



User Guide

Portable 3G/4G Wireless N Router
TL-MR3020

Contents

About This Guide	1
Chapter 1. Get to Know About Your Router	2
1. 1. Product Overview.....	3
1. 2. Appearance	3
Chapter 2. Connect the Hardware	5
2. 1. Position Your Router	6
2. 2. Connect Your Router.....	6
2. 2. 1.3G/4G Router Mode	6
2. 2. 2.Wireless Router Mode.....	6
2. 2. 3.WISP Client Router Mode.....	7
2. 2. 4.Access Point Mode.....	8
2. 2. 5.Repeater/Bridge Mode	8
Chapter 3. Set Up Internet Connection Via Quick Setup Wizard.....	9
3. 1. Log In to the Router.....	10
3. 2. Configure the Router.....	10
3. 2. 1.3G/4G Router Mode	10
3. 2. 2.Wireless Router Mode.....	12
3. 2. 3.WISP Client Router Mode.....	14
3. 2. 4.Access Point Mode.....	16
3. 2. 5.Repeater/Bridge Mode	18
Chapter 4. Guest Network.....	21
4. 1. Create a Network for Guests	22
4. 2. Customize Guest Network Options.....	22
Chapter 5. Parental Controls	24
Chapter 6. Bandwidth Control	28
6. 1. Set Upstream and Downstream Bandwidth.....	29
6. 2. Controlling Rules	29
Chapter 7. Network Security	31

7. 1.	Protect the Network from Cyber Attacks	32
7. 2.	Service Filtering	33
7. 3.	Access Control	33
7. 4.	IP & MAC Binding	35

Chapter 8. NAT Forwarding..... 37

8. 1.	Share Local Resources on the Internet by Virtual Servers.....	38
8. 2.	Open Ports Dynamically by Port Triggering.....	39
8. 3.	Make Applications Free from Port Restriction by DMZ	40
8. 4.	Make Xbox Online Games Run Smoothly by UPnP	41

Chapter 9. VPN..... 43

Chapter 10. Customize Your Network Settings..... 46

10. 1.	Change the LAN Settings	47
10. 2.	Specify DHCP Server Settings	47
10. 3.	Set Up a Dynamic DNS Service Account	49
10. 4.	Create Static Routes.....	49
10. 5.	Specify Wireless Settings.....	51
10. 6.	Extend Host Network.....	52
10. 7.	Use WPS for Wireless Connection	53
10. 7. 1.	Use the WPS Wizard for Wi-Fi Connections.....	53
10. 7. 2.	Use the PIN for Wi-Fi connections.....	54
10. 8.	Schedule Your Wireless Function	54

Chapter 11. Manage the Router 56

11. 1.	Set Up System Time	57
11. 2.	Test the Network Connectivity	58
11. 3.	Upgrade the Firmware	58
11. 4.	Backup and Restore Configuration Settings.....	59
11. 5.	Auto Reboot.....	60
11. 6.	Change the Login Password	60
11. 7.	Local Management	61
11. 8.	Remote Management.....	62
11. 9.	System Log.....	62
11. 10.	Monitor the Internet Traffic Statistics.....	64

FAQ.....66

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
<u>Underlined</u>	Underlined words or phrases are hyperlinks. You can click to redirect to a website or a specific section.
Teal	Contents to be emphasized and texts on the web page are in teal, including the menus, items, buttons, 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	<ul style="list-style-type: none"> 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.

More Info

The latest software, management app and utility can be found at [Download Center](http://www.tp-link.com/support) at <http://www.tp-link.com/support>.

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

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

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

Our Technical Support contact information can be found at the [Contact Technical Support](http://www.tp-link.com/support) page at <http://www.tp-link.com/support>.

Chapter 1

Get to Know About Your Router

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

It contains the following sections:

- [Product Overview](#)
- [Appearance](#)

1.1. Product Overview

To meet the wireless needs of almost any situation you might encounter, the TP-Link portable router, with multiple operation modes, is designed for home and travel use. The portable size of the router means that you can put it in your pocket and take it with you wherever you go.

1.2. Appearance



LED Explanation

LED	Status	Indication
⏻ (Power)	On	The router is on.
	Off	The router is off.
🌐 (Internet)	On	The internet is available.
	Off	The internet is unavailable.
📶 (Wireless)	On	The wireless network is enabled.
	Off	The wireless network is disabled.
🔌 (WAN/LAN)	On	The Ethernet port is connected.
	Off	The Ethernet port is not connected.

LED	Status	Indication
WPS/RESET	On	WPS connection has been established.
	Flashing	WPS connection is being established.
	Off	No WPS connection is established.

Port and Button Description

Item	Description
Mode Switch	This switch is used to determine the operation mode of the router.
WAN/LAN Port	LAN: 3G/4G (3G/4G Router), WISP, Access Point, Repeater/Bridge
	WAN: 3G/4G (3G/4G Router Mode With Ewan Backup, Wireless Router Mode, Wireless Router Mode With 3G/4G Backup)
Power Port	This port is used to connect to the power adapter.
WPS/RESET Button	To establish WPS connection, press the WPS button on your device and then press the WPS/RESET button on this router.
	To reset the router, press and hold this button until all the LEDs turn on and then release it.
3G/4G USB Port	This port is used to plug a 3G/4G USB modem into.

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 product away from the devices with strong electromagnetic interference, such as Bluetooth devices, cordless phones and microwaves.

2.2. Connect Your Router

There are five operation modes supported by this router: 3G/4G Router, Wireless Router, WISP Router, Access Point, and Repeater/Bridge. Please determine which operation mode you need and carry out the corresponding steps.

2.2.1. 3G/4G Router Mode

Create a private wireless network instantly and share the 3G/4G network with local devices.

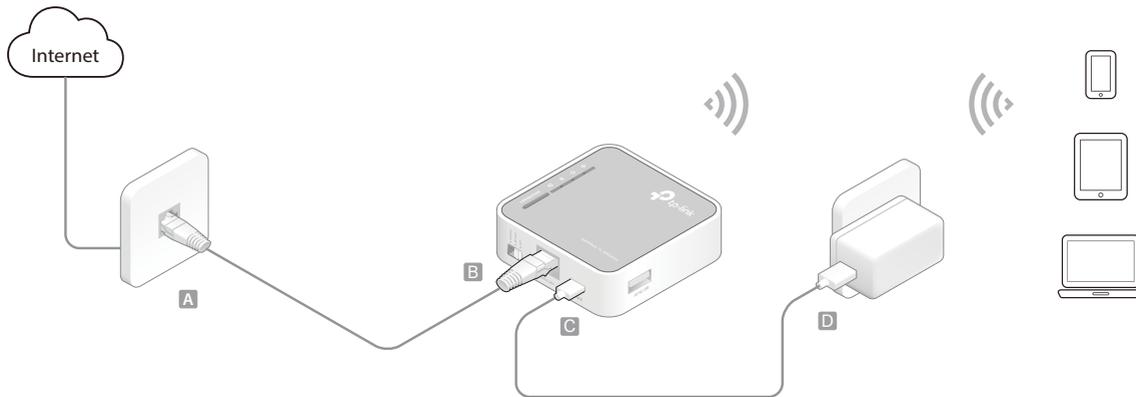
1. Switch the operation mode to **3G/4G** and connect the hardware according to Step A to C.
2. Connect your device to the router wirelessly. The SSID (wireless network name) and password are on the router's label.



2.2.2. Wireless Router Mode

In Wireless Router Mode, the router shares internet access with multiple wireless devices.

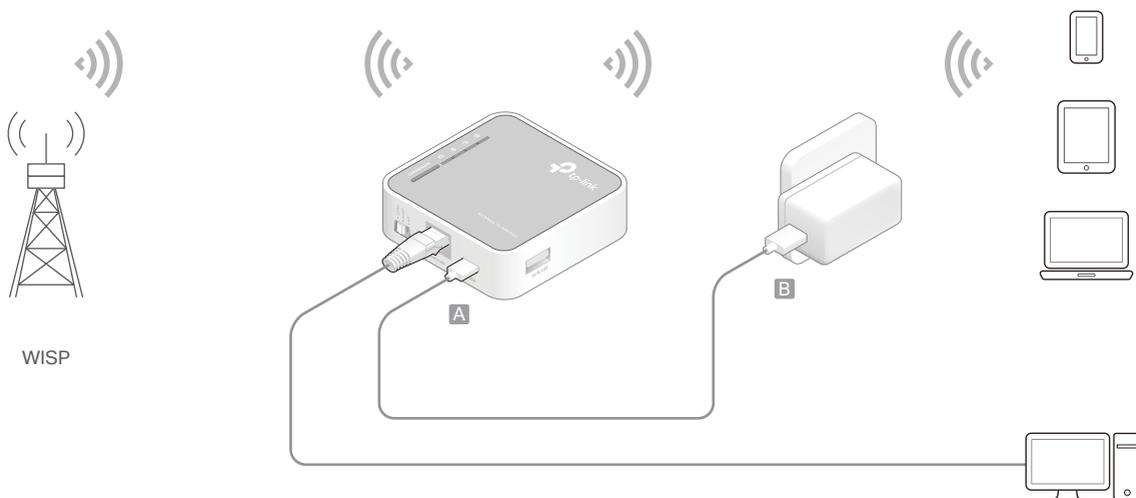
1. Switch the operation mode to **3G/4G** and connect the hardware according to Step A to D.
2. Connect your device to the router wirelessly. The SSID (wireless network name) and password are on the router's label.



2. 2. 3. WISP Client Router Mode

In WISP Client Router mode, the router enables multiple users to share internet connection from WISP.

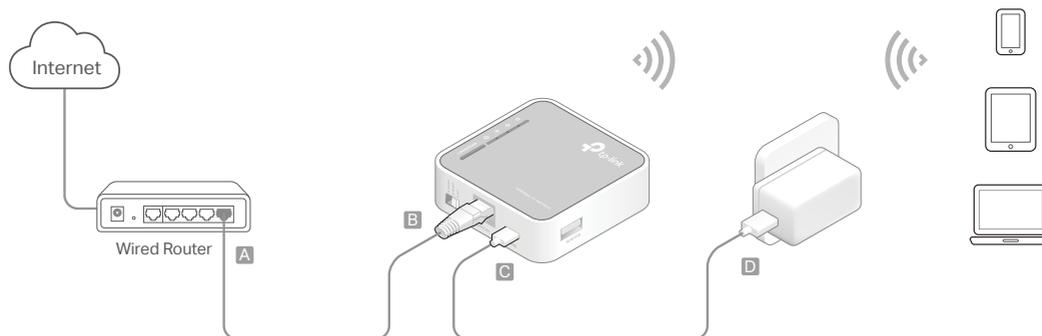
1. Switch the operation mode to **WISP** and connect the hardware according to Step A and B.
2. Connect your device to the router wirelessly or via an Ethernet cable. The SSID (wireless network name) and password are on the router's label.



2.2.4. Access Point Mode

Create a wireless network from an Ethernet connection. This mode is suitable for dorm rooms or homes where there's already a wired router but you need a wireless connection.

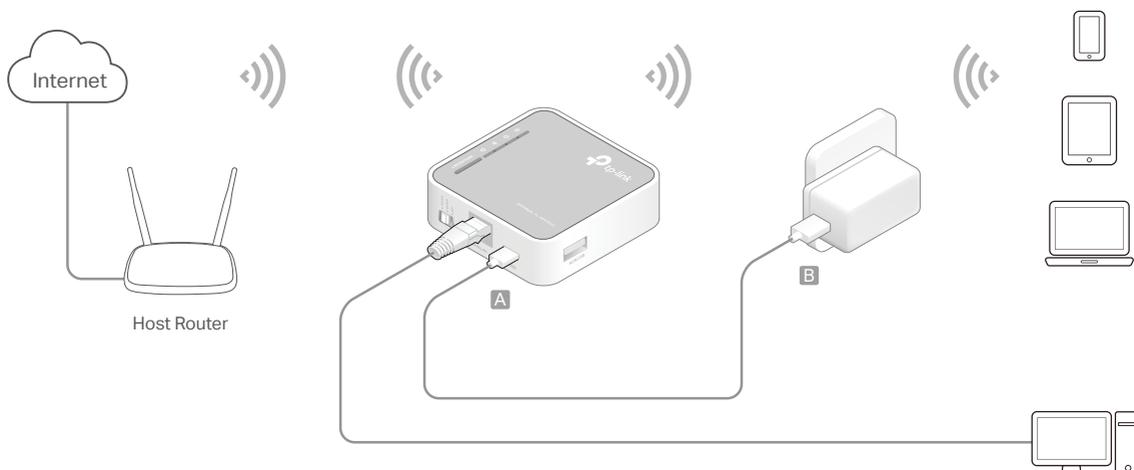
1. Switch the operation mode to **AP** and connect the hardware according to Step A to D.
2. Connect your device to the router wirelessly. The SSID (wireless network name) and password are on the router's label.



2.2.5. Repeater/Bridge Mode

Repeat signal from an existing wireless network. This mode is suitable to extend wireless coverage, reaching devices that were previously too far from your host router to maintain stable wireless connection.

1. Switch the operation mode to **AP** and connect the hardware according to Step A and B.
2. Connect your device to the router wirelessly or via an Ethernet cable. The SSID (wireless network name) and password are on the router's label.



Chapter 3

Set Up Internet Connection Via Quick Setup Wizard

This chapter introduces how to connect your router to the internet via the web-based Quick Setup Wizard.

It contains the following sections:

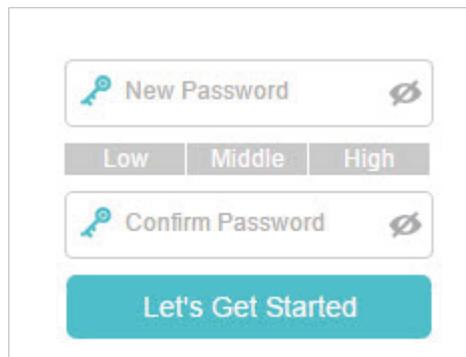
- [Log In to the Router](#)
- [Configure the Router](#)

3.1. Log In to the Router

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

Follow the steps below to log into your router.

1. Set up the TCP/IP Protocol in [Obtain an IP address automatically](#) mode on your computer.
2. Visit <http://tplinkwifi.net>, and create a password for future logins.



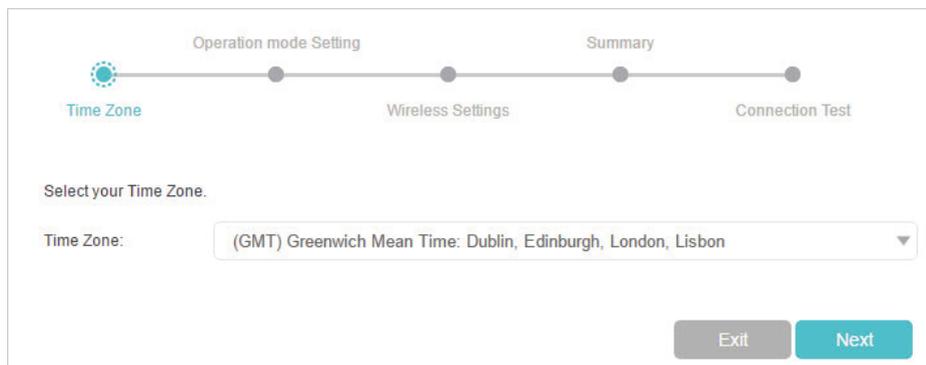
Note: If the login window does not appear, please refer to the [FAQ](#) section.

3.2. Configure the Router

The Quick Setup Wizard will walk you through the process to set up your router.

3.2.1. 3G/4G Router Mode

1. Select your [Time Zone](#) and click [Next](#).



2. Select [3G/4G Router Mode](#) and click [Next](#).

Note: The router can be configured with a primary 3G/4G connection and WAN connection as a backup solution to ensure "always-on" internet connectivity.

The screenshot shows the 'Operation mode Setting' screen in the Quick Setup Wizard. At the top, a progress bar indicates the current step is 'Operation mode Setting', with other steps being 'Time Zone', 'Wireless Settings', 'Summary', and 'Connection Test'. Below the progress bar, there are four radio button options for the operation mode:

- 3G/4G Router Mode
- 3G/4G Router Mode With Ewan Backup
- Wireless Router Mode
- Wireless Router Mode With 3G/4G Backup

At the bottom right, there are two buttons: 'Back' and 'Next'.

3. Select your **Mobile ISP** or manually set them if your ISP is not listed. Then click **Next**.

The screenshot shows the 'Operation mode Setting' screen with the following settings:

- USB 3G/4G Modem: Unplugged
- PIN Status: Unknown
- Mobile ISP: AT&T (selected in a dropdown menu)
- Set Dial Number, APN, Username and Password manually
- Connection Mode: Auto (selected in a dropdown menu)
- Authentication Type: AUTO_AUTH (selected in a dropdown menu)

At the bottom right, there are two buttons: 'Back' and 'Next'.

4. Either customize your **Network Name (SSID)** and **Password** or keep the default ones, and then click **Next**.

The screenshot shows the 'Wireless Settings' screen in the Quick Setup Wizard. At the top, a progress bar indicates the current step is 'Wireless Settings', with other steps being 'Time Zone', 'Operation mode Setting', 'Summary', and 'Connection Test'. Below the progress bar, there is a message: "You can change the wireless network name and password." The settings are:

- 2.4GHz Wireless: Enable Wireless Radio
- Network Name (SSID): TP-Link_8881
- Password: 12345670

At the bottom right, there are two buttons: 'Back' and 'Next'.

5. Check the wireless settings and click **Save**.

Operation mode Setting Summary

Time Zone Wireless Settings Connection Test

Time Zone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon

Operation mode: 3G/4G Router Mode

Mobile ISP: AT&T

Wireless Network (2.4GHz): Enabled

Network Name (SSID): TP-Link_8881

Password: 12345670

Back Save

6. Click **Finish** to complete the configuration. Now connect your devices to the internet!

Operation mode Setting Summary

Time Zone Wireless Settings Connection Test

Test Internet Connection

Back Finish

3. 2. 2. Wireless Router Mode

1. Select your **Time Zone** and click **Next**.

Operation mode Setting Summary

Time Zone Wireless Settings Connection Test

Select your Time Zone.

Time Zone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon

Exit Next

2. Select **Wireless Router Mode** and click **Next**.

Note: The router can be configured with a primary WAN connection and a 3G/4G USB modem as a backup solution to ensure "always-on" internet connectivity.

Operation mode Setting

Time Zone Wireless Settings Summary Connection Test

3G/4G Router Mode

3G/4G Router Mode With Ewan Backup

Wireless Router Mode

Note: In this mode, you won't be able to get access to Router by ethernet port. You can only connect to Router by wireless

Wireless Router Mode With 3G/4G Backup

Back Next

3. Select **Internet Connection Type** and enter corresponding parameters. If you are not sure, click **Auto Detect**. Then click **Next** and enter corresponding parameters.

Operation mode Setting

Time Zone Wireless Settings Summary Connection Test

Auto Detect

Dynamic IP

Static IP

PPPoE

L2TP

PPTP

Note: If you are not sure which Internet Connection Type you have, use Auto Detect or contact your Internet Service Provider (ISP) for assistance.

Back Next

4. Either customize your **Network Name (SSID)** and **Password** or keep the default ones, and then click **Next**.

Operation mode Setting Summary

Time Zone Wireless Settings Connection Test

You can change the wireless network name and password.

2.4GHz Wireless: Enable Wireless Radio

Network Name (SSID): TP-Link_8881

Password: 12345670

Back Next

5. Check the wireless settings and click **Save**.

Operation mode Setting Summary

Time Zone Wireless Settings Connection Test

Time Zone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon

Operation mode: Wireless Router Mode

Wan Connection Type: Dynamic IP

Wireless Network (2.4GHz): Enabled

Network Name (SSID): TP-Link_8881

Password: 12345670

Back Save

3. 2. 3. WISP Client Router Mode

1. Select your **Time Zone** and click **Next**.

Internet Setup Summary

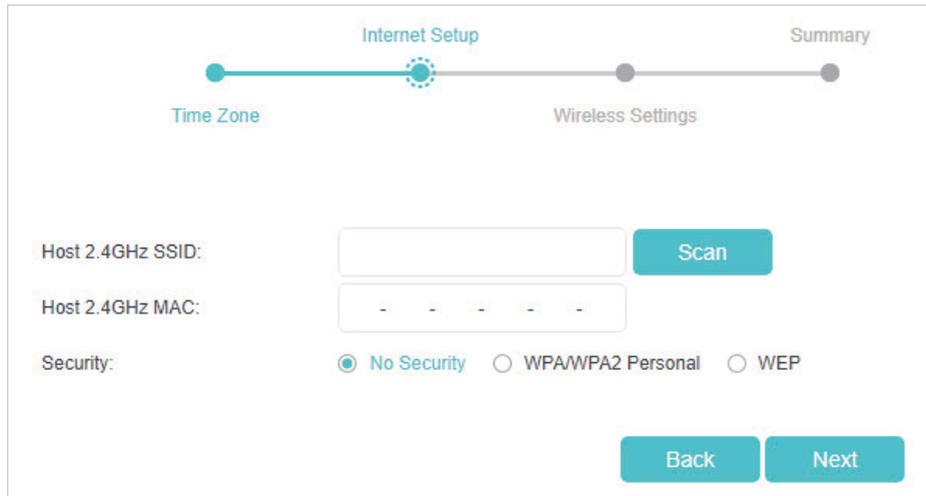
Time Zone Wireless Settings

Select your Time Zone.

Time Zone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon

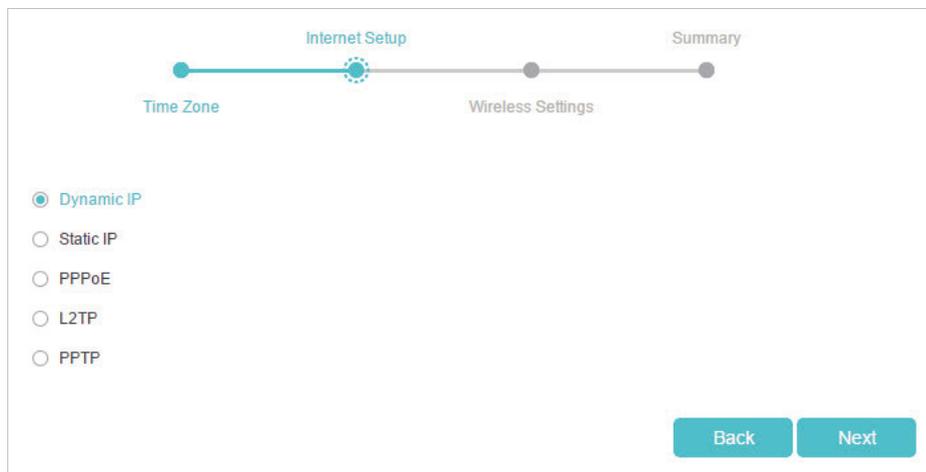
Exit Next

2. Click [Scan](#) to find the corresponding network of your WISP. Enter the [Password](#) for the selected wireless network if it is encrypted. Then click [Next](#).



The screenshot shows the 'Internet Setup' wizard with four steps: Time Zone, Internet Setup, Wireless Settings, and Summary. The 'Internet Setup' step is currently active. Below the progress bar, there are input fields for 'Host 2.4GHz SSID' and 'Host 2.4GHz MAC'. The 'Security' section has three radio button options: 'No Security' (selected), 'WPA/WPA2 Personal', and 'WEP'. There are 'Scan', 'Back', and 'Next' buttons.

3. Select [Internet Connection Type](#). Then click [Next](#) and enter corresponding parameters.



The screenshot shows the 'Internet Setup' wizard with the same four steps. The 'Internet Setup' step is active. Below the progress bar, there are five radio button options for 'Internet Connection Type': 'Dynamic IP' (selected), 'Static IP', 'PPPoE', 'L2TP', and 'PPTP'. There are 'Back' and 'Next' buttons.

4. Either customize your [Network Name \(SSID\)](#) and [Password](#) or keep the default ones, and then click [Next](#).

The screenshot shows a progress bar at the top with four steps: Time Zone, Internet Setup, Wireless Settings, and Summary. The 'Wireless Settings' step is currently active, indicated by a dashed circle around its progress indicator. Below the progress bar, the text reads: "You can change the wireless network name and password." Under the heading "2.4GHz Wireless:", there is a checked checkbox labeled "Enable Wireless Radio". Below this, there are two input fields: "Network Name (SSID)" with the value "TP-Link_8881" and "Password" with the value "12345670". At the bottom right, there are two buttons: "Back" and "Next".

5. Click [Save](#) to complete the configuration.

The screenshot shows the same progress bar as the previous step, but now the 'Summary' step is active, indicated by a solid circle with a checkmark around its progress indicator. The main content area displays a summary of the configuration in a table-like format:

Time Zone:	(GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon
Operation mode:	WISP
Wan Connection Type:	Dynamic IP
Host Network (2.4GHz):	Enabled
Host Network Name (SSID):	Deco test
Security:	PSK2Authentication&AESEncryption
Password:	12345670
Wireless Network (2.4GHz):	Enabled
Network Name (SSID):	TP-Link_8881
Password:	12345670

At the bottom right, there are two buttons: "Back" and "Save".

3.2.4. Access Point Mode

1. Select your [Time Zone](#) and click [Next](#).

The screenshot shows a progress bar at the top with four steps: Time Zone (highlighted with a blue dashed circle), Operation mode Setting, Wireless Settings, and Summary. Below the progress bar, the text "Select your Time Zone." is followed by a dropdown menu labeled "Time Zone:" containing the text "(GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon". At the bottom right, there are two teal buttons: "Exit" and "Next".

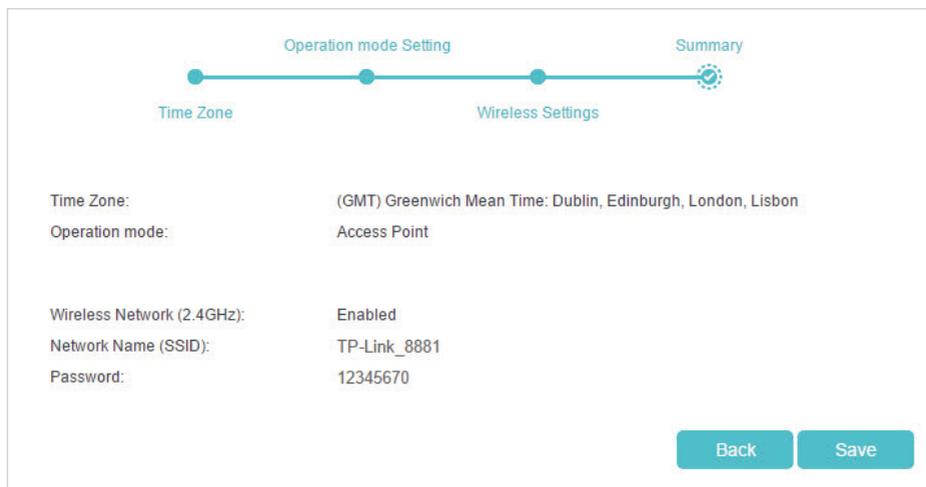
2. Select [Access Point Mode](#) and click [Next](#).

The screenshot shows the progress bar with "Operation mode Setting" highlighted by a blue dashed circle. Below it, there are two radio button options: "Access Point Mode" (selected) and "Repeater/Bridge Mode". At the bottom right, there are two teal buttons: "Back" and "Next".

3. Either customize your [Network Name \(SSID\)](#) and [Password](#) or keep the default ones, and then click [Next](#).

The screenshot shows the progress bar with "Wireless Settings" highlighted by a blue dashed circle. Below it, the text "You can change the wireless network name and password." is followed by a section for "2.4GHz Wireless:" which includes a checked checkbox for "Enable Wireless Radio". Below this are two input fields: "Network Name (SSID):" with the value "TP-Link_8881" and "Password:" with the value "12345670". At the bottom right, there are two teal buttons: "Back" and "Next".

4. Click [Save](#) to complete the configuration.



Time Zone Operation mode Setting Wireless Settings Summary

Time Zone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon

Operation mode: Access Point

Wireless Network (2.4GHz): Enabled

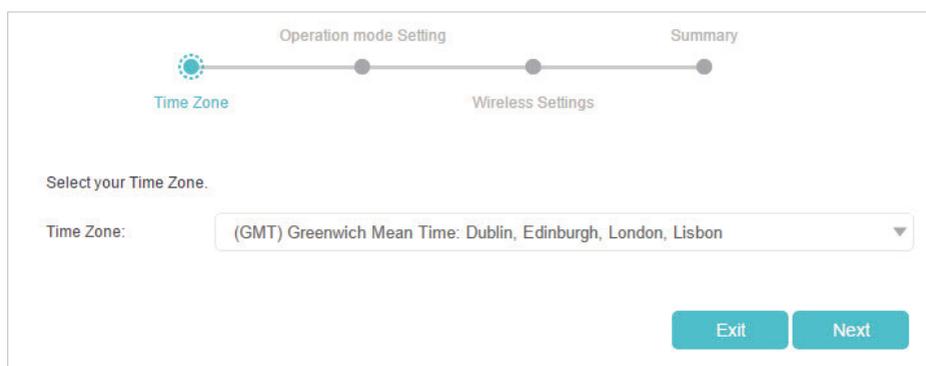
Network Name (SSID): TP-Link_8881

Password: 12345670

Back Save

3. 2. 5. Repeater/Bridge Mode

1. Select your **Time Zone** and click **Next**.



Time Zone Operation mode Setting Wireless Settings Summary

Select your Time Zone.

Time Zone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon

Exit Next

2. Select **Repeater/Bridge Mode** and click **Next**.



Time Zone Operation mode Setting Wireless Settings Summary

Access Point Mode

Repeater/Bridge Mode

Back Next

3. Click **Scan** to find the network you want to extend. Enter the **Password** for the selected wireless network if it is encrypted. Then click **Next**.

The screenshot shows the 'Wireless Settings' step in a four-step wizard. The progress bar at the top indicates the current step. The main content area includes a checkbox for 'Connect to 2.4GHz Network', input fields for 'Host 2.4GHz SSID' and 'Host 2.4GHz MAC', and radio buttons for 'Security' options: 'No Security', 'WPAWPA2 Personal', and 'WEP'. A 'Scan' button is positioned next to the SSID field. 'Back' and 'Next' buttons are at the bottom right.

4. Either customize your **Network Name (SSID)** and **Password** or keep the default ones, and then click **Next**.

This screenshot shows the 'Wireless Settings' screen with the 'Enable Wireless Radio' checkbox checked. The 'Network Name (SSID)' field contains 'TP-Link_8881' and the 'Password' field contains '12345670'. The 'Back' and 'Next' buttons are visible at the bottom right.

5. Click **Save** to complete the configuration.

Time Zone Operation mode Setting Wireless Settings Summary

Time Zone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, London, Lisbon

Operation mode: Repeater/Bridge

Host Network (2.4GHz): Enabled

Host Network Name (SSID): TP-LINK_50F2

Security: PSK2Authentication&AESEncryption

Password: 12345670

Wireless Network (2.4GHz): Enabled

Network Name (SSID): TP-Link_8881

Password: 12345670

Back Save

6. Relocate the router about **halfway** between your host router and the Wi-Fi dead zone.

Chapter 4

Guest Network

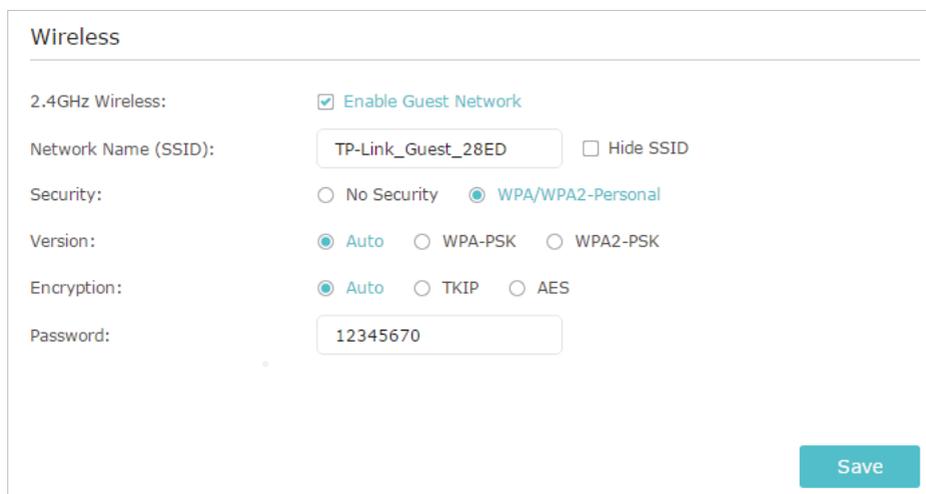
This function allows you to provide Wi-Fi access for guests without disclosing your main network. When you have guests in your house, apartment, or workplace, you can create a guest network for them. In addition, you can customize guest network options to ensure network security and privacy. Guest Network is only supported by the Router mode.

It contains the following sections:

- [Create a Network for Guests](#)
- [Customize Guest Network Options](#)

4. 1. Create a Network for Guests

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [Guest Network](#). Locate the [Wireless](#) section.
3. Create a guest network as needed.
 - 1) Tick the [Enable Guest Network](#) checkbox.
 - 2) Customize the SSID. Don't select [Hide SSID](#) unless you want your guests to manually input the SSID for guest network access.
 - 3) Set [Security](#) to [WPA/WPA2 Personal](#), keep the default [Version](#) and [Encryption](#) values, and customize your own password.



Wireless

2.4GHz Wireless: Enable Guest Network

Network Name (SSID): Hide SSID

Security: No Security WPA/WPA2-Personal

Version: Auto WPA-PSK WPA2-PSK

Encryption: Auto TKIP AES

Password:

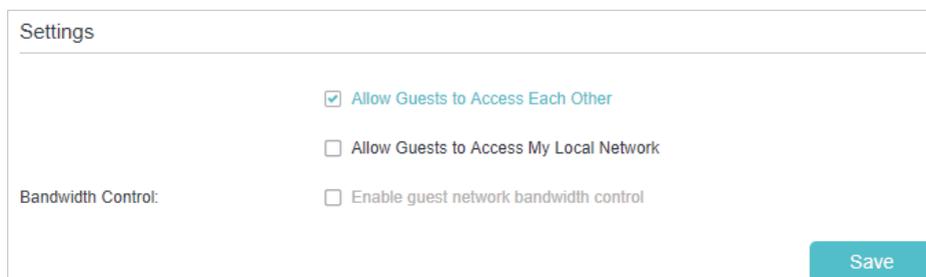
Save

4. Click [Save](#). Now your guests can access your guest network using the SSID and password you set!

 **Tips:** To view guest network information, go to [Advanced](#) > [Status](#) and locate the [Guest Network](#) section.

4. 2. Customize Guest Network Options

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [Guest Network](#). Locate the [Settings](#) section.
3. Customize guest network options as needed.



Settings

Allow Guests to Access Each Other

Allow Guests to Access My Local Network

Bandwidth Control: Enable guest network bandwidth control

Save

- [Allow Guests to Access Each Other](#)

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

- [Allow Guests to Access My Local Network \(in Router mode\)](#)

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

- [Enable guest network bandwidth control](#)

Tick this checkbox if you want to apply the Bandwidth Control settings to the wireless devices on your guest network .

4. Click [Save](#). Now you can ensure network security and privacy!

 **Tips:** To view guest network information, go to [Advanced](#) > [Status](#) and locate the [Guest Network](#) section.

Chapter 5

Parental Controls

This function allows you to block inappropriate, explicit and malicious websites, and control access to specified websites at specified time. Parental Controls are only supported by the Router mode.

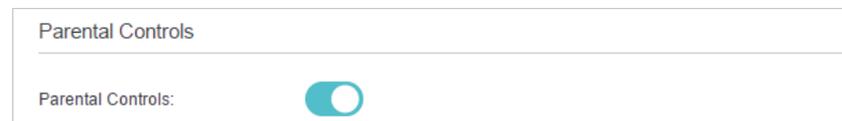
I want to:

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

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) at the weekend and not other times.

How can I do that?

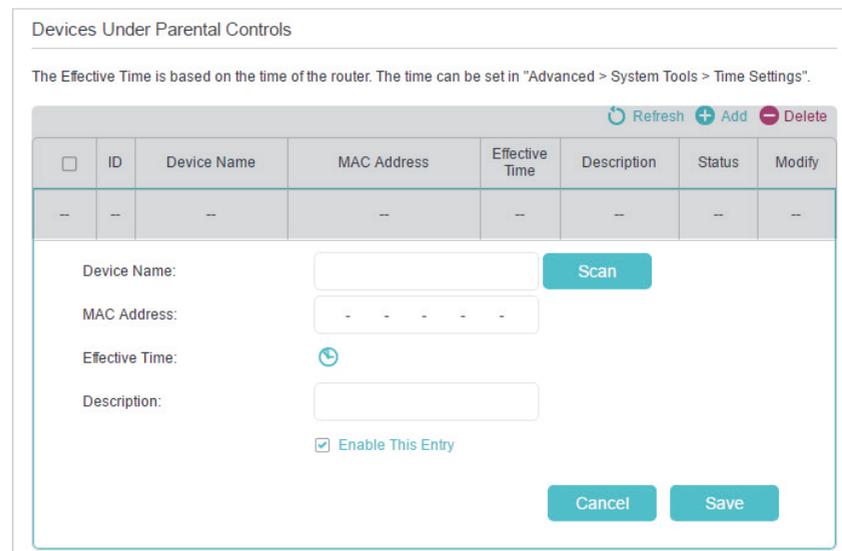
1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to **Advanced > Parental Controls** and enable **Parental Controls**.



Parental Controls

Parental Controls:

3. Click **Add**. And then Click **Scan**, and select the access device. Or, input the **Device Name** and **MAC Address** manually.



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

<input type="checkbox"/>	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 the  icon to set the Internet Access Time. Drag the cursor over the appropriate cell(s) and click **OK**.

System Time: 05/22/2017 09:47:14

	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

5. Enter a [Description](#) for the entry, tick the [Enable This Entry](#) checkbox, and then click [OK](#).

6. Select [Whitelist](#) as the restriction policy.

Content Restriction

Content Restriction:

Restriction Policy: Blacklist [Whitelist](#)

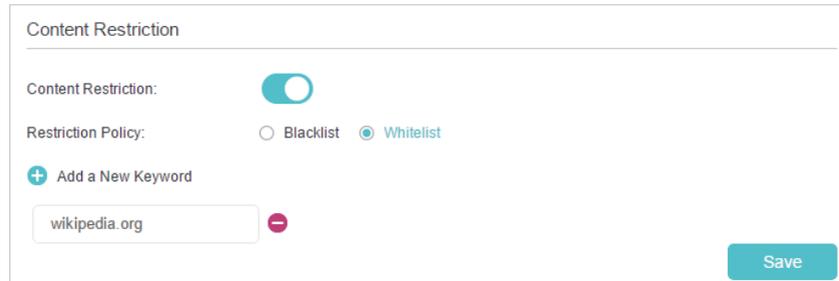
 **Tips:**

- With [Blacklist](#) selected, the controlled devices cannot access any websites containing the specified keywords during the Internet Access Time period.
- With [Whitelist](#) selected, the controlled devices can only access websites containing the specified keywords during the Internet Access Time period.

7. Click  [Add a New Keyword](#) . Enter a website and click [Save](#).

You can add up to 32 keywords for either [Blacklist](#) or [Whitelist](#). Below are some sample entries to allow access.

- [For Whitelist](#): Enter a web address (e.g. wikipedia.org) to allow access only to its related websites. If you wish to block all Internet browsing access, do not add any keyword to the [Whitelist](#).
- [For Blacklist](#): Specify a web address (e.g. wikipedia.org), a web address keyword (e.g. wikipedia) or a domain suffix (eg. .edu or .org) to block access only to the websites containing that keyword or suffix.



The screenshot shows a 'Content Restriction' settings panel. At the top, the title 'Content Restriction' is followed by a horizontal line. Below this, the 'Content Restriction' toggle is turned on. The 'Restriction Policy' section has two radio buttons: 'Blacklist' (unselected) and 'Whitelist' (selected). There is a '+ Add a New Keyword' button. Below it, a text input field contains 'wikipedia.org' and has a red minus sign to its right. A teal 'Save' button is located in the bottom right corner.

Done!

Now you can control your children's internet access as needed.

Chapter 6

Bandwidth Control

This chapter introduces how to set bandwidth limits minimize the impact caused when the connection is under heavy load. Bandwidth Control is only supported by the Router mode.

It contains the following sections:

- [Set Upstream and Downstream Bandwidth](#)
- [Controlling Rules](#)

6.1. Set Upstream and Downstream Bandwidth

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced > Bandwidth Control](#).
3. Enable [Bandwidth Control](#) and enter the [Total Upstream Bandwidth](#) and [Total Downstream Bandwidth](#).

Bandwidth Control

Bandwidth Control: Enable

Total Upstream Bandwidth: Kbps

Total Downstream Bandwidth: Kbps

[Save](#)

4. Click [Save](#).

6.2. Controlling Rules

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced > Bandwidth Control](#).
3. Click [Add](#) and fill in the blanks.

Controlling Rules

[+ Add](#) [- Delete](#)

☐	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

[Cancel](#) [Save](#)

- **IP Range:** Enter the IP range of your devices that you want to apply Bandwidth Control to.
- **Port Range:** Enter the Port range of the protocols.
- **Protocal:** Select the protocols of services that you want to control.
- **Priority:** Select priority from 1 to 5. 1 means the highest priority.
- **Upstream/Downstream:** Enter the minimun and maxmium upstream/downstream bandwidth you want to allocate.

4. Click **Save**.

Chapter 7

Network Security

This chapter guides you on how to protect your home network from cyber attacks and unauthorized users by implementing these three network security functions. You can protect your home network against DoS (Denial of Service) attacks from flooding your network with server requests using DoS Protection, block or allow specific client devices to access your network using Access Control, or you can prevent ARP spoofing and ARP attacks using IP & MAC Binding. Some features are only supported by a certain mode.

It contains the following sections:

- [Protect the Network from Cyber Attacks](#)
- [Service Filtering](#)
- [Access Control](#)
- [IP & MAC Binding](#)

7.1. Protect the Network from Cyber Attacks

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

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

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to **Advanced > Security > Firewall & DoS Protection**.
3. Enable **DoS Protection**.

DoS Protection:

DoS Protection

ICMP-Flood Attack Filtering: -Please Select-

UDP-Flood Attack Filtering: -Please Select-

TCP-Flood Attack Filtering: -Please Select-

Save

4. Set the level (**Low**, **Middle** or **High**) of protection for **ICMP-FLOOD Attack Filtering**, **UDP-FLOOD Attack Filtering** and **TCP-SYN-FLOOD Attack Filtering**.
 - **ICMP-FLOOD Attack Filtering** - Enable to prevent the ICMP (Internet Control Message Protocol) flood attack.
 - **UDP-FLOOD Attack Filtering** - Enable to prevent the UDP (User Datagram Protocol) flood attack.
 - **TCP-SYN-FLOOD Attack Filtering** - Enable to prevent the TCP-SYN (Transmission Control Protocol-Synchronize) flood attack.

Tips: The level of protection is based on the number of traffic packets. The protection will be triggered immediately when the number of packets exceeds the preset threshold value (the value can be set on **DoS Protection Level Settings**), and the vicious host will be displayed in the **Blocked DoS Host List**.

Blocked DoS Host List

Host Number: 0 Refresh Delete

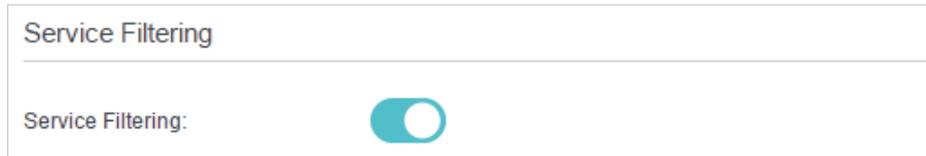
<input type="checkbox"/>	ID	IP Address	MAC Address
--	--	--	--

5. Click **Save**.

7.2. Service Filtering

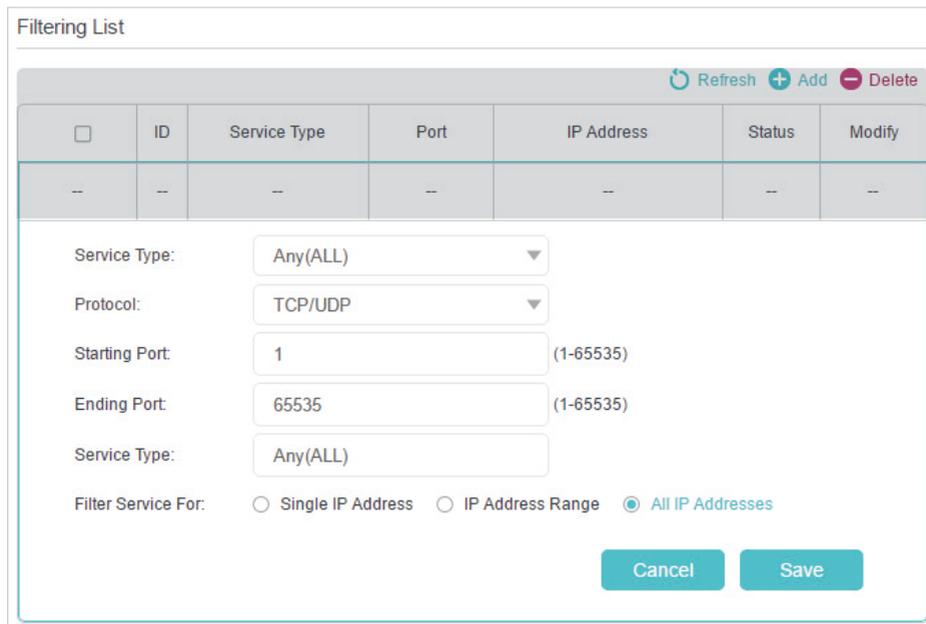
Service Filtering is used to prevent certain users from accessing a specific service. It can even block a user from accessing the internet.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [Security](#) > [Service Filtering](#).
3. Enable [Service Filtering](#).



The screenshot shows the 'Service Filtering' section of a router's web interface. At the top, the title 'Service Filtering' is displayed. Below it, the text 'Service Filtering:' is followed by a teal-colored toggle switch that is currently turned on.

4. Click [Add](#).



The screenshot shows the 'Filtering List' dialog box. At the top, there are buttons for 'Refresh', '+ Add', and '- Delete'. Below these is a table with the following columns: a checkbox, ID, Service Type, Port, IP Address, Status, and Modify. The table contains one row with dashes in all cells. Below the table, there are several input fields: 'Service Type' (dropdown menu with 'Any(ALL)' selected), 'Protocol' (dropdown menu with 'TCP/UDP' selected), 'Starting Port' (text input with '1' and '(1-65535)' range), 'Ending Port' (text input with '65535' and '(1-65535)' range), and another 'Service Type' dropdown menu with 'Any(ALL)' selected. At the bottom, there are radio buttons for 'Filter Service For': 'Single IP Address', 'IP Address Range', and 'All IP Addresses' (which is selected). There are 'Cancel' and 'Save' buttons at the bottom right.

5. Select a service type from the drop-down list and the corresponding parameters will be automatically filled in. Select Custom if your desired service type is not listed and enter the corresponding parameters.
6. Specify the IP address(es) this filtering rule will be applied to.
7. Click [Save](#).

7.3. 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 password you set for the router.
2. Go to [Advanced > Security > Access Control](#) or [Settings > Security > Access Control](#).
3. Enable [Access Control](#).



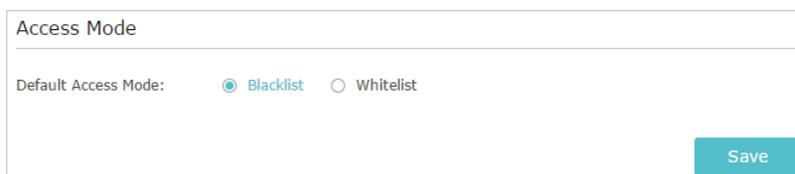
Access Control

Access Control:

4. 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](#).



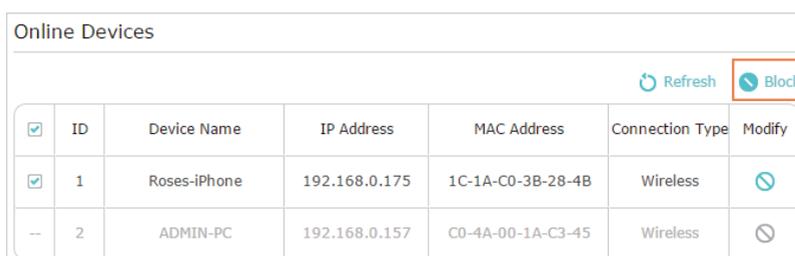
Access Mode

Default Access Mode: Blacklist Whitelist

[Save](#)

- 2) Select the device(s) to be blocked in the [Online Devices](#) table by ticking the checkbox(es).

- 3) Click [Block](#) above the [Online Devices](#) table. The selected devices will be added to [Devices in Blacklist](#) automatically.



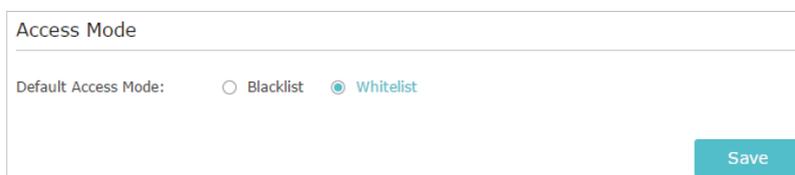
Online Devices

[Refresh](#) [Block](#)

<input checked="" type="checkbox"/>	ID	Device Name	IP Address	MAC Address	Connection Type	Modify
<input checked="" type="checkbox"/>	1	Roses-iPhone	192.168.0.175	1C-1A-C0-3B-28-4B	Wireless	Block
<input type="checkbox"/>	2	ADMIN-PC	192.168.0.157	C0-4A-00-1A-C3-45	Wireless	Block

To allow specific device(s):

- 1) Select [Whitelist](#) and click [Save](#).



Access Mode

Default Access Mode: Blacklist Whitelist

[Save](#)

- 2) Click [Add](#) in the [Devices in Whitelist](#) section. Enter the [Device Name](#) and [MAC Address](#) (You can copy and paste

the information from the [Online Devices](#) list if the device is connected to your network).

Devices in Whitelist

+ Add - Delete

<input type="checkbox"/>	ID	Device Name	MAC Address	Modify
	--	--	--	--

Device Name:

MAC Address:

Cancel OK

3) Click **OK**.

Done!

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

7.4. 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 password you set for the router.
2. Go to [Advanced](#) > [Security](#) > [IP & MAC Binding](#).
3. Enable [IP & MAC Binding](#).

IP & MAC Binding

IP & MAC Binding:

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

To bind the connected device(s):

Click to add the corresponding device to the [Binding List](#).

To bind the unconnected device:

- 1) Click [Add](#) in the [Binding List](#) section.

The screenshot shows a web interface titled "Binding List". At the top right, there are buttons for "+ Add" and "- Delete". Below this is a table with the following columns: a checkbox, ID, MAC Address, IP Address, Status, Enable, and Modify. The table contains one row with dashes in all cells. Below the table, there are input fields for "MAC Address:" and "IP Address:". Below these fields is a checkbox labeled "Enable This Entry" which is checked. At the bottom right, there are two buttons: "Cancel" and "Save".

- 2) Enter the **MAC address** and **IP address** that you want to bind.
- 3) Tick the **Enable This Entry** checkbox and click **Save**.

Done!

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

Chapter 8

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.

NAT Forwarding is only supported by the Router mode.

It contains the following sections:

- [Share Local Resources on the Internet by Virtual Servers](#)
- [Open Ports Dynamically by Port Triggering](#)
- [Make Applications Free from Port Restriction by DMZ](#)
- [Make Xbox Online Games Run Smoothly by UPnP](#)

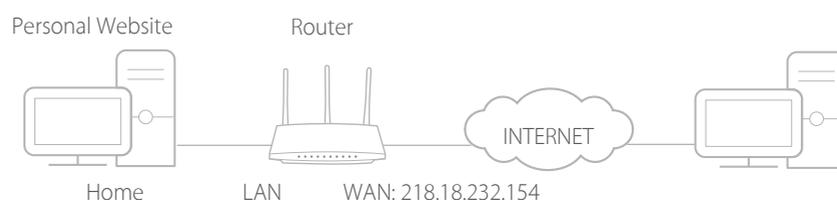
8. 1. Share Local Resources on the Internet by Virtual Servers

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 on my local network with my friends through the internet.

For example, the personal website has been built on my home PC (192.168.1.100). 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 192.168.1.100.
2. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
3. Go to **Advanced > NAT Forwarding > Virtual Servers**.
4. Click **Add**. Click **View Existing Services** and select **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 **OK**.

+ Add
 - Delete

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

Service Type: View Existing Services

External Port: (XX-XX or XX)

Internal IP:

Internal Port: (XX or Blank ,1-65535)

Protocol:

Enable This Entry

Cancel
OK

🔗 **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](http://WAN IP) (in this example: [http:// 218.18.232.154](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](http://domain name) to visit the website.
- If you have changed the default **External Port**, you should use [http:// WAN IP: External Port](http://WAN IP: External Port) or [http:// domain name: External Port](http://domain name: External Port) to visit the website.

8. 2. 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 the password you set for the router.
2. Go to **Advanced > NAT Forwarding > Port Triggering** and click **Add**.

3. Click [View Existing Applications](#), and select the desired application. The [Triggering Port](#), [External Port](#) and [Protocol](#) will be automatically filled in. The following picture takes application [MSN Gaming Zone](#) as an example.

4. Click [OK](#).

Port Triggering

+ Add - Delete

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

Application: [View Existing Applications](#)

Triggering Port: (XX,1-65535)

Triggering Protocol: ▼

External Port: (XX or XX-XX,1-65535,at most 5 pairs)

External Protocol: ▼

[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.

8.3. 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: When DMZ is enabled, the DMZ host is totally exposed to the internet, which may bring some potential safety hazards. If DMZ is not in use, please disable it in time.

I want to: Make the home PC join the internet online game without port restriction.

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

How can I do that?

1. Assign a static IP address to your PC, for example 192.168.1.100.
2. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
3. Go to **Advanced > NAT Forwarding > DMZ** and select **Enable DMZ**.
4. Enter the IP address 192.168.1.100 in the **DMZ Host IP Address** field.



DMZ

DMZ: Enable DMZ

DMZ Host IP Address:

Save

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.

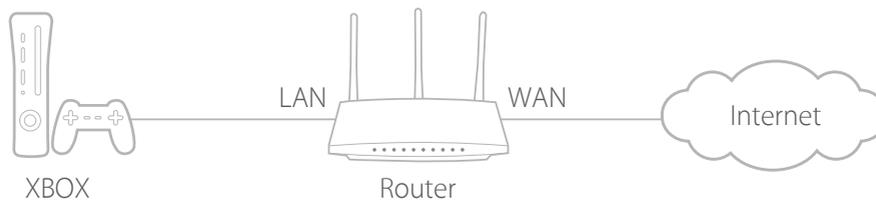
8.4. Make Xbox Online Games Run Smoothly by UPnP

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 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  Refresh

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

Chapter 9

VPN

The VPN (Virtual Private Networking) feature allows you to access your home network in a secured way through internet when you are out of home.

VPN is only supported by the Router mode.

With IPsec VPN, you can access the network securely when out of home. To use the VPN Service, you need to configure Dynamic DNS Service or assign a static IP address for the router's WAN port. And the System Time should be synchronized with the internet.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to **Advanced > VPN > IPsec VPN**.
3. Enable **Dead Peer Detection**.

IPsec VPN

Dead Peer Detection:

4. Click **Add** and enter correspond parameters.

+ Add - Delete

<input type="checkbox"/>	Connection Name	Remote Gateway	Local Address	Remote Address	Status	Enable	Modify
--	--	--	--	--	--	--	--

IPsec Connection Name:

Remote IPsec Gateway (URL):

Tunnel access from local IP addresses:

IP Address for VPN:

Subnet Mask:

Tunnel access from remote IP addresses:

IP Address for VPN:

Subnet Mask:

Key Exchange Method:

Authentication Method:

Pre-Shared Key:

Perfect Forward Secrecy:

Advanced

- **IPsec Connection Name:** Enter a name for the IPsec VPN connection.
- **Remote IPsec Gateway (URL):** Enter the destination gateway IP address which is the public WAN IP or domain name of the remote VPN server endpoint.

- **Tunnel access from local IP addresses:** Select **Subnet Address** if you want the whole LAN to join the VPN network, or select **Single Address** if you want a single IP to join the VPN network.
- **IP Address for VPN:** Enter the IP address of your LAN.
- **Subnet Mask:** Enter the subnet mask of your LAN.
- **Tunnel access from remote IP addresses:** Select **Subnet Address** if you want the whole remote LAN to join the VPN network, or select **Single Address** if you want a single IP to join the VPN network.
- **IP Address for VPN:** Enter the IP address of the remote LAN.
- **IP Subnet Mask:** Enter the subnet mask of the remote LAN.
- **Key Exchange Method:** Select **Auto (IKE)** or **Manual** to be used to authenticate IPSec peers.
- **Authentication Method:** Select **Pre-Shared Key** (recommended).
- **Pre-Shared Key:** Create a pre-shared key to be used for authentication.
- **Perfect Forward Secrecy:** Select **Enable** or **Disable** as an additional security protocol for the pre-shared key.

You can configure the advanced settings as needed. It's recommended to keep the default values. If you want to change these settings, make sure that both VPN server endpoints use the same Encryption Algorithm, Integrity Algorithm, Diffie-Hellman Group and Key Lifetime in both phase1 and phase2.

5. Click **Save**.

Chapter 10

Customize Your Network Settings

This chapter guides you on how to configure advanced network features. Some features are only supported by a certain mode.

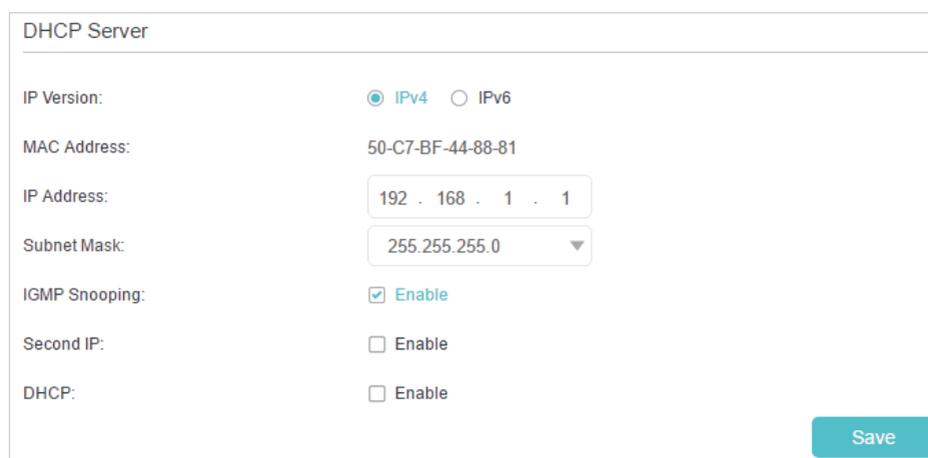
It contains the following sections:

- [Change the LAN Settings](#)
- [Specify DHCP Server Settings](#)
- [Set Up a Dynamic DNS Service Account](#)
- [Create Static Routes](#)
- [Specify Wireless Settings](#)
- [Extend Host Network](#)
- [Use WPS for Wireless Connection](#)
- [Schedule Your Wireless Function](#)

10.1. Change the LAN Settings

The router is preset with a default LAN IP 192.168.1.1, 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 on your local network or your network requires a specific IP subnet, you can change it.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Network > LAN Settings](#).
3. Type in a new IP Address appropriate to your needs. And leave the [Subnet Mask](#) as the default settings.



IP Version:	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
MAC Address:	50-C7-BF-44-88-81
IP Address:	192 . 168 . 1 . 1
Subnet Mask:	255.255.255.0
IGMP Snooping:	<input checked="" type="checkbox"/> Enable
Second IP:	<input type="checkbox"/> Enable
DHCP:	<input type="checkbox"/> Enable

Save

4. Click [Save](#).

Note: If you have set the Virtual Server, DMZ or DHCP address reservation, and the new LAN IP address is not in the same subnet with the old one, then you should reconfigure these features.

10.2. Specify DHCP Server Settings

By default, the DHCP (Dynamic Host Configuration Protocol) Server is enabled and the router acts as a DHCP server; it dynamically assigns TCP/IP parameters to client devices from the IP Address Pool. You can change the settings of the DHCP Server if necessary, and you can reserve LAN IP addresses for specified client devices. When in Access Point mode, select SmartIP for most cases.

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

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

DHCP: Enable

DHCP Server DHCP Relay

IP Address Pool: 192 . 168 . 1 . 100 - 192 . 168 . 1 . 199

Address Lease Time: 1440 minutes. (1-2880. The default value is 1440.)

Default Gateway: 192 . 168 . 1 . 1 (Optional)

Default Domain: (Optional)

Primary DNS: 0 . 0 . 0 . 0 (Optional)

Secondary DNS: 0 . 0 . 0 . 0 (Optional)

Save

1. Enable [DHCP Server](#).
2. Enter the starting and ending IP addresses in the [IP Address Pool](#).
3. Enter other parameters if the ISP offers. The [Default Gateway](#) is automatically filled in and is the same as the LAN IP address of the router.
4. Click [Save](#).

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

1. Click [Add](#) in the [Address Reservation](#) section.

Address Reservation

[+ Add](#) [- Delete](#)

<input type="checkbox"/>	MAC Address	Reserved IP Address	Group	Status	Modify
--	--	--	--	--	--

MAC Address: [Scan](#)

IP Address:

Group:

Enable This Entry

[Cancel](#) [Save](#)

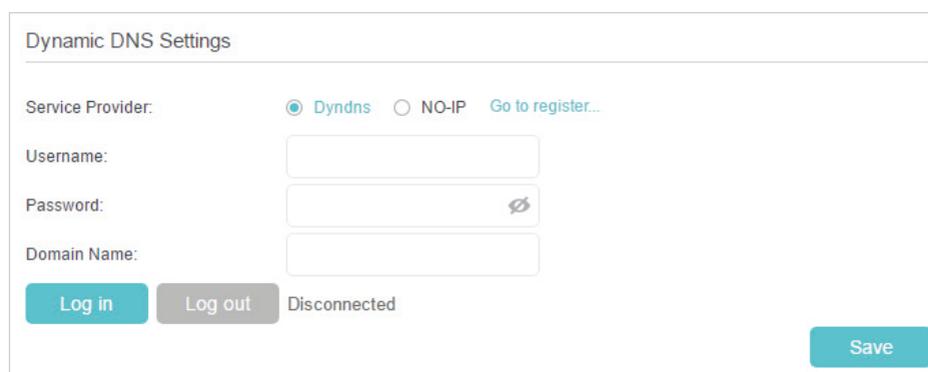
2. Click [Scan](#) to find a connected device you want to apply this rule to. You can also manually enter the MAC address of the device if it's currently disconnected from the router.
3. Enter the [IP address](#) to reserve for the client device.
4. Tick the [Enable This Entry](#) checkbox and click [Save](#).

10.3. Set Up a Dynamic DNS Service Account

Most ISPs 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 from time to time and you don't know when it changes. In this case, you might apply 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 a domain name without checking and remembering the IP address.

Note: DDNS does not work if the ISP assigns a private WAN IP address (such as 192.168.1.x) to the router.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to **Advanced > Network > Dynamic DNS**.
3. Select the DDNS **Service Provider**: NO-IP or DynDNS. If you don't have a DDNS account, you have to register first by clicking **Go to register**. Then enter the username, password and domain name of your account.



4. Click **Log In** and **Save**.

Tips: If you want to use a new DDNS account, please click **Log out** first, and then log in with a new account.

10.4. Create Static Routes

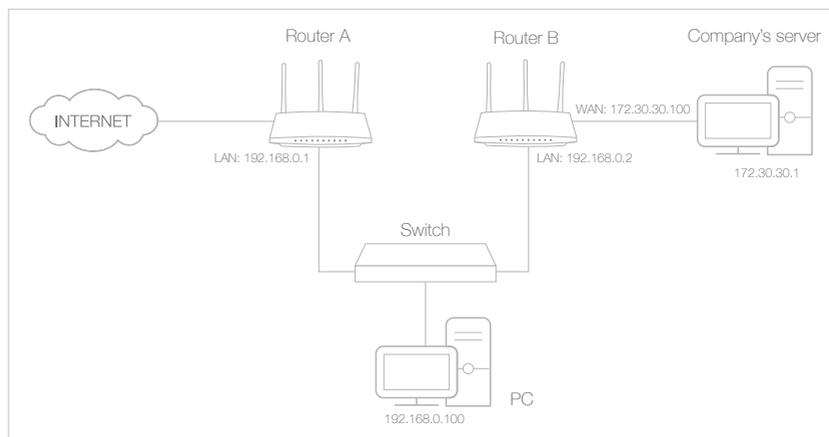
Static routing is a form of routing that is configured manually by a network administrator or a user by adding entries into a routing table. The manually-configured routing information guides the router in forwarding data packets to the specific destination.

I want to:

Visit multiple networks and servers at the same time.

For example, in a small office, my PC can surf the internet through Router A, but I also want to visit my company's network. Now I have a switch and Router B. 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. Change the routers' LAN IP addresses to two different IP addresses on the same subnet. Disable Router B's DHCP function.
2. Visit <http://tplinkwifi.net>, and log in with the password you set for Router A.
3. Go to **Advanced > Network > Advanced Routing**.
4. Click **Add** and finish the settings according to the following explanations:

<input type="checkbox"/>	ID	Network Destination	Subnet Mask	Gateway	Status	Modify
--	--	--	--	--	--	--

Network Destination:
 Subnet Mask:
 Gateway:
 Interface:

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.

Default Gateway: The IP address of the gateway device to which the data packets will be sent. This IP address must be on the same subnet with the router's IP which sends out data. In the example, the data packets will be sent to the LAN port of Router B and then to the Server, so the default gateway should be 192.168.0.2.

Interface: Determined by the port (WAN/LAN) that sends out data packets. In the example, the data are sent to the gateway through the LAN port of Router A, so LAN should be selected.

5. Click [Save](#).
6. Check the [System Routing Table](#) below. If you can find the entry you've set, the static routing is set successfully.

System Routing Table				
Active Routes Number: 3				Refresh
ID	Network Destination	Subnet Mask	Gateway	Interface
1	172.30.30.1	255.255.255.255	192.168.0.2	lan
2	192.168.0.0	255.255.255.0	0.0.0.0	lan
3	192.168.0.2	255.255.255.255	0.0.0.0	lan

Done!

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

10.5. Specify 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 label of the router. You can customize the wireless settings according to your needs.

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

➤ To enable or disable the wireless function:

1. Go to [Basic > Wireless](#), [Settings > Wireless > Wireless Settings](#) or [Settings > Wireless > Extended Network](#).
2. The wireless radio is enabled by default. If you want to disable the wireless function of the router, just untick the [Enable](#) checkbox. In this case, all the wireless settings will be invalid.

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

1. Go to [Basic > Wireless, Settings > Wireless > Wireless Settings](#) or [Settings > Wireless > Extended Network](#).
2. Create a new SSID in [Network Name \(SSID\)](#) and customize the password for the network in [Password](#). The value is case-sensitive.

■ **Note:** If you change the wireless settings with a wireless device, you will be disconnected when the settings are effective. Please write down the new SSID and password for future use.

➤ **To hide SSID:**

1. Go to [Basic > Wireless, Settings > Wireless > Wireless Settings](#) or [Settings > Wireless > Extended Network](#).
2. Select [Hide SSID](#), and your SSID won't display when you scan for local wireless networks on your wireless device and you need to manually join the network.

➤ **To change the security option:**

1. Go to [Advanced > Wireless > Wireless Settings, Settings > Wireless > Wireless Settings](#) or [Settings > Wireless > Extended Network](#).
2. Select an option from the [Security](#) drop-down list. We recommend you don't change the default settings unless necessary. If you select other options, configure the related parameters according to the help page.

In addition

- [Mode](#) - Select a transmission mode according to your wireless client devices. It is recommended to just leave it as default.
- [Channel Width](#) - Select a channel width (bandwidth) for the wireless network.
- [Channel](#) - Select an operating channel for the wireless network. It is recommended to leave the channel to [Auto](#), if you are not experiencing the intermittent wireless connection issue.

10.6. Extend Host Network

If you want to extend another host network after Quick Setup when the router works as a range extender, you can refer to this section.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Settings > Wireless > Connect to Network](#).
3. Enable [Connect to 2.4GHz Network](#) and click [Scan](#) to find all available networks.

Connect to Host Network

2.4GHz Network: Connect to 2.4GHz Network

Host 2.4GHz SSID: Scan

Host 2.4GHz MAC:

Security: No Security WPA/WPA2 Personal WEP

Version: WPA-PSK WPA2-PSK

Encryption: TKIP AES

Password:

Save

4. Select the host network you want to extend.

Note:

If the network you want to extend is on but not listed, please try the following steps.

- Move the router closer to your host router, and click [Refresh](#) in the top-right corner of the list.
- You can manually enter the SSID (network name) and password of the network you want to extend, and click [Save](#).

5. Once a host network is selected, its SSID, MAC address and security type will be automatically filled in. If it's encrypted, enter the password in the [Password](#) field.

6. Click [Save](#).

10.7. Use WPS for Wireless Connection

Wi-Fi Protected Setup (WPS) provides an easier approach to set up a security-protected Wi-Fi connection.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced](#) > [Wireless](#) > [WPS](#) or [Settings](#) > [Wireless](#) > [WPS](#).

10.7.1. Use the WPS Wizard for Wi-Fi Connections

1. Click the [Start WPS](#) button on the screen. Within two minutes, press the WPS button on the client device.

WPS Method

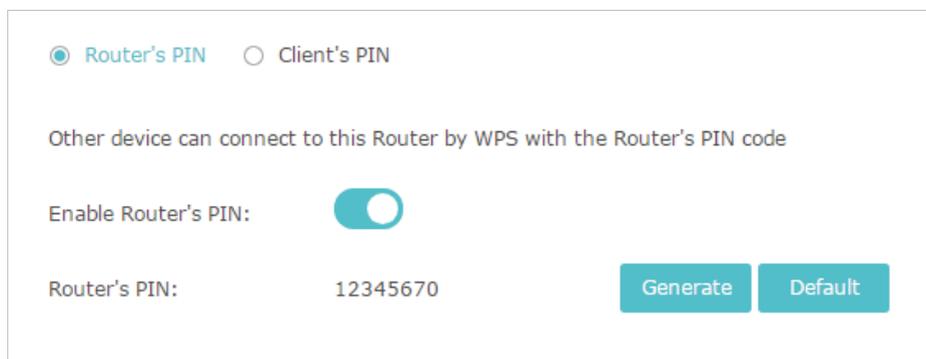
Method One—Push Button(recommended)

Start
WPS

2. **Success** will appear on the above screen and the WPS LED on the router will keep on for five minutes if the client has been successfully added to the network.

10.7.2. Use the PIN for Wi-Fi connections

Router's PIN is enabled by default to allow wireless devices to connect to the router using the PIN. You can use the default one or generate a new one.



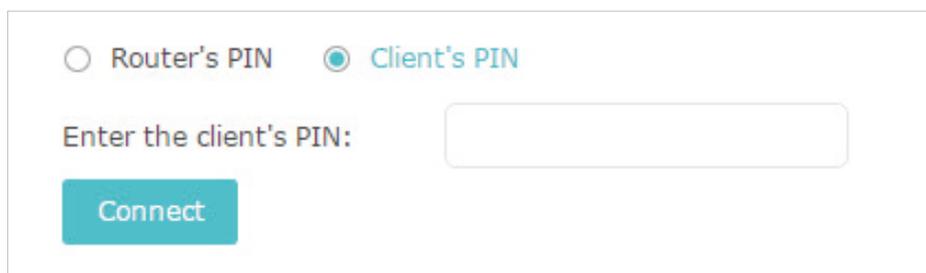
Router's PIN Client's PIN

Other device can connect to this Router by WPS with the Router's PIN code

Enable Router's PIN:

Router's PIN: 12345670 Generate Default

You can also enter the PIN of the device you want to connect to the Wi-Fi.



Router's PIN Client's PIN

Enter the client's PIN:

Connect

Note:

- If you want to enable/disable the WPS feature, go to [Advanced > Wireless > Advanced Settings](#). Locate the **WPS** section and tick or untick the **Enable** checkbox.
- PIN (Personal Identification Number) is an eight-character identification number preset to each router. WPS supported devices can connect to your router with the PIN. The default PIN is printed on the label of the router.

10.8. Schedule Your Wireless Function

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

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [Advanced > Wireless > Wireless Schedule](#).
3. Enable [Wireless Schedule](#).
4. Click [Add](#) to set the wireless off time. Specify the time period and days when the wireless network will be off.

Wireless Off Time

+ Add - Delete

<input type="checkbox"/>	ID	Wireless Off Time	Repeat	Modify
--	--	--	--	--

From:

To:

Repeat: Every Day Selected Day

5. Click [Save](#).

Chapter 11

Manage the Router

This chapter will show you the configuration for managing and maintaining your router. Some features are only supported by a certain mode.

It contains the following sections:

- [Set Up System Time](#)
- [Test the Network Connectivity](#)
- [Upgrade the Firmware](#)
- [Backup and Restore Configuration Settings](#)
- [Auto Reboot](#)
- [Change the Login Password](#)
- [Local Management](#)
- [Remote Management](#)
- [System Log](#)
- [Monitor the Internet Traffic Statistics](#)

11.1. Set Up System Time

System time is the time displayed while the router is running. The system time you configure here will be used for other time-based functions like Parental Controls.

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

➤ To get time from the PC :

1. Click [Get from PC](#).
2. Click [Save](#).

➤ To get time from the internet :

1. Select your local [Time Zone](#) from the drop-down list.

System Time

Current Time: 05/24/2017 16:42:52

Time Zone: (GMT+08:00) Beijing, Chongqing, Urumchi, Hong Kong, Taipei, Kuala Lumpur, Perth

Date: 5/24/2017 (MM/DD/YY)

Time: 16 : 42 : 47

NTP Server I: 0.0.0.0 (Optional)

NTP Server II: 0.0.0.0 (Optional)

Get from PC Get from the Internet Save

2. In the [NTP Server I](#) field, enter the IP address or domain name of your desired NTP Server.
3. (Optional) In the [NTP Server II](#) field, enter the IP address or domain name of the second NTP Server.
4. Click [Get from the Internet](#) and click [Save](#).

➤ To set up Daylight Saving Time:

1. Select [Enable Daylight Saving Time](#).

Daylight Saving Time

Enable Daylight Saving Time

Start: 2017 Mar Last Sun 02:00

End: 2017 Oct Last Sun 03:00

Save

2. Select the correct **Start** date and time when daylight saving time starts at your local time zone.
3. Select the correct **End** date and time when daylight saving time ends at your local time zone.
4. Click **Save**.

11.2. Test the Network Connectivity

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

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



3. Click **Start** to begin the diagnostics.

11.3. Upgrade the Firmware

TP-Link aims at providing better network experience for users.

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 the TP-Link official website www.tp-link.com, and you can download it from the **Support** page for free.

Note:

- Make sure you remove all attached USB devices from the router before the firmware upgrade to prevent data loss.
- Backup your router configuration before firmware upgrade.
- Do NOT turn off the router during the firmware upgrade.

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

Device Information

Firmware Version:

Hardware Version:

Local Upgrade

New Firmware File:

5. Wait a few minutes for the upgrade and reboot to complete.

11.4. Backup and Restore Configuration Settings

The configuration settings are stored as a configuration file in the router. You can backup 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 necessary you can erase the current settings and reset the router to the default factory settings.

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

➤ **To backup configuration settings:**

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

Backup

Save a copy of your current settings.

➤ **To restore configuration settings:**

1. Click [Browse](#) to locate the backup configuration file stored on your computer, and click [Restore](#).

Restore

Restore previous settings from a saved file.

File:

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

📌 **Note:** During the restoring process, do not turn off or reset the router.

➤ **To reset the router to factory default settings:**

1. Click [Factory Restore](#) to reset the router.



Factory Default Restore

Revert all the configuration settings to their default values.

[Factory Restore](#)

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

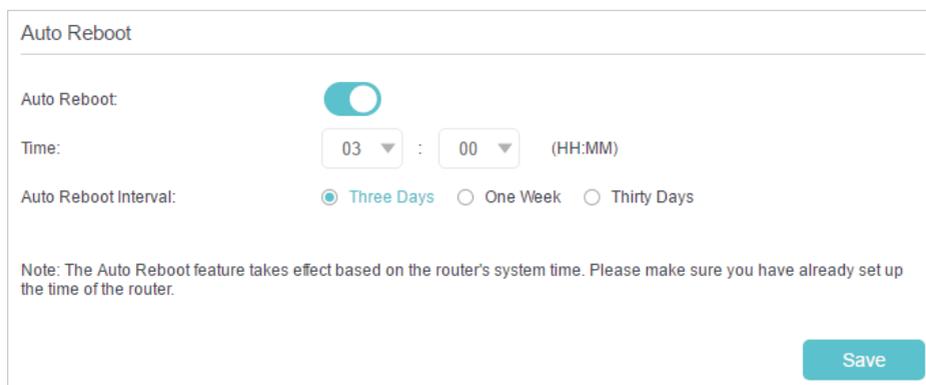
📌 **Note:**

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

11.5. Auto Reboot

Auto Reboot allows you to specify a time when the router will reboot automatically.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [System Tools](#) > [Reboot](#).
3. Enable [Auto Reboot](#).
4. Specify the time at which your router will reboot and the [Auto Reboot Interval](#).
5. Click [Save](#).



Auto Reboot

Auto Reboot:

Time: 03 : 00 (HH:MM)

Auto Reboot Interval: Three Days One Week Thirty Days

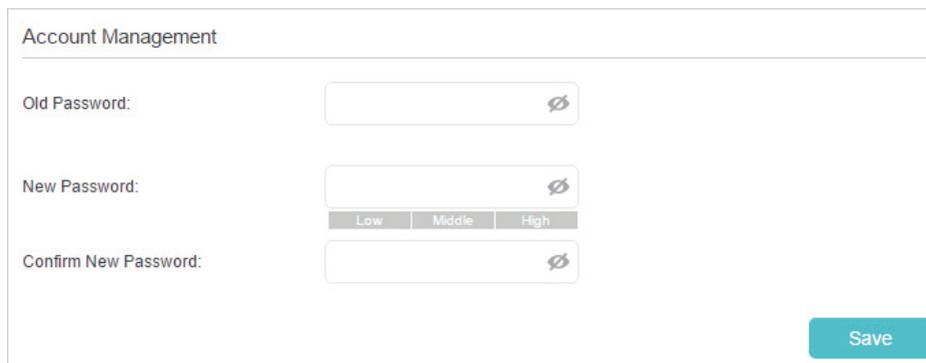
Note: The Auto Reboot feature takes effect based on the router's system time. Please make sure you have already set up the time of the router.

[Save](#)

11.6. Change the Login Password

The account management feature allows you to change your login password of the web management page.

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



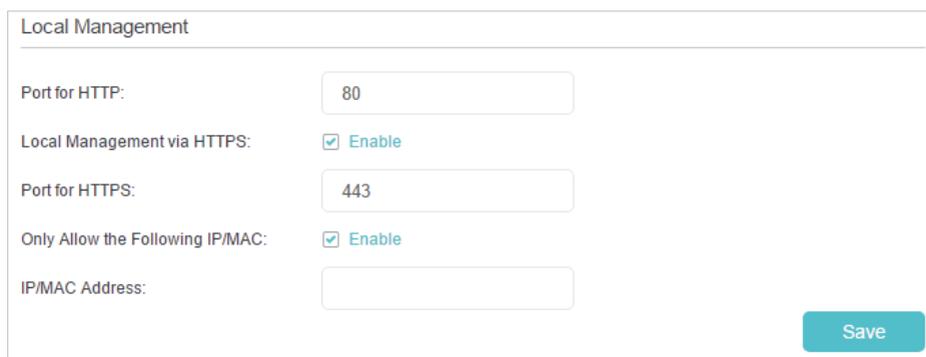
The screenshot shows the 'Account Management' section of a router's web interface. It contains three password input fields: 'Old Password', 'New Password', and 'Confirm New Password'. Each field has a toggle icon to the right. Below the 'New Password' field, there are three radio buttons labeled 'Low', 'Middle', and 'High' for password strength selection. A teal 'Save' button is located at the bottom right of the form.

3. Enter the old password, then a new password twice (both case-sensitive). Click [Save](#).
4. Use the new password for future logins.

11.7. Local Management

Local Management allows local devices to access and manage the router. By default, all local devices can access and manage the router via HTTP.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [System Tools](#) > [Administration](#) and complete the settings in [Local Management](#) section as needed.



The screenshot shows the 'Local Management' section of a router's web interface. It contains several settings: 'Port for HTTP' is set to 80; 'Local Management via HTTPS' is checked and labeled 'Enable'; 'Port for HTTPS' is set to 443; 'Only Allow the Following IP/MAC' is checked and labeled 'Enable'; and 'IP/MAC Address' is an empty text field. A teal 'Save' button is located at the bottom right of the form.

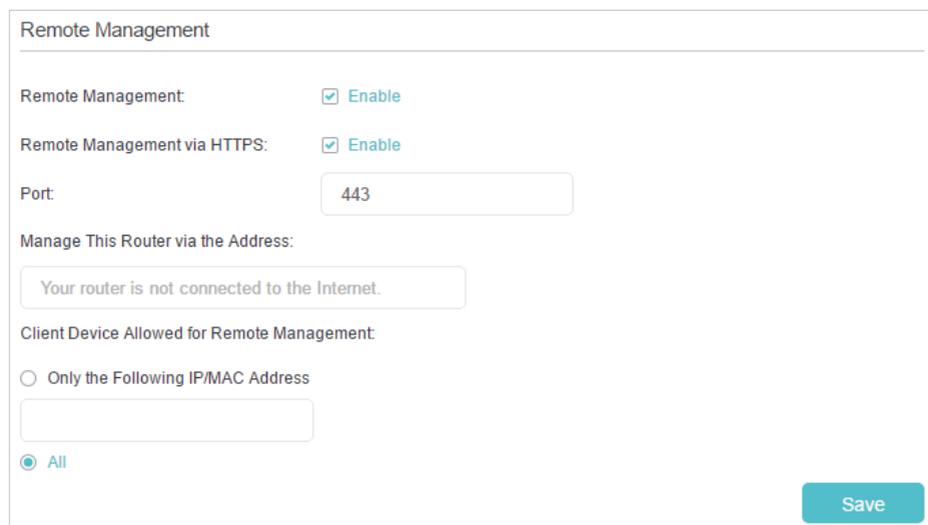
3. Enable [Local Management via HTTPS](#) if you want to access the router via both HTTPS and HTTP, or keep it disabled if you only want to access the router via HTTP.
4. Keep the Port for HTTP and Port for HTTPS as the default settings.
5. If you only want to allow one specific device to manage the router, enter the IP Address or MAC Address of the device in the [IP/MAC Address](#) field.
6. Click [Save](#).

■ Note: If a warning pops up when you visit <https://tplinkwifi.net>, click Trust (or a similar option) to continue.

11.8. Remote Management

Remote Management allows remote devices to access and manage the router. By default, all remote devices cannot access and manage the router.

1. Visit <http://tplinkwifi.net>, and log in with the password you set for the router.
2. Go to [System Tools](#) > [Administration](#) and complete the settings in [Remote Management](#) section as needed.



The screenshot shows the 'Remote Management' configuration page. It includes the following settings:

- Remote Management:** Enable
- Remote Management via HTTPS:** Enable
- Port:** 443
- Manage This Router via the Address:** A text box containing the message 'Your router is not connected to the Internet.'
- Client Device Allowed for Remote Management:**
 - Only the Following IP/MAC Address (with an empty text box below it)
 - All
- Save:** A blue button at the bottom right.

3. Enable [Remote Management](#) if you want to allow Remote Management via HTTPS, or enable [Remote Management](#) and then disable [Remote Management via HTTPS](#) if you want to allow Remote Management via HTTP.
4. Keep the Port as the default setting.
5. Decide which remote device can access the router remotely:
 - [Only the Following IP/MAC Address](#) - Enter the IP Address or MAC Address of the remote device to access the router.
 - [All](#) - All remote devices can access the router.
6. Click [Save](#).

📌 Note: If a warning pops up when you visit the above address remotely, click Trust (or a similar option) to continue.

11.9. System Log

When the router does not work normally, you can save the system log and send it to the technical support for troubleshooting.

➤ **To save the system log locally:**

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

3. Choose the type and level of the system logs as needed.
4. Click [Save Log](#) to save the system logs to a local disk.

System Log

Type:

Level:

[Refresh](#) [Delete All](#)

ID	Time	Type	Level	Log Content
1	2017-05-24 18:09:12	DHCP	Notice	Send DISCOVER with request ip 0.0.0.0 and unicast flag 1
2	2017-05-24 18:09:09	DHCP	Notice	Send DISCOVER with request ip 0.0.0.0 and unicast flag 1
3	2017-05-24 18:09:04	DHCP	Notice	Send DISCOVER with request ip 0.0.0.0 and unicast flag 0
4	2017-05-24 18:09:01	DHCP	Notice	Send DISCOVER with request ip 0.0.0.0 and unicast flag 0
5	2017-05-24 18:08:58	DHCP	Notice	Send DISCOVER with request ip 0.0.0.0 and unicast flag 0
6	2017-05-24 18:08:58	DHCP	Notice	Send DISCOVER with request ip 0.0.0.0 and unicast flag 1
7	2017-05-24 18:08:55	DHCP	Notice	Send DISCOVER with request ip 0.0.0.0 and unicast flag 1
8	2017-05-24 18:08:44	DHCP	Notice	Recv no OFFER, DHCP Service unavailable

◀ 1 2 3 4 5 6 7 8 ... 47 ▶

➤ **To send the system log to a remote server:**

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

Log Settings

Save Locally

Minimum Level: Information

Save Remotely

Minimum Level: Information

Server IP: 192.168.1.100

Server Port: 514

Local Facility Name: User

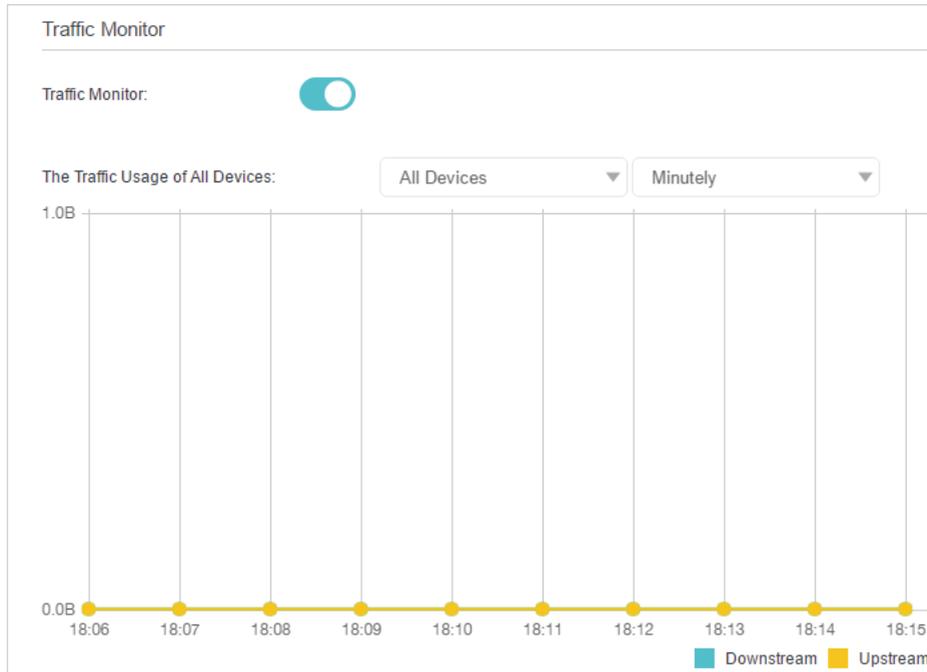
Back Save

4. Select [Save Remotely](#). 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.
5. Select the minimum level of system logs to be saved from the drop-down list. The list is in descending order, with the lowest level listed last.
6. Specify the IP address of the remote system log server in the Server IP field.
7. Specify the port number of the remote system log server in the Server Port field.
8. Select the local facility name of the remote server from the drop-down list.
9. Click [Save](#).

11. 10. Monitor the Internet Traffic Statistics

The Traffic Statistics page displays the traffic usage of a device in the past 10 minutes or that of all devices in the past 10 minutes/24 hours/7 days, 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 [System Tools > Traffic Monitor](#).
3. Toggle on [Traffic Monitor](#). You can monitor the traffic usage of a device in the past 10 minutes or that of all devices in the past 10 minutes/24 hours/7 days.



FAQ

Q1. What should I do if I can't access the Internet?

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

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

With the router powered on, press and hold the **WPS/RESET** button until all the LEDs turn on and then release the button.

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

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

- If you have not changed the default wireless password, it can be found on the label of the router.
- If you have changed the default wireless password, please refer to FAQ > Q2 to reset the router and go through the Quick Setup again.

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

1. Refer to FAQ > Q2 to reset the router to factory default settings.

2. Visit <http://tplinkwifi.net>, and create a new password for future logins.

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

Q5. What should I do if my wireless signal is unstable or weak?

It may be caused by too much interference.

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

COPYRIGHT & TRADEMARKS

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

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-Link Technologies Co., Ltd. Copyright © 2017 TP-Link Technologies Co., Ltd. All rights reserved.

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)

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.

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>.

Canadian Compliance Statement

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

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

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

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

Radiation Exposure Statement:

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

Déclaration d'exposition aux radiations:

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

Industry Canada Statement

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

Korea Warning Statements:

당해 무선설비는 운용중 전파혼신 가능성이 있음.

NCC Notice & BSMI Notice:

注意！

依據 低功率電波輻射性電機管理辦法

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

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

安全諮詢及注意事項

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



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



Safety Information

- When product has power button, the power button is one of the way to shut off the product; when there is no power button, the only way to completely shut off power is to disconnect the product or the power adapter from the power source.
- Don't disassemble the product, or make repairs yourself. You run the risk of electric shock and voiding the limited warranty. If you need service, please contact us.
- Avoid water and wet locations.
- Adapter shall be installed near the equipment and shall be easily accessible.
- The plug considered as disconnect device of adapter.
-  Use only power supplies which are provided by manufacturer and in the original packing of this product. If you have any questions, please don't hesitate to contact us.

Explanations of the symbols on the product label

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