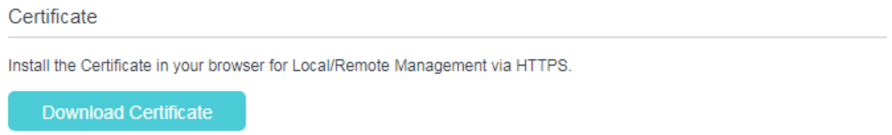
● All

3. Tick the checkbox to enable Remote Management. Enable Remote Management via HTTPS to allow for HTTPS connection. Keep the Port as the default setting.
4. Set the client device allowed for remote management. Select All to allow all remote devices to manage the router. If you just want to allow a specific device to manage the router, select Only the Following IP/MAC Address and enter the IP/MAC address of the remote device.
5. Click Save.

All devices or the specific device on the internet can log in to your router using the address displayed on the Manage This Router via the Address field to manage the router.

Tips:

1. If you were warned about the certificate when visiting the web management page remotely, click Trust (or a similar option) to continue. To avoid this warning, you can download and install the certificate on the router's web management page at Advanced > System Tools > Administration.



Certificate

Install the Certificate in your browser for Local/Remote Management via HTTPS.

Download Certificate

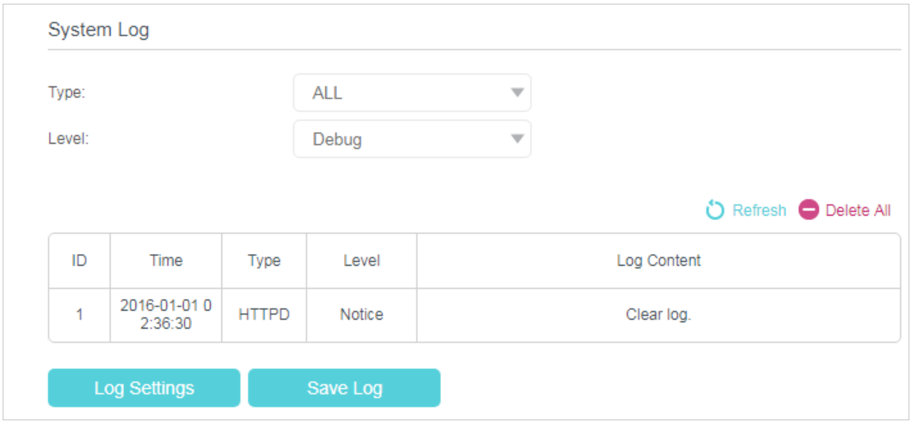
2. The router's WAN IP is usually a dynamic IP. Please refer to Set Up a Dynamic DNS Service Account if you want to log in to the router through a domain name.

12. 7. 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 the account you set for the router.

2. Click Advanced > System Tools > System Log page.



System Log

Type: ALL

Level: Debug

ID	Time	Type	Level	Log Content
1	2016-01-01 0 2:36:30	HTTPD	Notice	Clear log.

➢ **To view the system logs:**

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

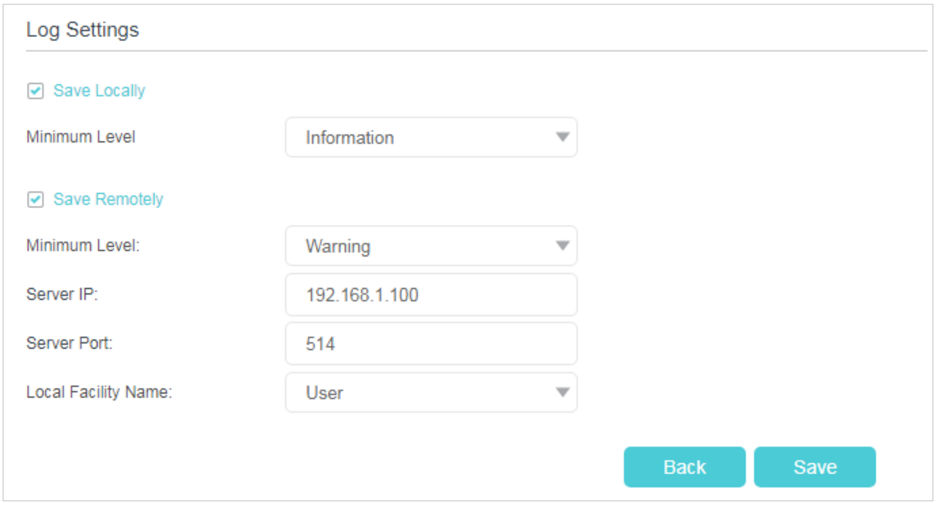
Click Refresh to refresh the log list.

➢ **To save the system logs:**

You can choose to save the system logs to your local computer or a remote server.

Click Save Log to save the logs in a txt file to your computer.

Click Log Settings to set the storage path of logs.



Log Settings

☑ Save Locally

Minimum Level: Information

☑ Save Remotely

Minimum Level: Warning

Server IP: 192.168.1.100

Server Port: 514

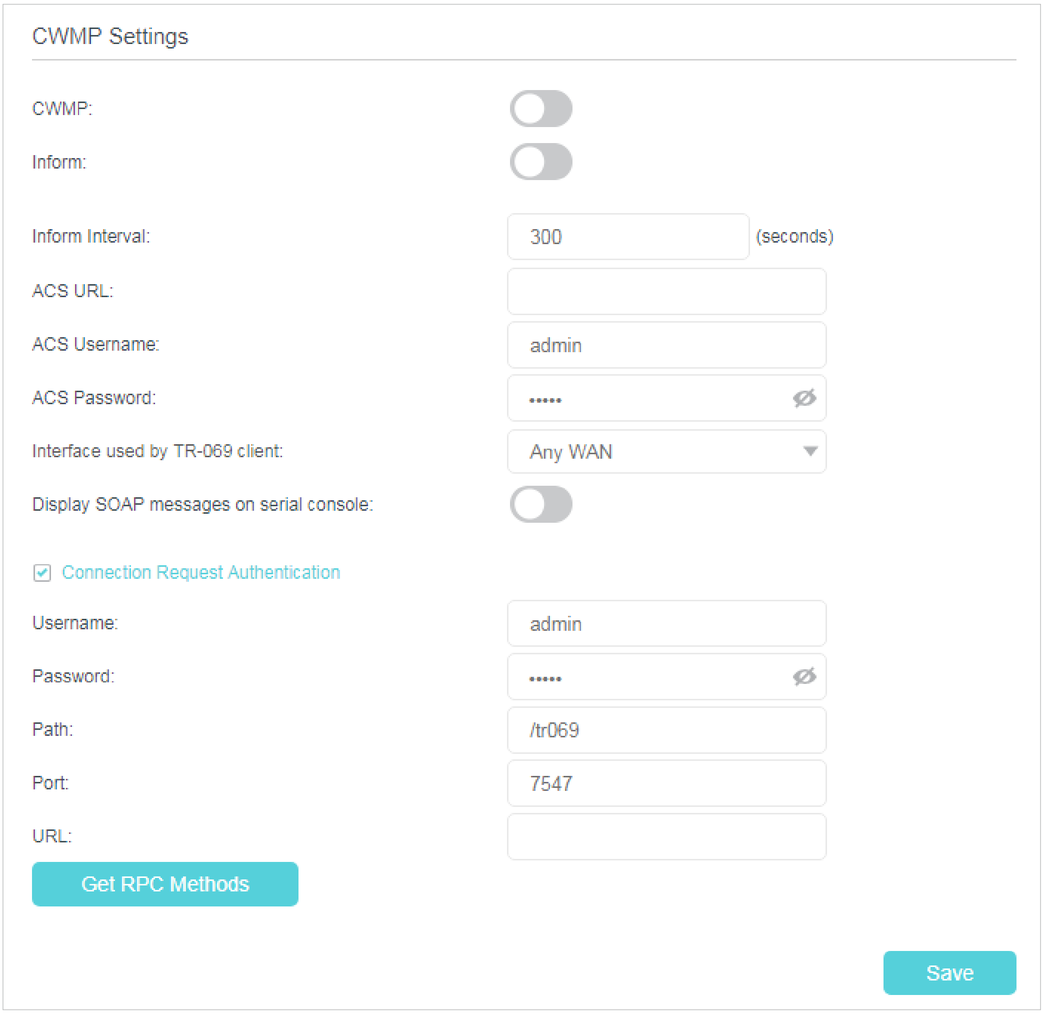
Local Facility Name: User

- Save Locally: Select this option to cache the system log to the router's local memory, select the minimum level of system log to be saved from the drop-down list. The logs will be shown in the table in descending order on the System Log page.
- Save Remotely: Select this option to send the system log to a remote server, select the minimum level of system log to be saved from the drop-down list and enter the information of the remote server. If the remote server has a log viewer client or a sniffer tool implemented, you can view and analyze the system log remotely in real-time.

12. 8. CWMP Settings

The router offers CWMP feature. The function supports TR-069 protocol which collects information, diagnoses the devices and configures the devices automatically via ACS (Auto-Configuration Server).

1. Visit http://tplinkwifi.net, and log in with the account you set for the router.
2. Go to Advanced > System Tools > CWMP Settings page.



CWMP Settings

CWMP: ○

Inform: ○

Inform Interval: 300 (seconds)

ACS URL:

ACS Username: admin

ACS Password: •••••

Interface used by TR-069 client: Any WAN

Display SOAP messages on serial console: ○

☑ Connection Request Authentication

Username: admin

Password: •••••

Path: /tr069

Port: 7547

URL:

- CWMP: Toggle On to enable the CWMP (CPE WAN Management Protocol) feature.
- Inform: Enable this feature to send an Inform message to the ACS (Auto Configuration Server) periodically.
- Inform Interval: Enter the time interval in seconds when the Inform message will be sent to the ACS.
- ACS URL: Enter the web address of the ACS which is provided by your ISP.
- ACS Username/Password: Enter the username/password to log in to the ACS server.
- Interface used by TR-069 client: Select which interface to be used by the TR-069 client.
- Display SOAP messages on serial console: Toggle to enable or disable this feature.
- Connection Request Authentication: Select this checkbox to enable authentication for the connection request.
- Username/Password: Enter the username/password for the ACS server to log in to the router.
- Path: Enter the path for the ACS server to log in to the router.

- Port: Enter the port that connects to the ACS server.
- URL: Enter the URL that connects to the ACS server.
- Get RPC methods: Click to get the methods to support CWMP.

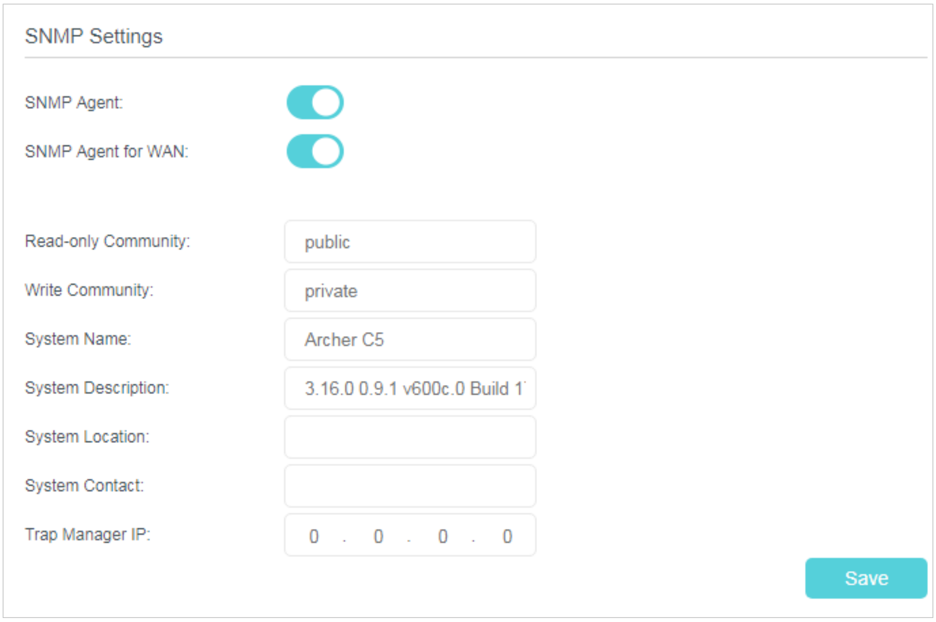
Click Save to make the settings effective.

12. 9. SNMP Settings

SNMP (Simple Network Management Protocol) has been widely applied in the computer networks currently, which is used for ensuring the transmission of the management information between two nodes. In this way, network administrators can easily search and modify the information on any node on the network. Meanwhile, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating.

An SNMP Agent is an application running on the router that performs the operational role of receiving and processing SNMP messages, sending responses to the SNMP manager, and sending traps when an event occurs. So a router contains SNMP "agent" software can be monitored and/or controlled by SNMP Manager using SNMP messages.

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



SNMP Settings

SNMP Agent:

SNMP Agent for WAN:

Read-only Community: public

Write Community: private

System Name: Archer C5

System Description: 3.16.0 0.9.1 v600c.0 Build 1

System Location:

System Contact:

Trap Manager IP: 0 . 0 . 0 . 0

- SNMP Agent: Toggle On to enable the built-in SNMP agent that allows the router to operate as the operational role in receiving and processing of SNMP messages, sending responses to the SNMP manager, and triggering SNMP traps when an event occurs.

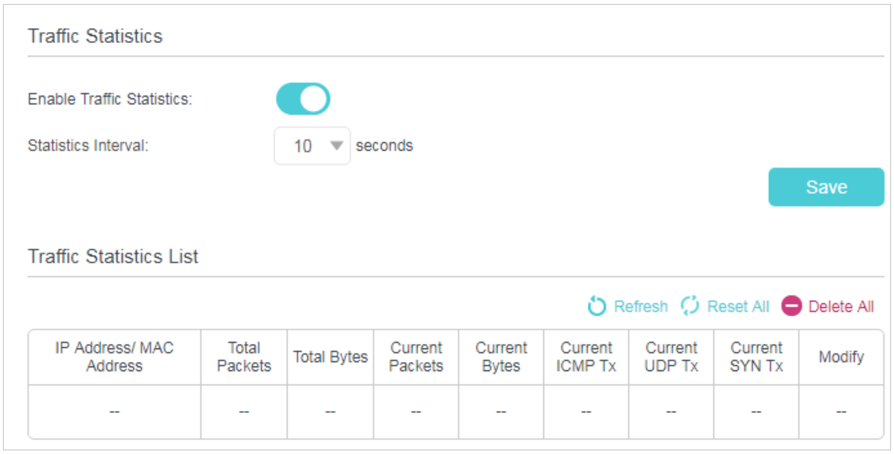
- Read-only Community: Displays the default public community string that protects the router from unauthorized access.
- Write Community: Displays the default write community string that protects the router from unauthorized changes.
- System Name: Displays the administratively-assigned name for this managed device.
- System Description: Displays the textual description of the managed device. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software.
- System Location: Displays the physical location of this device (e.g., telephone closet, 3rd floor).
- System Contact: Displays the textual identification of the contact person for this managed device, together with information on how to contact this person.
- Trap Manager IP: Displays the IP address of the host to receive the traps.

You are suggested to keep the default settings. Click Save to make the settings effective.

12. 10. Monitor the Internet Traffic Statistics

The Traffic Statistics page displays the network traffic of the LAN, WAN and WLAN sent and received packets, allowing you to monitor the volume of internet traffic statistics.

1. Visit http://tplinkwifi.net, and log in with the password you set for the router.
2. Go to Advanced > System Tools > Statistics.
3. Toggle on Traffic Statistics, and then you can monitor the traffic statistics in Traffic Statistics List section.



Traffic Statistics

Enable Traffic Statistics: ●

Statistics Interval: 10 ▼ seconds

Traffic Statistics List

IP Address/ MAC Address	Total Packets	Total Bytes	Current Packets	Current Bytes	Current ICMP Tx	Current UDP Tx	Current SYN Tx	Modify
--	--	--	--	--	--	--	--	--

Click Refresh to update the statistic information on the page.

Click Reset All to reset all statistic values in the list to zero.

Click Delete All to delete all statistic information in the list.

Troubleshooting

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

The default wireless password is printed on the label of the router. If the password has been altered:

1. Connect your computer to the router using an Ethernet cable.
2. Visit http://tplinkwifi.net, and log in the password you set for the router.
3. Go to Basic > Wireless to retrieve or reset your wireless password.

Q2. What should I do if I forget my web management password?

- If you have enabled the Password Recovery feature of the router, click Forgot password on the login page and then follow the instructions to reset it.
- Alternatively, press and hold the Reset button of the router until the Power LED binks to reset it, and then visit http://tplinkwifi.net to create a new login password.

Note:

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

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

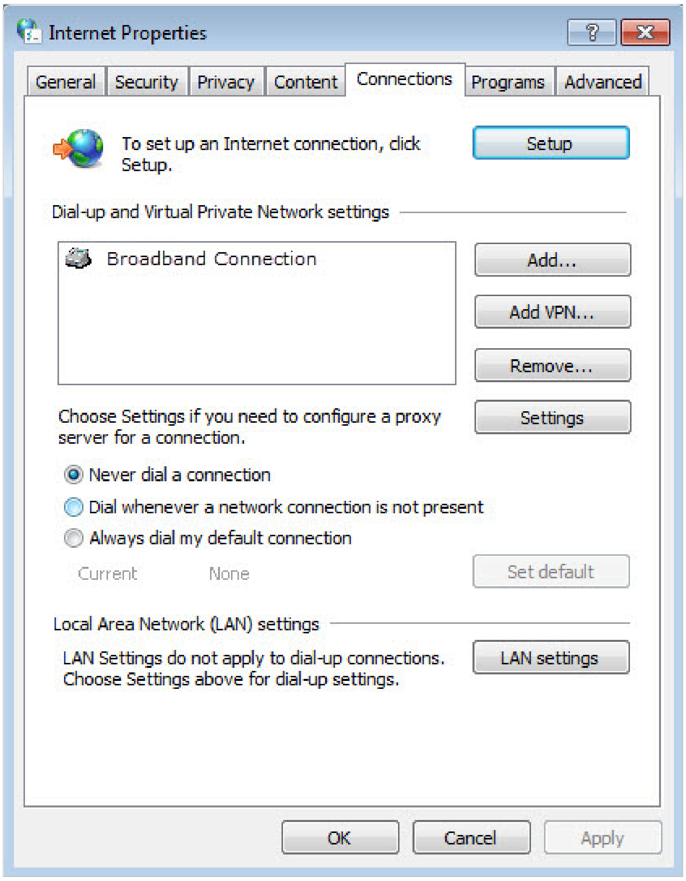
This can happen for a variety of reasons. Please try the methods below to log in again.

- Make sure your computer is connected to the router correctly and the corresponding LED indicator(s) light up.
- Make sure the IP address of your computer is configured as Obtain an IP address automatically and Obtain DNS server address automatically.
- Make sure http://tplinkwifi.net or http://192.168.0.1 is correctly entered.
- Check your computer's settings:

  1) Go to Start > Control Panel > Network and Internet, and click View network status and tasks.

  2) Click Internet Options on the bottom left.

  3) Click Connections and select Never dial a connection.



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Broadband Connection

Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection

○ Dial whenever a network connection is not present

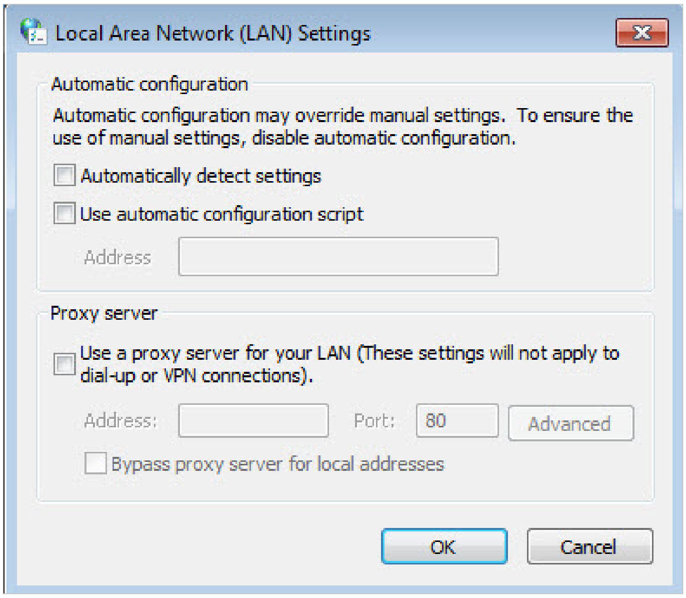
○ Always dial my default connection

Current None

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

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



Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address

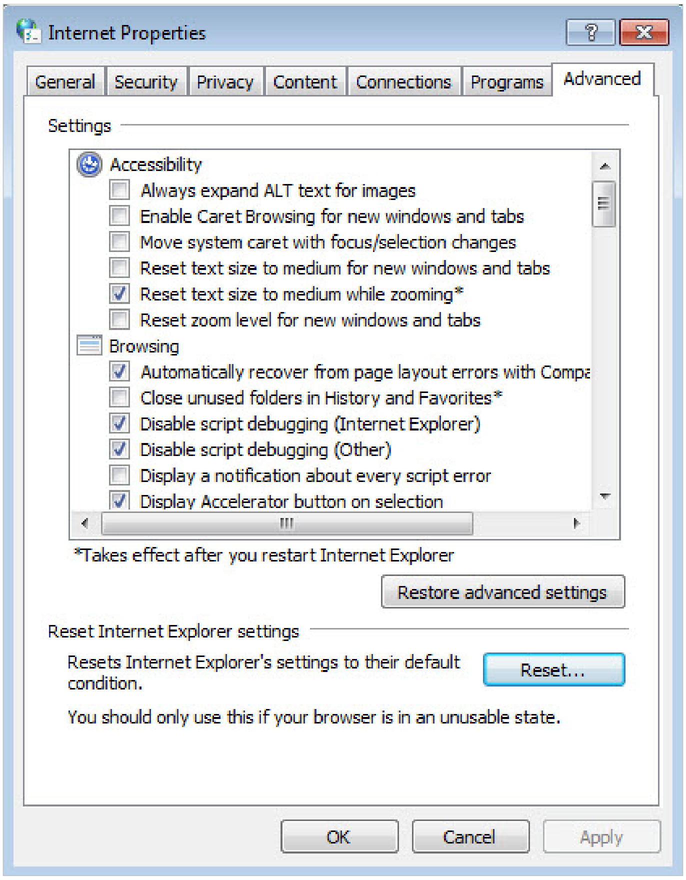
Proxy server

□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port: 80

□ Bypass proxy server for local addresses

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



Accessibility

□ Always expand ALT text for images

□ Enable Caret Browsing for new windows and tabs

□ Move system caret with focus/selection changes

□ Reset text size to medium for new windows and tabs

☑ Reset text size to medium while zooming*

□ Reset zoom level for new windows and tabs

Browsing

☑ Automatically recover from page layout errors with Compa

□ Close unused folders in History and Favorites*

☑ Disable script debugging (Internet Explorer)

☑ Disable script debugging (Other)

□ Display a notification about every script error

☑ Display Accelerator button on selection

*Takes effect after you restart Internet Explorer

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

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

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

Q4. What should I do if I cannot access the internet?

1. Check to see if all the connectors are connected well, including the Ethernet cables/ modem and power adapter.
2. Check to see if you can log in to the web management page of the router. If you can, try the following steps. If you cannot, please set your computer referring to Q3 and then try to see if you can access the Internet. If the problem persists, please go to the next step.
3. Consult your ISP and make sure all the VPI/VCI, Connection Type, account username and password are correct. If there are any mistakes, please correct the settings and try again.
4. Refer to Q5 to clone the MAC address.

5. If you still cannot access the Internet, please restore your router to its factory default settings and reconfigure your router by following the instructions in Use Quick Setup Wizard.

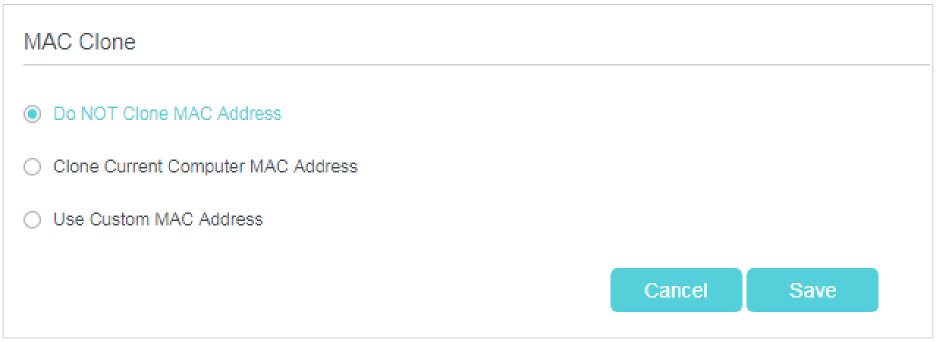
6. Please contact our Technical Support if the problem still exists.

Q5. How to configure MAC Clone?

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

2. Go to Advanced > Network > Internet page. Click the Add icon, and scroll down to get the MAC Clone section.



MAC Clone

● Do NOT Clone MAC Address

○ Clone Current Computer MAC Address

○ Use Custom MAC Address

- If you are using the computer with the authenticated MAC address to access the modem router, please select Clone Current Computer MAC Address.
- If you know the authenticated MAC address, please select Use Custom MAC Address and then enter the address.

3. Click Save to make the settings effective.

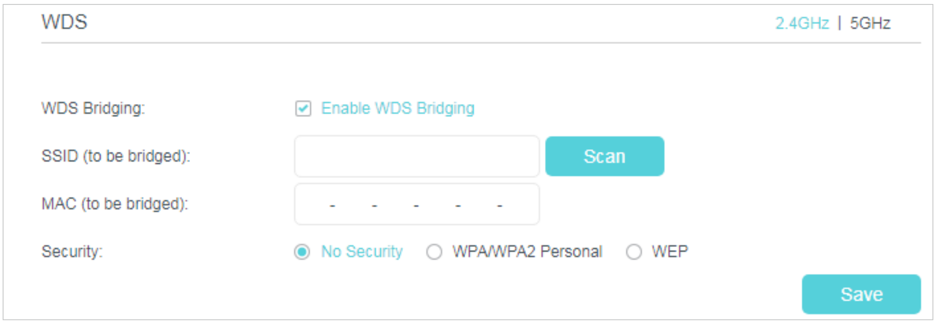
Q6. How to use the WDS Bridging function to extend my wireless network?

My house covers a large area. The wireless network coverage of the router I'm using (the root router) is limited. I want to use an extended router to extend the wireless network of the primary router. Follow the steps to configure the router.

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

2. Configure the LAN IP address of the router in the same subnet as the root router. For example, the IP address of the root router is 192.168.0.1, the IP address of the extended router should be from 192.168.0.2 to 192.168.0.254.).

3. Go to Advanced > Wireless > Advanced Settings page. Locate the WDS section and select the checkbox to enable the WDS Bridging function.



WDS

2.4GHz | 5GHz

WDS Bridging: ☑ Enable WDS Bridging

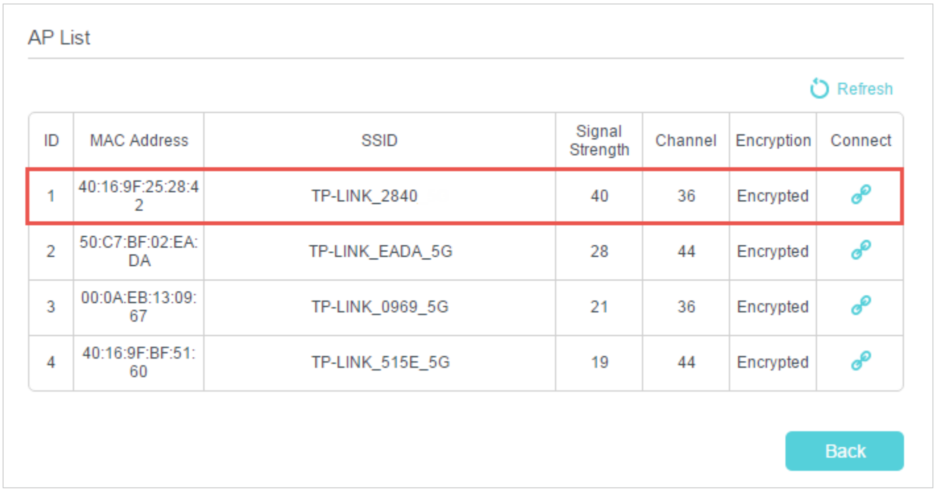
SSID (to be bridged): [ ] Scan

MAC (to be bridged): - - - - -

Security: ● No Security ○ WPA/WPA2 Personal ○ WEP

Save

4. Click Scan to scan all the AP devices and choose the root AP to be bridged.



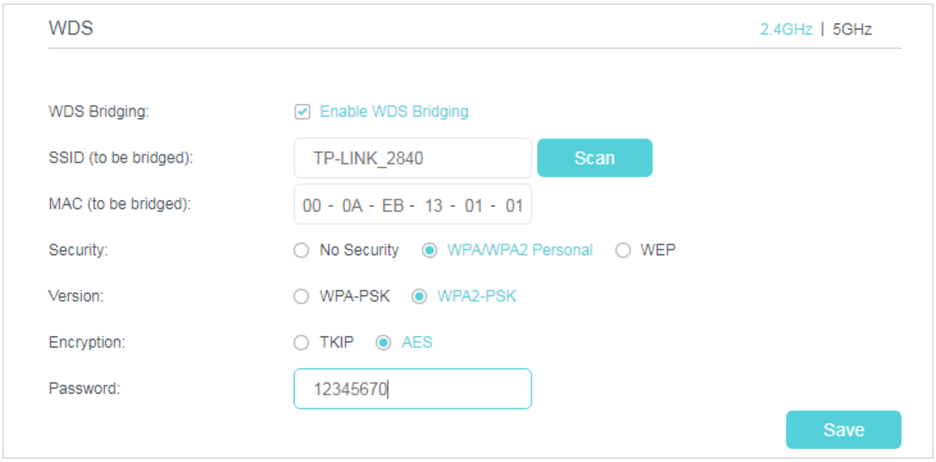
AP List

Refresh

ID	MAC Address	SSID	Signal Strength	Channel	Encryption	Connect
1	40:16:9F:25:28:42	TP-LINK_2840	40	36	Encrypted	🔗
2	50:C7:BF:02:EA:DA	TP-LINK_EADA_5G	28	44	Encrypted	🔗
3	00:0A:EB:13:09:67	TP-LINK_0969_5G	21	36	Encrypted	🔗
4	40:16:9F:BF:51:60	TP-LINK_515E_5G	19	44	Encrypted	🔗

Back

5. Click the connect icon and then the SSID and MAC will be automatically filled in. Configure the Security settings as the AP you choose to be bridged.



WDS

2.4GHz | 5GHz

WDS Bridging: ☑ Enable WDS Bridging

SSID (to be bridged): TP-LINK_2840 Scan

MAC (to be bridged): 00 - 0A - EB - 13 - 01 - 01

Security: ○ No Security ● WPA/WPA2 Personal ○ WEP

Version: ○ WPA-PSK ● WPA2-PSK

Encryption: ○ TKIP ● AES

Password: 12345670

Save

6. Click Save to make the settings effective.

7. Go to Advanced > Network > LAN Settings page to disable DHCP.

Now, the root's wireless network is extended and you can use the router's SSID and password to enjoy the network.

Note: The extended router can have different SSID and password from the root router, you can change yourrouter's SSID and password on Basic > Wireless page.

Q7. 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.

Q8. What should I do if I cannot find my wireless network or I cannot connect the wireless network?

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

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

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

  2) Click Troubleshoot and windows might be able to fix the problem by itself.

  - **On Windows XP**

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

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

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

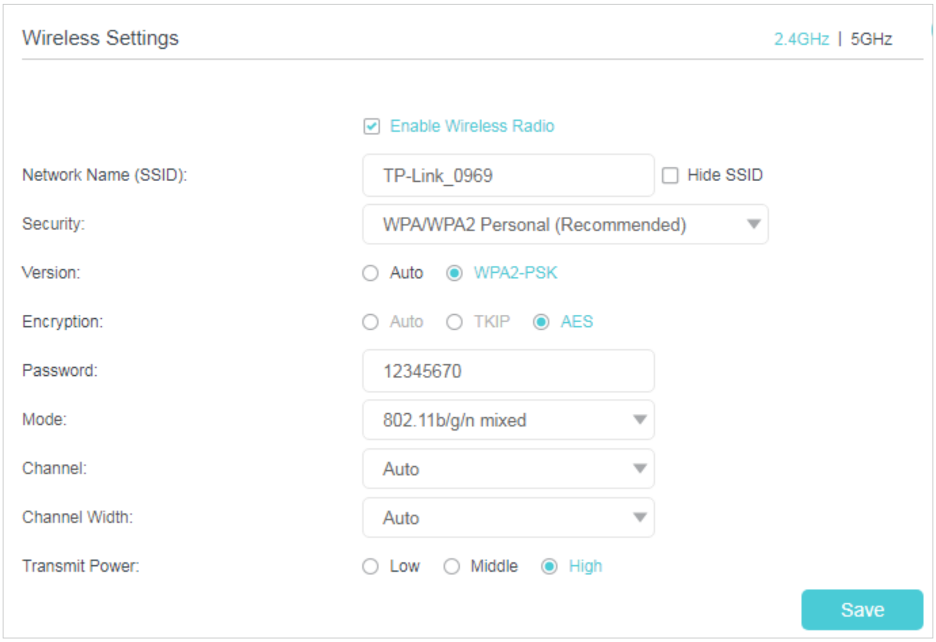
  4) Expand Services and Applications > Services, find and locate Wireless Zero Configuration in the Services list on the right side.

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

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

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

- Check the WLAN LED indicator on your wireless router/modem.
- Make sure your computer/device is still in the range of your router/modem. Move it closer if it is currently too far away.
- Go to Advanced > Wireless > Wireless Settings, and check the wireless settings. Double check your Wireless Network Name and SSID is not hided.



Wireless Settings

2.4GHz | 5GHz

☑ Enable Wireless Radio

Network Name (SSID): TP-Link_0969 □ Hide SSID

Security: WPA/WPA2 Personal (Recommended)

Version: ○ Auto ● WPA2-PSK

Encryption: ○ Auto ○ TKIP ● AES

Password: 12345670

Mode: 802.11b/g/n mixed

Channel: Auto

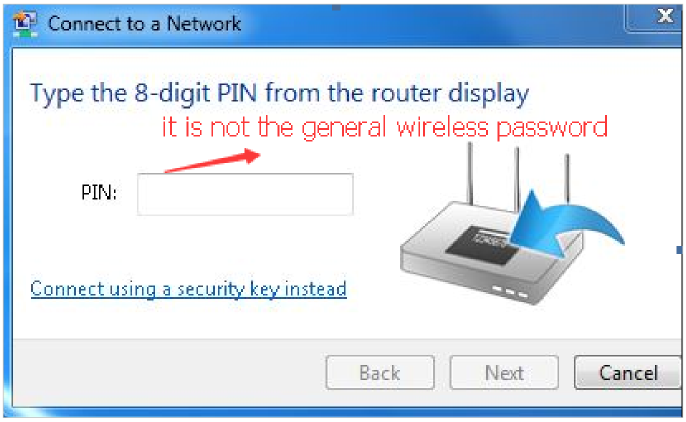
Channel Width: Auto

Transmit Power: ○ Low ○ Middle ● High

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

- **Authenticating problem/password mismatch:**

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



Connect to a Network

Type the 8-digit PIN from the router display

it is not the general wireless password

PIN:

Connect using a security key instead

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

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

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

- **Windows unable to connect to XXXX / Can not join this network / Taking longer than usual to connect to this network:**

- Check the wireless signal strength of your network. If it is weak (1~3 bars), please move the router closer and try again.
- Change the wireless Channel of the router to 1, 6 or 11 to reduce interference from other networks.
- Re-install or update the driver for your wireless adapter of the computer.

COPYRIGHT & TRADEMARKS

FCC 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.

OPERATING FREQUENCY(the maximum transmitted power)

2412MHz—2472MHz(20dBm)

5180MHz—5240MHz(23dBm)

EU declaration of conformity

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

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

RF Exposure Information

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

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

Restricted to indoor use.

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

Safety Information

- Keep the device away from water, fire, humidity or hot environments.
- Do not attempt to disassemble, repair, or modify the device.
- Do not use damaged charger or USB cable to charge the device.
- Do not use any other chargers than those recommended
- Do not use the device where wireless devices are not allowed.
- Adapter shall be installed near the equipment and shall be easily accessible.

Use only power supplies which are provided by manufacturer and in the original packing of this product.

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

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

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

Explanation of the symbols on the product label

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